Random unitaries that conserve energy

Liang Mao,[1,2] Laura Cui,[1] Thomas Schuster,[1,3] and Hsin-Yuan Huang[1,3]

[1] *California Institute of Technology, Pasadena, California 91125, USA*
[2] *Institute for Advanced Study, Tsinghua University, Beijing, 100084, China*
[3] *Google Quantum AI, Venice, California 90291, USA*

(Dated: October 9, 2025)

Random unitaries sampled from the Haar measure serve as fundamental models for generic quantum many-body dynamics. Under standard cryptographic assumptions, recent works have constructed polynomial-size quantum circuits that are computationally indistinguishable from Haar-random unitaries, establishing the concept of pseudorandom unitaries (PRUs). While PRUs have found broad implications in many-body physics, they fail to capture the energy conservation that governs physical systems. In this work, we investigate the computational complexity of generating PRUs that conserve energy under a fixed and known Hamiltonian H. We provide an efficient construction of energy-conserving PRUs when H is local and commuting with random coefficients. Conversely, we prove that for certain translationally invariant one-dimensional H, there exists an efficient quantum algorithm that can distinguish truly random energy-conserving unitaries from any polynomial-size quantum circuit. This establishes that energy-conserving PRUs cannot exist for these Hamiltonians. Furthermore, we prove that determining whether energy-conserving PRUs exist for a given family of one-dimensional local Hamiltonians is an undecidable problem. Our results reveal an unexpected computational barrier that fundamentally separates the generation of generic random unitaries from those obeying the basic physical constraint of energy conservation.

I. INTRODUCTION

Haar-random unitaries, which are unitaries drawn uniformly from the unitary group, provide a powerful theoretical model for generic quantum dynamics in complex quantum many-body systems. These ensembles capture universal signatures of quantum chaos and thermalization [1–8], and have found wide-ranging applications across quantum science, from quantum device benchmarking and tomography [9–13], to quantum machine learning [14–16], to black hole physics and holography [6, 8, 17, 18]. Despite their central role, Haar-random unitaries are computationally intractable: specifying or implementing an n-qubit Haar-random unitary requires exponential resources [19], rendering them physically unrealistic.

Pseudorandom unitaries (PRUs) address this issue by offering a practical alternative [20–23]. PRUs are ensembles of random unitaries that can be efficiently generated, yet are indistinguishable from Haar-random unitaries U in any polynomial-time quantum experiment with oracle access to U. Their existence hence provides crucial evidence for the use of Haar-random unitaries as models of chaotic polynomial-time quantum circuits in the real world. Recent constructions achieve this indistinguishability even at logarithmic circuit depths [24–27], leading to a broad range of physical implications: the hardness of recognizing quantum phases of matter [28, 29], the surprising efficiency of scrambling information [25, 30], and the existence of large families of indistinguishable states with completely different entanglement structures [23, 24, 31]. Despite these successes, PRUs suffer from a critical limitation: they fail to respect energy conservation, a fundamental and universal constraint governing physical systems.

A unitary evolution U conserves energy under a given Hamiltonian H if it satisfies the commutation relation, $[U, H] = 0$. This energy constraint distinguishes physical dynamics from unconstrained Haar-random unitaries, and dramatically alters dynamical phenomena. For examples, energy conservation is responsible for quantum thermalization to finite-temperature Gibbs states instead of maximally-mixed states [1, 3, 4, 32–34], the emergence of hydrodynamics at finite energy densities and at late times [35–41], non-ergodic behavior of some exotic models [42–44], and a high computational complexity for determining quantum equilibration [45–47]. Any realistic model of physical dynamics must therefore incorporate energy conservation. This motivates the following question:

Can we construct pseudorandom unitaries that respect energy conservation?

Our work provides a comprehensive answer to this question by establishing deep connections between the existence of energy-conserving PRUs and computational complexity theory. Our results reveal that the existence of energy-conserving PRUs depends critically on the specific structure of the Hamiltonian H, and that even determining their existence is, in general, undecidable.

To establish our results, we first formulate this question in a precise manner. We observe that for any local Hamiltonian $H \neq I$, any energy-conserving unitary can be efficiently distinguished from a Haar-random unitary (over the entire unitary group) by measuring the energy of $U|\psi\rangle$ for any non-zero

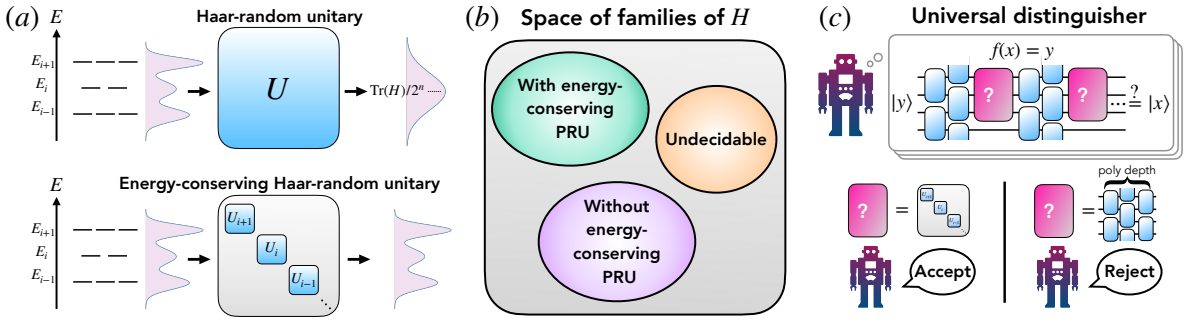

Figure 1. (a) Haar random unitary and energy-conserving Haar random unitary. Haar random unitaries are those that scramble the full Hilbert space. They transit each wavefunction to the infinite-temperature state. In contrast, energy-conserving Haar random unitaries are those that only scramble degenerated subspaces. They respect the energy-occupation of each wavefunction. (b) Summary of our results. We construct local Hamiltonian families with and without energy-conserving PRU. Further, we demonstrate there exists a certian set of Hamiltonian families such that determining if they have energy-conserving PRU is an undecidable problem. (c) We construct a universal distinguishing algorithm to prove Theorem 2. The algorithm accepts the energy-conserving Haar random unitaries of the hard Hamiltonian, whereas rejects any polynomial-size quantum circuit.

energy state $|\psi\rangle$. This motivates a refined definition: *energy-conserving PRUs* should be computationally indistinguishable not from Haar-random unitaries, but from *energy-conserving Haar-random unitaries*, i.e. unitaries drawn according to the Haar measure of the group containing all unitaries that commute with the given Hamiltonian H, $\{U : [U, H] = 0\}$.

Our main results establish a striking dichotomy. For a simple class of random commuting Hamiltonians, we prove that energy-conserving PRUs exist by providing an efficient construction. On the other hand, more surprisingly, we construct explicit families of one-dimensional, local, translationally invariant Hamiltonians for which energy-conserving PRUs provably cannot exist. Furthermore, we establish this non-existence by proving an even stronger statement: there is an efficient quantum algorithm that can distinguish energy-conserving Haar-random unitaries for these Hamiltonians from any polynomial-size quantum circuit. Both of these results hold under standard cryptographic and complexity-theoretic conjectures, such as the existence of quantum-secure one-way functions. Given these contrasting results, a natural question is how one can determine whether energy-conserving PRUs exist for a given Hamiltonian family. Unfortunately, using standard complexity-theoretic tools, we prove that this problem is in general undecidable: no algorithm can solve it, even given exponential time and space resources. Our results reveal fundamental computational barriers emerging from physical energy constraints, highlighting the tension between common models of ergodicity and the physical requirement of energy conservation. The results are summarized in Fig 1.

II. PSEUDORANDOM UNITARIES AND ENERGY CONSERVATION

We recall the standard definition for pseudorandom unitaries [20, 23]:

Definition 1 (Pseudorandom unitaries; informal)**.** *A sequence $\{\mathcal{U}_n\}_{n\in\mathbb{N}}$ of ensembles of n-qubit random unitaries is a pseudorandom unitary (PRU) if:*

1. *Efficiency: Every unitary in $\mathcal{U}_n$ can be implemented by a quantum circuit of size* $\mathsf{poly}(n)$.
2. *Pseudorandomness: For any polynomial-time quantum algorithm $\mathcal{A}$ that receives oracle access to a unitary U sampled either from $\mathcal{U}_n$ or from the Haar measure, the distinguishing advantage*

$$\left| \Pr_{U\sim\mathcal{U}_n}[\mathcal{A}^U(1^n) = 1] - \Pr_{U\sim\mathrm{Haar}}[\mathcal{A}^U(1^n) = 1] \right| \leq \mathsf{negl}(n), \tag{II.1}$$

where $\mathsf{negl}(n)$ *is a function smaller than any* $\frac{1}{\mathsf{poly}(n)}$.

The existence of PRUs has been proven under the existence of quantum-secure one-way functions [23]. Quantum-secure one-way functions are families of efficiently computable functions f_n that map $x \in \{0,1\}^n$ to $y \in \{0,1\}^m$ [48, 49]. The key feature is that given $y = f_n(x)$, no efficient quantum algorithm

can find a preimage x, hence their name *one-way*. These functions can be constructed explicitly using Learning With Errors (LWE) [50, 51]. For a comprehensive overview, we refer readers to Appendix A.

To incorporate energy conservation into random unitaries, we first observe that:

Observation 1 (Energy-based distinguisher)**.** *Any random unitary ensemble $\mathcal{U}_H$ that conserves energy for a local Hamiltonian H can be efficiently distinguished from a Haar-random unitary.*

To establish the above observation, consider the following simple distinguishing algorithm: prepare a product state $|\psi\rangle$ with an energy $\langle\psi| H |\psi\rangle$ sufficiently different from $\mathrm{Tr}(H)/2^n$ (the infinite temperature value), apply the unknown unitary U, and measure the energy $\langle\psi| U^\dagger H U |\psi\rangle$. For Haar-random unitaries, this expectation value concentrates around $\mathrm{Tr}(H)/2^n$, while for energy-conserving unitaries it equals $\langle\psi| H |\psi\rangle$. Existing results [52–54] guarantee that product states with significant energy deviation from the infinite temperature value can be efficiently prepared for any local Hamiltonian, hence the distinguishing algorithm is efficient. See Theorem 1 in Appendix B for a detailed description and proof.

This observation motivates our proposed definition of energy-conserving PRUs:

Definition 2 (Energy-Conserving PRUs; informal)**.** *Let n denote system size, let $\{H_n\}_{n\in\mathbb{N}}$ be a sequence of n-qubit local Hamiltonians, and let $\{\mathcal{C}_n^H\}_{n\in\mathbb{N}}$ denote the ensemble of energy-conserving Haar-random unitaries, i.e., Haar measure over the group $\{U_n : [U_n, H_n] = 0\}$ for each n. A sequence $\{\mathcal{U}_n\}_{n\in\mathbb{N}}$ of ensembles of n-qubit random unitaries is an energy-conserving PRU with respect to $\{H_n\}$ if:*

1. *Efficiency: Every unitary in $\mathcal{U}_n$ can be implemented by a quantum circuit of size $\mathsf{poly}(n)$.*
2. *Pseudorandomness: For any polynomial-time quantum algorithm $\mathcal{A}$ that receives oracle access to a unitary U sampled either from $\mathcal{U}_n$ or from $\mathcal{C}_n^H$, the distinguishing advantage*

$$\left| \Pr_{U\sim\mathcal{U}_n}[\mathcal{A}^U(1^n) = 1] - \Pr_{U\sim\mathcal{C}_n^H}[\mathcal{A}^U(1^n) = 1] \right| \leq \mathsf{negl}(n), \tag{II.2}$$

where $\mathsf{negl}(n)$ is a function smaller than any $\frac{1}{\mathsf{poly}(n)}$.

With this definition, we can formally ask the question of whether energy-conserving PRUs exist for a family of local Hamiltonians. Note that because pseudorandom objects are, by definition, asymptotic with respect to a parameter n (we require that no polynomial-time algorithm exists, which is itself an asymptotic statement), we can only discuss the existence or absence of energy-conserving PRUs for a *sequence* of local Hamiltonians H_n for varying system sizes n.

III. MAIN RESULTS

We first provide a simple and efficient construction of energy-conserving PRUs, for random commuting Hamiltonians of the form $H = \sum_i \mathcal{J}_i h_i$, where $\mathcal{J}_i$ are Gaussian random coefficients, and $\{h_i\}$ form a complete set of commuting local observables. Here, a complete set means all common eigenstates of $\{h_i\}$ can be determined by specifying the local eigenstates of each h_i. This additional constraint is introduced to prevent insufficient covering, i.e., to ensure that no qubits exist that do not support any h_i.

Theorem 1 (Constructing energy-conserving PRUs for random commuting Hamiltonians)**.** *Let $H = \sum_i \mathcal{J}_i h_i$ be an n-qubit commuting Hamiltonian with Gaussian random coefficients $\mathcal{J}_i$, where $\{h_i\}$ forms a complete set of commuting observables. There exists an efficient ensemble of unitaries that forms an energy-conserving PRU of H with probability at least $1 - \mathrm{negl}(n)$.*

The concrete constructions are described in Section V A, and a detailed statement and proof of the theorem is given in Theorem 2 in Appendix C.

Having shown that energy-conserving PRUs exist for random commuting Hamiltonians, we now construct a different family of Hamiltonians for which energy-conserving PRUs provably do *not* exist. The Hamiltonians we consider are one-dimensional, local, and translationally invariant. We establish the non-existence of their energy-conserving PRUs by providing an efficient quantum algorithm to distinguish an energy-conserving Haar-random unitary (under this family of Hamiltonians) from any polynomial-size quantum circuit. This provision is even stronger than strictly proving non-existence.

Theorem 2 (Hard Hamiltonians with no energy-conserving PRUs)**.** *There exists a uniform family of one-dimensional, local, and translationally invariant Hamiltonians $\mathcal{H}$ whose matrix elements belong to $\{0, 1, 10, 1/2, 1/4\}$, such that there is a universal algorithm to distinguish the energy-conserving Haar-random unitaries of $\mathcal{H}$ from any polynomial-size quantum circuit.*

We choose the stated coefficients to ensure that each Hamiltonian H in the family $\mathcal{H}$ is directly representable on digital computers. Our construction builds upon the Feynman-Kitaev Hamiltonian for quantum simulation of Turing machines [55, 56]. We make several significant improvements over this standard construction to enable the energy-conserving Haar-random unitary of H to solve PSPACE-complete problems, a set of problems believed to be hard for quantum computers. In particular, PSPACE-complete problems can be used to invert quantum-secure one-way functions, which we utilize to construct the universal distinguishing algorithm in Theorem 2. Our constructions of the Hamiltonian and distinguishing algorithm are overviewed in Section V B. A detailed statement and proof of the theorem are provided in Theorem 5 in Appendix G.

Our results so far have shown that some simple Hamiltonians allow energy-conserving PRUs, while other Hamiltonians do not. This naturally raises the question: How can one determine whether energy-conserving PRUs exist for a given Hamiltonian H? Our final result proves that this problem is undecidable. We prove this by combining the two theorems above and embedding the canonical undecidable problem, the halting problem, into the degeneracy of Hamiltonians.

Theorem 3 (Undecidability of existence of energy-conserving PRUs)**.** *Determining whether a given uniform family of local Hamiltonians has energy-conserving PRUs is an undecidable problem.*

Our construction is described in Section V C. A detailed statement and proof of this theorem is given in Theorem 6 in Appendix H.

IV. DISCUSSIONS

Energy-conserving PRUs produce dynamics indistinguishable from truly random dynamics that satisfy energy conservation, making them natural tools for investigating and mimicking chaotic and thermalizing quantum dynamics in local Hamiltonians. Our results lead to several implications and open questions from this perspective.

To obtain physical intuition about energy-conserving PRUs, let us first clarify what energy-conserving Haar-random unitaries represent. Energy-conserving Haar-random unitaries are most directly related to Hamiltonian dynamics when the Hamiltonian H has a generic non-degenerate energy spectrum. Consider an n-qubit Hamiltonian $H = \sum_{k=1}^{2^n} E_k |k\rangle\langle k|$ with a generic non-degenerate spectrum. The subgroup of unitaries that conserve energy under H are of the simple form $U = \sum_k e^{i\theta_k} |k\rangle\langle k|$, for an arbitrary phase $\theta_k \in [0, 2\pi)$ for each k from 1 to 2^n. An energy-conserving Haar-random unitary is hence:

$$U = \sum_k e^{i\theta_k} |k\rangle\langle k|, \tag{IV.1}$$

for uniformly random phases $\theta_k \in [0, 2\pi)$. When the energy spectrum is generic, the set of energy-conserving random unitaries is the same as the set of unitaries e^{-iHt} for time $t \in (-\infty, \infty)$ [57, 58]. An energy-conserving Haar-random unitary corresponds to e^{-iHt} for an extremely large random time t. We note that the same insight is used to prove Theorem 1 and 2, where the constructed Hamiltonians have nondegnerated spectra (with high probability).

The 2^n independent random phases $\theta_1, \ldots, \theta_{2^n}$ require $O(2^n)$ bits to even specify a single unitary. Hence, the total degree of randomness of this set is $2^{O(2^n)}$. This extreme randomness requirement cannot be efficiently achieved through finite-time Hamiltonian evolution by the following counting argument. If we consider unitaries generated by H through evolution over $t \in [-T, T]$, the number of distinct unitaries is at most $O(T)$. Therefore, achieving exponentially many bits of randomness requires T to be doubly exponential in n. Even for fast-forwardable Hamiltonians [59, 60] such as commuting systems, creating an energy-conserving Haar-random unitary requires simulating e^{-iHt} for doubly exponentially large t, demanding exponentially large quantum circuits. When H has energy degeneracies, energy-conserving Haar-random unitaries are even stronger than extremely-long-time Hamiltonian dynamics: they require the unitary to scramble every degenerate subspace. Energy-conserving PRUs attempt to circumvent these intrinsic barriers by providing computationally efficient approximations that are indistinguishable from these exponentially complex objects.

Our central finding is that this circumvention is not always possible. For our hard Hamiltonians (Theorem 2), the exponential complexity inherent in energy-conserving Haar-random unitaries creates detectable computational signatures. The key insight is that certain features of this exponential complexity can be revealed in polynomial time, allowing an observer to efficiently distinguish genuine energy-conserving Haar unitaries from any polynomial-size quantum circuit. An observer need only interact with

the unitary polynomially many times to obtain evidence that the underlying dynamics encode super-polynomially complex circuits, thereby distinguishing genuine energy-conserving Haar unitaries from any attempted polynomial-size circuit approximation. Under standard subexponential-hardness assumptions for quantum-secure one-way functions, our distinguishing algorithms can separate energy-conserving Haar unitaries from any subexponential-size quantum circuit.

These findings represent worst-case statements about the computational complexity of constructing energy-conserving pseudorandom dynamics. The dichotomy between efficient energy-conserving PRUs for commuting Hamiltonians, and their proven impossibility for our hard systems, represent extreme ends of the computational spectrum. The central open question is whether generic random Hamiltonians or naturally-occurring Hamiltonians are likely to admit energy-conserving PRUs. This average-case complexity question remains unresolved and is not precluded by our undecidability result, since probabilistic statements about random Hamiltonian families could potentially be established even when no algorithm can decide individual cases. Resolving this question would determine whether the computational barriers we have identified constitute fundamental obstacles to mimicking energy-conserving random quantum dynamics, or merely represent pathological edge cases within the broad space of physically realizable Hamiltonians.

V. PROOF OVERVIEW

In this section, we provide detailed descriptions of the theoretical constructions and proofs underlying each of our main results, Theorems 1, 2, and 3.

A. Hamiltonians with energy-conserving PRUs

In this section, we describe how to construct energy-conserving PRUs for random commuting Hamiltonians. We focus on Hamiltonians of the form $H = \sum_i \mathcal{J}_i h_i$, where $\{h_i\}$ forms a complete set of local terms that commute with each other, and $\{\mathcal{J}_i\}$ are i.i.d. Gaussian random variables (more precisely, Gaussian random variables with proper digitization). Technical details can be found in Appendix C.

To construct energy-conserving PRUs, we first clarify the structure of energy-conserving Haar-random unitaries. As already mentioned, any unitary that commutes with H must be block-diagonal with respect to its eigenspaces. The energy-conserving Haar-random unitaries then scramble each subspace independently.

Observation 2 (Structure of energy-conserving Haar-random unitaries, Fact 1 in Appendix A)**.** *Let $\mathcal{H}^k$, $1 \le k \le m$ be the degenerate subspaces of H, then any $U \in \mathcal{C}_H$ takes the form $U = \bigoplus_{k=1}^{m} U_k$, where U_k is a random unitary inside $\mathcal{H}^k$.*

Specifically, when H has no energy degeneracy, $U = \sum_{k=1}^{2^n} e^{i\theta_k} |k\rangle\langle k|$, where $|k\rangle$ is the k-th eigenstate, and θ_k is a random phase factor. This ensemble is called the random phase ensemble in the literature [57, 58]. The simplified structure of the random phase ensemble enables an efficient construction. This is where the random Gaussian coefficients $\{\mathcal{J}_i\}$ prove essential: they prevent H from having energy degeneracies since it lacks level repulsion.

To add random phases to each energy eigenstate, we use the quantum phase estimation (QPE) algorithm [61] as a subroutine. The algorithm requires ancilla qubits to set the estimation precision [56, 62, 63]. Assume we are working with an n-qubit system with m ancillas. Denote U to be the n-qubit unitary, and $|\psi\rangle$ to be an eigenstate of U with eigenvalue $e^{i2\pi\psi}$, where $\psi \in [0, 1)$. QPE then transforms $|\psi\rangle |0^m\rangle$ to $|\psi\rangle |\widetilde{\psi}\rangle$, where $|\widetilde{\psi}\rangle$ represents the digitization of ψ stored in the ancilla qubits. To achieve 2^{-m} precision, QPE applies m controlled operations $U_c^{2^j}$ for $j = 1, 2, \ldots, m$, where U_c is the controlled U by a single qubit. We refer readers to Appendix A for a more detailed introduction.

Using linearity, QPE transforms any superposition state $\left(\sum_\psi c_\psi |\psi\rangle\right) |0^m\rangle$ into $\sum_\psi c_\psi |\psi\rangle |\widetilde{\psi}\rangle$. Then we add phase factors to each eigenstate by applying an oracle $\mathcal{O}_f : |x\rangle \to (-1)^{f(x)} |x\rangle$ for $x \in \{0,1\}^m$ to the ancilla register, where $f : \{0,1\}^m \to \{0,1\}$ is a Boolean function. By choosing f from pseudorandom Boolean functions (which can be constructed from one-way functions), $\mathcal{O}_f$ can be efficiently constructed, and generates pseudorandom phases that are computationally indistinguishable from truly random phases. After applying the inverse of QPE to uncompute the ancillas, the resulting state $\left(\sum_\psi (-1)^{f(\widetilde{\psi})} c_\psi |\psi\rangle\right) |0^m\rangle$ is computationally indistinguishable from $\left(\sum_\psi e^{i\theta_\psi} c_\psi |\psi\rangle\right) |0^m\rangle$ for truly random $\{\theta_\psi\}$. Therefore, when choosing U to be e^{iH}, the sequential application of QPE, pseudorandom

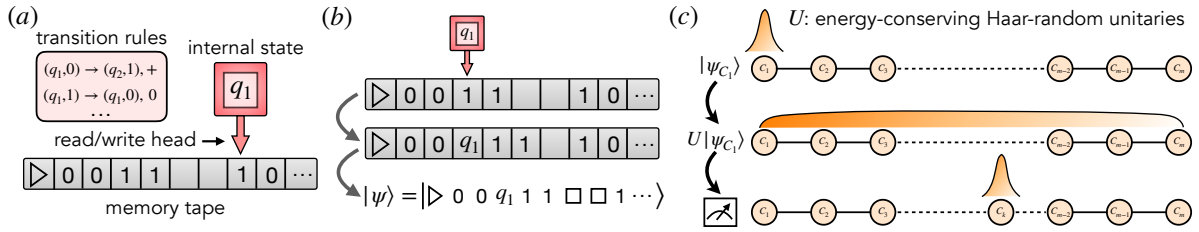

Figure 2. (a) Illustration of Turing machines. A TM consists of an infinite tape storing symbols, a read/write head that moves left or right who has a internal state, and a set of transition rules to determine the actions and movements of the head. (b) To represent any configuration of TMs (with finite memory size) with a product state, we first put the head state into the tape to make the whole system strictly one dimensional. Then the configuration can be represented by a quantum product state with local Hilbert spaces containing all the symbols and internal states. (c) The idea of using energy-conserving Haar-random unitaries to do fast computation: any computation process can be viewed as moving along a one-dimensional path with vertices labeled by TM's configurations. After initialize the wavefunction to the left terminal corresponding to inputs, the Haar-random unitaries scramble the wavefunction to disperse along the whole path. Then a subsequent measurement collapses the wavefunction to any vertex with almost equal probability, making an exponentially large step forward at once. This idealized picture faces practical obstacles, see Section V B.

phases, and QPE-inverse acts indistinguishably from a random phase unitary, providing a construction for energy-conserving PRUs.

To properly discriminate different energy eigenvalues by QPE, we need to choose m to be polynomial in n to achieve an inverse exponential precision. This requires applying m different controlled operations e^{iHt} with $t = O(2^m)$. Nevertheless, since $H = \sum_i \mathcal{J}_i h_i$ is a commuting Hamiltonian, one can factorize $e^{iHt} = \prod_j e^{i\mathcal{J}_j h_j t}$ and simulate each local evolution to achieve efficient simulation, a property known as fast-forwardability [59, 60]. Together, the overall running time for the construction is polynomial in n.

B. Hamiltonians without energy-conserving PRUs

Now we turn to the construction of our hard Hamiltonian H whose energy-conserving PRU do not exist. We prove the non-existence by presenting a universal algorithm to distinguish energy-conserving Haar-random unitaries of H from any polynomial-size quantum circuit (or subexponential-size quantum circuit under subexponential hardness assumption for quantum-secure one-way functions).

The essential feature of H is that its energy-conserving Haar-random unitary can be used to solve PSPACE-complete problems: problems that can be solved with polynomial memory cost but unbounded time complexity. These problems are believed to be extremely hard even for quantum computers. With a PSPACE-complete solver, one can efficiently invert quantum-secure one-way functions, which cannot be achieved by any polynomial-size quantum circuit. We construct the universal distinguishing algorithm by verifying whether one has successfully inverted the one-way function.

1. *Turing machine and Hamiltonian construction*

We first describe the construction of our hard Hamiltonian satisfying the mentioned properties. Our construction proceeds by embedding the dynamics of a Turing machine (TM) into a local Hamiltonian, similar to the Feynman-Kitaev construction of computational Hamiltonians [55, 56].

A TM, as illustrated in Fig. 2, can be thought of as a one-dimensional dynamical system: it consists of an infinite tape storing symbols from a finite set Γ, a read/write head that moves left or right, and a finite set of internal states Q of the head that together evolve under simple local update rules Δ. When performing computation, we first load the inputs consecutively into the tape. Then the machine updates the tape and internal state according to the rules until it halts, if at all. The output of computation, Accept or Reject, can then be read out. The number of steps the TM takes before halting is referred to as the time complexity of the problem. Despite this elementary structure, TMs are computationally universal in the sense that any algorithm can be expressed as such a sequence of updates. Thus, TMs serve as the foundation for modern theoretical computer science. For a more detailed overview, see Appendix A or standard textbooks [64–66].

For our purpose, we restrict the tape length to be finite and polynomial in input size, and require the TM to be reversible, i.e., any configuration of the machine has at most one predecessor. Note that the problems solvable by this type of TM form the set of PSPACE problems, named for the finite memory space of the TMs. We further require the tape to have periodic boundary conditions. With these restrictions, we can map any configuration of the TM with tape length L to a one-dimensional quantum product state with length $L+1$, as illustrated in Figure 2. In this mapping, each local Hilbert space contains all the symbols and internal states, thus forming identical qudit Hilbert spaces. Furthermore, since the update rules are local and homogeneous along the tape, we can express them as quantum isometries $V_\delta = \sum_{i=1}^{L} V_{\delta,i}$ for $\delta \in \Delta$, where $V_{\delta,i}$ represents the realization of transition rule δ at site i. Details of the mapping can be found in Appendix D. Therefore, we define $H = \sum_{\delta\in\Delta} \left(V_\delta + V_\delta^\dagger\right)$ as a one-dimensional, local, and translationally invariant Hamiltonian.

By definition, $V_{\text{forward}} = \sum_{\delta\in\Delta} V_\delta$ encodes all the transition rules. For example, let $|\psi_{\mathcal{C}}\rangle$ be the state that corresponds to some configuration $\mathcal{C}$ of the TM. Then $|\psi_{\mathcal{C}'}\rangle = V_{\text{forward}} |\psi_{\mathcal{C}}\rangle$ represents the successor configuration after one step of update. Moreover, since the TM is designed to be reversible, $V_{\text{forward}}^\dagger |\psi_{\mathcal{C}'}\rangle = |\psi_{\mathcal{C}}\rangle$. Therefore, we can view a computation process upon some input configuration as a unidirectional hopping along a one-dimensional path formed by successive configurations, as illustrated in Figure 2. Each computational process corresponds to an invariant subspace, with effective Hamiltonian being the hopping Hamiltonian along the one-dimensional path. The initial configuration corresponds to a localized wavefunction at the initial terminal of the path. The hardness of PSPACE-complete problems lies in the exponential length of the corresponding paths, thus having exponential time complexity.

This picture suggests that, if we have access to the energy-conserving Haar-random unitaries of H, difficult problems may be solved efficiently using the following method. To begin with, one prepares the product state $|\psi_{\mathcal{C}_1}\rangle$ that corresponds to the input configuration $\mathcal{C}_1$ for a given input x. This state serves as the source of the path, whose sink encodes the solution. Then one can sample a unitary U from the energy-conserving Haar-random ensemble and apply it to $|\psi_{\mathcal{C}_1}\rangle$. The scrambling nature of U will produce a wavefunction $U|\psi_{\mathcal{C}_1}\rangle$ dispersing along the entire path. A follow-up measurement in the computational basis will collapse $U|\psi_{\mathcal{C}_1}\rangle$ to any state $|\psi_{\mathcal{C}_t}\rangle$ along the chain with almost equal probabilities. In this way, with high probability, one can make an exponentially large step forward using one query of U. The core ideas are illustrated in Fig 2.

This method, while plausible, faces two obstacles. First, even if we can make an exponentially large step forward along the path at once, the probability of precisely collapsing to the sink is still exponentially small. This can be overcome by adding idling steps to the TM after the solution is reached. In Appendix D, we introduce duplications of the TM to double the length while keeping the solution readable along the second half of the path. Thus, the probability of reading out the solution after one query of U is amplified to $O(1)$.

Second, different subspaces of chains can have energy degeneracies when, e.g., two paths have the same lengths. In this case, the energy-conserving Haar-random unitaries entangle multiple subspaces, causing a false readout. The way we overcome this is to add perturbations to the Hamiltonian to break degeneracies. More concretely, we demonstrate that perturbations with coefficients drawn from $\{0, 1, 10, 1/2, 1/4\}$ suffice to energetically separate all the Accept and Reject paths from each other and the rest of the Hilbert space. The proof can be found in Appendix D, with additional details given in Appendices I and J.

Using these results, we can construct a one-dimensional, local, and translationally invariant Hamiltonian whose energy-conserving Haar-random unitaries can be used to solve PSPACE-complete problems.

Lemma 1 (Energy-conserving random unitary can be used to solve PSPACE problems, Theorem 3 in Appendix D)**.** *For any* PSPACE*-complete problem, there exists a one-dimensional, local, and translational-invariant Hamiltonian H, whose matrix elements belong to $\{0, 1, 10, 1/2, 1/4\}$, such that a polynomial quantum algorithm with query access to the energy-conserving Haar-random unitaries of H exists to solve the problem with high probabilities.*

2. *Distinguishing a* PSPACE*-solver from efficient quantum circuits*

A solver for PSPACE-complete problems can be used to invert quantum-secure one-way functions, a property not possessed by any polynomial-size quantum circuit. To see this, we use the *True Quantified Boolean Formula* problem (TQBF), a canonical PSPACE-complete problem [67, 68], as an illustration. TQBF consists of all fully quantified Boolean formulas that evaluate to true over the Boolean domain.

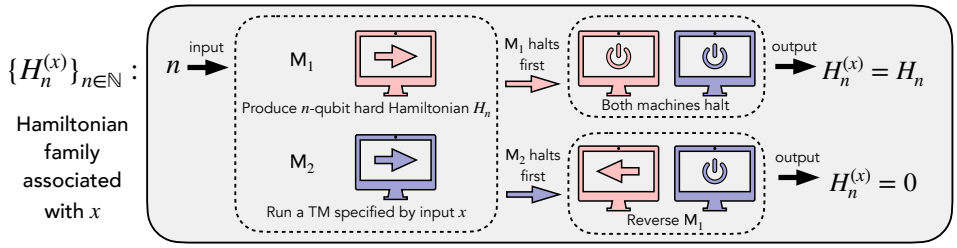

Figure 3. Turing machine that generates a Hamiltonian family $H_n^{(x)}$ with or without energy-conserving PRU, depending on whether universal TM halts upon input x. After receiving an put n, two machines run in parallel: M_1 generates the hard Hamiltonian H from Section V B, and M_2 is a UTM operating upon input x. If M_1 halts, then the whole system halts with output H. If M_2 halts, M_1 halts and does the reverse computing. Thus the system outputs 0.

Formally, the language is defined as:

$$\text{TQBF} := \left\{ \varphi = Q_1 x_1 \cdots Q_n x_n \; \psi(x_1, \ldots, x_n) \;\middle|\; \begin{array}{l} Q_i \in \{\forall, \exists\}, \; \psi \text{ is a Boolean formula} \\ \text{and } \varphi \text{ evaluates to true.} \end{array} \right\}.$$

We assume all quantifiers precede the propositional formula, and that ψ is encoded either in conjunctive normal form or as a Boolean circuit. The input size of a formula is the number of bits required to encode the quantifiers and ψ. For example, the formula $\phi = \forall x_1 \exists x_2 \forall x_3 \; [(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3)]$ is in TQBF.

Given a circuit C computing the one-way function f and target y, we construct the TQBF formula: $\Phi_{C,y} := \exists x_1, \ldots, x_n \; \psi(x_1, \ldots, x_n, y)$ where $\psi(x_1, \ldots, x_n, y)$ is a Boolean formula that evaluates to true if and only if $C(x_1, \ldots, x_n) = y$. This formula can be constructed in polynomial time by simulating the circuit C. First, we query the TQBF solver on $\Phi_{C,y}$. If it returns Reject, then no preimage exists. If it returns Accept, we extract a witness using binary search: for each bit position $i = 1, \ldots, n$, we construct the formula: $\Phi_i^0 = \exists x_{i+1}, \ldots, x_n \; \psi(a_1, \ldots, a_{i-1}, 0, x_{i+1}, \ldots, x_n)$ where $a_1, \ldots, a_{i-1}$ are the bits determined in previous iterations. We query the solver on Φ_i^0. If it returns Accept, we set $a_i = 0$; otherwise, we set $a_i = 1$. After n such queries, we obtain $(a_1, \ldots, a_n)$, which is guaranteed to be a valid preimage since the original formula was satisfiable and the oracle is correct. The total number of oracle queries is $n + 1$. In this way, we invert the one-way function efficiently.

In contrast, any polynomial-size quantum circuit cannot invert one-way functions. So, we can construct an efficient algorithm to distinguish a PSPACE-complete solver from any polynomial-size quantum circuit by checking if it correctly inverts the one-way function. Details are in Appendices E and F.

Lemma 2 (Distinguishing the TQBF solver, Theorem 4 in Appendix F)**.** *Assume quantum-secure one-way functions exist. There exists a polynomial-time classical algorithm $\mathcal{V}$ (the verifier) that, given black-box access to a purported* TQBF *solver $\mathcal{O}$, such that if $\mathcal{O}$ solves* TQBF *correctly, outputs* Accept *with high probability, if $\mathcal{O}$ implements any polynomial size quantum circuit, outputs* Reject *with high probability.*

Combining Lemmas 1 and 2, we can prove Theorem 2. Proof details are shown in Appendix G.

C. Undecidability of existence energy-conserving PRU

Given that both easy and hard instances exist, it is natural to seek an algorithm that can decide whether a given family of Hamiltonians has energy-conserving PRUs. However, this problem is inherently undecidable, meaning that no algorithm, even with exponential computational resources, can solve it.

To meaningfully define a computational problem, we are not asking only for the solution for a given input length, where one can always solve it by brute force. Rather, we specify an infinite series of problems $\{f_n\}_{n\in\mathbb{N}^+}$ with all possible input lengths, and ask about the asymptotic cost to solve them when n grows. When stating the aforementioned problem rigorously, we are asking whether *a uniform family of* Hamiltonians $\{H_n\}_{n\in\mathbb{N}^+}$ has energy-conserving PRUs or not. What we take as input is in fact a set of rules that specifies the Hamiltonian for any system size, and more concretely, a TM that generates the Hamiltonian's description when taking n as input.

Since we are taking TMs as inputs, the existence of energy-conserving PRUs can be linked to the solution of the halting problem, a canonical undecidable problem [69, 70]. The halting problem asks whether the universal Turing machine (UTM), a TM that can simulate all other TMs, eventually halts or not upon given inputs.

Suppose we let two TMs run in parallel. The first TM generates the description of the hard Hamiltonian in Theorem 2, and the second one is a UTM that operates upon a fixed input x. If the first TM halts, then the whole system halts. If the second one halts, then the first one stops and performs exactly the inverse operations to uncompute the previous outputs. In this way, if the UTM eventually halts upon x, the whole machine outputs 0 for sufficiently large n, whose energy-conserving PRU is the conventional PRU. Otherwise the machine outputs the hard Hamiltonian. Therefore, if we can decide whether a family of Hamiltonians has energy-conserving PRUs or not, we must be able to decide whether the UTM halts upon any given input x. The whole construction is illustrated in Fig 3.

We note that when restricted to translationally invariant Hamiltonians, our proof does not apply. There a Hamiltonian is completely specified by its finite set of local terms. It is unclear whether determining the existence of energy-conserving PRUs is still hard in those cases.

ACKNOWLEDGMENTS

We are grateful to Adam Bouland, Jeongwan Haah, Tony Metger, and John Preskill for insightful discussions about energy-conserving pseudorandom unitaries. L.M. is grateful to the helpful discussions with Hongkang Ni on the proof of Lemma 11. L.M. acknowledges support from Tsinghua University. T.S. acknowledges support from the Walter Burke Institute for Theoretical Physics at Caltech. T.S. and H.H. acknowledge support from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. The Institute for Quantum Information and Matter is an NSF Physics Frontiers Center.

Appendices

CONTENTS

I. Introduction 1

II. Pseudorandom unitaries and energy conservation 2

III. Main results 3

IV. Discussions 4

V. Proof overview 5
A. Hamiltonians with energy-conserving PRUs 5
B. Hamiltonians without energy-conserving PRUs 6
1. Turing machine and Hamiltonian construction 6
2. Distinguishing a PSPACE-solver from efficient quantum circuits 7
C. Undecidability of existence energy-conserving PRU 8

Acknowledgments 9

A. Preliminaries 11
1. Notations and matrix norms 11
2. Pseudorandom unitaries 11
3. Cryptographic primitives 12
4. Turing machines and complexity classes 13
5. Quantum phase estimation 14

B. Distinguishing energy-conserving ensemble from Haar-random unitaries 15

C. Energy-conserving PRU for commuting random Hamiltonians 16
1. Smallest energy gap 17
2. Random phase unitary with quantum phase estimation 19
3. Constructing energy-conserving PRU 22

D. Solving PSPACE problems with energy-conserving random unitary 26
1. Quantum simulation of reversible Turing machines 26
2. Duplicated Turing machine 28
3. Lifting the degeneracy 29
4. Construct the PSPACE solver 31

E. True Quantified Boolean Formula (TQBF) 34
1. Problem Statement 34
2. Power of TQBF 34

F. Verifying TQBF Oracles via One-Way Function 35
1. Verifier Algorithm 35
2. Supporting Lemmas 36
3. Main Proof 36

G. Verifier for random unitaries that conserve energy 37

H. Undecidability of the existence of energy-conserving PRUs 37

I. One-dimensional hopping problem 38

J. Proof of Lemma 11 39

References 42

Appendix A: Preliminaries

1. Notations and matrix norms

We use the standard notations O, Ω and Θ to denote asymptotic upper, lower, and tight bound, respectively. We use the $\mathsf{poly}(n)$ ($\mathsf{exp}(n)$) to denote any functions $f(n)$ such that there exists $c > 0$ satisfying $f(n) = O(n^c)$ ($O(e^{n^c})$). $\mathsf{negl}(n)$ denotes $f(n)$ smaller than any inverse polynomial functions of n.

Throughout the appendices, we will mostly use capital letter like U to denote a unitary matrix, or a quantum circuit, and calligraphic letter like $\mathcal{U}$ to denote an ensemble of unitary matrices, or other types of sets. The only exception that we use $\mathcal{O}$ to denote an oracle, which is also a circuit, since O is used to denote the asymptotic upper bound.

Norms of matrices and vectors are denoted as $\|A\|$ and $\|v\|$. In this paper, we will use the trace norm of matrices, defined for matrices of any size

$$\|A\|_1 := \mathrm{tr}\sqrt{A^\dagger A}. \tag{A.1}$$

It satisfies submultiplicativity, and triangle inequality

$$\|A_1 A_2\|_1 \le \|A_1\|_1 \cdot \|A_2\|_1, \quad \|A_1 + A_2\|_1 \le \|A_1\|_1 + \|A_2\|_1 \tag{A.2}$$

If the matrix is a vector, we will use the standard concept of Euclidean norm, which is equivalent to the trace norm if the vector is viewed as a $n \times 1$ matrix.

$$\|v\|_2 = \sqrt{v^\dagger v} = \sqrt{\sum_i |v_i|^2}. \tag{A.3}$$

We use $\|\cdot\|_2$ instead of $\|\cdot\|_1$ to emphasize the vector form.

We will use sans-serif letter as U to denote a quantum channel. Different from multiplication of matrices, we use $\mathsf{A} \circ \mathsf{B}$ to denote subsequent actions of channels, i.e., $\mathsf{A} \circ \mathsf{B}[\rho] := \mathsf{A}[\mathsf{B}[\rho]]$. Channels are subjected to the measure of diamond norm,

$$\|\mathsf{A}\|_\diamond := \sup_\rho \|(\mathsf{A} \otimes \mathsf{I})[\rho]\|_1, \tag{A.4}$$

where I is the identity channel of an ancillary system of any size, and ρ is a density matrix. The diamond norm also satisfies submultiplicativity, and triangle inequality. Note that since $\|\rho\|_1 = 1$ when ρ is a density matrix, $\|\mathsf{A}\|_\diamond = 1$ when A is a complete positive trace-preserving mapping.

We will also use sans-serif letter as S to denote registers, a collection of qubits to define "system" or "ancillas". Different usages can be easily identified from the context. We use $|\mathsf{S}| = n$ to denote the number of qubits in a register. We sometimes use subscript like $|0_\mathsf{S}\rangle$ to specify the register that a state lives in.

Specifically, M and $\mathsf{D}[\mathsf{M}]$ are used to denote Turing machines (TMs), which we will define more clearly later.

2. Pseudorandom unitaries

In this section we review the properties of pseudorandom unitary (PRU) ensembles. We are interested in ensembles which reproduce the characteristics of, and are indistinguishable from, *uniformly* random unitary transformations sampled via the Haar measure.

Definition 1 (Haar ensemble)**.** *Given a compact Lie subgroup $\mathbb{V}$ of the n-qubit unitary group $\mathbb{U}(2^n)$, the Haar ensemble $\mu(\mathbb{V})$ is the unique ensemble over $\mathbb{V}$ with normalized probability measure d that is both left- and right-invariant, i.e., for any subset $\mathbb{S} \subseteq \mathbb{V}$ and any $V \in \mathbb{V}$, $d(\mathbb{S}) = d(V \cdot \mathbb{S}) = d(\mathbb{S} \cdot V)$.*

A PRU ensemble over $\mathcal{U}$ is a unitary ensemble that can be efficiently generated, but can not be efficiently distinguished from $\mu(\mathcal{U})$[20, 23].

Definition 2 (Pseudorandom unitaries)**.** *Let $\{\mathcal{U}_n\}_{n\in\mathbb{N}^+}$ be a uniform family of unitary ensembles $\mathcal{U}_n = \{U_k\}_{k\in\mathcal{K}_n}$, where $U_k \in \mathbb{U}(2^n)$ and $\mathcal{K}_n$ denotes the key subspace. We call $\{\mathcal{U}_n\}$ a pseudorandom unitary ensemble if the followings are satisfied:*

- *There exists a* $\mathsf{poly}(n)$*-time quantum algorithm parametrized by* $k \in \mathcal{K}_n$ *to implement all* $U_k \in \mathcal{U}_n$*.*
- *For any* $\mathsf{poly}(n)$*-time quantum algorithm* $\{\mathcal{A}_n^{\mathcal{E}}()\}_{n\in\mathbb{N}^+}$ *with query access to unitary ensemble* $\mathcal{E}$*, if* k *is uniformly drawn from* $\mathcal{K}_n$*,*

$$\left|\Pr[\mathcal{A}_n^{\mu(\mathbb{U}(2^n))}() = 1] - \Pr[\mathcal{A}_n^{\mathcal{U}_n}() = 1]\right| \leq \mathsf{negl}(n)$$

holds for sufficiently large n*.*

In this paper, we focus on the cases where the subgroup is a commuting group with some fixed local Hamiltonian. With energy-conservation, the Haar-random unitaries factorize to the sum of random unitaries inside each degenerated subspace.

Fact 1. *Let* $\mathcal{H}_n^i$*,* $i = 1 \leq i \leq k$ *be the degenerated subspaces of* H_n*, then any* $U \in \mu(\mathcal{C}_n[H_n])$ *takes the form of* $U = \oplus_{i=1}^k U_i$*, where* $U_i \in \mu(\mathbb{U}(\mathcal{H}_n^i))$*. Specifically, when* H_n *has no energy degeneracy,* $U = \sum_E e^{i\theta_E}|E\rangle\langle E|$*, where* E *spans over all the energy eigenstates, and* $\theta_E \overset{i.i.d.}{\sim} \mathrm{Unif}(0, 2\pi)$*.*

This definition of PRU generalizes to the setting with conserved energy or charges.

Definition 3 (Energy-conserving pseudorandom unitary ensemble)**.** *Let* $\{H_n\}_{n\in\mathbb{N}^+}$ *be a uniform family of* n*-qubits Hamiltonians. Define the commuting subgroup* $\mathcal{C}_n^H = \{U|U \in \mathbb{U}(2^n), UH_n = H_nU\}$*. Let* $\{\mathcal{U}_n\}_{n\in\mathbb{N}^+}$ *be a uniform family of unitary ensembles* $\mathcal{U}_n = \{U_k\}_{k\in\mathcal{K}_n}$*, where* $U_k \in \mathbb{U}(2^n)$ *and* $\mathcal{K}_n$ *denotes the key subspace. We call* $\mathcal{U}_n$ *a energy-conserving pseudo-random unitary ensemble if the followings are satisfied:*

- *There exists a* $\mathsf{poly}(n)$*-time quantum algorithm parametrized by* $k \in \mathcal{K}_n$ *to implement all* $U_k \in \mathcal{U}_n$*.*
- *For any* $\mathsf{poly}(n)$*-time quantum algorithm* $\{\mathcal{A}_n^{\mathcal{E}}()\}_{n\in\mathbb{N}^+}$ *with query access to unitary ensemble* $\mathcal{E}$*, if* k *is uniformly drawn from* $\mathcal{K}_n$*,*

$$\left|\Pr[\mathcal{A}_n^{\mu(\mathcal{C}_n^H)}() = 1] - \Pr[\mathcal{A}_n^{\mathcal{U}_n}() = 1]\right| \leq \mathsf{negl}(n)$$

holds for sufficiently large n*.*

In above, we state standard definitions of energy-conserving PRU for qubit systems. They can be generalized to qudit systems for $d = O(1)$ in a straightforward way, where we skip the explicit statements.

3. Cryptographic primitives

Previous constructions of PRU[24, 26, 27] assume the existence of quantum-secure one-way functions, which is a standard cryptography assumption and widely believed to hold.

Definition 4 (Quantum-Secure One-Way Function)**.** *A function* $f : \{0,1\}^* \to \{0,1\}^*$ *is a* quantum-secure one-way function *if:*

1. f *is computable in polynomial time;*
2. *For any* $\mathsf{poly}(n)$*-time quantum algorithm* $\{\mathcal{A}_n()\}_{n\in\mathbb{N}^+}$*, for sufficiently large* n *we have*

$$\Pr_{x\in\{0,1\}^n}[f(\mathcal{A}_n(f(x))) = f(x)] \leq \mathsf{negl}(n) \tag{A.5}$$

holds for sufficiently large n*.*

Throughout this paper, we will make the same assumption in the proofs of both easy and hard Hamiltonians. In the construction of energy-conserving PRU for random commuting Hamiltonians, we will use the pseudo-random functions, which can be constructed out of one-way functions.

Definition 5 (Pseudorandom function)**.** *Let* $\{\mathcal{F}_n\}$ *denote a uniform family of functions* $\mathcal{K}_n = \{f_k\}_{k\in\mathcal{K}_n}$*, where* $f_k : \{0,1\}^n \to \{0,1\}$ *and* $\mathcal{K}_n$ *denotes the key subspace. We say* $\{\mathcal{F}_n\}$ *are pseudorandom functions if*

- f_k *is computable in polynomial time;*
- *For any* $\mathsf{poly}(n)$*-time quantum algorithm* $\{\mathcal{A}_n^{\mathcal{O}}()\}_{n\in\mathbb{N}^+}$ *with query access to an oracle* $\mathcal{O}$*, if* k *is uniformly drawn from* $\mathcal{K}_n$*,*

$$\left|\Pr[\mathcal{A}_n^{\mathcal{O}_\mathcal{F}}() = 1] - \Pr[\mathcal{A}_n^{\mathcal{O}_\mathcal{R}}() = 1]\right| \leq \mathsf{negl}(n)$$

holds for sufficiently large n*, where* $\mathcal{O}_\mathcal{F} : |x\rangle \to (-1)^{f_k(x)}|x\rangle$ *for* $x \in \{0,1\}^n$*, and* $\mathcal{O}_\mathcal{R} : |x\rangle \to e^{i\theta}|x\rangle$ *for* $\theta \sim \mathrm{Unif}[0, 2\pi)$*.*

4. Turing machines and complexity classes

We now review Turing machines (TM), a model for universal computation[64–66]. We will use this framework to define notions of computational complexity. We focus on decision problems where the answer is either Accept or Reject.

Definition 6 (Decision problem). *A decision problem is specified by a language* $L \subseteq \{0,1\}^* = \cup_{n=0}^{\infty}\{0,1\}^n$. *The problem is that give any* $x \in \{0,1\}^*$, *output* Accept *if* $x \in L$, *otherwise output* Reject. $|x|$ *is called the size of input.*

Given an instance of a decision problem, we can consider the corresponding TM. Informally, a TM consists of three parts, as illustrated in Fig 2: a tape with some symbols, a read-write head with some internal states set Q, and a set of transition rules Δ. The tape provides the space for storage information and doing operations. Each cell of the tape contains one symbol from a *finite* set of alphabet Γ, like 0,1. The head can read the symbol of the cell it currently locates, and is associated with an internal state $q_\mu \in Q$. Then according to the symbol and the current internal state q_μ, the head can change the internal state, rewrite the symbol, and then move left or right or stay still. The rules that determine the behavior of the head is the transition function $\Delta : Q \times \Gamma \to Q \times \Gamma \times \{+,-,0\}$. Here q, x denote the current internal state and symbol, and in one round of operation they will be changed to q' and x', respectively. After then the head will move right, left, or stay, depending on $s = +,-,0$. In this way a TM change the contents of the tape step by step and arrive the final output.

More formally,

Definition 7 (Turing machines). *A (deterministic) Turing Machine* M *is defined by a triple* $\langle Q, \Gamma, \Delta\rangle$, *such that*

- Q *is a finite set of internal states that contains the initial state* $q_0 \in Q$ *and two halting states* $q_r, q_a \in Q$, *corresponding to* Accept *and* Reject.
- Γ *is a finite set of symbols that contains the blank symbol* b.
- Δ *is a finite set of transition functions* $\Delta : Q \times \Gamma \to Q \times \Gamma \times \{+,-,0\}$ *that satisfies for any* $(q, x, q', x', s) \in \Delta$, $q \neq q_a, q_r$ *and* $q' \neq q_0$.

The TM has a two-way infinite tape of cells indexed by $\mathbb{Z}$ *and a single read/write tape head that moves along the tape. A configuration of* M, $\mathcal{C} = (q, B, i) \in Q \times \Gamma^* \times \mathbb{Z} =: \mathscr{C}$, *is a complete description of the contents of the tape* B, *the location of the tape head* i *and the internal state* q *of the head. At any time, only a finite number of the tape cells may contain non-blank symbols.*

For any configuration $\mathcal{C} \in \mathscr{C}$, *the successor configuration* $\mathcal{C}'$ *is defined by applying the transition function to the current state and the symbol scanned by the head, replacing them by those specified in the transition function and moving the head right (+), left (−), or stay still (*0*).*

The initial configuration satisfies the following conditions: the head is in cell 0, called the starting cell, and the machine is in state q_0. *We say that an initial configuration has input* $x \in (\Gamma \setminus \{b\})^*$ *if* x *is written on the tape in positions* $0, 1, 2, \cdots, |x|$ *and all other tape cells are blank. The TM halts on input* x *if it eventually enters the final state* q_a *or* q_r. *The output of this computation task is then* Accept *or* Reject, *depending on halting state. The number of steps a TM takes to halt on input* x *is its running time on input* x.

By choosing appropriate alphabet, internal states set and transition functions set, a TM runs an *algorithm* which solves a corresponding decision problem.

To simulate the TM with a quantum Hamiltonian we need to use TMs with a fixed-size memory, i.e., TMs with a fixed tape-length. The tape-length will correspond to the length of the one-dimensional Hilbert space that the Hamiltonian residues.

Definition 8 (Turing machines with fixed-size memory). *Given a Turing machine* $\mathsf{M} = \langle Q, \Gamma, \Delta\rangle$, *the corresponding Turing machine with fixed memory-size is denoted as* $\mathsf{M}(l)$, *where* $l \in \mathbb{N}^+$ *is the tape length. For any* $\mathsf{M}(l)$, *we choose a periodic boundary condition, i.e., the left-most cell of the tape is linked to the* $l-$*the cell. The configuration of TM with fixed-size memory is defined analogously.*

TMs have many variants. One useful variant is the *Reversible Turing machines* (RTM), which is the TM that each configuration has at most one predecessor.

Definition 9 (Reversible Turing machine). *A Reversible Turing machine is a TM* $\langle Q, \Gamma, \Delta\rangle$ *that any configuration has at most one predecessor and one successor.*

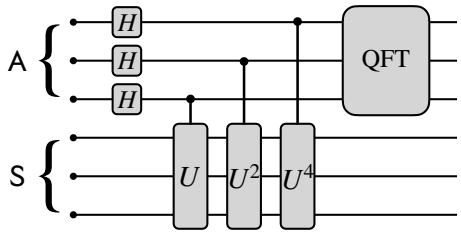

Figure 4. Circuit structure for quantum phase estimation.

Fact 2 (Structure of RTM; cf.[64–66]). *Let* $\mathsf{M} = \langle Q, \Gamma, \Delta \rangle$ *be a TM defined by Definition. A 4.* M *is reversible iff* Δ *satisfies the follows:*

- *Unidirection: For any* $\delta = (q, x, q', x', s) \in \Delta$, s *is uniquely determined by* q'.
- *One-to-one: Ignoring* s *and viewing* Δ *as a map from* $Q \times \Gamma$ *to* $Q \times \Gamma$, *it is an injection.*

The construction of RTM insures every configuration has at most one predecessor and one successor. Then is it possible to construct another RTM to reverse all the computational processes? The answer is definitely yes, but with non-standard form of transition rules. Recall the transition rule (q, x, q', x', s) is defined that the head movement is always the final action. As a result, to exactly reverse the computation of a RTM, we need to move the head first.

Definition 10 (Reverse transition rules). *Given a RTM* $\mathsf{M} = \langle Q, \Gamma, \Delta \rangle$, *one can always construct a set of transition rules to reverse its computation,* $\Delta^{-1} = \{(q, s, x, q', x') \mid (q', x', q, x, -s) \in \Delta\}$. *Here* (q, s, x, q', x') *means that depending on the current internal state* q, *the head first moves along* s *direction and then read the current symbol* x. *Subsequently, the head modifies of internal state and symbol to* q' *and* x'. *We refer transition rules of this form the reverse form. Note that* $(q, 0, x, q', x') = (q, x, q', x', 0)$, *so we always regard the transition rules with* $s = 0$ *as the standard form.*

In the following, we regard a machine that satisfies the definition of TM except for containing reverse form transition rules also as a TM.

The class PSPACE contains the languages that can be solved by a TM with polynomial-size tape with the input. But the computing time is unlimited.

Definition 11 (PSPACE). $\mathsf{PSPACE} = \{L\}$ *is the set of languages* L *where there exists a Turing machine* M_L *and a polynomial* $p(\cdot)$, *such that any* $x \in \{0,1\}^*$, *one can determine if* $x \in L$ *using* $\mathsf{M}_L(l)$ *for* $l = \mathfrak{O}(p(|x|))$. *We call this* M_L *the Turing machine that solves* L *in polynomial space.*

5. Quantum phase estimation

In this section we review the properties of the quantum phase estimation (QPE) algorithm[56, 61–63], which we use as a subroutine in the construction of energy-conserving PRUs. The circuit implementation of QPE is sketched in Fig 4.

Let $|\psi\rangle$ be a n-qubit quantum state on register S and U be a unitary such that $U|\psi\rangle = e^{i2\pi\theta}|\psi\rangle$. The goal of QPE is to estimate the phase $\theta \in [0, 1)$. For this, we need an ancilla register A to restore the digitalization of θ, which we take to be $m = \mathsf{poly}(n)$ qubits.

Starting from $|\psi\rangle \otimes |0^m\rangle$, the first step is to apply $H^{\otimes m}$ of A, where H is Hadamard gate.

$$|\psi\rangle \otimes |0^m\rangle \xrightarrow{H^{\otimes m}} \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} |\psi\rangle \otimes |x\rangle . \tag{A.6}$$

Second, we apply controlled $U^{2^{i-1}}$ on S controlled by the i-th qubit in A for $1 \le i \le m$. After this step,

$$\frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} |\psi\rangle \otimes |x\rangle \xrightarrow{\text{controlled } U} \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} e^{i2\pi\hat{x}\theta} |\psi\rangle \otimes |x\rangle , \tag{A.7}$$

where $\hat{x}$ is the decimal number of x. Finally, we utilize the inverse quantum Fourier transformation (QFT),

$$\mathrm{QFT}^\dagger : \quad |x \in \{0,1\}^m\rangle \to \frac{1}{\sqrt{2^m}} \sum_{y\in\{0,1\}^m} e^{-i2\pi\hat{x}\hat{y}/2^m} |y\rangle . \tag{A.8}$$

Applying inverse QFT on the register A, we have

$$\begin{aligned}\frac{1}{\sqrt{2^m}} \sum_{x\in\{0,1\}^m} e^{i2\pi\hat{x}\theta} |\psi\rangle \otimes |x\rangle \xrightarrow{\mathrm{QFT}^\dagger} \frac{1}{2^m} \sum_{x,y\in\{0,1\}^m} e^{i2\pi\hat{x}(\theta-\hat{y}/2^m)} |\psi\rangle \otimes |y\rangle \\ = \sum_{y\in\{0,1\}^m} \alpha_y(\theta) |\psi\rangle \otimes |y\rangle ,\end{aligned} \tag{A.9}$$

where

$$\alpha_y(\theta) = \frac{1}{2^m} \frac{1-e^{i2\pi 2^m(\theta-\hat{y}/2^m)}}{1-e^{i2\pi(\theta-\hat{y}/2^m)}}. \tag{A.10}$$

The amplitude distribution $\alpha_y(\theta)$ is sharply peaked around θ. From standard error analysis, we have

Fact 3 (Accuracy of quantum phase estimation, cf.[56, 61–63])**.** *For a n-qubit unitary $U \in \mathbb{U}(2^n)$ and a n-qubit state $|\psi\rangle$ such that $U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle$, $m \in \mathbb{N}^+$ and $\epsilon \in (0,1)$, there is a quantum circuit acting on $n+k \equiv n+m+1+\lceil 2\log_2 \epsilon^{-1}\rceil$ qubits that satifies the following: When taking $|\psi\rangle\otimes|0\rangle_k$ as input, outputs a state $|\psi\rangle\otimes|\phi_{m,\epsilon}\rangle$, such that $\left\|\prod_{\phi,m,\epsilon}|\phi_{m,\epsilon}\rangle\right\|_2 \le \epsilon$, where $\prod_{\phi,m,\epsilon} = \sum_{b\in\{0,1\}^k,|\hat{b}/2^k-\phi|>2^{-(m+1)}} |b\rangle\langle b|$, with $\hat{b}$ the decimal number of b. The circuit uses 2^k-1 times of controlled U.*

The main cost of QPE is the repeated implements of controlled U, with other parts implemented efficiently. As we have seen, to achieve a precision 2^{-m}, we need to implement U^{2^j} for j from 1 to m. This means that an inverse exponential precision generally requires exponential time complexity to achieve. For our application later, however, we will use a specific U such that the cost could be significantly reduced.

Appendix B: Distinguishing energy-conserving ensemble from Haar-random unitaries

To motivate the energy-conserving PRU, we begin by proving any energy-conserving unitary ensemble does not form PRU (with no energy constraint). The intuition for this result is to simply check the energy. Let $|\psi\rangle$ be an arbitrary input state, one can estimate the energy expectation $\mathbb{E}_U\left[\langle\psi|U^\dagger H U|\psi\rangle\right]$ for U drawn from some random unitary ensemble. When U is drawn from Haar-random unitaries, $\mathbb{E}_U\left[\langle\psi|U^\dagger H U|\psi\rangle\right] \propto \mathrm{tr}\, H$, which is the energy expectation of infinite temperature state. When U is drawn from any ensemble $\{U\}$ satisfying $[U,H]=0, \forall U$, $\mathbb{E}_U\left[\langle\psi|U^\dagger H U|\psi\rangle\right] = \langle\psi|H|\psi\rangle$. Thus, a distinguishing algorithm for $\{U\}$ and Haar-random unitaries can be constructed by checking the average energy.

More precisely, we consider the local sparse Hamiltonian: H is given by the sum of k-local terms, where each qubit is acted by at most d k-local terms. This is often referred to as k-local Hamiltonians with bounded degree d. Existing results [52–54] demonstrated that for such Hamiltonians, a product state with significant energy deviation from the Haar-random ones can be efficiently constructed.

Lemma 1 (Product state with large deviation. Corollary 2 of [52])**.** *Given an n-qubit k-local Hamiltonian $H = \sum_{P\in\{I,X,Y,Z\}^n:|P|\le k} \alpha_P P$ with bounded degree d, $|\alpha_P| \le 1$ for all P, and $k = O(1)$. There is a random algorithm that runs in time $O(nd)$ and produces either a random maximizing state $|\psi\rangle = |\psi_1\rangle\otimes\cdots|\psi_n\rangle$ satisfying*

$$\mathbb{E}_{|\psi\rangle}\left[\langle\psi|H|\psi\rangle\right] \ge \mathbb{E}_{|\phi\rangle:\mathrm{Haar}}\left[\langle\phi|H|\phi\rangle\right] + \frac{C}{\sqrt{d}} \sum_{P\neq I} |\alpha_P|, \tag{B.1}$$

or a random minimizing state $|\psi\rangle = |\psi_1\rangle\otimes\cdots|\psi_n\rangle$ satisfying

$$\mathbb{E}_{|\psi\rangle}\left[\langle\psi|H|\psi\rangle\right] \le \mathbb{E}_{|\phi\rangle:\mathrm{Haar}}\left[\langle\phi|H|\phi\rangle\right] - \frac{C}{\sqrt{d}} \sum_{P\neq I} |\alpha_P| \tag{B.2}$$

for some constant C.

This result enables explicit construction of an efficient distinguishing algorithm.

Theorem 1 (Energy-conserving unitary ensemble does not form PRU)**.** *Given an n-qubit k-local Hamiltonian with bounded degree d satisfying $k, d = O(1)$. Any random unitary ensemble $\{U\}$ satisfying $[U, H] = 0$ for all U can be efficiently distinguished from Haar-random ensemble.*

Proof. To prove this, we demonstrate that there is a universal efficient algorithm to distinguish $\{U\}$ from the Haar-random ensemble.

a. The algorithm. The algorithm takes two steps. First, estimating $E_{\text{Haar}} = \mathbb{E}_{|\phi\rangle:\text{Haar}}\big[\langle\phi| H |\phi\rangle\big]$ to a high precision by simulating pseudo-random states $|\phi\rangle$. Second, estimating

$$E_U = \mathbb{E}_{|\psi\rangle,U}\big|\big[\langle\psi| U^\dagger H U |\psi\rangle\big] - E_{\text{Haar}}\big| \tag{B.3}$$

for $|\psi\rangle$ sampled by Lemma 1, and for U sampled from the unitary ensemble to be distinguished. If E_U is smaller than $\frac{C}{2\sqrt{d}}\sum_{P\neq I}|\alpha_P|$, output Accept. Otherwise output Reject.

b. Performance guarantee. When U is drawn from the Haar-random ensemble,

$$\begin{aligned}
E_U &= \mathbb{E}_{|\psi\rangle,U}\big|\big[\langle\psi| U^\dagger H U |\psi\rangle\big] - \mathbb{E}_{|\phi\rangle:\text{Haar}}\big[\langle\phi| H |\phi\rangle\big]\big| \\
&\le \mathbb{E}_{|\psi\rangle}\Big[\sqrt{\mathbb{E}_{|\phi\rangle:\text{Haar}}[\langle\phi| H |\phi\rangle\langle\phi| H |\phi\rangle] - \mathbb{E}_{|\phi\rangle:\text{Haar}}\big[\langle\phi| H |\phi\rangle\big]^2}\Big] \\
&= \mathbb{E}_{|\psi\rangle}\left[\sqrt{\frac{1}{2^n(2^n+1)}\Big(\operatorname{tr} H^2 - \frac{\operatorname{tr} H^2}{2^n}\Big)}\right] \\
&= \sqrt{\frac{1}{2^n(2^n+1)}}\left\|H - \frac{\operatorname{tr} H}{2^n}\mathrm{I}\right\|_F \\
&\le \sqrt{\frac{1}{2^n+1}}\left\|H - \frac{\operatorname{tr} H}{2^n}\mathrm{I}\right\|_\infty \\
&= \mathcal{O}(n/2^{\frac{n}{2}}).
\end{aligned} \tag{B.4}$$

When U is drawn from any energy-conserving unitary ensemble,

$$E_U = \mathbb{E}_{|\psi\rangle,U}\big|\big[\langle\psi| U^\dagger H U |\psi\rangle\big] - \mathbb{E}_{|\phi\rangle:\text{Haar}}\big[\langle\phi| H |\phi\rangle\big]\big| \ge \frac{C}{\sqrt{d}}\sum_{P\neq I}|\alpha_P| = \Omega(1) \tag{B.5}$$

by Lemma 1. Therefore, there is an exponential separation for E_U between these two cases. Estimating E_{Haar} and E_U up to an inverse polynomial precision suffices to distinguish these two cases.

c. Runtime. Since H is k-local with bounded degree d, estimating $\langle\psi| H |\psi\rangle$ up to ϵ error requires $O(\log(n)/\epsilon^2)$ samples of $|\psi\rangle$ using, e.g., classical shadow tomography [13]. While $\|H\|_\infty = O(n)$, estimating $\mathbb{E}_{|\psi\rangle}\big[\langle\psi| H |\psi\rangle\big]$ up to ϵ precision requires $O(n^2/\epsilon^2)$ samples of $\langle\psi| H |\psi\rangle$ by Chernoff bound. Combining these two, one can estimate E_{Haar} and E_U to an inverse polynomial precision by querying U polynomial times. □

Appendix C: Energy-conserving PRU for commuting random Hamiltonians

In this section, we construct the energy-conserving PRU for commuting Hamiltonians with random coefficients drawn from Gaussian distribution. Roughly speaking, our construction takes three steps: first, introduce ancillary qubits and apply QPE to rotate into energy eigenbasis. Second, apply quantum-secure pseudo-random function to ancilla qubits. This amounts to add a pseudo-random phase to each energy eigenstates. Finally, applying $\text{QPE}^\dagger$ to rotate back to original basis. Pseudo-random phase unitaries, which are energy-conserving PRU for non-degenerated Hamiltonians, are constructed this way. Crucially, commuting Hamiltonians enable the application of e^{iHt} for $t = \mathsf{exp}(n)$, which makes it possible to reserve every energy eigenstate perfectly.

To avoid insufficient covering, we restrict ourselves to local terms that are drawn from a complete set

Definition 12 (Complete set of commuting observables)**.** *A set of observables $\{A_1, \cdots, A_k\}$ is called a complete set of commuting observables, iff the followings hold*

- $[A_i, A_j] = 0$ *for* $i \neq j$.

- *Let $\{|\psi(l)\rangle\}$ be a set of common basis such that $A_i|\psi(l)\rangle = \mu_i(l)|\psi(l)\rangle$ for all i, then the ordered tuple $(\mu_1(l), \cdots, \mu_k(l))$ uniquely determine $|\psi(l)\rangle$.*

In words, in the complete set of commuting observables the quantum numbers of all A_is together complete specify the quantum state.

Ideally, we consider the family of commuting Hamiltonians $H_n = \sum_i \mathcal{J}_i h_i$, where $\{h_i\}$ forms a complete set and $\mathcal{J}_i$s are drawn from Gaussian distribution. However, to facilitate computation on digital computers, one needs to digitalize every continuous variable. Therefore, we use the digitalized Gaussian random variable as coefficients.

Definition 13 (Digitalization of Gaussian random variable)**.** *Let $R, \delta > 0$ such that R/δ is an odd integer. A (R,δ)-digitalization of Gaussian random variable $\mathcal{J}$ is denoted as $\mathcal{J}' = Q_{R,\delta}(\mathcal{J})$. $\mathcal{J}'$ is a random variable taking the values $-R, -R+\delta, \cdots, -\delta, 0, \delta, \cdots, R-\delta, R$ such that*

$$\mathcal{J}' = \begin{cases} k\delta, & \mathcal{J} \in \left(\left(k-\frac{1}{2}\right)\delta, \left(k+\frac{1}{2}\right)\right] \\ -R, & \mathcal{J} \in \left(-\infty, -R+\frac{1}{2}\delta\right] \\ R, & \mathcal{J} \in \left(R-\frac{1}{2}\delta, \infty\right). \end{cases} \tag{C.1}$$

A (R,δ)-digitalization takes $O(\log_2(R/\delta))$ number of bits to represent a Gaussian random variable.

Definition 14 (Random commuting local Hamiltonian ensemble)**.** *Fix a locality parameter $d \geq 1$ and a set of precision parameter (R,δ). Lett $\mathcal{T}$ be a finite set of Hermitian operators with dimensions at most 2^d and no spectral degeneracy. For each system size n, pick up $M(n) = \Theta(n)$ number of template observables $h^{(\alpha_i)} \in \mathcal{T}$, $1 \leq i \leq M(n)$, and assign local supports $S_i \subseteq [n]$ with $|S_i| = |\operatorname{supp}(h^{(\alpha_i)})|$ for each $h^{(\alpha_i)}$, such that $\{h_i\} := \{(h^{(\alpha_i)})_{S_i} \otimes I_{[n]\setminus S_i}\}$ is a complete set of commuting observables. Draw i.i.d. coefficients $\mathcal{J}_i \sim Q_{R,\delta}(\mathcal{N}(0,1))$, independent of the h_i, the commuting random local Hamiltonian is defined as $H_n = \sum_{i=1}^{M(n)} \mathcal{J}_i h_i$.*

As a simple example, we can take $\mathcal{T} = \{\sigma_z\}$ and $\{h_1, h_2, \cdots h_n\} = \{\sigma_z^1, \sigma_z^2, \cdots \sigma_z^n\}$.

Throughout the rest of this section, if $\lambda \in \{0,1\}^*$ is a bitstring, we will denote its corresponding decimal number (i.e, $\sum_{i=0}^{|\lambda|-1} 2^i \lambda_{|\lambda|-i}$) be $\hat{\lambda}$.

1. Smallest energy gap

In this subsection, we prove that random commuting Hamiltonians have at least exponentially small energy gap with high probability, enabling an accurate discrimination of eigenstates by QPE with polynomial number of ancillas.

To warm up, we first prove the claim first for random commuting Hamiltonians with coefficients drawn from the continuous Gaussian distribution.

Fact 4 (Convolution of Gaussian distributions)**.** *Let $X_i \sim \mathcal{N}(\mu_i, \sigma_i)$, $1 \leq i \leq n$ be Gaussian random variables. Then the random variable $\sum_{i=1}^n \alpha_i X_i$ obeys distribution $\mathcal{N}(\sum_{i=1}^n \alpha_i \mu_i, \sum_{i=1}^n |\alpha_i|\sigma_i)$ for any $\alpha_1, \cdots \alpha_n \in \boldsymbol{R}$.*

Lemma 2 (Smallest energy gap of random commuting Hamiltonians)**.** *Let $H_n = \sum_{i=1}^{M(n)} \mathcal{J}_i h_i$ be a random commuting Hamiltonian with $\mathcal{J}_i \overset{i.i.d.}{\sim} \mathcal{N}(0,1)$. $\{\lambda_i\}_{1\leq i\leq 2^n}$ labels the eigenvalues of H_n. Then for sufficiently large $\beta > 0$,*

$$\Pr\left(\min_{(k,k')\in[2^{M(n)}]^2, k\neq k'} \{|\lambda_k - \lambda_{k'}|\} \leq 2^{-\beta n}\right) = O(2^{-(\beta n - 2M(n))}). \tag{C.2}$$

Proof. Let $\mathcal{E} = \bigcup_{h\in\mathcal{T}} \operatorname{Spec}(h)$. There exists a set of eigenstates $|\psi(\mathbf{e})\rangle$ completely specified by ordered tuple $\mathbf{e} = (e_1, \cdots, e_{M(n)})$ for $e_i \in \mathcal{E}$, whose eigenvalues are $\lambda(\mathbf{e}) = \sum_{i=1}^{M(n)} \mathcal{J}_i e_i$. As a result,

$$\lambda_k - \lambda_{k'} = \left|\sum_{i=1}^{M(n)} \mathcal{J}_i e_{k_i} - \sum_{i=1}^{M(n)} \mathcal{J}_i e_{k'_i}\right| = \left|\sum_{i=1}^{M(n)} \mathcal{J}_i (e_{k_i} - e_{k'_i})\right| =: \left|E(\mathbf{e}_k, \mathbf{e}_{k'})\right| \tag{C.3}$$

for $\mathbf{e}_k \neq \mathbf{e}_{k'}$.

Due to Fact.4,

$$E(\mathbf{e}_k, \mathbf{e}_{k'}) \sim \mathcal{N}(0, \sum_{i=1}^{M(n)} |e_{k_i} - e_{k'_i}|). \tag{C.4}$$

As a result, for any constant $\beta > 0$,

$$\Pr\left(|E(\mathbf{e}_k, \mathbf{e}_{k'})| \leq 2^{-\beta n}\right) = 2\,\mathrm{erf}\left(\frac{2^{-\beta n}}{\sum_{i=1}^{M(n)} |e_{k_i} - e_{k'_i}|}\right) \leq \frac{4}{\sqrt{\pi}} \frac{2^{-\beta n}}{\sum_{i=1}^{M(n)} |e_{k_i} - e_{k'_i}|} \leq \frac{4 \cdot 2^{-\beta n}}{\sqrt{\pi} e_{\min}}. \tag{C.5}$$

In the last inequality we introduce $e_{\min} = \min_{e,e' \in \mathcal{E}, e \neq e'}\{|e - e'|\}$ and use the fact that $\mathbf{e}_k \neq \mathbf{e}_{k'}$. Due to union bound,

$$\begin{aligned}\Pr\Big(\min_{\{k,k'\} \subset [2^{M(n)}]} \{|\lambda_k - \lambda_{k'}|\} \leq 2^{-\beta n}\Big) &\leq \sum_{\{k,k'\} \in [2^{M(n)}]} \Pr\left(|\lambda_k - \lambda_{k'}| \leq 2^{-\beta n}\right) \\ &\leq \frac{2^{2M(n)+1-\beta n}}{\sqrt{\pi} e_{\min}}.\end{aligned} \tag{C.6}$$

Since $M(n) = \Theta(n)$, we can always choose a β such that RHS is smaller. □

Built upon Lemma 2, we prove the same property holds for digitalized coefficients.

Lemma 3 (Smallest gap under digitalization)**.** *Let $H_n = \sum_{i=1}^{M(n)} \mathcal{J}_i h_i$ be a random commuting Hamiltonian with $\mathcal{J}_i$ being (R, δ)-digitalizatio of $\mathcal{N}(0, 1)$. $\{\lambda_i\}_{1 \leq i \leq 2^n}$ labels the eigenvalues of H_n. Then for $R = \mathsf{poly}(n)$, $\delta = O(1/(e^{\beta n} M(n)))$, and sufficiently large $\beta > 0$,*

$$\Pr\Big(\min_{(k,k') \in [2^{M(n)}]^2, k \neq k'} \{|\lambda_k - \lambda_{k'}|\} \leq 2^{-\beta n}\Big) = \mathsf{negl}(n). \tag{C.7}$$

The digitalization using $\mathsf{poly}(n)$ number of bits in total.

Proof. Let $\mathcal{E} = \bigcup_{h \in \mathcal{T}} \mathrm{Spec}(h)$. For $\mathbf{e} \neq \mathbf{e}' \in \mathcal{E}^{M(n)}$, let

$$f_n^{(\mathbf{e},\mathbf{e}')}(x_1, \cdots, x_{M(n)}) = \Big|\sum_{i=1}^{M(n)} x_i (e_i - e'_i)\Big|. \tag{C.8}$$

$f_n^{(\mathbf{e},\mathbf{e}')}$ satisfies

$$\begin{aligned}\left|f_n^{(\mathbf{e},\mathbf{e}')}(x_1, \cdots, x_{M(n)}) - f_n^{(\mathbf{e},\mathbf{e}')}(x'_1, \cdots, x'_{M(n)})\right| &\leq \left|\sum_{i=1}^{M(n)} (x_i - x'_i)(e_i - e'_i)\right| \\ &\leq e_{\max}\sqrt{M(n)}\,\|\mathbf{x} - \mathbf{x}\|_2\,,\end{aligned} \tag{C.9}$$

where $e_{\max} = \max_{e,e' \in \mathcal{E}} |e - e'|$, and $\mathbf{x} = (x_1, \cdots, x_{M(n)})$. As a result, $f_n^{(\mathbf{e},\mathbf{e}')}$ is $e_{\max}\sqrt{M(n)}$-Lipschitz for all $\mathbf{e} \neq \mathbf{e}'$.

$$f_n(x_1, x_2, \cdots, x_{M(n)}) = \min_{\mathbf{e},\mathbf{e}' \in \mathcal{E}^{M(n)}, \mathbf{e} \neq \mathbf{e}'} f_n^{(\mathbf{e},\mathbf{e}')}(x_1, \cdots, x_{M(n)}) \tag{C.10}$$

is also a $e_{\max}\sqrt{M(n)}$-Lipschitz function.

Let $\mathcal{J}'_i$ be the random Gaussian seed to define $\mathcal{J}_i$. Using the fact that if $|\mathcal{J}'_i| < R - \delta/2$ for all i, then $\left\|(\mathcal{J}_1, \cdots, \mathcal{J}_{M(n)}) - (\mathcal{J}'_1, \cdots, \mathcal{J}'_{M(n)})\right\|_2 \leq \delta\sqrt{M(n)}/2$, we have

$$\begin{aligned}\Pr\Big(\min_{(k,k') \in [2^{M(n)}]^2, k \neq k'} \{|\lambda_k - \lambda_{k'}|\} \leq 2^{-\beta n}\Big) &\leq \Pr\left(f_n(\mathcal{J}_1, \mathcal{J}_2, \cdots, \mathcal{J}_{M(n)}) \leq 2^{-\beta n}\right) \\ &= \Pr\left(f_n(\mathcal{J}_1, \mathcal{J}_2, \cdots, \mathcal{J}_{M(n)}) \leq 2^{-\beta n}\ ,\ \exists |\mathcal{J}'_i| \geq R - \delta/2\right) \\ &\quad + \Pr\left(f_n(\mathcal{J}_1, \mathcal{J}_2, \cdots, \mathcal{J}_{M(n)}) \leq 2^{-\beta n}\ ,\ \forall i, |\mathcal{J}'_i| < R - \delta/2\right) \\ &\leq \Pr\left(\exists |\mathcal{J}'_i| \geq R - \delta/2\right)\end{aligned}$$

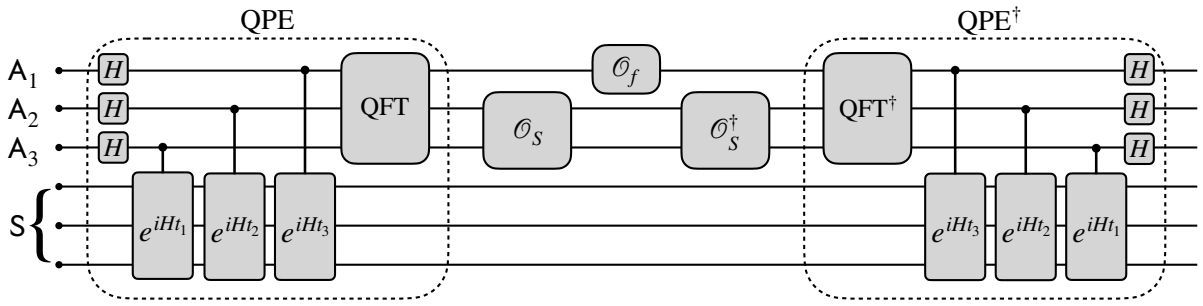

Figure 5. Entire construction of energy-conserving PRU for random commuting Hamiltonians.

$$+\Pr\left(f_n(\mathcal{J}_1',\mathcal{J}_2',\cdots,\mathcal{J}_{M(n)}')\le 2^{-\beta n}+\delta e_{\max}M(n)/2\right). \tag{C.11}$$

In the last inequality, we use $\Pr(|f(x)|\le a)\le\Pr(|f(y)|\le a+L\left\|x-y\right\|_2)$ if f is L-Lipschitz and x depends on y. For the first term, using union bound,

$$\Pr\left(\exists|\mathcal{J}_i|\ge R-\delta/2\right)\le M(n)\sqrt{\frac{2}{\pi}}e^{-(R-\delta/2)^2/2} \tag{C.12}$$

For the second term, taking $\delta\le 1/(2^{\beta n}M(n)e_{\max})$ and using Lemma 2,

$$\begin{aligned}\Pr\left(f_n(\mathcal{J}_1,\mathcal{J}_2,\cdots,\mathcal{J}_{M(n)})\le 2^{-\beta n-1}+\delta e_{\max}M(n)/2\right)&\le\Pr\left(f_n(\mathcal{J}_1,\mathcal{J}_2,\cdots,\mathcal{J}_{M(n)})\le 2^{-\beta n}\right)\\&=O(2^{-(\beta n-2M(n))}).\end{aligned} \tag{C.13}$$

As a result, taking $R=\mathsf{poly}(n)$, $\delta=\mathcal{O}(1/(2^{\beta n}M(n))$ and sufficiently large β, RHS of Eq. (C.11) is $\mathsf{negl}(n)$. The number of bits used for digitalization is $M(n)\cdot O(\log_2(R/\delta))=\mathsf{poly}(n)$. □

2. Random phase unitary with quantum phase estimation

In this subsection, we describe how to construct an arbitrary phase unitary $U_\theta=\sum_{k=1}^{2^n}e^{i\theta_k}|\lambda_k\rangle\langle\lambda_k|$, given a unitary $U=\sum_{k=1}^{2^n}e^{i2\pi\lambda_k}|\lambda_k\rangle\langle\lambda_k|$ with significantly large energy gap, using oracles. We will promote this to the pseudo-random ensemble and discuss the implementation of oracles in the next subsection.

We denote S as the n-qubit system register that U residues, and introducing an ancillary register A to facilitate the construction. For convenience, we split the ancillary register into three disjoint subset, $\mathsf{A}=\mathsf{A}_1\cup\mathsf{A}_2\cup\mathsf{A}_3$, with sizes m_1,m_2,m_3, respectively. Our construction uses the following three oracles:

- A QPE oracle $\mathcal{O}_{\mathrm{QPE}}$ that performs quantum phase estimation for U, on system S and ancilla A.
- A random offset oracle $\mathcal{O}_S$. We choose $\mathcal{O}_S$ to act only on $\mathsf{A}_2\cup\mathsf{A}_3$, i.e., $S\in\{0,1\}^{m_2+m_3}$, and $\mathcal{O}_S:|x\rangle\to|x+0_{\mathsf{S}\cup\mathsf{A}_1}\cdot S_{\mathsf{A}_2\cup\mathsf{A}_3}\mod 2^{m_1+m_2+m_3}\rangle$, where we use $0_{\mathsf{S}\cup\mathsf{A}_1}\cdot S_{\mathsf{A}_2\cup\mathsf{A}_3}$ to denote the concatenation to two bitstrings $0_{\mathsf{S}\cup\mathsf{A}_1}$ and $S_{\mathsf{A}_2\cup\mathsf{A}_3}$.
- A phase oracle acting on A_1. Let $f:\{0,1\}^{m_1}\to[0,2\pi)$, then $\mathcal{O}_f:|x\rangle\to e^{if(x_{\mathsf{A}_1})}|x\rangle$.

We will demonstrate that $U_{f,S}=\mathcal{O}_{\mathrm{QPE}}^\dagger\mathcal{O}_S^\dagger\mathcal{O}_f\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}$ approximates $V_{f,S}=\sum_{i=1}^{2^n}e^{if(\widetilde{\lambda}_k^S)}|\lambda_k\rangle\langle\lambda_k|$ well, with $\widetilde{\lambda}_k^S$ the following coarse-grained value of λ_k:

$$\widetilde{\lambda}_k^S:\hat{\widetilde{\lambda}}_k^S=\underset{N/2^{m_1},N\in\mathbb{Z}}{\arg\max}\left\{\lambda_k+\frac{\hat{S}'}{2^{m_1+m_2+m_3}}\ge\frac{N}{2^{m_1}}\right\},\quad S'=0_{\mathsf{A}_1}S_{\mathsf{A}_2\cup\mathsf{A}_3}. \tag{C.14}$$

When the gap of U is larger than 2^{-m_1}, different λ_k corresponds to different $\widetilde{\lambda}_k^S$. Thus every $|\lambda_k\rangle$ could have different phases. We will later take $U=e^{iH}$ to implement the energy-conserving PRU. The entire circuit is sketched in Fig 5.

We emphasize that the coarse-grained resolution of oracle $\mathcal{O}_f$ and the random offset oracle $\mathcal{O}_S$ are necessary. At its core, the QPE algorithm performs the following transformation: $|\lambda_k\rangle|0_{\mathsf{A}}\rangle \to |\lambda_k\rangle|\phi_k\rangle$, where $|\phi_k\rangle$ encodes a binary approximation of λ_k. However, since QPE is of finite precision, $|\phi_k\rangle$ as non-negligible weight on several neighboring bitstrings on A. We choose $\mathcal{O}_f$ to depend only on m_1 coarse bits of the phase register A, ignoring the remaining "fine" bits on $\mathsf{A}_2 \cup \mathsf{A}_3$. Any $|\phi_k\rangle$ has approximately the same coarse-bit over its support (with high probability). This ensures $\mathcal{O}_{\mathrm{QPE}}^{\dagger}$ can coherently uncompute the phase register to return it to $|0_{\mathsf{A}}\rangle$.

The random offset $\mathcal{O}_S$ eliminates the principle worst case: if λ_k lies near the coarse-bin boundary, i.e., $\lambda_k \approx N/2^{m_1}$ for integer N, then $|\phi_k\rangle$ straddles two different coarse values, spoiling the uncomputation. By adding a uniformly random shift to the fine bits, $\mathcal{O}_S$ moves $|\phi_k\rangle$ away from boundary with high probability, thus rescuing the uncomputation.

We begin by showing that $\mathcal{O}_S$ can prevent "hitting the boundary of coarse-bin".

Lemma 4 (Random offset prevents hitting the boundary)**.** *Let U be a n-qubit untary acting on the system register S with the set of eigenvalues and eigenstates $\{e^{i2\pi\lambda_i}, |\lambda_i\rangle\}_{1\le i\le 2^n}, \lambda_i \in [0,1)$, and they satisfy $|\lambda_i - \lambda_j| > 2^{-\beta n}$ for all $i \neq j$. Introducing ancilla register $\mathsf{A} = \mathsf{A}_1 \cup \mathsf{A}_2 \cup \mathsf{A}_3$ such that $m_1 > \beta n$. Denote $\mathcal{O}_{\mathrm{QPE}}$ to be the QPE oracle performed on system S and ancilla A, and O_S to be the random offset oracle acting on $\mathsf{A}_2 \cup \mathsf{A}_3$. Then for any state $|\psi\rangle$ on S,*

$$\Pr_S\left(\left\|\exists i \in [2^n], \prod_m \mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}|\lambda_i\rangle|0_{\mathsf{A}}\rangle\right\|_2 > 2^{-m_3/2}\right) \le 2^{-(m_1-n-2)}, \tag{C.15}$$

where

$$\prod_m = \mathrm{I}_{\mathsf{S}} \otimes \sum_{x\in\{0,1\}^{m_1}} \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, |\hat{b}/2^{m_1+m_2+m_3} - \hat{x}/2^{m_1}| < 2^{-(m_1+m_2)}} |b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}| \tag{C.16}$$

is the projector to bitstrings near the boundary (See Fig 6).

Proof. From Fact 3,

$$\begin{aligned}\left\|\prod_{\lambda_i}\mathcal{O}_{\mathrm{QPE}}|\lambda_i\rangle|0_{\mathsf{A}}\rangle\right\|_2 &\le 2^{-m_3/2},\\ \prod_{\lambda_i} = \mathrm{I}_{\mathsf{S}} \otimes \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, |\hat{b}/2^{m_1+m_2+m_3} - \lambda_i| > 2^{-(m_1+m_2)}} &|b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}|.\end{aligned} \tag{C.17}$$

This leads to

$$\begin{aligned}\left\|\prod_{\lambda_i,S}\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}|\lambda_i\rangle|0_{\mathsf{A}}\rangle\right\|_2 &\le 2^{-m_3/2},\\ \prod_{\lambda_i,S} = \mathrm{I}_{\mathsf{S}} \otimes \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, |\hat{b}/2^{m_1+m_2+m_3} - \lambda_i - \hat{S}'/2^{m_1+m_2+m_3}| > 2^{-(m_1+m_2)}} &|b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}|,\end{aligned} \tag{C.18}$$

where $S' = 0_{\mathsf{A}_1} S_{\mathsf{A}_2\cup\mathsf{A}_3}$. When uniformly sampling S, $\hat{S}'/2^{m_1+m_2+m_3}$ is uniformly distributed over $[0, 2^{-m_1})$. As a result,

$$\begin{aligned}\Pr_S\left(\left\|\prod_m \mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}|\lambda_i\rangle|0_{\mathsf{A}}\rangle\right\|_2 > 2^{-m_3/2}\right) &\le \Pr_S\left(\mathrm{im}\left(\prod_m\right) \not\subseteq \mathrm{im}\left(\prod_{\lambda_i,S}\right)\right)\\ &\le \frac{2(2^{-(m_1+m_2)} + 2^{-(m_1+m_2)})}{2^{-m_1}}\\ &= 2^{-(m_2-2)}\end{aligned} \tag{C.19}$$

The second to last line comes from sweeping over the region of length 2^{-m_1} that contains λ_i. See Fig 6 for an illustration. Then a union bound yields the desired inequality. □

Based on Lemma 4, we can prove that $U_{f,S}$ approximates the phase unitary well, using the number of ancillas $m_1, m_2, m_3 = O(n)$.

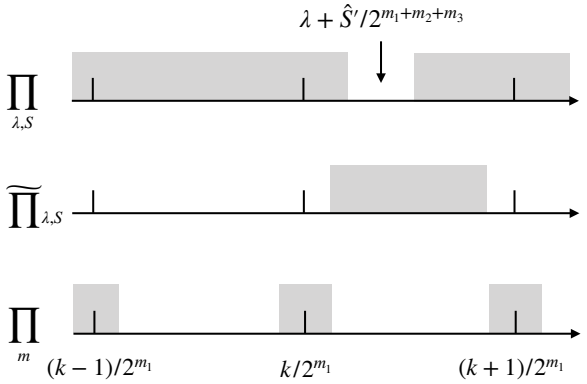

Figure 6. Definitions of projectors used in Lemma 4 and Lemma 5.

Lemma 5 (Constructing arbitrary phase unitary)**.** *Let U be a n-qubit untary acting on the system register S with the set of eigenvalues and eigenstates $\{e^{i2\pi\lambda_i}, |\lambda_i\rangle\}_{1\le i\le 2^n}, \lambda_i \in [0,1)$, and they satisfy $|\lambda_i - \lambda_j| > 2^{-\beta n}$ for all $i \neq j$. Introducing ancilla register $\mathsf{A} = \mathsf{A}_1 \cup \mathsf{A}_2 \cup \mathsf{A}_3$ such that*

$$m_1 > \beta n, \quad m_2 > n+2, \quad m_3 > 2n, \quad m_1 > m_3. \tag{C.20}$$

Denote $\mathcal{O}_{\mathrm{QPE}}$ be the oracle to implement the QPE for U, acting on system S and ancilla A. Denote $\mathcal{O}_S$ to be the random offset oracle acting on $\mathsf{A}_2 \cup \mathsf{A}_3$, and $\mathcal{O}_f$ be the oracle that applies the phase function $|x\rangle \to e^{if(x)}|x\rangle$ for $f : \{0,1\}^{m_1} \to [0, 2\pi)$ on A_1. Then $U_{f,S} = \mathcal{O}_{\mathrm{QPE}}^\dagger \mathcal{O}_S^\dagger \mathcal{O}_f \mathcal{O}_S \mathcal{O}_{\mathrm{QPE}}$ satisfies that for any quantum state $|\psi\rangle$ on S,

$$\Pr_S\left(\left\| U_{f,S}|\psi\rangle \otimes |0_{\mathsf{A}}\rangle - \sum_{i=1}^{2^n} e^{if(\widetilde{\lambda}_k^S)} \langle\lambda_i k|\psi\rangle |\lambda_k\rangle \otimes |0_{\mathsf{A}}\rangle \right\|_2 \le 2^{-(m_3/2+2+n)}\right) > 1 - 2^{-(m_2-n-2)}. \tag{C.21}$$

Proof. Denote,

$$\mathcal{O}_S \mathcal{O}_{\mathrm{QPE}} |\lambda_k\rangle |0_{\mathsf{A}}\rangle = |\lambda_k\rangle |\phi_k\rangle . \tag{C.22}$$

From Fact 3,

$$\left\| \prod_{k,S} |\lambda_k\rangle |\phi_k\rangle \right\|_2 \le 2^{-m_3/2},$$

$$\prod_{k,S} = \mathrm{I}_{\mathsf{S}} \otimes \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, |\hat{b}/2^{m_1+m_2+m_3} - \lambda_k - \hat{S}'/2^{m_1+m_2+m_3}| > 2^{-(m_1+m_2)}} |b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}|. \tag{C.23}$$

Define

$$\widetilde{\prod}_{k,S} = \mathrm{I}_{\mathsf{S}} \otimes \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, 2^{-(m_2+m_3)} < |\hat{b}/2^{m_1+m_2+m_3} - \widetilde{\lambda}_k^S| < 2^{-m_1} - 2^{-(m_2+m_3)}} |b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}|. \tag{C.24}$$

We have

$$\begin{aligned} \mathcal{O}_f |\lambda_k\rangle |\phi_k\rangle &= \mathcal{O}_f \left(\widetilde{\prod}_{k,S} |\lambda_k\rangle |\phi_k\rangle + \left(1 - \widetilde{\prod}_{k,S}\right) |\lambda_k\rangle |\phi_k\rangle \right) \\ &= e^{if(\widetilde{\lambda}_k^S)} \widetilde{\prod}_{k,S} |\lambda_k\rangle |\phi_k\rangle + \mathcal{O}_f \left(1 - \widetilde{\prod}_{k,S}\right) |\lambda_k\rangle |\phi_k\rangle . \end{aligned} \tag{C.25}$$

Define

$$\prod_{m} = \mathrm{I}_{\mathsf{S}} \otimes \sum_{x\in\{0,1\}^{m_1}} \sum_{b\in\{0,1\}^{m_1+m_2+m_3}, |\hat{b}/2^{m_1+m_2+m_3} - \hat{x}/2^{m_1}| < 2^{-(m_2+m_3)}} |b_{\mathsf{A}}\rangle\langle b_{\mathsf{A}}|. \tag{C.26}$$

We assume to sample S such that for all $i \in [2^n]$

$$\left\| \prod_m |\lambda_k\rangle |\phi_k\rangle \right\|_2 \leq 2^{-m_3/2}. \tag{C.27}$$

The probability is at least $1 - 2^{-(m_2-n-2)}$ according to Lemma 4. Note that when $m_1 > m_3$,

$$\mathrm{im}\left(1 - \widetilde{\prod}_{k,S}\right) \subset \mathrm{im}\left(\prod_{k,S}\right) \bigcup \mathrm{im}\left(\prod_m\right) \tag{C.28}$$

As a result,

$$\left\| \left(1 - \widetilde{\prod}_{k,S}\right) |\lambda_k\rangle |\phi_k\rangle \right\|_2 \leq \left\| \prod_{k,S} |\lambda_k\rangle |\phi_k\rangle \right\|_2 + \left\| \prod_m |\lambda_k\rangle |\phi_k\rangle \right\|_2 \leq 2^{-m_3/2+1}. \tag{C.29}$$

Combining this with Eq. (C 2), we have

$$\left\| \mathcal{O}_f |\lambda_k\rangle |\phi_k\rangle - e^{if(\widetilde{\lambda}_k^S)} \widetilde{\prod}_{k,S} |\lambda_k\rangle |\phi_k\rangle \right\|_2 \leq 2^{-m_3/2+1}. \tag{C.30}$$

Using triangle inequality,

$$\left\| O_f |\lambda_k\rangle |\phi_k\rangle - e^{if(\widetilde{\lambda}_k^S)} |\lambda_k\rangle |\phi_k\rangle \right\|_2 \leq 2^{-m_3/2+2}. \tag{C.31}$$

Now we analyze $\mathcal{O}_S \mathcal{O}_{\mathrm{QPE}} |\psi\rangle |0_{\mathsf{A}}\rangle = \sum_k \langle\lambda_k|\psi\rangle |\lambda_k\rangle |\phi_k\rangle$.

$$\begin{aligned} \left\| \mathcal{O}_f \mathcal{O}_S \mathcal{O}_{\mathrm{QPE}} |\psi\rangle |0_{\mathsf{A}}\rangle - \sum_k \langle\lambda_k|\psi\rangle e^{if(\widetilde{\lambda}_k^S)} |\lambda_k\rangle |\phi_k\rangle \right\|_2 &\leq \sum_k \left| \langle\lambda_k|\psi\rangle \right| \left\| \mathcal{O}_f |\lambda_k\rangle |\phi_k\rangle - e^{if(\widetilde{\lambda}_k^S)} |\lambda_k\rangle |\phi_k\rangle \right\|_2 \\ &\leq 2^{-m_3/2+2+n}. \end{aligned} \tag{C.32}$$

Applying $\mathcal{O}_{\mathrm{QPE}}^\dagger \mathcal{O}_S^\dagger$ to the two terms in the LHS, we get the desired inequality. □

3. Constructing energy-conserving PRU

In this subsection, we turn the oracle-based construction of arbitary phase unitary given in the previous subsection to an explicit construction energy-conserving PRU for random commuting Hamiltonians.

We introduce the following two technical lemmas that are helpful.

Lemma 6 (From state distance to channel distance)**.** *Let* S, A *be two registers and* U, V *be unitaries acting on* $\mathsf{S} \cup \mathsf{A}$ *and* S*, respectively. If for all state* $|\psi\rangle$ *on* S*,*

$$\left\| (U - V \otimes \mathrm{I}_{\mathsf{A}}) |\psi\rangle |0_{\mathsf{A}}\rangle \right\|_2 \leq \epsilon, \tag{C.33}$$

then the following two channels

$$\mathsf{U}[\rho] := \mathrm{tr}_{\mathsf{A}} \left[U \left(\rho \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}| \right) U^\dagger \right], \quad \mathsf{V}[\rho] := V \rho V^\dagger \tag{C.34}$$

are close in diamond distance, i.e.,

$$\left\| \mathsf{U} - \mathsf{V} \right\|_\diamond \leq 2\epsilon. \tag{C.35}$$

Proof. Let B be any ancillary system. It is sufficient to prove that,

$$\left\| (U \otimes \mathrm{I}_{\mathsf{B}})(\rho \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}|)(U^\dagger \otimes \mathrm{I}_{\mathsf{B}}) - (V \otimes \mathrm{I}_{\mathsf{A}\cup\mathsf{B}})(\rho \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}|)(V^\dagger \otimes \mathrm{I}_{\mathsf{A}\cup\mathsf{B}}) \right\|_1 \leq 2\epsilon \tag{C.36}$$

holds for any pure state $\rho = |\Psi\rangle\langle\Psi|$ on $\mathsf{S} \cup \mathsf{B}$.

Denote the Schmidt decomposition of $|\Psi\rangle$ as $|\Psi\rangle = \sum_i \mu_i |\psi_{\mathsf{S}}^i\rangle |\psi_{\mathsf{B}}^i\rangle$, where μ_i is real positive and $\sum_i \mu_i^2 = 1$. We have

$$\left\| (U \otimes \mathrm{I}_{\mathsf{B}})(\rho \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}|)(U^\dagger \otimes \mathrm{I}_{\mathsf{B}}) - (V \otimes \mathrm{I}_{\mathsf{A}\cup\mathsf{B}})(\rho \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}|)(V^\dagger \otimes \mathrm{I}_{\mathsf{A}\cup\mathsf{B}}) \right\|_1$$

$$
\begin{aligned}
&= \left\| \sum_{ij} \mu_i \mu_j \left(\left(U|\psi_{\mathsf{S}}^i\rangle\langle\psi_{\mathsf{S}}^j| \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}| U^\dagger \right) - \left(V \otimes \mathrm{I}_{\mathsf{A}} |\psi_{\mathsf{S}}^i\rangle\langle\psi_{\mathsf{S}}^j| \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}| V^\dagger \otimes \mathrm{I}_{\mathsf{A}} \right) \right) \otimes \left(|\psi_{\mathsf{B}}^i\rangle\langle\psi_{\mathsf{B}}^j| \right) \right\|_1 \\
&\leq \sum_{ij} \mu_i \mu_j \left\| \left(U\,|\psi_{\mathsf{S}}^i\rangle\,\langle\psi_{\mathsf{S}}^j| \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}| U^\dagger \right) - \left(V \otimes \mathrm{I}_{\mathsf{A}}\,|\psi_{\mathsf{S}}^i\rangle\,\langle\psi_{\mathsf{S}}^j| \otimes |0_{\mathsf{A}}\rangle\langle 0_{\mathsf{A}}| V^\dagger \otimes \mathrm{I}_{\mathsf{A}} \right) \right\|_1 \\
&\leq \sum_{ij} \mu_i \mu_j \Big(\left\| U\,|\psi_{\mathsf{S}}^i\rangle\,|0_{\mathsf{A}}\rangle - V \otimes \mathrm{I}_{\mathsf{A}}\,|\psi_{\mathsf{S}}^i\rangle\,|0_{\mathsf{A}}\rangle \right\|_2 + \left\| U\,|\psi_{\mathsf{S}}^j\rangle\,|0_{\mathsf{A}}\rangle - V \otimes \mathrm{I}_{\mathsf{A}}\,|\psi_{\mathsf{S}}^j\rangle\,|0_{\mathsf{A}}\rangle \right\|_2 \Big) \\
&\leq 2\epsilon \sum_{ij} \mu_i \mu_j \\
&\leq 2\epsilon. \qquad \text{(C.37)}
\end{aligned}
$$

In the third line we use $\||\psi\rangle\langle\phi|\|_1 = 1$ and triangle inequality. In the fourth line we use

$$
\||\psi_1\rangle\langle\phi_1| - |\psi_2\rangle\langle\phi_2|\|_1 \leq \||\psi_1\rangle - |\psi_2\rangle\|_2 + \||\phi_1\rangle - |\phi_2\rangle\|_2 . \qquad \text{(C.38)}
$$

In the last line we use Cauchy-Schwartz inequality. □

Lemma 7 (Simulate the random phase unitary)**.** *Let U be a n-qubit untary with the set of eigenvalues and eigenstates $\{e^{i2\pi\lambda_k}, |\lambda_k\rangle\}_{1\leq k\leq 2^n}, \lambda_k \in [0,1)$. Assume the eigenvalues are well-separated. Define the following two ensemble of unitaries:*

- *The random phase ensemble, $\mathcal{U}_{\mathrm{RU}} = \{\sum_{k=1}^{2^n} e^{i\theta_k}|\lambda_k\rangle\langle\lambda_k|\}_\theta$, $(\theta_1, \cdots \theta_{2^n}) \sim \mathrm{Unif}[0,2\pi)^{2^n}$.*
- *The random function ensemble, $\mathcal{V}_{\mathrm{RF}} = \{V_{f,S}\}_{f,S} = \{\sum_{k=1}^{2^n} e^{if(\widetilde{\lambda}_k^S)}|\lambda_k\rangle\langle\lambda_k|\}_{f,S}$. S is uniformly sampled from $\{0,1\}^{m_2+m_3}$, with m_1, m_2, m_3 satisfying the requirement in Lemma 5. $f \sim \mathrm{Unif}[0,2\pi)^{2^n}$ is a random function.*

Then $\mathcal{U}_{\mathrm{RU}} = \mathcal{V}_{\mathrm{RF}}$.

Proof. Denote $\mathbb{N}_N = [N/2^{m_1}, (N+1)/2^{m_1})$, $N = [2^{m_1} - 1]$. By the requirement of Lemma 5, each $\mathbb{N}_N$ contains at most one λ_k. As a result, different $\widetilde{\lambda}_k^S$ belongs to different $\mathbb{N}_N$. Thus for each S, $f(\widetilde{\lambda}_k^S)$ are independent random numbers drawn from $\mathrm{Unif}[0,2\pi)$. This concludes $\mathcal{U}_{\mathrm{RU}} = \mathcal{V}_{\mathrm{RF}}$. □

Based on these preparations, we now demonstrate that any exponentially-accurate approximation of $\mathcal{U} = \{U_{f,S}\}_{f,S} = \{\mathcal{O}_{\mathrm{QPE}}^\dagger \mathcal{O}_S^\dagger \mathcal{O}_f \mathcal{O}_S \mathcal{O}_{\mathrm{QPE}}\}_{f,S}$ is indistinguishable from the random phase ensemble $\mathcal{U}_{\mathrm{RU}}$ against any quantum algorithms that makes adaptive queries.

Lemma 8 (Secure against adaptive queires)**.** *Let U be a n-qubit untary on the system register S whose the eigenvalues are well-separated. Let A be an ancillary register whose size satisfying the requirement of Lemma 5.*

Define $U_{f,S} = \mathcal{O}_{\mathrm{QPE}}^\dagger \mathcal{O}_S^\dagger \mathcal{O}_f \mathcal{O}_S \mathcal{O}_{\mathrm{QPE}}$ as the ideal oracle on $\mathsf{S}\cup\mathsf{A}$ and the associated channel as $\mathsf{U}_{f,S}[\rho] := U_{f,S}\rho U_{f,S}^\dagger$. Define $\mathcal{U}_{\mathrm{RU}}$ being the random phase ensemble w.r.t. U and the associated channel as $\mathsf{U}_\theta[\rho] := U_\theta \rho U_\theta^\dagger, U_\theta \in \mathcal{U}_{\mathrm{RU}}$.

Let $\{\mathsf{W}_{f,S}\}_{f,S}$ be a set of quantum channels implemented to approximate $\mathsf{U}_{f,S}$, such that $\|\mathsf{W}_{f,S} - \mathsf{U}_{f,S}\|_\diamond \leq 2^{-\alpha n}$ for a positive constant α and all f, S.

Introduce an ancillary register B with $|\mathsf{B}| = \mathsf{poly}(n)$. Fix a sequence of unitaries $\{A_1, \cdots A_t, A_{t+1}\}$ acting on $\mathsf{S}\cup\mathsf{B}$, and write $\mathsf{A}_i[\rho] := A_i \rho A_i^\dagger$. Define the following two adaptive adversaries

$$
\mathsf{AW}_{f,S} = \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \left(\mathsf{W}_{f,S} \circ \mathsf{A}_i \right), \quad \mathsf{AU}_\theta[\rho_0] = \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \left(\mathsf{U}_\theta \circ \mathsf{A}_i \right). \qquad \text{(C.39)}
$$

Then for S uniformly drawn from $\{0,1\}^{m_2+m_3}$, and f is uniformly drawn from $[0,2\pi)^{2^n}$,

$$
\begin{aligned}
&\left\| \mathbb{E}_{S,f} \left[\mathsf{AW}_{f,S} \left[|0_{\mathsf{S}\cup\mathsf{A}\cup\mathsf{B}}\rangle\langle 0_{\mathsf{S}\cup\mathsf{A}\cup\mathsf{B}}| \right] \right] - \mathbb{E}_{U_\theta \sim \mathcal{U}_{\mathrm{RU}}} \left[\mathsf{AU}_\theta \left[|0_{\mathsf{S}\cup\mathsf{A}\cup\mathsf{B}}\rangle\langle 0_{\mathsf{S}\cup\mathsf{A}\cup\mathsf{B}}| \right] \right] \right\|_1 \\
&< t\left(2^{-(m_3/2+1+n)} + 2^{-\alpha n} \right) + 2^{-(m_2-n-3)} \qquad \text{(C.40)}
\end{aligned}
$$

Proof. Introduce the following two channels

$$\mathsf{AV}_{f,S} = \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \Big(\mathsf{V}_{f,S} \circ \mathsf{A}_i \Big), \quad \mathsf{AU}_{f,S} = \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \Big(\mathsf{U}_{f,S} \circ \mathsf{A}_i \Big), \tag{C.41}$$

where $\mathsf{V}_{f,S}[\rho] := V_{f,S} \rho V_{f,S}^\dagger$, and $V_{f,S} = \sum_{k=1}^{2^n} e^{if(\widetilde{\lambda}_k^S)} |\lambda_k\rangle\langle\lambda_k|$. Lemma 7 asserts that $\mathbb{E}_\theta[\mathsf{AU}_\theta] = \mathbb{E}_{f,S}[\mathsf{AV}_{f,S}]$. Using triangle inequality,

$$\begin{aligned}
&\Big\| \mathbb{E}_{S,f} \Big[\mathsf{AW}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \Big] - \mathbb{E}_\theta \Big[\mathsf{AU}_\theta \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \Big] \Big\|_1 \\
&\le \mathbb{E}_{S,f} \Big[\big\| \mathsf{AW}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] - \mathsf{AV}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \big\|_1 \Big] \\
&\le \mathbb{E}_{S,f} \Big[\big\| \mathsf{AW}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] - \mathsf{AU}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \big\|_1 \\
&\quad + \big\| \mathsf{AU}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] - \mathsf{AV}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \big\|_1 \Big].
\end{aligned} \tag{C.42}$$

Using $\|\mathsf{W}_{f,S} - \mathsf{U}_{f,S}\|_\diamond \le 2^{-\alpha n}$, the submultiplicative of diamond norm, and $\|\Phi\|_\diamond = 1$ when Φ is a channel,

$$\begin{aligned}
\|\mathsf{AW}_{f,S} - \mathsf{AU}_{f,S}\|_\diamond &= \left\| \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \Big(\mathsf{W}_{f,S} \circ \mathsf{A}_i \Big) - \mathsf{A}_{t+1} \circ \prod_{i=1}^{t} \Big(\mathsf{U}_{f,S} \circ \mathsf{A}_i \Big) \right\|_\diamond \\
&= \left\| \prod_{i=1}^{t} \Big(\mathsf{W}_{f,S} \circ \mathsf{A}_i \Big) - \prod_{i=1}^{t} \Big(\mathsf{U}_{f,S} \circ \mathsf{A}_i \Big) \right\|_\diamond \\
&= \left\| \sum_{j=1}^{t} \Big(\prod_{i=j+1}^{t} \mathsf{W}_{f,S} \circ \mathsf{A}_i \Big) \circ \Big(\mathsf{W}_{f,S} \circ \mathsf{A}_j - \mathsf{U}_{f,S} \circ \mathsf{A}_j \Big) \circ \Big(\prod_{i=1}^{j-1} \mathsf{U}_{f,S} \circ \mathsf{A}_i \Big) \right\|_\diamond \\
&\le \sum_{j=1}^{t} \left\| \Big(\prod_{i=j+1}^{t} \mathsf{W}_{f,S} \circ \mathsf{A}_i \Big) \circ \Big(\mathsf{W}_{f,S} \circ \mathsf{A}_j - \mathsf{U}_{f,S} \circ \mathsf{A}_j \Big) \circ \Big(\prod_{i=1}^{j-1} \mathsf{U}_{f,S} \circ \mathsf{A}_i \Big) \right\|_\diamond \\
&\le \sum_{j=1}^{t} \|\mathsf{W}_{f,S} - \mathsf{U}_{f,S}\|_\diamond \\
&\le t 2^{-\alpha n}.
\end{aligned} \tag{C.43}$$

As a result,

$$\mathbb{E}_{S,f} \Big[\big\| \mathsf{AW}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] - \mathsf{AU}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \big\|_1 \Big] \le t 2^{-\alpha n} \tag{C.44}$$

Define

$$\begin{aligned}
\mathcal{S}_1 &:= \Big\{ S \;\Big|\; \big\| U_{f,S} |\psi\rangle \otimes |0_{\mathsf{A}}\rangle - \big(V_{f,S} \otimes \mathrm{I}_{\mathsf{A}} \big) |\psi\rangle \otimes |0_{\mathsf{A}}\rangle \big\|_2 \le 2^{-(m_3/2+2+n)}, \quad \forall |\psi\rangle \in \mathsf{S} \Big\}, \\
\mathcal{S}_2 &:= \{0,1\}^{m_2+m_3} \setminus \mathcal{S}_1.
\end{aligned} \tag{C.45}$$

When $S \in \mathcal{S}_1$, using Lemma 6,

$$\|\mathsf{U}_{f,S} - \mathsf{V}_{f,S}\|_\diamond \le 2^{-(m_3/2+1+n)}. \tag{C.46}$$

By repeating the calculation of Eq. (C.43), we have

$$\big\| \mathsf{AU}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] - \mathsf{AV}_{f,S} \big[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}| \big] \big\|_1 \le t 2^{-(m_3/2+1+n)}. \tag{C.47}$$

Therefore,

$$\begin{aligned}
&\mathbb{E}_{f,S} \Big[\|\mathsf{U}_{f,S}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|] - \mathsf{V}_{f,S}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|] \|_1 \Big] \\
&= \Pr(\mathcal{S}_1) \cdot \mathbb{E}_f \Big[\|\mathsf{U}_{f,S\in\mathcal{S}_1}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|] - \mathsf{V}_{f,S\in\mathcal{S}_1}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|] \|_1 \Big]
\end{aligned}$$

$$
\begin{aligned}
&+\Pr(\mathcal{S}_2)\cdot\mathbb{E}_f\left[\left\|\mathsf{U}_{f,S\in\mathcal{S}_2}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|]-\mathsf{V}_{f,S\in\mathcal{S}_2}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|]\right\|_1\right]\\
&\le t2^{-(m_3/2+1+n)}+\Pr(\mathcal{S}_2)\left\|\mathsf{U}_{f,S\in\mathcal{S}_2}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|]-\mathsf{V}_{f,S\in\mathcal{S}_2}[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|]\right\|_1\\
&< t2^{-(m_3/2+1+n)}+2^{-(m_2-n-3)}. \qquad \text{(C.48)}
\end{aligned}
$$

In the last line we use $\Pr(\mathcal{S}_2)<2^{-(m_2-n-2)}$ from Lemma 5, and the fact $\|\rho_1-\rho_2\|_1\le 2$.

These together give

$$
\begin{aligned}
&\left\|\mathbb{E}_{S,f}\left[\mathsf{AW}_{f,S}\left[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|\right]\right]-\mathbb{E}_{\theta}\left[\mathsf{AU}_{\theta}\left[|0_{\mathsf{SUAUB}}\rangle\langle 0_{\mathsf{SUAUB}}|\right]\right]\right\|_1\\
&< t\left(2^{-(m_3/2+1+n)}+2^{-\alpha n}\right)+2^{-(m_2-n-3)}. \qquad \text{(C.49)}
\end{aligned}
$$

□

By choosing large enough $m_1, m_2, m_3 = O(n)$, these two adversaries give an order-$\mathsf{negl}(n)$ difference even when t is super-polynomially large. Thus, any inverse-exponentially accurate approximations of ensemble $\{\mathcal{O}_{\mathrm{QPE}}^{\dagger}\mathcal{O}_S^{\dagger}\mathcal{O}_f\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}\}_{f,S}$ is computationally indistinguishable from the random phase ensemble of U.

Finally, we turn to explicit constructions of $U_{f,S}$. We note that the QPE oracle, which uese e^{iHt} for exponentially-long t, can be constructed efficiently for commuting Hamiltonians. There the time evolution operator $e^{iHt}=e^{i\sum_j h_j t}$ can be factorized into $\prod_j e^{ih_j t}$. One only needs to run the quantum simulation algorithm for each local term. In other words, the commuting Hamiltonians can be fast-forwarded.

Fact 5 (Fast-forwarding of commuting Hamiltonians, cf.[59])**.** *For any exponentially small precision ϵ, there exists an efficient quantum algorithm $\{U_n(T)\}$ acting on $n+c=n+\mathsf{poly}(n)$ qubits such that for any $T=2^{O(n)}$ and any n-qubit state $|\psi\rangle$,*

$$
\left\|(e^{-iH_nT}\otimes\mathbb{I}_c-U_n(T))\,|\psi\rangle\otimes|0_c\rangle\right\|_2\le\epsilon, \qquad \text{(C.50)}
$$

where H_n is any n-qubit commuting Hamiltonian with $d=\mathcal{O}(\log n)$.

Putting everything together, we have

Theorem 2 (Constructing energy-conserving PRU for random commuting Hamiltonians)**.** *Let $H_n=\sum_i \mathcal{J}_i h_i$ be a commuting Hamiltonian with digitalized Gaussian random coefficients $\mathcal{J}_i$. There is an efficient ensemble of unitary $\{U_{g,S}\}$ that forms the energy-conerving PRU of H_n with probability at least $1-\mathsf{negl}(n)$. Each unitary $U_{g,S}$ is an exponentially accurate approximation of $\mathcal{O}_{\mathrm{QPE}}^{\dagger}\mathcal{O}_S^{\dagger}\mathcal{O}_g\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}$, where $\mathcal{O}_{\mathrm{QPE}}$ is the QPE oracle of $U=e^{i2\pi\widetilde{H}_n}$ with $\widetilde{H}_n$ being the normalized version of H_n such that all the eigenvalues belong to $[0,1)$, $\mathcal{O}_S$ is the random offset oracle, and $O_g:|x\rangle\to(-1)^{g(x)}|x\rangle$ implements a pseudo-random function $g:\{0,1\}^*\to\{0,1\}$. The oracles acting on system and ancillary registers with sizes properly specified by Lemma 5.*

Proof. The construction is sketched in Fig 5. Lemma 3 asserts that with probability at least $1-\mathsf{negl}(n)$, H_n has at a least inverse-exponentially small energy gap. We prove that the construction forms energy-conserving PRU for this case.

a. Security. Replace the pseudo-random function g by a truly random function f. By Lemma 8, any inverse-exponentially accurate approximation of the ensemble $\{\mathcal{O}_{\mathrm{QPE}}^{\dagger}\mathcal{O}_S^{\dagger}\mathcal{O}_f\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}\}_{f,S}$ is computationally indistinguishable from the random phase ensemble of $U=e^{i2\pi\widetilde{H}_n}$, which is exactly the energy-conserving random unitary ensemble of H_n due to Fact 1. Since a pseudo-random function g is indistinguishable from the truly random function f, ensemble $\{\mathcal{O}_{\mathrm{QPE}}^{\dagger}\mathcal{O}_S^{\dagger}\mathcal{O}_g\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}\}_{g,S}$ is also indistinguishable from the energy-conserving random unitary ensemble. Thus, $\{U_{g,S}\}$ is the energy-conserving PRU.

b. Construction time. Oracle $\mathcal{O}_g$ is the standard phase oracle. Since g can be efficiently specified and computed, this oracle is efficiently constructable. $\mathcal{O}_S$ is the addition oracle, which is also efficiently constructable when S is drawn from a set of size $2^{O(n)}$.

$\mathcal{O}_{\mathrm{QPE}}$ uses $O(n)$ number of unitary $U(t)=e^{i2\pi\widetilde{H}_n t}$, with $t=2^{O(n)}$. By Fact 5, each $U(t)$ can be efficiently implemented up to any inverse-exponentially small precision. By choosing a large enough precision, an approximation of $\mathcal{O}_{\mathrm{QPE}}$ with inverse exponential error can be constructed. As a result, $U_{g,S}$ is an inverse exponentially accurate approximation for $\mathcal{O}_{\mathrm{QPE}}^{\dagger}\mathcal{O}_S^{\dagger}\mathcal{O}_g\mathcal{O}_S\mathcal{O}_{\mathrm{QPE}}$. □

Appendix D: Solving PSPACE problems with energy-conserving random unitary

From this section, we delve into the construction and demonstration of 1D translational-invariant local Hamiltonian whose energy-conserving PRU does not exist. The distinctive feature for this Hamiltonian is that its energy-conserving random unitary can be used to solve PSPACE-complete problems, therefore essentially differs from any efficient quantum circuit.

In this section, we construct the Hamiltonian and PSPACE solver. Using the Feynman-Kitaev type construction[55, 56], one can construct 1D translational-invariant local Hamiltonians that encode the dynamics of any classical Turing machine up to polynomial memory size (limited by the system length). Our method generalizes this construction to enable its energy-conserving random unitary to solve PSPACE problems.

1. Quantum simulation of reversible Turing machines

We begin by describe our construction for RTM. The procedure is illustrated in Fig 2.

Fix the length of the tape, the configuration space of any RTM can be embedded into a Hilbert space made up of local pieces. The core idea is illustrated in Fig. 2. First, we can put the head inside the tape, so that the entire RTM is an one-dimensional system. This one-dimensional system can be represented by a product state $|\psi\rangle = |x_{k_1}\rangle_1 |x_{k_2}\rangle_2 \cdots |x_{k_{R-1}}\rangle_{R-1} |q_\mu\rangle_R |x_{k_R+1}\rangle_{R+1} \cdots |x_{k_{l+1}}\rangle_{l+1} \in \otimes_{i=1}^{l+1}\mathcal{H}_i$, where l is the tape length, R denotes the location of the head, and $x_{k_m} \in \Gamma$, $q_\mu \in Q$.

Having the quantum state representation, the transition functions δ can be represented as a set of local quantum isometries. For example, for $\delta_k : (q_\mu \to q_\nu, x \to y, +)$, it can be represented by

$$V_{\delta_k} = \sum_{i=1}^{l} |y\rangle_i |q_\nu\rangle_{i+1} \langle q_\mu| \langle x|_{i+1} .$$

V_{δ_k} encodes transition function δ_k in the following sense: For any quantum product state $|\psi_{\mathcal{C}}\rangle$ that corresponds to the configuration $\mathcal{C}$ of the RTM, $V_k |\psi_{\mathcal{C}}\rangle = |\psi_{\mathcal{C}'}\rangle$, where $\mathcal{C}' : \mathcal{C} \xrightarrow{\delta_k} \mathcal{C}'$. While V_k is not unitary, it is local and translational-invariant. So we can encode the transition functions δ of the TM into a local, translational-invariant Hamiltonian defined as $H = V + V^\dagger$.

In below we summarize this construction. For later convenience, we include the cases where the RTM contains reverse form of transition rules (Definition 10).

Definition 15 (Hamiltonian and state representations of reversible of Turing machine)**.** *Given a reversible Turing machine* M*, whose transition rules may contain both standard and reverse forms,* $\Delta = \Delta_s \cup \Delta_n$*. The Hamiltonian representation* $\{H_n\}_{n\in\mathbb{N}^+}$ *of* M *is a uniform family of qudits Hamiltonians where* H_n *is the Hamiltonian representation of* $\mathsf{M}(n)$*.* H_n *is defined on Hilbert space* $\mathcal{H}_{\mathsf{M}(n)} = \otimes_{i=1}^{n+1}\mathcal{H}_i$*, such that* $\mathcal{H}_i$ *is spanned by orthonormal states* $\{|x\rangle_i, |q\rangle_i\}$ *for all* $x \in \Gamma$ *and* $q \in Q$*.*

Let $\mathcal{T}$ *be the translation operator that maps any* $|\psi\rangle_i \in \mathcal{H}_i$ *to* $|\psi\rangle_{i+1} \in \mathcal{H}_{i+1}$ *(with periodic boundary condition).* H_n *is defined as*

$$H_n = \sum_{i=0}^{n} \mathcal{T}^{-1,i}\Big(\sum_{|v_k\rangle\langle v_l|\in\mathcal{V}} (|v_k\rangle + |v_l\rangle)(\langle v_k| + \langle v_l|)\Big)\mathcal{T}^i, \tag{D.1}$$

where

- $\mathcal{V} = (\mathcal{V}_+^s \cup \mathcal{V}_-^s \cup \mathcal{V}_0^s) \cup (\mathcal{V}_+^n \cup \mathcal{V}_-^n)$.
- $\mathcal{V}_+^s = \{|x'\rangle_1 |q'\rangle_2 \langle q|_1 \langle x|_2 \mid (q, x, q', x', +) \in \Delta^s\}$. $\mathcal{V}_+^n = \{|y\rangle_1 |q'\rangle_2 |x'\rangle_3 \langle q|_1 \langle y|_2 \langle x|_3 \mid (q, +, x, q', x') \in \Delta^n, y \in \Gamma\}$.
- $\mathcal{V}_-^s = \{|q'\rangle_1 |y\rangle_2 |x'\rangle_3 \langle y|_1 \langle q|_2 \langle x|_3 \mid (q, x, q', x', -) \in \Delta^s, y \in \Gamma\}$. $\mathcal{V}_-^n = \{|q'\rangle_1 |x'\rangle_2 \langle x|_1 \langle q|_2 \mid (q, -, x, q', x') \in \Delta^n\}$.
- $\mathcal{V}_0^s = \{|q'\rangle_1 |x'\rangle_2 \langle q|_1 \langle x|_2 \mid (q, x, q', x', 0) \in \Delta^s\}$.

H_n is a local, translational-invariant Hamiltonian that encodes the dynamics of $\mathsf{M}(n)$*.*

Any configuration $\mathcal{C} = \langle q, x, R\rangle$ *of* $\mathsf{M}(n)$ *can be represented by a product state in* $\mathcal{H}_{\mathsf{M}(n)}$*:*

$$|\psi_{\mathcal{C}}\rangle = |x_1\rangle_1 |x_2\rangle_2 \cdots |x_{j-1}\rangle_{R-1} |q\rangle_R |x_j\rangle_{R+1} \cdots |x_l\rangle_{l+1} , \tag{D.2}$$

which we named the configuration state. We call the subspace of $\mathcal{H}_{\mathsf{M}(n)}$ spanned by all configuration states the computational subspace $\mathcal{H}^{\mathscr{C}}_{\mathsf{M}(n)}$.

To study the structure of this Hamiltonian, we find that the configuration space of a RTM (with fixed-size memory) can be enumerated.

Fact 6. *Let $\mathsf{M}(n)$ be a RTM with fixed-size memory, and $\mathscr{C}$ be the (finite) set of configurations of $\mathsf{M}(n)$. Let $\mathcal{G} = (\mathscr{C}, E)$ be a directed graph whose vertices are the configurations. The edges are defined as follows: if C_2 is the successor of C_1, draw a directed edge from C_1 to C_2.*

$\mathcal{G}$ can be divided into disjoint subgraphs of loops and paths:

1. *Directed loops where q_0, q_a, q_r are never contained.*
2. *Directed paths where q_0, q_a, q_r are never contained.*
3. *Directed paths where a configuration that contains q_0 as the source. q_0, q_a, q_r are never contained in other vertices.*
4. *Directed paths where a configuration that contains q_a or q_r as the sink. q_0, q_a, q_r are never contained in other vertices.*
5. *Directed paths where a configuration that contains q_0 as the source and a configuration that contains q_a or q_r as the sink. q_0, q_a, q_r are never contained in other vertices.*

We emphasize that any configurations that contain q_0 (q_r or q_a) must be the source (sink) of a path, because they are designed to not have predecessor (successor).

This fact asserts that H_n is highly fragmented in the subspace $\mathcal{H}^{\mathscr{C}}_{\mathsf{M}(n)}$. In each subspace, the effective Hamiltonian is as follows.

Lemma 9. *Let H_n be the Hamiltonian representation of a RTM $\mathsf{M}(n)$. For any configuration $\mathcal{C} \in \mathscr{C}$ that belongs to a "path", there exist $T_1, T_2 \in \mathbb{N}^+$ and a $T_1 + T_2 + 1$-dimensional invariant subspace $\mathcal{H}^{\mathcal{C}}_{\mathsf{M}(n)} \subseteq \mathcal{H}^{\mathscr{C}}_{\mathsf{M}(n)}$ that contains $|\psi_{\mathcal{C}}\rangle$, where the effective Hamiltonian reads*

$$H_n\Big|_{\mathcal{H}^{\mathcal{C}}_{\mathsf{M}(n)}} = \sum_{t=-T_1}^{T_2-1} \big(|\psi_{\mathcal{C}_{t+1}}\rangle\langle\psi_{\mathcal{C}_t}| + h.c.\big) + 2\sum_{t=-T_1+1}^{T_2-1} \big(|\psi_{\mathcal{C}_t}\rangle\langle\psi_{\mathcal{C}_t}|\big) + |\psi_{\mathcal{C}_{T_1}}\rangle\langle\psi_{\mathcal{C}_{T_1}}| + |\psi_{\mathcal{C}_{T_2}}\rangle\langle\psi_{\mathcal{C}_{T_2}}|,$$

where $\mathcal{C}_0 = \mathcal{C}$, and $\mathcal{C}_{t+1}$ denotes the successor of $\mathcal{C}_t$.

If $\mathcal{C}$ belongs to a "loop", the effective Hamiltonian reads

$$H_n\Big|_{\mathcal{H}^{\mathcal{C}}_{\mathsf{M}(n)}} = \sum_{t=-T_1}^{T_2} \big(|\psi_{\mathcal{C}_{t+1}}\rangle\langle\psi_{\mathcal{C}_t}| + h.c.\big) + 2\sum_{t=-T_1}^{T_2+1} \big(|\psi_{\mathcal{C}_t}\rangle\langle\psi_{\mathcal{C}_t}|\big),$$

where $\mathcal{C}_{-T_1} = \mathcal{C}_{T_2+1}$.

Proof. We prove the result for the case of $\mathcal{C}$ belonging to a path. The case that $\mathcal{C}$ belongs to a loop follows directly.

Let $V_{\text{forward}} = \sum_{i=0}^{n} T^{-1,i}\big(\sum_{|v_k\rangle\langle v_l|\in\mathcal{V}} |v_k\rangle\langle v_l|\big)T^i$. Since $|v_k\rangle\langle v_l|$ corresponds to a transition rule of M, we have $V_{\text{forward}}|\psi_{\mathcal{C}_t}\rangle = |\psi_{\mathcal{C}_{t+1}}\rangle$. $V_{\text{forward}} + V^{\dagger}_{\text{forward}}$ becomes the first term of effective Hamiltonian.

The remaining part is $V_p = \sum_{i=0}^{n} T^{-1,i}\big(\sum_{|v_k\rangle\langle v_l|\in\mathcal{V}} |v_k\rangle\langle v_k| + |v_l\rangle\langle v_l|\big)T^i$. V_p gives energy penalty 1 to every configuration with one predecessor and also to every configuration with one successor. So the energy penalty of source and sink terms is 1 while those for the remaining terms are 2.

Since a RTM is reversible, each configuration can appear only once in a subspace. Furthermore, different configuration states are orthogonal to each other. So the dimension of $\mathcal{H}^{\mathcal{C}}_{\mathsf{M}(n)} = \text{span}\{|\psi_{\mathcal{C}_t}\rangle\}$ is $T_1 + T_2 + 1$. □

In each invariant subspace, the effective Hamiltonian can be interpreted as a 1D hopping Hamiltonian along the chain noded by $|\psi_{\mathcal{C}_t}\rangle$. The hardness of the PSPACE problem lies in the fact that this path could be exponentially long, preventing any local updating algorithm on $|\psi_{\mathcal{C}_t}\rangle$ to efficiently get the solution. The energy-conserving Haar-random unitary of H_n can potentially overcome this difficulty, with the following ideas.

To begin with, one prepares the product state $|\psi_{\mathcal{C}_1}\rangle$ that corresponds to the input configuration $\mathcal{C}_1$ of a PSPACE RTM for a given instance x. This state serves as the source of one path, whose sink encodes

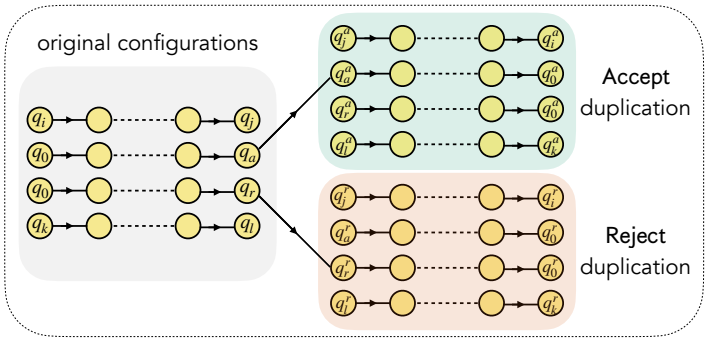

Figure 7. Configuration space of the duplicated RTM.

the solution. Then one can sample a unitary U from the energy-conserving Haar-random ensemble, and acting it on $|\psi_{\mathcal{C}_1}\rangle$. The scrambling nature of U will produce a wavefunction $U|\psi_{\mathcal{C}_1}\rangle$ dispersing along the entire path. A follow-up measurement on the basis $\mathrm{span}\{|x\rangle_i, |q\rangle_i\}$ will collapse $U|\psi_{\mathcal{C}_1}\rangle$ to any state $|\psi_{\mathcal{C}_t}\rangle$ along the path with almost equal probabilities. In this way, with high probability, one can make an exponentially large step forward using one query of U. This procedure is illustrated by Fig 2.

However, there are two obstacles in the way turning this intuition into a practical protocol. First of all, even if one can make a big step forward, the probability to precisely collapse to the sink is still exponentially small. More severely, different paths and loops could have energy degeneracies. Therefore, a energy-conserving Haar-random unitary could mix different subspaces with Accept and Reject as outputs, producing a wrong solution.

In the next two subsections, we resolve these two issues.

2. Duplicated Turing machine

In this subsection, we introduce a construction we named the duplicated TM to amplify the probability to collapse to a state containing the solution information.

A duplicated TM $\mathsf{D}[\mathsf{M}]$ is constructed from a reference RTM $\mathsf{M} = \langle Q, \Gamma, \Delta\rangle$. It contains two additional sets of internal states Q^a and Q^r, together with two extra sets of transition rules Δ^a and Δ^r. $Q^{a,r}$ are duplications of Q, i.e., $Q^{a,r} = \{q^{a,r} \mid q \in Q\}$. Similarly, $\Delta^{a,r}$ are duplications of Δ^{-1} (the inverse transition rules, see Definition 10) whose internal states are chosen from $Q^{a,r}$ instead. In addition, when the machine has configuration $\mathcal{C} = (q_a, B, i)$ or (q_r, B, i), we forward it to $\mathcal{C}' = (q_a^a, B, i)$ or (q_r^r, B, i), respectively. The global halting states for $\mathsf{D}[\mathsf{M}]$ are q_0^a and q_0^r instead.

Following this construction, whenever the machine enters the old halting states q_a or q_r, it enters q_a^a or q_r^r and does exactly the inverse computation. As a result, every computation process from legitimate input states now requires a doubled computation time, whereas the solution (i.e., a or r) is encoded in all the configurations belonging to the latter half process. Using the ideas at the end of D 1, we can read out the solution as long as the measured state collapses to the latter half path, whose probability is roughly $1/2 = \mathcal{O}(1)$.

Definition 16 (Duplicated RTM)**.** *Given a RTM* $\mathsf{M} = \langle Q, \Gamma, \Delta\rangle$ *whose transition rules are of the standard form, the Duplicated reversible Turing machine is another Turing machine,* $\mathsf{D}[\mathsf{M}] = \langle Q^{\mathsf{D}}, \Gamma, \Delta^{\mathsf{D}}\rangle$*, where*

- $Q^{\mathsf{D}} = Q \cup Q^a \cup Q^r$*, where* $Q^{a,r} = \{q^{a,r} \mid q \in Q\}$*. The halting state are now* q_0^a *and* q_0^r*.*
- $\Delta^{\mathsf{D}} = \Delta \cup \Delta^a \cup \Delta^r \cup \Delta^{\mathrm{trans}}$*, where* $\Delta^{a,r} = \{(q^{a,r}, s, x, (q^{a,r})', x' \mid (q, s, x, q', x') \in \Delta^{-1}\}$*, and* $\Delta^{\mathrm{trans}} = \{(q_a, x, q_a^a, x, 0), (q_r, x, q_r^r, x, 0) \mid x \in \Gamma\}$*.*

In other words, when the RTM enters its own halting state $q_{a,r}$*, the Duplicated RTM then enters* $Q^{a,r}$ *and does the exact reverse operation until reaching the global halting state* $q_0^{a,r}$*. The duplicated machine of a RTM with fixed-size memory can be defined analogously and labeled as* $\mathsf{D}[\mathsf{M}(n)]$*,*

Following Fact 6, we can also enumerate the configuration space of $\mathsf{D}[\mathsf{M}]$. The structure is illustrated in Fig 7.

Lemma 10. *Let* $\mathsf{M} = \langle Q, \Gamma, \Delta \rangle$ *be a RTM and* $\mathsf{D}[\mathsf{M}(n)]$ *be the duplicated RTM with fixed-size memory, and* $\mathscr{C}$ *be the (finite) set of configurations of* $\mathsf{D}[\mathsf{M}(n)]$*. Let* $\mathcal{G} = (\mathscr{C}, E)$ *be a directed graph whose vertices are the configurations. The edges are defined as follows: if* C_2 *is the successor of* C_1*, draw a directed edge from* C_1 *to* C_2*.*

$\mathcal{G}$ *can be divided into disjoint subgraphs of loops and paths of the following types:*

1. *Directed loops where* q_0, q_0^a, q_0^r *are never contained.*
2. *Directed paths where* q_0, q_0^a, q_0^r *are never contained.*
3. *Directed paths where a configuration that contains* q_0 *as the source.* q_0, q_0^a, q_0^r *are never contained in other vertices.*
4. *Directed paths where a configuration that contains* q_0^a *or* q_0^r *as the sink.* q_0, q_0^a, q_0^r *are never contained in other vertices.*
5. *Directed paths where a configuration that contains* q_0 *as the source and a configuration that contains* q_0^a *or* q_0^r *as the sink.* q_0, q_0^a, q_0^r *are never contained in other vertices.*

Moreover they have the following properties,

- *Any configuration belongs to directed path of type-3 does not contain* $q \in Q^{a,r}$ *as internal states.*
- *Any configuration belongs to directed path of type-4 kind does not contain* $q \in Q$ *as internal states.*
- *Any direct path of type-5 has length* $2T$*, where the first half of vertices contain* $q \in Q$ *as internal states, and the second half of vertices contain* $q \in Q^r$ *or* Q^a *as internal states.*
- *Any initial configuration of* $\mathsf{D}[\mathsf{M}(n)]$ *corresponding to some legal inputs belongs to directed path of the 5th kind.*

Proof. By construction, $\mathsf{D}[\mathsf{M}(n)]$ is a RTM. So the enumeration of configuration space follows from Fact. 6.

Let $P = (\mathcal{C}_1, \mathcal{C}_2 \cdots, \mathcal{C}_T)$ be a directed path where $\mathcal{C}_1$ contains q_0 as internal state. If $\mathcal{C}_t$ contains $q \in Q^a$ as internal state for some $2 \leq t \leq T$, by construction there must be $\mathcal{C}_{t'}$ with $t' \leq t$ that contains q_a^a as internal state. As a result, $\mathcal{C}_{t'-1}$ contains q_a as internal state.

Since Δ^a is the reverse of Δ, the $\mathsf{D}[\mathsf{M}(n)]$ does exactly the reverse computation after reaching $\mathcal{C}_{t'}$. That is, for any $0 \leq s \leq t' - 1$, $\mathcal{C}_{t'-1+s}$ and $\mathcal{C}_{t'-s}$ are the same configuration except the former contains internal state $q_\mu \in Q$ and the latter contians q_μ^a. As a result, whenever P has a vertex that contains internal state in Q^a, P must be symmetric with sink contains q_0^a. Otherwise, P does not have any vertex that contains internal state in Q^a. This argument extends to the cases where $\mathcal{C}_T$ contains q_0^a as internal state, and to the cases relative to Q^r. This proves the first three properties.

Legal input configuration of $\mathsf{D}[\mathsf{M}(n)]$ is also a legal input configuration of $\mathsf{M}(n)$, thus it must contains q_0 and be the source of a direct path. Moreover, this path must contain q_r or q_a and then contain q_0^r or q_0^a by above arguments. So it belongs to the 5th kind. □

From now, we denote H_n to be the Hamiltonian representation of $\mathsf{D}[\mathsf{M}(n)]$. It is clear the Hilbert subspace spanned by configuration states of any path (loop) is an invariant subspace of H_n. We call these subspaces the type-i ($i = 1, 2, 3, 4, 5$) path (loop) subspace with length T, and denote $\mathcal{H}^{(i)}_{\mathsf{D}[\mathsf{M}(n)]}$ as the union of all the type-i subspaces. Every path (loop) subspace is contained in the computation subspace $\mathcal{H}^{C}_{\mathsf{D}[\mathsf{M}(n)]}$ (Definition 15) of H_n. $\cup_{1 \leq i \leq 5} \mathcal{H}^{(i)}_{\mathsf{D}[\mathsf{M}(n)]} = \mathcal{H}^{\mathscr{C}}_{\mathsf{D}[\mathsf{M}(n)]}$

In below we will choose M to be a RTM that solves a PSPACE-complete problem specified by language L. Assume M decides if $x \in L$ using space $p(|x|) \in \mathbb{N}^+$. For all $n \in \mathbb{N}^+$, the Hamiltonian representation of $\mathsf{D}[\mathsf{M}(p(n))]$ is $H_{p(n)}$, which forms a uniform family of Hamiltonians.

3. Lifting the degeneracy

Loop and path subspaces of $H_{p(n)}$ can have energy degeneracy. Therefore energy-conserving Haar-random unitary of $H_{p(n)}$ can mix a subspace containing $\mathcal{C}_x$ with $x \in L$ and the one with $x \notin L$, and even with a subspace not corresponding to any legitimate computation process. This will cause unexpected computational errors.

In the following we energetically separate out the path subspaces corresponding to legitimate computation processes. Furthermore, we separate out the Accept and Reject path subspaces, so that the energy-conserving Haar-random unitary can be safely used to solve L.

In below we will call a directed path of type-4 that contains q_0^a (q_0^r) as the sink the type-4a (type-4r) path, and use the same notations for type-5a and 5r.

First, $\mathcal{H}_{\mathsf{D}[\mathsf{M}_L(p(n))]}$ contains not only the computational subspace $\mathcal{H}^{\mathscr{C}}_{\mathsf{D}[\mathsf{M}(n)]}$, but also the subspaces spanned by illegal configurations, i.e, the configurations containing multiple internal states $|q\rangle$s. To energetically separate the computational subspace, consider the following Hamiltonian

$$H = H_{p(n)} + \gamma \sum_{q\in Q} \sum_{i=1}^{p(n)+1} |q\rangle_i \langle q|_i \,. \tag{D.3}$$

Note that the second term commutes with $H_{p(n)}$. After adding this term, the total Hilbert space $\mathcal{H}_{\mathsf{D}[\mathsf{M}_L(p(n))]}$ is divided into:

- The subspace spanned by the states that do not contain $|q\rangle$. This subspace has energy exactly 0.
- The subspace spanned by the states that contain one $|q\rangle$ (the computational subspace). Due to Lemma 9, this subspace has energy $\gamma \le E \le \gamma + 4$
- Any subspace containing state with more than one $|q\rangle$. Since $H_{p(n)}$ is a positive semidefinite Hamiltonian, this kind of subspaces has non-negative energy before adding $\gamma \sum_{q\in Q} \sum_{i=1}^{p(n)+1} |q\rangle_i \langle q|_i$. So after adding the penalty term, their energies are at least 2γ.

As a result, one can always energetically separate out the computational subspace by choosing large enough $\gamma > 4$.

Now we separate the type-5a&4a and type-5r&4r paths subspaces from rest of the states in the computation subspace. The key technical tool is the following lemma.

Lemma 11. *For the following equation*

$$-\frac{1}{2^{m+1}-1}\tan\left(\frac{k}{2}\right) = \tan(Nk), \quad k \in (0,\pi), \quad m, N \in \mathbb{N}^+, \tag{D.4}$$

denote $\mathcal{S}(m,N)$ as the solution set for k with fixed m and N. Define $\mathcal{S}(m) = \bigcup_{N\in\mathbb{N}^+} \mathcal{S}(m,N)$, then it satisfies the following:

- *For $m_1 \neq m_2$, $\mathcal{S}(m_1) \bigcap \mathcal{S}(m_2) = \mathcal{S}(m_1) \bigcap \pi\mathbb{Q} = \mathcal{S}(m_2) \bigcap \pi\mathbb{Q} = \emptyset$.*
- *For any m and $N_1 \neq N_2$, $\mathcal{S}(m,N_1) \bigcap \mathcal{S}(m,N_2) = \emptyset$.*

We provide the proof in Appendix J.

Combining the two results above, we have the following lemma.

Lemma 12. *Let $H_{p(n)}$ be the Hamiltonian representation of a duplicated RTM with memory-size $p(n)$. Define the computation Hamiltonian as*

$$H_{\text{comp}} = H_{p(n)} + \sum_{i=1}^{p(n)+1} \left(10 \sum_{q\in Q} (|q\rangle_i \langle q|_i) + \frac{1}{2} |q_0^a\rangle_i \langle q_0^a|_i + \frac{1}{4} |q_0^r\rangle_i \langle q_0^r|_i \right). \tag{D.5}$$

The additional terms preserve all the loop and path subspaces. Furthermore, H_{comp} satisfies:

- *Any energy eigenstate contained in $\mathcal{H}^{(4a)}_{\mathsf{D}[\mathsf{M}(p(n))]} \cup \mathcal{H}^{(5a)}_{\mathsf{D}[\mathsf{M}(p(n))]}$ has no energy degeneracy with rest of the eigenstates, and so as the ones contained in $\mathcal{H}^{(4r)}_{\mathsf{D}[\mathsf{M}(p(n))]} \cup \mathcal{H}^{(5r)}_{\mathsf{D}[\mathsf{M}(p(n))]}$.*
- *Inside $\mathcal{H}^{(4a)}_{\mathsf{D}[\mathsf{M}(p(n))]} \cup \mathcal{H}^{(5a)}_{\mathsf{D}[\mathsf{M}(p(n))]}$, the path subspaces with different lengths have no energy degeneracy with each other. The same for paths in $\mathcal{H}^{(4r)}_{\mathsf{D}[\mathsf{M}(p(n))]} \cup \mathcal{H}^{(5r)}_{\mathsf{D}[\mathsf{M}(p(n))]}$.*

Proof. First choose a large enough γ to energetically separate out the computational subspace. As described before, $\gamma = 10$ suffices. Now we analyze the energy spectra of loop and path subspaces from type-1 to type-5. In this proof we use $|\psi_{\mathcal{C}_1}\rangle$ and $|\psi_{\mathcal{C}_T}\rangle$ to denote the source and sink of a length-T path, respectively.

Type-1: The eigenvalues of type-1 loops are not changed by the additional terms. Due to Lemma 9, for a loop of length T, the energy eigenvalues are $12+2\cos(2\pi t/T)$ for $t=0,1,\cdots,T-1$. Any eigenvalue of loops is contained in $12+2\cos(\pi\mathbb{Q})$.

Type-2&3: The eigenvalues of type-2&3 paths are not changed by the additional terms. Due to Lemma 9, the effective Hamiltonian is a hopping Hamiltonian along an one-dimensional chain with boundary potentials $-|\psi_{\mathcal{C}_1}\rangle\langle\psi_{\mathcal{C}_1}|-|\psi_{\mathcal{C}_T}\rangle\langle\psi_{\mathcal{C}_T}|$. This problem is analyzed in details in Appendix I. The energy eigenvalue is $E=12+2\cos k$, where k is determined by $\tan(Tk)=0$. So $k=n\pi/T$, $n=1,2,\cdots,T$. As a result, any eigenvalue of type-2 paths is contained in $12+2\cos(\pi\mathbb{Q})$.

Type-4&5: The effective Hamiltonians of type-4a&5a paths are hopping Hamiltonians with boundary potential -1 and $-1/2$. Leveraging the result from Appendix I, the eigenvalues are $E=12+2\cos k$, where k is determined by

$$-\frac{1}{3}\tan\frac{k}{2}=\tan Tk, \tag{D.6}$$

where T is the length of the path. Similarly, the eigenvalue of type-4r&5r paths is also $E=12+2\cos k$, where

$$-\frac{1}{7}\tan\frac{k}{2}=\tan Tk. \tag{D.7}$$

Due to the first statement of Lemma 11, eigenstates contained in $\mathcal{H}^{(4a)}_{\mathsf{D}[\mathsf{M}(p(n))]}\cup\mathcal{H}^{(5a)}_{\mathsf{D}[\mathsf{M}(p(n))]}$ and $\mathcal{H}^{(4r)}_{\mathsf{D}[\mathsf{M}(p(n))]}\cup\mathcal{H}^{(5r)}_{\mathsf{D}[\mathsf{M}(p(n))]}$ have no energy degeneracy with rest of the eigenstates. Due to the second statement of Lemma 11, type-4a&5a (4r&5r) paths with different lengths have no energy degeneracy with each other. □

Note that it is not necessary to separate a type-4a path from a type-5a one with the same length, because they both contain q^as as internal states, serving as the signal for Accept. Similarly, we can keep type-4r and 5r paths degenerated.

4. Construct the PSPACE solver

In this subsection, we put everything together and demonstrate how to use the energy-conserving random unitary of H_{comp} to solve PSPACE problems.

Note that while Lemma 12 successfully separate out the desired subspaces, the effective Hamiltonian of one subspace becomes the hopping Hamiltonian with unequal boundary potentials. Thus, the collapse probability to the second half of the chain is no longer guaranteed to be 1/2. Luckily, it can still be bounded. To this end, we need to first deal with the normalization factor of wavefunctions of H_{comp} from Appendix I.

Lemma 13. *Let $C_k(T)=T-\sin(Tk)/\sin k$. Let $k_1,\cdots k_T\in(0,\pi)$ be the solutions of Eq. (D.6) or Eq. (D.7). There exists constants $T_0\in\mathbb{N}^+$, such that for all $T>T_0$, the following holds:*

- *$C_{k_t}(T)/C_{k_t}(2T)\le 5/6$ for $t=2,3,\cdots,T-1$.*
- *$C_{k_1}(T)/C^2_{k_1}(2T), C_{k_T}(T)/C^2_{k_T}(2T)\le 1/96$.*

Proof. The solutions of Eq (D.6) satisfies $(t-1/2)\pi/T\le k_t\le t\pi/T$ for all $t\in[T]$. First, we prove the first statement. Notice

$$\frac{C_{k_t}(T)}{C_{k_t}(2T)}=\frac{T-\frac{\sin Tk}{\sin k}}{2T-\frac{\sin 2Tk}{\sin k}}\le\frac{T+\frac{1}{\sin k}}{2T-\frac{1}{\sin k}}=\frac{1+\frac{1}{T\sin k}}{2-\frac{1}{T\sin k}} \tag{D.8}$$

For $2\le t\le T-1$, $k_t\in(3\pi/(2T),\pi-\pi/T)$. Using the fact that there always exists $T_1>0$ such that for all $T>T_1$,

$$\min\left\{\sin\left(\frac{3\pi}{2T}\right),\sin\left(\pi-\frac{\pi}{T}\right)\right\}=\sin\left(\pi-\frac{\pi}{T}\right)\ge\frac{\pi}{0.99T}. \tag{D.9}$$

As a result, for $T>T_1$, $1/(T\sin k_t)\le 0.99/\pi\le 1/3$. Then

$$\frac{C_{k_t}(T)}{C_{k_t}(2T)}=\frac{1+\frac{1}{T\sin k}}{2-\frac{1}{T\sin k}}\le\frac{1}{2}+\frac{1}{T\sin k}\le\frac{5}{6}. \tag{D.10}$$

Now we prove the second statement. To prove this, we first analyze the behavior of k_T. Note that for $k \in (\pi - \pi/(2T) + 0^+, \pi)$, the LHS of Eq. (D.6) monotonically decreases, whereas the RHS monotonically increases. At $k = \pi - \pi/(2T) + 0^+$,

$$-\frac{\alpha}{\alpha+2}\tan\left(\frac{\pi}{2} - \frac{\pi}{4T}\right) = \text{LHS} > \text{RHS} = -\infty. \tag{D.11}$$

At $k = \pi - \pi/(3T)$, there exists $T_2 > 0$ such that for all $T > T_2$,

$$-\frac{\alpha}{\alpha+2}\tan\left(\frac{\pi}{2} - \frac{\pi}{6T}\right) = \text{LHS} < \text{RHS} = -\sqrt{3} \tag{D.12}$$

As a result, for $T > T_2$, $k_T \in (\pi - \pi/(2T), \pi - \pi/(3T))$. Following this result, we have

$$\max\left\{\frac{1}{C_{k_1}(2T)}, \frac{1}{C_{k_T}(2T)}\right\} \leq \frac{1}{2T - \frac{1}{\min_{k_1,k_T}\{\sin k\}}} = \frac{1}{2T - \frac{1}{\sin(\pi/(3T))}}. \tag{D.13}$$

Now use the fact that there exists $T_3 > 0$, such that for all $T > T_3$, $1/\sin(\pi/(3T)) \leq 3 \cdot 0.99T/\pi$. Then

$$\max\left\{\frac{1}{C_{k_1}(2T)}, \frac{1}{C_{k_T}(2T)}\right\} \leq \frac{1}{T} \cdot \frac{\pi}{2\pi - 3 \cdot 0.99}. \tag{D.14}$$

Next, following the same proof the the first statement, there exists $T_4 > 0$ such that for $T > T_4$,

$$\max\left\{\frac{C_{k_1}(T)}{C_{k_1}(2T)}, \frac{C_{k_T}(T)}{C_{k_T}(2T)}\right\} \leq \frac{1}{2} + \frac{1}{T\sin(\pi/(3T))} \leq \frac{1}{2} + \frac{3}{0.99 \cdot \pi}. \tag{D.15}$$

As a result,

$$\max\left\{\frac{C_{k_1}(T)}{C^2_{k_1}(2T)}, \frac{C_{k_T}(T)}{C^2_{k_T}(2T)}\right\} \leq \frac{1}{T}\left(\frac{1}{2} + \frac{3}{0.99 \cdot \pi}\right)\left(\frac{\pi}{2\pi - 3 \cdot 0.99}\right) \tag{D.16}$$

Let $T_5 > 0$ be defined such that for all $T > T_5$, RHS of above equation is smaller than $1/96$.

Combining these two, we have that for $T_0 = \max\{T_1, T_2, T_3, T_4, T_5\}$, the two statements hold.

□

Using the above lemma, we can prove that the random phase unitary of H_{comp} can be used to solve the PSPACE problem. See the following two lemmas.

Lemma 14. *Let H_{comp} be the computation Hamiltonian of $\mathsf{D}[\mathsf{M}(p(n)]$, and $\mathcal{U}$ is the random phase unitary ensemble w.r.t. eigenstates of H_{comp}. Let $|\psi_{\mathcal{C}_1}\rangle$ be the configuration state corresponds to the initial state of $\mathsf{D}[\mathsf{M}(p(n))]$ with x, where $|x| = n$. And T (being even) denotes the running time of $\mathsf{D}[\mathsf{M}(p(n)]$ on input x. Then there exists $T_0 > 0$, such that when $T > T_0$ the following holds:*

Prepare $|\psi_{\mathcal{C}_1}\rangle$ and randomly draw $U \in \mathcal{U}$, then doing measurement on $U|\psi_{\mathcal{C}_1}\rangle$ on the local basis $\{|x\rangle_i, |q\rangle_i\}$ of $\mathsf{D}[\mathsf{M}(p(n))]$. The probability to collapse to the second half path, i.e., states $|\psi_{\mathcal{C}_t}\rangle$, $t = T/2+1, \cdots, T$, is greater than $1/12$.

Proof. Let E_k and $|k\rangle$ denote the eigenvalue and eigenstate of the effective Hamiltonian of the Type-5 path that contains $|\psi_{\mathcal{C}_1}\rangle$. Then $|\psi_{\mathcal{C}_1}\rangle = \sum_k |k\rangle\langle k|\psi_{\mathcal{C}_1}\rangle$. So after applying the random phase unitary, $|\psi_{\mathcal{C}_1}\rangle \to \sum_k e^{i\theta_k}|k\rangle\langle k|\psi_{\mathcal{C}_1}\rangle$, where θ_k is i.i.d. from uniform distribution over $[0, 2\pi)$.

The probability to get any of the output state $|\psi_{\mathcal{C}_t}\rangle$ is

$$\Pr(|\psi_{\mathcal{C}_t}\rangle) = \mathbb{E}_{\theta_1\cdots\theta_T}\Big[\Big|\sum_k \langle\psi_{\mathcal{C}_t}|k\rangle\langle k|\psi_{\mathcal{C}_1}\rangle e^{i\theta_k}\Big|^2\Big] = \sum_k |\langle k|\psi_{\mathcal{C}_t}\rangle|^2 |\langle k|\psi_{\mathcal{C}_1}\rangle|^2. \tag{D.17}$$

In the last equality we use $\mathbb{E}_{\theta_1\cdots\theta_T}[e^{i(\theta_i-\theta_j)}] = \delta_{ij}$. Using the solution from Appendix I, above expression is further simplified

$$\Pr(|\psi_{\mathcal{C}_t}\rangle) = \sum_k \frac{1}{N_k(2T)^2}|e^{-ikt} - e^{ikt-ik}|^2|e^{-ik} - 1|^2. \tag{D.18}$$

Here we introduce $N_k(2T) = \sum_{t=1}^{T}|e^{-ikt} - e^{ikt-ik}|^2 = 2T - \sin 2Tk/\sin k$. According to Lemma. 13, there exists $T_0 > 0$ such that for all $T > T_0$, the probability to get measurement outcome $t = T/2+1, \cdots T$ is

$$\Pr\left(\frac{T}{2} + 1 \leq t \leq T\right) = 1 - \sum_{t=1}^{T/2}\Pr(|\psi_{\mathcal{C}_t}\rangle)$$

$$
\begin{aligned}
&= 1 - \sum_{t=1}^{T} \frac{N_{k_t}(T)}{N_{k_t}^2(2T)} |e^{-ik_t} - 1|^2 \\
&= 1 - \sum_{t=2}^{T-1} \frac{N_{k_t}(T)}{N_{k_t}^2(2T)} |e^{-ik_t} - 1|^2 - \frac{N_{k_1}(T)}{N_{k_1}^2(2T)} |e^{-ik_1} - 1|^2 - \frac{N_{k_T}(T)}{N_{k_T}^2(2T)} |e^{-ik_T} - 1|^2 \\
&\geq 1 - \frac{5}{6} \sum_{t=1}^{T} \frac{|e^{-ik_t} - 1|^2}{N_{k_t}(2T)} - \frac{1}{96} \left(|e^{-ik_1} - 1|^2 + |e^{-ik_T} - 1|^2 \right) \\
&\geq \frac{1}{12}
\end{aligned} \tag{D.19}
$$

In the last inequality, we use $\sum_{t=1}^{T} |e^{-ik_t} - 1|^2 / N_{k_t}(2T) = \sum_{t=1}^{T} |\langle \psi_{\mathcal{C}_1} | k_t \rangle|^2 = 1$ and $|e^{-ik_1} - 1|^2 \leq 4$. □

Lemma 15. *Let $L \in \mathsf{PSPACE}$. Then there exists one Turing machine $\mathsf{M} = \langle Q, \Gamma, \Delta \rangle$ that can determine if $x \in L$ using polynomial space $p(|x|)$, such that the followings are satisfied for large-enough $|x|$:*

Denote the computation Hamiltonian of $\mathsf{D}[\mathsf{M}(p(n))]$ as H_{comp}, and its energy-conserving random unitary ensemble as $\{\mathcal{U}_{p(n)}\}$. Let

$$
P_{a,r} = \sum_{i=1}^{p(n)} \sum_{q \in Q} |q^{a,r}\rangle_i \langle q^{a,r}|_i \tag{D.20}
$$

be operators in $\mathcal{H}_{\mathsf{D}[\mathsf{M}(p(n))]}$, and $|\psi_{\mathcal{C}_1}\rangle$ be the configuration state corresponds to initial configuration of $\mathsf{D}[\mathsf{M}(p(n))]$ with input x where $|x| = n$. Then there exists n_0 that for all $n > n_0$, if $x \in L$,

$$
\mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_a U | \psi_{\mathcal{C}_1} \rangle] \geq \frac{1}{12}, \quad \mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_r U | \psi_{\mathcal{C}_1} \rangle] = 0, \tag{D.21}
$$

and if $x \notin L$,

$$
\mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_r U | \psi_{\mathcal{C}_1} \rangle] \geq \frac{1}{12}, \quad \mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_a U | \psi_{\mathcal{C}_1} \rangle] = 0. \tag{D.22}
$$

Proof. First, choose a M that determines if $x \in L$ in polynomial space, such that for energy legitimate input x with $|x| = n$, the running time is at least n. This can be easily achieved by demanding M to first sweep the whole input string before doing computation. In the following, we prove the $x \in L$ statement holds for H_{comp} defined from M. Generalization to $x \notin L$ cases is straightforward.

We begin by dealing with an idealized situation. Assume the subspace of path that contains $|\psi_{\mathcal{C}_1}\rangle$ (type-5a) has no energy degeneracy with rest of the eigenstates, then the energy-conserving PRU in this subspace is equivalent to the random phase unitary ensemble. Due to Lemma 14, when the length of the path is greater than T_0, measuring the local basis projects the state $U |\psi_{\mathcal{C}_1}\rangle$ to the second half path with probability $\geq 1/12$. By our construction of M, this always holds for large enough $|x$. Finally, notice that since the second half path contains configurations having q^a as internal state (Lemma 10), the probability to collapse to the second half path is exactly equal to $\mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_a U | \psi_{\mathcal{C}_1} \rangle]$. So we prove the theorem with the aforementioned assumption.

In reality, the path that contains $|\psi_{\mathcal{C}_1}\rangle$ can have energy degeneracy with other type-4a&5a paths with the same length. $U |\psi_{\mathcal{C}_1}\rangle$ has equal probabilities to collapse to each of the path. However, recall that type-4a paths have q^a as internal states along the whole path. Therefore, whether the degenerated path is of type-4a or 5a, the second half path must contain configurations with q^a as internal states. As a result, $\mathbb{E}_{U \sim \mathcal{U}_{p(n)}} [\langle \psi_{\mathcal{C}_1} | U^\dagger P_a U | \psi_{\mathcal{C}_1} \rangle]$ cannot decrease. That completes the proof. □

Putting everything together, we prove that with query access to the energy-conserving random unitary ensemble of H_{comp}, one can construct a PSPACE solver.

Theorem 3 (Energy-conserving random unitary can be used to solve PSPACE problems)**.** *For any language $L \in \mathsf{PSPACE}$, there exists a (uniform family of) translational-invariant one-dimensional local Hamiltonian H, whose matrix elements belong to $\{0, 1, 10, 1/2, 1/4\}$, such that a polynomial quantum algorithm with query access to the energy-conserving random unitary ensemble of H can solve all the instances of L with sufficiently large input size, with success probability at least $2/3$.*

Proof. Let M be the Turing machine specified in Lemma 15 which solves L in polynomial space $p(\cdot)$, and choose H_{comp} to be the (uniform family of) computational Hamiltonian of $\mathsf{D}[\mathsf{M}_L]$ specified by Lemma 12. With query access to the energy-conserving PRU of H_{comp}, Algo 1 can efficiently solve L for sufficiently large input size. Due to Lemma 15, the failure probability is at most $(1 - 1/12)^5 \approx 0.27 < 1/3$. □

Algorithm 1: PSPACE solver

Input: Input $x \in \{0,1\}^*$, query access to the unitary ensemble $\{\mathcal{U}_n\}$, and a polynomial $p(n)$
Output: Accept or Reject

Construct state $|\psi_{\mathcal{C}_1}\rangle$ that corresponds to the input x in the Hilbert space of length-$p(|x|)$ chain.;
for $t = 1$ **to** 15 **do**
  Query the unitary ensemble and get $U|\psi_{\mathcal{C}_1}\rangle$ for $U \in \mathcal{U}_{p(|x|)}$.;
  Measure $U|\psi_{\mathcal{C}_1}\rangle$ on the local basis. ;
  if q^a *appears in the measurement outcome* **then**
    return Accept
  else if q^r *appears in the measurement outcome* **then**
    return Reject
return Accept

Appendix E: True Quantified Boolean Formula (TQBF)

In the following three sections, we construct an algorithm to distinguish a PSPACE-complete solver from any polynomial size quantum circuit. With query access to the solver, one can efficiently invert quantum-secure one-way functions, a property not held by any efficient quantum circuit.

We use *True Quantified Boolean Formula* problem (TQBF) to demonstrate this property.

1. Problem Statement

TQBF is the canonical PSPACE-complete problem. It consists of all fully quantified Boolean formulas that evaluate to true over the Boolean domain. Formally, the language is defined as:

$$\text{TQBF} := \left\{ \varphi = Q_1 x_1 \cdots Q_n x_n \; \psi(x_1, \ldots, x_n) \;\middle|\; \begin{array}{l} Q_i \in \{\forall, \exists\},\ \psi \text{ is a Boolean formula} \\ \text{and } \varphi \text{ evaluates to true.} \end{array} \right\}. \tag{E.1}$$

We assume that formulas are written in *prenex normal form*, with all quantifiers preceding the propositional formula, and that ψ is encoded either in conjunctive normal form or as a Boolean circuit. The input size of a formula is the total number of bits required to encode the quantifiers and ψ. As an example, the formula $\phi = \forall x_1 \exists x_2 \forall x_3 \; [(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3)]$ is in TQBF.

TQBF is PSPACE-complete as TQBF $\in$ PSPACE and every language in PSPACE reduces to TQBF under polynomial-time reductions. As such, TQBF serves as the standard complete problem for reasoning about the computational power of PSPACE.

Fact 7. *TQBF is a* PSPACE*-complete problem, cf. [67, 68].*

2. Power of TQBF

Lemma 16 (TQBF oracle can invert one-way function)**.** *Let $f : \{0,1\}^n \to \{0,1\}^m$ be any polynomial-time computable function. There exists a polynomial-time algorithm that, given oracle access to a correct* TQBF *solver, can invert f on any input $y \in \{0,1\}^m$. That is, the algorithm either finds $x \in \{0,1\}^n$ such that $f(x) = y$, or correctly determines that no such x exists.*

Proof. Given a circuit C computing f and target y, we construct the TQBF formula: $\Phi_{C,y} := \exists x_1, \ldots, x_n \; \psi(x_1, \ldots, x_n, y)$ where $\psi(x_1, \ldots, x_n, y)$ is a Boolean formula that evaluates to true if and only if $C(x_1, \ldots, x_n) = y$. This formula can be constructed in polynomial time by simulating the circuit C. First, we query the TQBF oracle on $\Phi_{C,y}$. If the oracle returns False, then no preimage exists, and we output Fail. If the oracle returns True, we extract a witness using binary search: for each bit position $i = 1, \ldots, n$, we construct the formula: $\Phi_i^0 = \exists x_{i+1}, \ldots, x_n \; \psi(a_1, \ldots, a_{i-1}, 0, x_{i+1}, \ldots, x_n)$ where $a_1, \ldots, a_{i-1}$ are the bits determined in previous iterations. We query the oracle on Φ_i^0. If it returns True, we set $a_i = 0$; otherwise, we set $a_i = 1$. After n such queries, we obtain $(a_1, \ldots, a_n)$, which is guaranteed to be a valid preimage since the original formula was satisfiable and the oracle is correct. The total number of oracle queries is $n + 1$, and each formula has polynomial size, so the algorithm runs in polynomial time. □

The algorithm for establishing Lemma 16 is given in the following.

Algorithm 2: Function Inversion with TQBF Oracle

Input: Circuit C computing f, target y
Output: x such that $f(x) = y$, or Fail

Construct TQBF formula $\Phi_{C,y} = \exists x_1, \ldots, x_n \; \psi(x_1, \ldots, x_n, y)$, where $\psi(x_1, \ldots, x_n, y) \equiv [C(x_1, \ldots, x_n) = y]$;
Query oracle: $b \leftarrow \mathcal{O}(\Phi_{C,y})$;
if $b =$ False **then**
  return Fail
for $i = 1$ **to** n **do**
  Construct $\Phi_i^0 = \exists x_{i+1}, \ldots, x_n \; \psi(a_1, \ldots, a_{i-1}, 0, x_{i+1}, \ldots, x_n)$;
  Query oracle: $b_i \leftarrow \mathcal{O}(\Phi_i^0)$;
  if $b_i =$ True **then**
    $a_i \leftarrow 0$
  else
    $a_i \leftarrow 1$
return $(a_1, \ldots, a_n)$

Appendix F: Verifying TQBF Oracles via One-Way Function

We consider the problem of distinguishing between a true TQBF oracle and a pseudo TQBF oracle constructed from a uniform family of polynomial-size quantum circuit claiming to solve TQBF.

Theorem 4 (TQBF Oracle Verification)**.** *Assume quantum-secure one-way functions exist. There exists a polynomial-time classical algorithm $\mathcal{V}$ (the verifier) that, given black-box access to a purported* TQBF *oracle $\mathcal{O}$, outputs either* True *or* Pseudo *such that:*

1. *If $\mathcal{O}$ correctly solves all* TQBF *instances with probability at least $2/3$, then the verifier $\mathcal{V}^{\mathcal{O}}$ outputs* True *with probability at least $2/3$;*

2. *If $\mathcal{O}$ is implemented by polynomial-size quantum circuits, then for sufficiently large system sizes, the verifier $\mathcal{V}^{\mathcal{O}}$ outputs* Pseudo *with probability at least $2/3$.*

1. Verifier Algorithm

The verifier uses Algorithm 2 for function inversion with TQBF oracle as a subroutine to test whether the oracle can be used to consistently invert quantum-secure one-way functions.

Algorithm 3: TQBF Oracle Verifier

Input: System size parameter n, oracle $\mathcal{O}$
Output: True or Pseudo

Let f be a quantum-secure one-way function;
Set $T = 100 \log n$ *// Number of test instances*;
Initialize success counter $S = 0$;
for $i = 1$ *to* T **do**
  Choose input size $n' \leftarrow \{1, 2, \ldots, n\}$ uniformly at random;
  Sample $x \leftarrow \{0,1\}^{n'}$ uniformly at random;
  Compute $y \leftarrow f(x)$;
  Run $x' \leftarrow$ Algorithm 2(C_f, y) where C_f computes f;
  if $x' \neq$ Fail *and* $f(x') = y$ **then**
    $S \leftarrow S + 1$
if $S \geq 2T/3$ **then**
  return True
else
  return Pseudo

2. Supporting Lemmas

Lemma 17 (Amplified TQBF oracle)**.** *Given a probabilistic oracle $\mathcal{O}$ that correctly solves* TQBF *instances with probability at least $2/3$, there exists a polynomial-time procedure that creates an amplified oracle $\mathcal{O}'$ which correctly solves any* TQBF *instance with probability at least $1 - 2^{-k}$ for any desired parameter k.*

Proof. For any TQBF query ϕ, the amplified oracle $\mathcal{O}'(\phi)$ queries $\mathcal{O}$ on ϕ exactly $6k$ times, obtaining answers $b_1, b_2, \ldots, b_{6k}$, then outputs the majority value among these answers. Since each individual query to $\mathcal{O}$ succeeds with probability at least $2/3$, the expected number of correct answers is at least $\mathbb{E}[\text{correct}] = 6k \cdot (2/3) = 4k$. Let X be the number of correct answers. By Chernoff bound, $\Pr[X < 3k] = \Pr[X < \mathbb{E}[X] - k] \leq \exp(-2k^2/(6k)) = \exp(-k/3) \leq 2^{-k/5}$. For $k \geq 5$, we have $2^{-k/5} \leq 2^{-k}$. Since the majority of $6k$ answers is correct when at least $3k$ answers are correct, we have $\Pr[\mathcal{O}'(\phi) \text{ is correct}] \geq 1 - 2^{-k}$. □

Lemma 18 (Function inversion with true oracle)**.** *Let f be any polynomial-time computable function and $\mathcal{O}$ be a probabilistic oracle that correctly solves* TQBF *instances with probability at least $2/3$. Then there exists a polynomial-time algorithm that uses $\mathcal{O}$ to invert f with probability at least $1 - \text{negl}(n)$.*

Proof. We modify Algorithm 2 to use the amplified oracle $\mathcal{O}'$ from Lemma 17 with parameter $k = 2n$. This ensures each individual TQBF query succeeds with probability at least $1 - 2^{-2n}$. Algorithm 2 makes at most $n + 1$ queries to the oracle: one initial query to check if a preimage exists, and at most n queries for witness extraction. By union bound, the probability that any of these queries fails is at most $(n + 1) \cdot 2^{-2n} \leq 2^n \cdot 2^{-2n} = 2^{-n}$, which is negligible in n. Therefore, the algorithm successfully inverts f for any given image $y = f(x)$ with probability at least $1 - 2^{-n} \geq 1 - \text{negl}(n)$. □

Lemma 19 (Function inversion with quantum circuit oracle)**.** *If $\mathcal{O}$ is implemented by polynomial-size quantum circuits and f is a quantum-secure one-way function, then for sufficiently large n, Algorithm 2 using oracle $\mathcal{O}$ succeeds in inverting f on a random input with probability at most* $\text{negl}(n)$.

Proof. When $\mathcal{O}$ is implemented by polynomial-size quantum circuits, the composition of Algorithm 2 with $\mathcal{O}$ yields a uniform family of polynomial-size quantum circuits attempting to invert f. The verifier samples $x \leftarrow \{0,1\}^n$ uniformly at random, computes $y = f(x)$, then runs Algorithm 2 to find a preimage of y. By Definition 4, for any uniform family of polynomial-size quantum circuits $\{Q_n\}$, there exists n_0 such that for all $n \geq n_0$, $\Pr_{x \leftarrow \{0,1\}^n}[f(Q_n(f(x))) = f(x)] \leq \text{negl}(n)$. Since our algorithm only succeeds if it finds a correct preimage of $f(x)$, and any correct preimage x' satisfies $f(x') = f(x)$, the success probability is at most $\text{negl}(n)$ for sufficiently large n. □

3. Main Proof

Proof of Theorem 4. We analyze both cases of the theorem and the runtime.

a. Case 1: $\mathcal{O}$ correctly solves TQBF *with probability $\geq 2/3$.* By Lemma 18, Algorithm 2 succeeds in inverting f on any given input with probability at least $1 - 2^{-n}$. In Algorithm 3, we perform $T = 100 \log n$ independent tests, where each test succeeds with probability at least $1 - 2^{-n}$. Let X be the number of successful inversions. Then $\mathbb{E}[X] \geq T(1 - 2^{-n}) \geq T - T \cdot 2^{-n} \geq T - 1$ for sufficiently large n. By Chernoff bound, $\Pr[X < 2T/3] = \Pr[X < \mathbb{E}[X] - (T - 1 - 2T/3)] = \Pr[X < \mathbb{E}[X] - T/3 + 1] \leq \Pr[X < \mathbb{E}[X] - T/4] \leq \exp(-2(T/4)^2/T) = \exp(-T/8) = \exp(-12.5 \log n) = n^{-12.5}$ for sufficiently large n. Therefore, $\mathcal{V}^{\mathcal{O}}$ outputs True with probability at least $1 - n^{-12.5} \geq 2/3$ for sufficiently large n.

b. Case 2: $\mathcal{O}$ is implemented by polynomial-size quantum circuits. By Lemma 19, for sufficiently large n, Algorithm 2 succeeds in inverting f on a random input with probability at most $\text{negl}(n)$. Let X be the number of successful inversions in Algorithm 3. Then $\mathbb{E}[X] \leq T \cdot \text{negl}(n)$. Since $\text{negl}(n) = o(n^{-c})$ for any constant $c > 0$, and $T = 100 \log n$, for sufficiently large n we have $\mathbb{E}[X] \leq T \cdot n^{-2} = 100 n^{-2} \log n \leq T/6$. By Chernoff bound, $\Pr[X \geq 2T/3] = \Pr[X \geq \mathbb{E}[X] + (2T/3 - \mathbb{E}[X])] \geq \Pr[X \geq \mathbb{E}[X] + T/2] \leq \exp(-2(T/2)^2/T) = \exp(-T/2) = \exp(-50 \log n) = n^{-50}$. Therefore, $\mathcal{V}^{\mathcal{O}}$ outputs Pseudo with probability at least $1 - n^{-50} \geq 2/3$ for sufficiently large n.

c. Runtime: Algorithm 3 makes $T = 100 \log n$ calls to Algorithm 2. Each call to the amplified oracle takes $O(n)$ repetitions, and each TQBF query takes polynomial time. Therefore, the total runtime is polynomial in n. □

Appendix G: Verifier for random unitaries that conserve energy

The framework developed for verifying TQBF oracles can be extended to efficiently distinguish between truly random unitaries (Haar-random) that conserve energy and pseudorandom unitaries generated by polynomial-size quantum circuits. This extension relies on the computational power that access to Haar-random unitaries can provide.

Theorem 5 (Universal distinguisher)**.** *Assume quantum-secure one-way functions exist. There exists a family of one-dimensional, local, and translational-invariant Hamiltonian whose matrices elements belong to* $\{0, 1, 10, 1/2, 1/4\}$*, and a polynomial-time quantum algorithm* $\mathcal{V}_{unitary}$ *(the universal distinguisher) that, given black-box access to a unitary oracle* U*, outputs either* HaarRandom *or* Pseudorandom *such that:*

1. *If* U *is a Haar-random unitary conserving the Hamiltonian, then the distinguisher* $\mathcal{V}^U_{unitary}$ *outputs* HaarRandom *with probability at least* $2/3$*;*
2. *If* U *is generated by a uniform family of polynomial-size quantum circuits, then for sufficiently large system sizes, the distinguisher* $\mathcal{V}^U_{unitary}$ *outputs* Pseudorandom *with probability at least* $2/3$*.*

Proof. The proof follows by combining Theorem 3 with Theorem 4. We construct the universal distinguisher $\mathcal{V}_{\text{unitary}}$ as follows:

1. Given access to unitary oracle U, use the construction from Theorem 3 to build a purported TQBF oracle $\mathcal{O}_U$.
2. Run the TQBF oracle verifier $\mathcal{V}$ from Algorithm 3 on $\mathcal{O}_U$.
3. If $\mathcal{V}^{\mathcal{O}_U}$ outputs True, return HaarRandom.
4. If $\mathcal{V}^{\mathcal{O}_U}$ outputs Pseudo, return Pseudorandom.

a. Case 1: U is Haar-random. By Theorem 3, the constructed oracle $\mathcal{O}_U$ correctly solves TQBF instances with probability at least $2/3$. By Theorem 4, the verifier $\mathcal{V}^{\mathcal{O}_U}$ outputs True with probability at least $2/3$. Therefore, $\mathcal{V}^U_{\text{unitary}}$ outputs HaarRandom with probability at least $2/3$.

b. Case 2: U is generated by polynomial-size quantum circuits. When U is pseudorandom (i.e., generated by a polynomial-size quantum circuits), the construction in Theorem 3 yields an oracle $\mathcal{O}_U$ that is also implementable by polynomial-size quantum circuits. By Theorem 4, for sufficiently large system sizes, the verifier $\mathcal{V}^{\mathcal{O}_U}$ outputs Pseudo with probability at least $2/3$. Therefore, $\mathcal{V}^U_{\text{unitary}}$ outputs Pseudorandom with probability at least $2/3$.

c. Runtime: The construction of $\mathcal{O}_U$ from U takes polynomial time by Lemma 3, and running the TQBF verifier takes polynomial time by Theorem 4. Therefore, the total runtime of $\mathcal{V}_{\text{unitary}}$ is polynomial in the system size. □

Appendix H: Undecidability of the existence of energy-conserving PRUs

In this section, we prove that determining if a given local Hamiltonian has energy-conserving PRU is an undecidable problem. The reason is to define uniform family of Hamiltonians, one need to specify a TM that generates the description of that Hamiltonian family. That is, the problem in fact takes TMs as inputs. As a result, we can construct a Hamiltonian family, who has or does not have energy-conserving PRU depending on the solution of halting problem for a given input.

Lemma 20 (Simulating two machines simutaneously)**.** *Let* $\mathsf{M}_1 = \langle Q_1, \Gamma_1, \Delta_1 \rangle$ *and* $\mathsf{M}_2 = \langle Q_2, \Gamma_2, \Delta_2 \rangle$ *be two Turing machines. When taking* $x_1, x_2 \in \{0,1\}^*$ *as inputs, respectively, the maximum memory cost in the first* T *steps is* $S(T, x_1, x_2)$*. Then there is a simulating Turing machine* M *that can simulate the first* T *steps of operations of both* M_1 *and* M_2 *simultaneously, with simulation time* $O(T \cdot S(T, x_1, x_2))$ *for any* x_1, x_2 *and* T*.*

Proof. M can be constructed in the following sense. Define the new alphabet as $\Gamma = Q_1 \cup Q_2 \cup (\Gamma_1 \times \Gamma_2)$. That is, we introduce two tapes to write the symbols of M_1 and M_2 simultaneously, and put the head internal state into the tape. A symbol $q \in Q_1$ at cell i in the tape represents the head of M_1 is located at cell $i+1$ and has internal state q, and so as any $q \in Q_2$. Then to simulate one step of M_1 and M_2, the head of M sweeps along the length $S(T, x_1, x_2)$ region of tape and update the symbol according

to the transition rule of M_1 (M_2) when encountering any $q \in Q_1$ (Q_2). The time overhead of each step is at most $O(S(T, x_1, x_2))$. So the total running time to simulate until the T-th step is at most $O(T \cdot S(T, x_1, x_2))$ □

Lemma 21 (PRU and halting problem)**.** *Let* UM *denotes the universal Turing machine.* $\{H_n\}$ *is the uniform family of Hamiltonians whose energy-conserving PRU does not exist. Then for any* $x \in \{0,1\}^*$*, there exists a Turing machine* M_x *and a constant* $\alpha > 0$*, such that for any* $n \in \mathbb{N}^+$ *as input, if* UM *does not halt in time* $\leq \alpha n$ *upon input* x*,* M_x *generates* H_n*, otherwise generates* 0*. The overall running time of* M_x *is* $\mathsf{poly}(n)$*. The whole process takes time at most* $\mathsf{poly}(n)$*.*

Proof. Let M_d be the Turing machine that generates $\{H_n\}$ upon any input size n. Since H_n is a local Hamiltonian, the running time of M_d is αn for some $\alpha > 0$. We design M_d to be reversible. Let $\mathsf{M}_d^{(\mathrm{rev})}$ be the reverse Turing machine of M_d, and UM be the universal Turing machine. Then M_x can be constructed as follows. For each n, simulate the operations of M_d upon input n and UM upon input x simultaneously using Lemma.20. If UM halts before M_d halts (which takes αn steps for M_d), switch to $\mathsf{M}_d^{(\mathrm{rev})}$ to reverse all the operations of M_d. □

Lemma.21 asserts that for any x, there is a uniform family of Hamiltonians (generated by M_x), such that whether it has energy-conserving PRU depends on if the universal Turing machine halts upon input x. As a direct consequence, we have

Theorem 6 (Undecidability of the existence of energy-conserving PRU)**.** *If we have an algorithm that takes any uniform family of local Hamiltonians as input (more precisely, we should take the Turing machine that generates this Hamiltonian family as input), we can solve the halting problem.*

Proof. Lemma 21 says that for any x, we can design a uniform family of Hamiltonians $\{H_n\}$ efficiently generated by M_x, such that if UM halts upon input x, H_n is 0 for sufficiently large n, whose energy-conserving PRU is the conventional PRU. If UM does not halt upon x, $\{H_n\}$ does not have energy-conserving PRU. So deciding the existence of PRU requires solving the halting problem for all instances. □

Appendix I: One-dimensional hopping problem

In this section we exactly solve the one-dimensional hopping problem with boundary potentials. Let the Hamiltonian be

$$H = \sum_{i=1}^{N-1} |i\rangle \langle i+1| + |i+1\rangle \langle i| + V_1 |1\rangle \langle 1| + V_2 |N\rangle \langle N| . \tag{I.1}$$

Choose ansatz wavefunction

$$|E_k\rangle = \sum_{n=1}^{N} \psi_n |n\rangle , \quad \psi_n = A_k e^{ikn} + B_k e^{-ikn}. \tag{I.2}$$

The corresponding energy in bulk is $E_k = 2\cos k$. Now consider the boundary terms. The boundary conditions are

$$\psi_2 + V_1 \psi_1 = E\psi_1, \quad \psi_{N-1} + V_2 \psi_N = E\psi_N. \tag{I.3}$$

This gives us

$$A_k(V_1 e^{ik} - 1) + B_k(V_1 e^{-ik} - 1) = 0, \quad A_k(V_2 e^{iNk} - e^{i(N+1)k}) + B_k(V_2 e^{-iNk} - e^{-i(N+1)k}) = 0. \tag{I.4}$$

To bring solutions to exist,

$$\frac{V_1 e^{ik} - 1}{V_1 e^{-ik} - 1} = \frac{V_2 e^{iNk} - e^{i(N+1)k}}{V_2 e^{-iNk} - e^{-i(N+1)k}} \tag{I.5}$$

Equivalently,

$$\tan(Nk) = -\frac{(1 - V_1 V_2)\sin k}{(V_1 V_2 + 1)\cos k - (V_1 + V_2)}. \tag{I.6}$$

One obvious solution for the above equation is $k = 0$. But this solution is not consistent with boundary conditions, except for $V_1 = V_2 = 1$. Similarly, $k = \pi$ is a solution only when $V_1 = V_2 = -1$. In the main text we deal with the case of $V_1 = -1$. In this case Eq. (I.6) becomes

$$\frac{1+V_2}{V_2-1}\tan\left(\frac{k}{2}\right) = \tan(Nk). \tag{I.7}$$

For $V_2 \in (-1, 1)$, the above equation has N real solutions of $k \in (0, \pi)$. Thus, the system has no bound state. For wavefunction, using

$$\frac{A_k}{B_k} = -\frac{e^{-ik}+1}{e^{ik}+1} = -e^{-ik}. \tag{I.8}$$

This leads to

$$|\psi_k\rangle = \frac{1}{\sqrt{C_k}}\sum_{n=1}^{N}(e^{-ikn} - e^{ikn-ik})\,|n\rangle\,, \tag{I.9}$$

where the normalization factor is determined by

$$C_k = \sum_{n=1}^{N}|e^{-ikn} - e^{ikn-ik}|^2 = \sum_{n=1}^{N} 2 - e^{i(2n-1)k} - e^{-i(2n-1)k} = 2N - \frac{\sin 2Nk}{\sin k} \tag{I.10}$$

Appendix J: Proof of Lemma 11

Lemma 11. *For the following equation*

$$-\frac{1}{2^{m+1}-1}\tan\left(\frac{k}{2}\right) = \tan(Nk), \quad k \in (0,\pi), \quad m, N \in \mathbb{N}^+, \tag{J.1}$$

denote $\mathcal{S}(m, N)$ as the solution set for k with fixed m and N. Define $\mathcal{S}(m) = \cup_{N\in\mathbb{N}^+}\mathcal{S}(m, N)$, then it satisfies the following:

- *For $m_1 \neq m_2$, $\mathcal{S}(m_1)\bigcap\mathcal{S}(m_2) = \mathcal{S}(m_1)\bigcap\pi\mathbb{Q} = \mathcal{S}(m_2)\bigcap\pi\mathbb{Q} = \emptyset$.*
- *For any m and $N_1 \neq N_2$, $\mathcal{S}(m, N_1)\bigcap\mathcal{S}(m, N_2) = \emptyset$.*

The proof idea is as follows. Defining $x = \tan(k/2)$, $\tan(Nk)$ can be written as the ration of two polynomials with integer coefficients, by iteratively using the formulas for double angles. Therefore, x is the root of some polynomial with degree depending on N and integer coefficients depending on n. It is sufficient to prove all of these polynomials are irreducible for different n and N. In this case, they have no common roots.

Definition 17 (Irreducible polynomials)**.** *A polynomial $f(x)$ over $\mathbb{Z}$ (which means all the coefficients of f belong to $\mathbb{Z}$) is an irreducible polynomial if it is non-constant and cannot be written as $f(x) = g(x)h(x)$ for g and h are both non-constant polynomails over $\mathbb{Z}$.*

Fact 8 (Irreducible polynomials have no common roots)**.** *Let $f(x)$ and $g(x)$ be two non-constant polynomials over $\mathbb{Z}$, and $f(x) \neq \alpha g(x)$ for all $\alpha \in \mathbb{Z}$. Then f and g have no common roots.*

The proof idea for this fact is that both f and g must divide the minimal polynomial of the common root, contradicting with irreducibility. For a comprehensive overview for polynomials, one can refer to standard textbooks for number theory or Galois theory, e.g., [71–73].

To prove the irreducibility of these polynomials, we use (1) the fundamental theorem for Galois theory; (2) the properties of Cyclotomic polynomials. We state these standard results in a superficial and non-rigorous manner for accessibility.

Fact 9 (Fundamental theorem of Galois theory)**.** *Let $f(x)$ be a polynomial over $\mathbb{Q}$. Let K be the splitting field, i.e., smallest field that contains $\mathbb{Q}$ and all the roots of f. Define the Galois group* Gal(K/$\mathbb{Q}$) *as the group of all symmetries over K that leaves $\mathbb{Q}$ invariant (e.g., permutations of irrational numbers in K). Then*

- *Every subgroup H of* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ *corresponds to an intermediate field $E : \mathbb{Q} \subseteq E \subseteq K$ left invariant by the action of H, and vice versa.*

- *The correspondence is inclusion-reversing, i.e., the larger the subgroup H, the smaller the field E. In particular,* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ *corresponds to $\mathbb{Q}$.*

Definition 18 (Cyclotomic polynomials)**.** *The n-th order cyclotomic polynomial refers to a unique irreducible monic polynomial (the coefficient for highest order monomial is 1) $\Phi_n(x)$ over $\mathbb{Z}$, such that its roots are all n-th primitive roots of unit $e^{i2\pi\frac{k}{n}}$. In other words,*

$$\Phi_n(x) = \prod_{1\le k\le n, \gcd(n,k)=1} \big(x - e^{i2\pi\frac{k}{n}}\big). \tag{J.2}$$

Examples of cyclotomic polynomials for $n = 1, 2, 3, 4, 5$ are

$$\begin{aligned}
&\Phi_1(x) = x - 1,\\
&\Phi_2(x) = x + 1,\\
&\Phi_3(x) = x^2 + x + 1,\\
&\Phi_4(x) = x^2 + 1,\\
&\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.
\end{aligned} \tag{J.3}$$

We these preparations, we prove the following two technical lemmas.

Lemma 22 (Kronecker's lemma)**.** *Let $f(x)$ be a monic polynomial over $\mathbb{Z}$. If all roots of f have absolute values at most 1, then f is the product of cyclotomic polynomials and powers of x.*

Proof. Let r be the multiplicity of root 0. Denote $f(x) = x^r g(x)$. $g(x)$ is a monic polynomial that has only nonzero roots. Denote $\Lambda = \{\lambda_1, \cdots \lambda_n\}$ as the multiset of roots of $g(x)$. All λ_i are algebraic integers (roots of some monic polynomial over $\mathbb{Z}$).

Then define

$$g_k(x) = \prod_{i=1}^{n} \big(x - \lambda_i^k\big), \quad k \in \mathbb{N}^+. \tag{J.4}$$

Every coefficients of $g_k(x)$ are algebraic integers. i.e., sum and multiplicity of numbers that are the roots of monic polynomials over $\mathbb{Z}$. Furthermore, every coefficients are symmetric sum of λs, which means that the are left invariant under any permutations of λs. Thus, they are rational numbers due to Fact 9. These together assert that coefficients of $g_k(x)$ must be integers.

Since $|\lambda_i| \le 1$, the norm of coefficient of x^m is at most $\binom{n}{m}$. As a result, for all $k \in \mathbb{N}^+$, possible forms of $g_k(x)$ are finite. Hence, there must exist integers $k_1 \ne k_2$, such that $g_{k_1}(x) = g_{k_2}(x)$. Therefore, multisets $\{\lambda_1^{k_1}, \cdots \lambda_n^{k_1}\}$ and $\{\lambda_1^{k_2}, \cdots \lambda_n^{k_2}\}$ coincide. That is, there exist a permutation σ of $\{1, 2, \cdots, n\}$, such that

$$\lambda_i^{k_1} = \lambda_{\sigma(i)}^{k_2}, \quad 1 \le i \le n. \tag{J.5}$$

Iterating along a cycle of length l gives

$$\lambda_i^{k_1^l} = \lambda_i^{k_2^l}. \tag{J.6}$$

Since $\lambda_i \ne 0$, this gives $\lambda_i = e^{i2\pi\frac{p}{k_1^l - k_2^l}}$ for $p \in \mathbb{N}^+$. Thus, every λ_i is the root of a cyclotomic polynomial. This completes the proof □

Lemma 23. *Let $n \in \mathbb{N}^+$. For any $N \in \mathbb{N}^+$, the solutions of following equation*

$$-\frac{1}{2^{n+1} - 1} \tan\left(\frac{k}{2}\right) = \tan(Nk), \quad k \in (0, \pi), \tag{J.7}$$

have no intersection with $\pi\mathbb{Q}$.

Proof. Denote $x = e^{ik/2}$. We have

$$\tan\left(\frac{k}{2}\right) = \frac{x-1}{i(x+1)}, \quad \tan(Nk) = \frac{x^{2N}-1}{i(x^{2N}+1)}. \tag{J.8}$$

Using this expression, solutions of Eq. (J.7) correspond to roots of

$$g_N(x) = 2^n x^{2N} + (2^{n+1}-1)(x^{2N-1} + x^{2N-2} + \cdots + x^2 + x) + 2^n. \tag{J.9}$$

Note that roots of $g_N(x)$ are in x, x^* pairs. So we can only consider the roots where $\operatorname{Im} x > 0$, which correspond to $k \in (0, \pi)$. Assume for $N = N_0$ there is solution $y = e^{i2\pi p/q}$ for contradiction, where $p, q \in \mathbb{N}^+$, $p < q/2$ and $\gcd(p, q) = 1$. Then y is the root of cyclotomic polynomial $\Phi_q(x)$. As a result, $\Phi_q(x) \mid g_{N_0}(x)$. Since $e^{i2\pi/q}$ must also be a root of $\Phi_q(x)$, is is also a root of $g_{N_0}(x)$, i.e.,

$$-\frac{1}{2^{n+1}-1}\tan\left(\frac{2\pi}{q}\right) = \tan\left(\frac{4\pi N}{q}\right). \tag{J.10}$$

Let

$$\delta := \min_{s\in\mathbb{Z}} \left|\frac{2N}{q} - s\right| \in [0, \frac{1}{2}]. \tag{J.11}$$

Since tan is periodic with π, $|\tan(4\pi N/q)| = |\tan(2\pi\delta)|$. Clearly, $\delta \neq 0, 1/2$. In this case, $\delta \geq 1/q$. As a result,

$$\left|\tan\left(\frac{4\pi N}{q}\right)\right| = |\tan(2\pi\delta)| \geq \left|\tan\left(\frac{2\pi}{q}\right)\right| > \frac{1}{2^{n+1}-1}\left|\tan\left(\frac{2\pi}{q}\right)\right|, \tag{J.12}$$

contradicting Eq. (J.10). □

Now we prove the desired lemma.

Proof of Lemma 11. $\mathcal{S}(m_1) \cap \pi\mathbb{Q} = \mathcal{S}(m_2) \cap \pi\mathbb{Q} = \emptyset$ is a direct consequence of Lemma 23. Denote $x = e^{ik/2}$, then solutions of Eq. (J.1) are roots of

$$g_{m,N}(x) = 2^m x^{2N} + (2^{m+1}-1)(x^{2N-1} + x^{2N-2} + \cdots + x^2 + x) + 2^m. \tag{J.13}$$

Assume for $m_0, N_0 \in \mathbb{N}^+$, $g_{m_0,N_0}(x)$ is reducible, i.e., there exists a polynomial $\phi(x) = a_0 x^k + a_1 x^{k-1} + \cdots$ over $\mathbb{Z}$ such that $\phi(x) \mid g_{m_0,N_0}(x)$. If $a_0 = 2^s$ for $1 \leq s \leq m-1$, the coefficient for the highest order monomial in $g_{m_0,N_0}(x)/\phi(x)$ is 2^{m-s}. As a result, the coefficient of x^{2N-1} in g_{m_0,N_0} is even, which is a contradiction. If $a_0 = 1$, since the roots of $\phi(x)$ are also roots of $g_{m_0,N_0}(x)$, $\phi(x)$ is a cyclotomic polynomial by Lemma 22, contraditing with Lemma 23. If $a_0 = 2^s$, same argument applies to $g_{m_0,N_0}(x)/\phi(x)$. As a result, for all $m, N \in \mathbb{N}^+$, $g_{m,N}(x)$ is a irreducible polynomial. Moreover, every two such polynomials are not proportional to each other, thus they have no common roots. This gives $\mathcal{S}(m_1) \cap \mathcal{S}(m_2) = \emptyset$ for $m_1 \neq m_2$, and $\mathcal{S}(m, N_1) \cap \mathcal{S}(m, N_2) = \emptyset$ for $N_1 \neq N_2$. □

[1] J. M. Deutsch, Quantum statistical mechanics in a closed system, Phys. Rev. A **43**, 2046 (1991).
[2] M. P. Fisher, V. Khemani, A. Nahum, and S. Vijay, Random quantum circuits, Annual Review of Condensed Matter Physics **14**, 335 (2023).
[3] M. Srednicki, Chaos and quantum thermalization, Phys. Rev. E **50**, 888 (1994).
[4] M. Rigol, V. Dunjko, and M. Olshanii, Thermalization and its mechanism for generic isolated quantum systems, Nature **452**, 854 (2008).
[5] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, Quantum Entanglement Growth Under Random Unitary Dynamics, Phys. Rev. X **7**, 031016 (2017).
[6] Y. Sekino and L. Susskind, Fast scramblers, Journal of High Energy Physics **2008**, 065 (2008).
[7] J. Cotler, N. Hunter-Jones, and D. Ranard, Fluctuations of subsystem entropies at late times, Physical Review A **105**, 022416 (2022).
[8] P. Hayden and J. Preskill, Black holes as mirrors: quantum information in random subsystems, JHEP **2007** (09), 120.
[9] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).
[10] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, Physical Review A **77**, 012307 (2008).
[11] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, The randomized measurement toolbox, Nature Reviews Physics **5**, 9 (2023).
[12] M. Guţă, J. Kahn, R. Kueng, and J. A. Tropp, Fast state tomography with optimal error bounds, Journal of Physics A: Mathematical and Theoretical **53**, 204001 (2020).
[13] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nature Physics **16**, 1050 (2020).
[14] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven, Barren plateaus in quantum neural network training landscapes, Nat. Commun. **9**, 1 (2018).
[15] H.-Y. Huang, S. Chen, and J. Preskill, Learning to predict arbitrary quantum processes, PRX Quantum **4**, 040337 (2023).
[16] M. Larocca, S. Thanasilp, S. Wang, K. Sharma, J. Biamonte, P. J. Coles, L. Cincio, J. R. McClean, Z. Holmes, and M. Cerezo, Barren plateaus in variational quantum computing, Nature Reviews Physics , 1 (2025).
[17] A. R. Brown, H. Gharibyan, S. Leichenauer, H. W. Lin, S. Nezami, G. Salton, L. Susskind, B. Swingle, and M. Walter, Quantum gravity in the lab. i. teleportation by size and traversable wormholes, PRX quantum **4**, 010320 (2023).
[18] S. Nezami, H. W. Lin, A. R. Brown, H. Gharibyan, S. Leichenauer, G. Salton, L. Susskind, B. Swingle, and M. Walter, Quantum gravity in the lab. ii. teleportation by size and traversable wormholes, PRX quantum **4**, 010321 (2023).
[19] E. Knill, Approximation by quantum circuits, arXiv preprint quant-ph/9508006 (1995).
[20] Z. Ji, Y.-K. Liu, and F. Song, Pseudorandom quantum states, in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38* (Springer, 2018) pp. 126–152.
[21] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Simple constructions of linear-depth t-designs and pseudorandom unitaries, arXiv preprint arXiv:2404.12647 (2024).
[22] C.-F. Chen, A. Bouland, F. G. Brandão, J. Docter, P. Hayden, and M. Xu, Efficient unitary designs and pseudorandom unitaries from permutations, arXiv preprint arXiv:2404.16751 (2024).
[23] F. Ma and H.-Y. Huang, How to construct random unitaries, arXiv preprint arXiv:2410.10116 (2024).
[24] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, Science **389**, 92 (2025).
[25] T. Schuster, F. Ma, A. Lombardi, F. Brandão, and H.-Y. Huang, Strong random unitaries and fast scrambling, arXiv preprint arXiv:2509.26310 (2025).
[26] L. Cui, T. Schuster, F. Brandão, and H.-Y. Huang, Unitary designs in nearly optimal depth, arXiv preprint arXiv:2507.06216 (2025).
[27] B. Foxman, N. Parham, F. Vasconcelos, and H. Yuen, Random unitaries in constant (quantum) time, arXiv preprint arXiv:2508.11487 (2025).
[28] X. Feng, Z. Cheng, and M. Ippoliti, Hardness of observing strong-to-weak symmetry breaking, arXiv preprint arXiv:2504.12233 (2025).
[29] T. Schuster, D. Kufel, N. Y. Yao, and H.-Y. Huang, Hardness of recognizing phases of matter, Forthcoming (2025).
[30] A. Gu, Y. Quek, S. Yelin, J. Eisert, and L. Leone, Simulating quantum chaos without chaos, arXiv preprint arXiv:2410.18196 (2024).
[31] C. Akers, A. Bouland, L. Chen, T. Kohler, T. Metger, and U. Vazirani, Holographic pseudoentanglement and the complexity of the ads/cft dictionary, arXiv preprint arXiv:2411.04978 (2024).
[32] A. Polkovnikov, K. Sengupta, A. Silva, and M. Vengalattore, Colloquium: Nonequilibrium dynamics of closed interacting quantum systems, Reviews of Modern Physics **83**, 863 (2011).
[33] R. Nandkishore and D. A. Huse, Many-body localization and thermalization in quantum statistical mechanics, Annu. Rev. Condens. Matter Phys. **6**, 15 (2015).

[34] C. Gogolin and J. Eisert, Equilibration, thermalisation, and the emergence of statistical mechanics in closed quantum systems, Reports on Progress in Physics **79**, 056001 (2016).
[35] D. Forster, *Hydrodynamic fluctuations, broken symmetry, and correlation functions* (CRC Press, 2018).
[36] P. Kovtun, Lectures on hydrodynamic fluctuations in relativistic theories, Journal of Physics A: Mathematical and Theoretical **45**, 473001 (2012).
[37] J. Sirker, R. Pereira, and I. Affleck, Diffusion and ballistic transport in one-dimensional quantum systems, Physical review letters **103**, 216602 (2009).
[38] C. W. von Keyserlingk, T. Rakovszky, F. Pollmann, and S. L. Sondhi, Operator hydrodynamics, otocs, and entanglement growth in systems without conservation laws, Physical Review X **8**, 021013 (2018).
[39] M. Ljubotina, M. Žnidarič, and T. Prosen, Kardar-parisi-zhang physics in the quantum heisenberg magnet, Physical review letters **122**, 210602 (2019).
[40] C. Zu, F. Machado, B. Ye, S. Choi, B. Kobrin, T. Mittiga, S. Hsieh, P. Bhattacharyya, M. Markham, D. Twitchen, *et al.*, Emergent hydrodynamics in a strongly interacting dipolar spin ensemble, Nature **597**, 45 (2021).
[41] D. Wei, A. Rubio-Abadal, B. Ye, F. Machado, J. Kemp, K. Srakaew, S. Hollerith, J. Rui, S. Gopalakrishnan, N. Y. Yao, *et al.*, Quantum gas microscopy of kardar-parisi-zhang superdiffusion, Science **376**, 716 (2022).
[42] A. Pal and D. A. Huse, Many-body localization phase transition, Physical Review B—Condensed Matter and Materials Physics **82**, 174411 (2010).
[43] J.-y. Choi, S. Hild, J. Zeiher, P. Schauß, A. Rubio-Abadal, T. Yefsah, V. Khemani, D. A. Huse, I. Bloch, and C. Gross, Exploring the many-body localization transition in two dimensions, Science **352**, 1547 (2016).
[44] C. J. Turner, A. A. Michailidis, D. A. Abanin, M. Serbyn, and Z. Papić, Weak ergodicity breaking from quantum many-body scars, Nature Physics **14**, 745 (2018).
[45] C. Moore, Unpredictability and undecidability in dynamical systems, Physical Review Letters **64**, 2354 (1990).
[46] N. Shiraishi and K. Matsumoto, Undecidability in quantum thermalization, Nature communications **12**, 5084 (2021).
[47] D. Devulapalli, T. Mooney, and J. D. Watson, The complexity of thermalization in finite quantum systems, arXiv preprint arXiv:2507.00405 (2025).
[48] C. Peikert *et al.*, A decade of lattice cryptography, Foundations and trends® in theoretical computer science **10**, 283 (2016).
[49] D. J. Bernstein and T. Lange, Post-quantum cryptography, Nature **549**, 188 (2017).
[50] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, Journal of the ACM **56**, 1 (2009).
[51] M. R. Albrecht, R. Player, and S. Scott, On the concrete hardness of learning with errors, Journal of Mathematical Cryptology **9**, 169 (2015).
[52] H.-Y. Huang, Learning quantum states from their classical shadows, Nature Reviews Physics **4**, 81 (2022).
[53] A. Anshu, D. Gosset, K. J. Morenz Korol, and M. Soleimanifar, Improved approximation algorithms for bounded-degree local hamiltonians, Physical Review Letters **127**, 250502 (2021).
[54] F. G. Brandao and A. W. Harrow, Product-state approximations to quantum ground states, in *Proceedings of the forty-fifth annual ACM symposium on Theory of computing* (2013) pp. 871–880.
[55] R. P. Feynman, Quantum mechanical computers., Found. Phys. **16**, 507 (1986).
[56] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*, 47 (American Mathematical Soc., 2002).
[57] D. K. Mark, F. Surace, A. Elben, A. L. Shaw, J. Choi, G. Refael, M. Endres, and S. Choi, Maximum entropy principle in deep thermalization and in hilbert-space ergodicity, Physical Review X **14**, 041051 (2024).
[58] W.-K. Mok, T. Haug, A. L. Shaw, M. Endres, and J. Preskill, Optimal conversion from classical to quantum randomness via quantum chaos, Physical Review Letters **134**, 180403 (2025).
[59] Y. Atia and D. Aharonov, Fast-forwarding of hamiltonians and exponentially precise measurements, Nature communications **8**, 1572 (2017).
[60] S. Gu, R. D. Somma, and B. Şahinoğlu, Fast-forwarding quantum evolution, Quantum **5**, 577 (2021).
[61] A. Y. Kitaev, Quantum measurements and the abelian stabilizer problem, arXiv preprint quant-ph/9511026 (1995).
[62] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Quantum algorithms revisited, Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **454**, 339 (1998).
[63] A. M. Dalzell, S. McArdle, M. Berta, P. Bienias, C.-F. Chen, A. Gilyén, C. T. Hann, M. J. Kastoryano, E. T. Khabiboulline, A. Kubica, *et al.*, Quantum algorithms: A survey of applications and end-to-end complexities, arXiv preprint arXiv:2310.03011 (2023).
[64] M. Sipser, Introduction to the theory of computation, ACM Sigact News **27**, 27 (1996).
[65] C. H. Papadimitriou, Computational complexity (Encyclopedia of computer science, 2003).
[66] S. Arora and B. Barak, *Computational complexity: a modern approach* (Cambridge University Press, 2009).
[67] L. J. Stockmeyer and A. R. Meyer, Word problems requiring exponential time (preliminary report), in *Proceedings of the fifth annual ACM symposium on Theory of computing* (1973) pp. 1–9.
[68] A. K. Chandra, D. C. Kozen, and L. J. Stockmeyer, Alternation, Journal of the ACM (JACM) **28**, 114 (1981).
[69] A. M. Turing *et al.*, On computable numbers, with an application to the entscheidungsproblem, J. of Math **58**, 5 (1936).
[70] A. Church, An unsolvable problem of elementary number theory, American journal of mathematics **58**, 345

(1936).
[71] D. S. Dummit, R. M. Foote, *et al.*, *Abstract algebra*, Vol. 3 (Wiley Hoboken, 2004).
[72] S. Lang, *Algebra*, Vol. 211 (Springer Science & Business Media, 2012).
[73] I. Stewart, *Galois theory* (Chapman and Hall/CRC, 2022).