

Computational Complexity of Unitary and State Design Properties


Yoshifumi Nakata^{1,*}, Yuki Takeuchi^{2,3,†}, Martin Kliesch⁴, and Andrew Darmawan¹

¹*Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto 606-8502, Japan*

²*NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

³*NTT Research Center for Theoretical Quantum Information, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

⁴*Institute for Quantum Inspired and Quantum Optimization, Hamburg University of Technology, 21079 Hamburg, Germany*

 (Received 17 January 2025; revised 27 May 2025; accepted 29 July 2025; published 9 September 2025)

We investigate unitary and state t -designs from a computational complexity perspective. First, we address the problems of computing frame potentials that characterize (approximate) t -designs. We present a quantum algorithm for computing frame potentials and establish the following: (1) exact computation can be achieved by a single query to a $\#P$ oracle and is $\#P$ -hard; (2) for state vectors, deciding whether the frame potential is larger than or smaller than certain values is BQP -complete, provided that the promise gap between the two values is inverse polynomial in the number of qubits; and (3) for both state vectors and unitaries, this promise problem is PP -complete if the promise gap is exponentially small. Second, we address the promise problem of deciding whether or not a given set is a good approximation to a design. Given a certain promise gap that could be constant, we show that this problem is PP -hard, highlighting the inherent computational difficulty of determining properties of unitary and state designs. We further identify implications of our results, including variational methods for constructing designs, diagnosing quantum chaos, and exploring emergent designs in Hamiltonian systems.

DOI: [10.1103/21vm-bz3t](https://doi.org/10.1103/21vm-bz3t)

I. INTRODUCTION

Quantum randomness is a fundamental resource in quantum information processing. It is commonly formulated by a *Haar-random unitary*, a unitary drawn uniformly at random with respect to the uniform probability measure on the unitary group, i.e., the normalized Haar measure. Applications of quantum randomness range from quantum cryptography [1–5], algorithms [6–10], and sensing [11–14], to quantum communication [15–24]. In theoretical physics, quantum randomness provides powerful tools to explore far-from-equilibrium dynamics, yielding novel insights into thermalization

[25–30], the holographic principle [31–33], and scrambling [34–40]. Experimentally, it plays a key role in benchmarking noisy quantum devices [41–50] and studying complex quantum many-body dynamics [51,52].

A Haar-random unitary is, however, computationally expensive, as most unitaries require exponentially many quantum gates to implement [53]. This fact necessitates approximations of a Haar-random unitary [54,55], among which a *unitary t -design* is a commonly used formulation. A unitary t -design is a random unitary that has the same t th moment as a Haar-random one. Similarly, a *state t -design* is defined as a random state vector that has the same t th moment as a *Haar-random state*, i.e., a state vector obtained by applying a Haar-random unitary to a fixed state vector. In many applications, unitary and state t -designs can be used instead of Haar-random ones.

Given their significance, implementations of designs have long been studied. While it has been known in combinatorial mathematics [56,57] that unitary and state t -designs exist for any t , their explicit constructions have been found only recently [58,59]. In quantum information, approximate implementations have attracted substantial

*Contact author: yoshifumi.nakata@yukawa.kyoto-u.ac.jp

†Present address: Information Technology R&D Center, Mitsubishi Electric Corporation.

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

attention. A standard approach is to use quantum circuits on n qubits [60–70], and it has recently been shown that $\mathcal{O}(t \log n/\delta)$ depth circuits suffice for generating the δ -approximation of a unitary t -design [69,70]. Another approach leverages the *frame potential*, which achieves its minimum for t -designs, enabling variational constructions of designs [71]. Additionally, implementations of designs that exploit quantum many-body dynamics offer a more exotic method [38,51,72–76], further introducing novel frameworks to study complex quantum many-body systems, such as *deep thermalization* [29,30] and *complete Hilbert-space ergodicity* [39,40].

In recent years, computation-theoretic properties of designs have also been studied, since designs and related concepts [51,54] have proven to be extremely useful for, e.g., cryptography uses [3–5]. A fundamental question in this context is: *Can we efficiently determine whether a given distribution constitutes a design?* Since designs can be characterized by the frame potential, this question can be reframed as: *Can we efficiently compute the frame potential?* Given the numerous applications of designs, these questions are not only foundational but also of practical importance.

In this paper, we formulate these questions as computational problems and initiate a computational complexity-theoretic analysis of unitary and state design properties. We begin by providing a quantum algorithm for estimating the frame potential and show that while the algorithm achieves $1/\text{poly}(n)$ accuracy for state vectors in polynomial time, where n is the number of qubits, achieving exponential accuracy or estimating the frame potential of unitaries takes exponential time.

To check if more efficient algorithms exist, we introduce and investigate computational problems about the frame potential. First, we show that *exactly* computing the frame potential can be achieved by a single query to a $\#\text{P}$ oracle and is $\#\text{P}$ -hard. We then consider a problem of *approximately* computing frame potentials. We formulate this as a promise problem to decide whether the frame potential of a given set is larger or smaller than certain values, with the promise that either one of the two is the case. For state vectors, this problem is shown to be BQP -complete and PP -complete if the promise gap between the two values is $\Theta(1/\text{poly}(n))$ and $\Theta(2^{-\text{poly}(n)})$, respectively. For unitaries, the problem is PP -complete if the promise gap is $\Theta(2^{-\text{poly}(n)})$. These results imply that general algorithms, whether quantum or classical, for computing the frame potential with exponential accuracy in polynomial time are unlikely to exist, indicating that our quantum algorithm cannot be drastically improved.

We also propose and investigate the problems more directly related to designs, i.e., promise problems to decide whether a given set is a δ -approximate t -design or not a δ' -approximate t' -design, where $t \leq t'$, under the promise

that only one of the two is the case. We show that this promise problem is in PP for $t = t'$ if the gap between δ' and δ is not too small. We also show that, for any $t \leq t'$, this problem is PP -hard if $\delta' - \delta \in \Theta(2^{c(t'-t)n}\delta)$ for $t < t'$ and $\delta' - \delta \in \Theta(2^{-cn}\delta)$ for $t = t'$, where $c = 1$ for a set of state vectors and $c = 2$ for a set of unitaries. This result is particularly remarkable when $t' = t + 1$. By setting δ as $\Theta(2^{-n})$ for state vectors and $\Theta(2^{-2n})$ for unitaries, our result implies that it is PP -hard to decide if a given set is an exponentially accurate approximation to a t -design or a worse-than-constant approximation to a $(t + 1)$ -design that is not an exponentially accurate approximate t -design. This large gap in the approximation accuracy in particular demonstrates the computationally hard nature of checking unitary and state design properties.

Due to the broad generality of our complexity-theory-based approach and the universal significance of unitary and state designs, our results have the following immediate implications:

- (1) *Variational constructions of designs.* A promising application of the frame potentials is a variational construction of designs [71]. Our results suggest that variational methods with a general ansatz do not scale due to the absence of efficient algorithms for computing frame potentials, highlighting the crucial importance of choosing a good ansatz.
- (2) *Quantum chaos through OTOCs.* The frame potential of a set of unitaries is closely related to the out-of-time-ordered correlators (OTOCs) [37]. Therefore, our hardness results for computing frame potentials directly apply to OTOCs. As OTOCs are used to diagnose quantum chaos [36], this reveals the complex nature of quantum chaos from a computational viewpoint, establishing a connection between quantum many-body physics and complexity theory.
- (3) *Designs in quantum many-body systems.* Several lines of evidence suggest that sufficiently complex quantum many-body Hamiltonian dynamics are highly useful for generating a unitary or state design [38,51,72–76]. Except a few solvable cases in the thermodynamic limit [74,75], most studies rely on numerical simulations. Our results indicate that direct numerical simulations do not scale unless they are specifically tailored to the Hamiltonian dynamics being investigated.

This paper is organized as follows. We begin with preliminaries in Sec. II, where we explain our notation and overview basic properties of unitary and state designs. Our results and their implications are all summarized in Sec. III. Proofs are provided in Secs. IV, V, and VI. After the conclusions in Sec. VII, we provide supplementary proofs in the appendices.

II. PRELIMINARIES

We introduce our notation in Sec. II A. A brief overview of unitary and state designs is provided in Sec. II B. The computational complexity classes that we use are summarized in Sec. II C.

A. Notation

We use the Schatten p -norms for linear operators, which are defined by $\|X\|_p := (\text{Tr}[|X|^p])^{1/p}$ ($p \in [1, \infty]$) with $|X| = \sqrt{X^\dagger X}$. We particularly use the trace ($p = 1$), the Hilbert-Schmidt ($p = 2$), and the spectral ($p = \infty$) norms. They satisfy

$$\begin{aligned} \|O\|_\infty &\leq \|O\|_2 \leq \|O\|_1 \\ &\leq \sqrt{\text{rank}(O)} \|O\|_2 \leq \text{rank}(O) \|O\|_\infty. \end{aligned} \quad (1)$$

For superoperators, we use the diamond norm $\|\cdot\|_\diamond$, which is defined by $\|\mathcal{T}\|_\diamond = \max_{n \geq 1} \|\mathcal{T} \otimes \text{id}_n\|_{1 \rightarrow 1}$, where id_n is the identity map on the n -dimensional Hilbert space, and $\|\mathcal{E}\|_{1 \rightarrow 1} = \max_X \|\mathcal{E}(X)\|_1 / \|X\|_1$, with the maximization over all nonzero operators X .

Throughout the paper, we consider probability measures over multisets of state vectors or unitaries. An average is written as $\mathbb{E}_{|\psi\rangle \sim \mu}[\cdot]$ for the probability measure μ of state vectors and as $\mathbb{E}_{U \sim \nu}[\cdot]$ for the probability measure ν of unitaries. When a finite multiset of state vectors or unitaries is given, the uniform distribution over the multiset is naturally defined. Hence, with a slight abuse of notation, we use the same symbol for the multiset and the uniform distribution over the multiset. For instance, for a finite multiset of state vectors $\mathcal{S} = \{|\psi_j\rangle\}_{j=1, \dots, K}$, we express its average such as $\mathbb{E}_{|\psi\rangle \sim \mathcal{S}}[\cdot] = 1/K \sum_{j=1}^K (\cdot)$. Hereafter, we refer to a multiset as a set unless it is necessary to clearly distinguish them.

An important probability measure on the unitary group $\mathbb{U}(d)$ is the (normalized) *Haar* measure \mathbb{H} . A unitary U drawn uniformly at random with respect to the Haar measure \mathbb{H} is called a Haar-random unitary and is conventionally denoted by $U \sim \mathbb{H}$.

By applying a Haar-random unitary to a fixed state vector $|\varphi_0\rangle$, a unitarily invariant probability measure on the set of all state vectors can be defined, which we call a *Haar-random state*. Due to the unitarily invariant property of a Haar-random unitary, a Haar-random state is independent of the choice of the fixed vector $|\varphi_0\rangle$. Similarly to a Haar-random unitary, we use the notation $|\varphi\rangle \sim \mathbb{H}$ for a Haar-random state.

B. Unitary and state designs

We provide a brief overview of definitions and important properties of state and unitary designs.

1. State designs

In the original definition from design theory [56,57], a state t -design ($t \in \mathbb{Z}^+$) is defined as the uniform distribution over a finite set (not a multiset) of state vectors that has the same t th moment as a Haar-random state. However, in quantum information, it is common to define a design as the uniform distribution over a finite multiset, which more closely aligns with the concept of a *weighted* t -design in design theory. We follow the convention in quantum information and adopt the following definition of a state design.

Definition 1 (δ -approximate state t -design). When the uniform probability measure over a finite multiset \mathcal{S} of d -dimensional state vectors satisfies

$$\left\| \mathbb{E}_{|\psi\rangle \sim \mathcal{S}} [|\psi\rangle\langle\psi|^{\otimes t}] - \mathbb{E}_{|\psi\rangle \sim \mathbb{H}} [|\psi\rangle\langle\psi|^{\otimes t}] \right\|_\infty \leq \frac{\delta}{d_t}, \quad (2)$$

it is called a δ -approximate state t -design. Here, $d_t = \binom{d+t-1}{t}$ is the dimension of the symmetric subspace in $(\mathbb{C}^d)^{\otimes t}$. When $\delta = 0$, it is called an *exact* state t -design.

The expectation of the second term in Eq. (2) can be explicitly spelt out using Schur-Weyl duality. Denoting by Π_{sym} the projection onto the symmetric subspace in $(\mathbb{C}^d)^{\otimes t}$, we have

$$\mathbb{E}_{|\psi\rangle \sim \mathbb{H}} [|\psi\rangle\langle\psi|^{\otimes t}] = \frac{\Pi_{\text{sym}}}{d_t}. \quad (3)$$

In Definition 1, we measure the approximation precision by using the spectral norm following one of the original proposals [77]. In recent years, the trace norm has also been used instead, to define a δ -approximate state t -design by

$$\left\| \mathbb{E}_{|\psi\rangle \sim \mathcal{S}} [|\psi\rangle\langle\psi|^{\otimes t}] - \mathbb{E}_{|\psi\rangle \sim \mathbb{H}} [|\psi\rangle\langle\psi|^{\otimes t}] \right\|_1 \leq \delta. \quad (4)$$

This definition is weaker than Definition 1 in the sense that Eq. (2) implies Eq. (4), which is due to Eq. (1) and the fact that the support of the operators is the symmetric subspace in $(\mathbb{C}^d)^{\otimes t}$. Hence we use Definition 1 in this paper.

A useful quantity that characterizes a state design is a *state frame potential*.

Definition 2 (State frame potential). Let μ be a probability measure on a multiset of state vectors. The state frame potential of degree t , $F_t(\mu)$, is defined as

$$F_t(\mu) := \left\| \mathbb{E}_{|\psi\rangle \sim \mu} [|\psi\rangle\langle\psi|^{\otimes t}] \right\|_2^2 \quad (5)$$

$$= \mathbb{E}_{|\psi\rangle, |\phi\rangle \sim \mu} [|\langle\psi|\phi\rangle|^{2t}]. \quad (6)$$

Important properties of the state frame potential are summarized in Proposition 1. These properties are well

known, but for completeness, we provide a proof in Appendix A. Note that the assumption $t \leq d$ in Proposition 1 is for the sake of convenience. Even if it is not satisfied, similar statements hold.

Proposition 1. Let $d, t \in \mathbb{Z}^+$ be such that $t \leq d$, and let $d_t = \binom{d+t-1}{t}$. The following hold for the state frame potential of degree t :

- (1) $F_t(\mathbb{H}) = 1/d_t$.
- (2) For any probability measure μ on a nonempty set of state vectors,

$$F_t(\mu) \in [1/d_t, 1], \quad (7)$$

where equality of the lower bound holds if and only if it is an exact state t -design. For the uniform measure on a finite set \mathbb{S} with cardinality K ,

$$F_t(\mathbb{S}) \in [\max\{1/d_t, 1/K\}, 1]. \quad (8)$$

- (3) If a finite set \mathbb{S} of state vectors is a δ -approximate state t -design, then

$$F_t(\mathbb{S}) \leq \frac{1}{d_t} + \frac{\delta^2}{d_t}. \quad (9)$$

- (4) If a finite set \mathbb{S} of state vectors satisfies

$$F_t(\mathbb{S}) \leq \frac{1}{d_t} + \frac{\delta^2}{d_t^2}, \quad (10)$$

then \mathbb{S} is a δ -approximate state t -design.

- (5) For a finite set \mathbb{S} of state vectors to be a δ -approximate state t -design, it has to contain at least $K_{\text{st}}(d, t, \delta)$ state vectors, where

$$K_{\text{st}}(d, t, \delta) := \frac{d_t}{1 + \delta^2}. \quad (11)$$

From property (2) in Proposition 1, one observes that the frame potential is indeed a potential in the sense that a state t -design can be obtained by minimizing the frame potential of degree t . This is extended to approximate state designs by properties (3) and (4). However, if the frame potential $F_t(\mathbb{S})$ takes the value such as

$$\frac{1}{d_t} + \frac{\delta^2}{d_t^2} < F_t(\mathbb{S}) < \frac{1}{d_t} + \frac{\delta^2}{d_t}, \quad (12)$$

we cannot conclude whether or not the set is a δ -approximate unitary t -design. The final property (5) implies that if a set has small cardinality, it cannot be a state design. This is naturally expected, as state designs should be able to mimic the uniform distribution over the set of all state vectors.

2. Unitary designs

To define a δ -approximate unitary t -design, it is convenient to use the *moment operator of degree t* of a probability measure of unitaries. So, let μ be a probability measure on the unitary group $\mathbb{U}(d)$. The moment operator is given by

$$M_\mu^{(t)} := \mathbb{E}_{U \sim \mu} [U^{\otimes t} \otimes \bar{U}^{\otimes t}], \quad (13)$$

where $\bar{\cdot}$ denotes the complex conjugate in a fixed orthonormal basis.

Based on the moment operator, a unitary t -design can be defined as follows.

Definition 3 (δ -approximate unitary t -design). When the uniform probability measure over a finite multiset $\mathbb{U} = \{U_j\}_{j=1, \dots, K}$ satisfies

$$\left\| M_{\mathbb{U}}^{(t)} - M_{\mathbb{H}}^{(t)} \right\|_1 \leq \delta, \quad (14)$$

it is called a δ -approximate unitary t -design. When $\delta = 0$, it is called an *exact* unitary t -design.

Similarly to state designs, Schur-Weyl duality allows us to identify the expectation in Eq. (14) over the Haar measure. Let $\pi_t : U \in \mathbb{U}(d) \mapsto U^{\otimes t} \otimes \bar{U}^{\otimes t}$ be a representation of the unitary group $\mathbb{U}(d)$. Then, taking the expectation yields a projection onto trivial irreducible representations of π_t .

Approximate unitary designs can also be defined in terms of different norms to measure the approximation. One of the standard definitions is based on the diamond norm of superoperators. For a given probability measure μ on the unitary group $\mathbb{U}(d)$, let $\mathcal{G}_\mu^{(t)}$ be the CPTP map given by

$$\mathcal{G}_\mu^{(t)}(X) = \mathbb{E}_{U \sim \mu} [U^{\otimes t} X U^{\dagger \otimes t}], \quad (15)$$

where X is an operator on a d^t -dimensional Hilbert space. A δ -approximate unitary t -design in terms of the diamond norm is the uniform probability measure over a finite multiset \mathbb{U} that satisfies

$$\left\| \mathcal{G}_{\mathbb{U}}^{(t)} - \mathcal{G}_{\mathbb{H}}^{(t)} \right\|_{\diamond} \leq \delta. \quad (16)$$

While these two definitions are not exactly the same, using either one generally does not yield significant differences in applications of unitary designs. Indeed, if \mathbb{U} is a δ -approximate unitary t -design in one of the two definitions, then \mathbb{U} is a $(\text{poly}(d^t)\delta)$ -approximate unitary t -design

in the other definition. This is guaranteed by

$$\begin{aligned} d^{-2t} \left\| M_{\mathbf{U}}^{(t)} - M_{\mathbf{H}}^{(t)} \right\|_1 &\leq \left\| \mathcal{G}_{\mathbf{U}}^{(t)} - \mathcal{G}_{\mathbf{H}}^{(t)} \right\|_{\diamond} \\ &\leq d^t \left\| M_{\mathbf{U}}^{(t)} - M_{\mathbf{H}}^{(t)} \right\|_1 \end{aligned} \quad (17)$$

(for the derivation, see the comment after Proposition 2). As most circuit constructions of δ -approximate unitary t -designs on n qubits use $\text{poly}(n, t, \log 1/\delta)$ gates [60–70], the overhead of the number of gates due to the factor $\text{poly}(d^t) = \text{poly}(2^{tm})$ in the approximation accuracy δ is only linear in tm , which is not dominant in most cases.

It is also important that one can, in general, amplify the approximation accuracy simply by repeating the unitaries. That is, for any δ -approximate unitary t -design $\mathbf{U} = \{U_j\}_j$ in terms of the moment operators (Definition 3), $\mathbf{U}^m = \{U_{j_m} \dots U_{j_1}\}_{j_1, \dots, j_m}$ is a $(d^t \delta^m)$ -approximate or even better unitary t -design in terms of the diamond norm. Hence, if one has an accurate approximate unitary t -design in terms of the moment operators, such as $\delta = d^{-1}$, it can be converted to an accurate approximate t -design in the diamond norm by a constant number of repetitions.

For these reasons, we mostly focus on the definition based on Definition 3 in this work.

Unitary designs are also characterized by the unitary frame potential. With a slight abuse of notation, we use the same symbol F_t as the state frame potential.

Definition 4 (Unitary frame potential). Let μ be a probability measure of unitaries. The unitary frame potential of degree t is defined as

$$F_t(\mu) := \|M_{\mu}^{(t)}\|_2^2 = \mathbb{E}_{U, V \sim \mu} \left[|\text{Tr}[U^\dagger V]|^{2t} \right]. \quad (18)$$

The unitary frame potential has similar properties to the state frame potential, which are summarized in Proposition 2. The assumption $t \leq d$ in the proposition is for the sake of simplicity. A proof is provided in Appendix A, to be self-contained.

Proposition 2. Let $d, t \in \mathbb{Z}^+$ be such that $t \leq d$. The following hold for the unitary frame potential:

- (1) $F_t(\mathbf{H}) = t!$.
- (2) For any probability measure μ on a nonempty set in $\mathbb{U}(d)$,

$$F_t(\mu) \in [t!, d^{2t}], \quad (19)$$

where equality of the lower bound holds if and only if it is an exact unitary t -design. For the uniform measure on a finite set \mathbf{U} with cardinality K ,

$$F_t(\mathbf{U}) \in [\max\{t!, d^{2t}/K\}, d^{2t}]. \quad (20)$$

- (3) If a finite set \mathbf{U} of unitaries is a δ -approximate unitary t -design, then

$$F_t(\mathbf{U}) \leq t! + \delta^2. \quad (21)$$

- (4) If a finite set \mathbf{U} of unitaries satisfies

$$F_t(\mathbf{U}) \leq t! + \frac{\delta^2}{d^{2t}}, \quad (22)$$

then \mathbf{U} is a δ -approximate unitary t -design.

- (5) For a finite set \mathbf{U} of unitaries to be a δ -approximate unitary t -design, it has to contain at least $K_{\text{uni}}(d, t, \delta)$ unitaries, where

$$K_{\text{uni}}(d, t, \delta) := \frac{d^{2t}}{t! + \delta^2}. \quad (23)$$

- (6) Let $\mathcal{G}_{\mu}^{(t)}$ be the superoperator defined by Eq. (15) for a probability measure μ on $\mathbb{U}(d)$. For a finite set \mathbf{U} of unitaries, it satisfies

$$\begin{aligned} d^{-t} \sqrt{F_t(\mathbf{U}) - F_t(\mathbf{H})} &\leq \left\| \mathcal{G}_{\mathbf{U}}^{(t)} - \mathcal{G}_{\mathbf{H}}^{(t)} \right\|_{\diamond} \\ &\leq d^t \sqrt{F_t(\mathbf{U}) - F_t(\mathbf{H})}. \end{aligned} \quad (24)$$

The final property (6) implies Eq. (17) by using the fact that

$$\left\| M_{\mathbf{U}}^{(t)} - M_{\mathbf{H}}^{(t)} \right\|_2 = \sqrt{F_t(\mathbf{U}) - F_t(\mathbf{H})} \quad (25)$$

and Eq. (1).

C. Complexity classes

The standard idea for characterizing the difficulty of a computational problem is to identify which complexity class the problem belongs to and to show that it is among the most difficult problems in that class. We briefly review the complexity classes #P, PP, PQP, BQP, and $\text{FP}^{\#\text{P}}$, which are important for this work.

The class #P is a set of all problems of counting the number of accepting paths of a nondeterministic polynomial-time Turing machine. By definition, the output of a #P-problem is a non-negative integer.

We take the common view in quantum information theory that the classes PP, PQP, and BQP are *promise problems* [78,79]. For such a problem, the answer is either true or false but has to be given (correctly) only for certain problem instances, which are specified by a promise. That is, each problem comes along with a potential promise and only has to be solved when it is fulfilled.

The class PP is the set of promise problems for each of which some classical algorithm with polynomially bounded run-time (more formally, a probabilistic

TABLE I. A summary of the problems that we introduce in this paper and our results about their computational complexity. As our main focus is on state and unitary designs, we have assumed here that the cardinality of the set is at least $K_{\text{st}}(2^n, t, \delta)$ for a set of state vectors and $K_{\text{uni}}(2^n, t, \delta)$ for a set of unitaries. See the respective theorems for the cases that do not satisfy these assumptions.

		Compute FP	Decide: $\text{FP} \geq \alpha$ versus $\text{FP} \leq \alpha - \epsilon$		Decide: a δ -approximate t -design or not a δ' -approximate t' -design
State vectors	Problem	$\text{compSFP}(t)$ (Problem 1)	$\text{SFP}(t, \epsilon)$ (Problem 3)		$\text{StDes}(t, t', \delta, \delta')$ (Problem 5)
	Complexity	$\text{FP}^{\#\text{P}} \cap \#\text{P-hard}$ (Theorems 3 and 4)	$\text{BQP-complete for } \epsilon \in \Omega(1/\text{poly}(n))$ (Theorems 7 and 8)	$\text{PP-complete for } \epsilon \in \Theta(2^{-\text{poly}(n)})$ (Theorems 9 and 10)	PP for $t = t'$ and suitable δ and δ' . PP-hard if $\delta' - \delta \in \begin{cases} \Theta(2^{(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-n}\delta), & \text{for } t = t'. \end{cases}$ (Theorems 13 and 14)
Unitaries	Problem	$\text{compUFP}(t)$ (Problem 2)	$\text{UFP}(t, \epsilon)$ (Problem 4)		$\text{UniDes}(t, t', \delta, \delta')$ (Problem 6)
	Complexity	$\text{FP}^{\#\text{P}} \cap \#\text{P-hard}$ (Theorems 5 and 6)	$\text{PP-complete for } \epsilon \in \Theta(2^{-\text{poly}(n)})$ (Theorems 11 and 12)		PP for $t = t'$ and suitable δ and δ' . PP-hard if $\delta' - \delta \in \begin{cases} \Theta(2^{2(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-2n}\delta), & \text{for } t = t'. \end{cases}$ (Theorems 15 and 16)

polynomial-time Turing machine) can output their correct answer with probability strictly larger than $1/2$. Since the probability may be exponentially close to $1/2$, PP contains the problems that are unlikely to be solvable by classical algorithms in polynomial time. The class PQP is a quantum analog of PP , in which the probabilistic polynomial-time Turing machine is replaced with a polynomial-time quantum algorithm. The class BQP is defined similarly to PQP but with a higher success probability of $\geq 2/3$.

Obviously, $\text{BQP} \subseteq \text{PQP}$ and $\text{PP} \subseteq \text{PQP}$. It is also known that $\text{PQP} \subseteq \text{PP}$ [79]. Hence $\text{BQP} \subseteq \text{PQP} = \text{PP}$. It is expected that $\text{BQP} \neq \text{PQP}$, i.e., $\text{PQP} = \text{PP}$ is expected to contain problems that are intractable even for scalable universal quantum computers.

We will rely on the concepts of hard and complete problems. Informally, a problem is *hard* for some class if it is at least as difficult as the most difficult problem of that class in the sense that a solver for that problem can be used to solve any other problem of the class with some “small overhead.” Technically, hardness is always defined with respect to a specific type of reduction, which depends on the class in question. If a problem is hard for some class and, at the same time, a member of that class, then it is *complete* for that class.

Particularly important complete problems in this work are $\#\text{SAT}$ and MAJ-SAT , which are $\#\text{P}$ -complete and PP -complete problems, respectively.

Definition 5 (#SAT). Given the input as a classically efficiently computable function $f : \{0, 1\}^N \rightarrow \{0, 1\}$ specified by a Boolean circuit, output the number of $x \in \{0, 1\}^N$ satisfying $f(x) = 1$.

Note that this problem $\#\text{SAT}$ is equivalent to calculating the number of satisfying assignments of a Boolean formula, which is the origin of its name.

Definition 6 (MAJ-SAT [80]). Let $f : \{0, 1\}^m \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time and let $s(f)$ be $\sum_{x \in \{0, 1\}^m} f(x)$. Decide whether $0 \leq s(f) < 2^{m-1}$ or $2^{m-1} \leq s(f) \leq 2^m$.

Theorem 1 (See, e.g., Ref. [81]). $\#\text{SAT}$ is $\#\text{P}$ -complete and MAJ-SAT is PP -complete.

Finally, $\text{FP}^{\#\text{P}}$ is the class of functions that can be computed by a deterministic algorithm in polynomial time with additional query access to a solver for $\#\text{SAT}$. That is, once a part of the algorithm has specified an instance of $\#\text{SAT}$, its solution can be obtained in a single computation step.

III. MAIN RESULTS

In this section, we provide our main results about complexities of various computational problems. We begin with a condition that must be satisfied by the sets of states or unitaries for our complexity results to hold, and then summarize our results. A summary of our complexity results is also given in Table I. The proofs will be provided in later sections. As usual, if necessary, complex numbers are represented by floating-point numbers, with finite precision controlled by the number of digits.

A. Data format for sets of states and unitaries

When we consider computational problems related to unitary or state designs, it is natural to suppose that the

input of the problem is a set of unitaries acting on \mathbb{C}^d or states in \mathbb{C}^d . If a set consists of $\text{poly}(d)$ elements, such problems may be tractable in polynomial time with respect to d . However, in a quantum setting, it is standard to start with quantum circuits on $n = \log_2 d$ qubits consisting of $\text{poly}(n)$ gates and to ask about the efficiency in terms of n . Throughout the paper, we focus on such situations.

When concerned with designs on n qubits, we need to deal with the set consisting of $\Omega(\exp(n))$ elements. In fact, property (5) in Proposition 1 and property (5) in Proposition 2 imply that a set S of n -qubit state vectors with cardinality $|S| < K_{\text{st}}(2^n, t, \delta)$ is not a δ -approximate state t -design and that a set U of n -qubit unitaries with cardinality $|U| < K_{\text{uni}}(2^n, t, \delta)$ is not a δ -approximate unitary t -design. Note that both $K_{\text{st}}(2^n, t, \delta)$ and $K_{\text{uni}}(2^n, t, \delta)$ are exponentially large in n .

To efficiently handle a set with an exponentially large cardinality, the set should be well structured. We formalize this by introducing a *set of unitaries with a computationally efficient description*.

Definition 7 (Computationally efficient descriptions). A multiset $U = \{U_j\}_{j=1}^K \subseteq \mathbb{U}(2^n)$ of n -qubit unitaries, where $K \in \mathcal{O}(2^{\text{poly}(n)})$, is said to have a *computationally efficient description* if it is specified by a partial function f defined on $\{0, 1\}^m$ with $m := \lceil \log_2 K \rceil$, which is computable in classical polynomial time, that outputs a classical description $f(j)$ ($j \in \{0, 1\}^m$) of a $\text{poly}(n)$ -sized quantum circuit of U_j .

Trivial instances of a set of unitaries with a computationally efficient description are a set of n -qubit Pauli operators and that of n -qubit Clifford unitaries. The former can be specified by $2n$ bits $x \in \{0, 1\}^{2n}$, and the description $f(x)$ specifies a tensor product of single-qubit Pauli unitaries, which is a quantum circuit with depth 1. The latter can be similarly specified by $\mathcal{O}(\text{poly}(n))$ bits with a suitable efficiently computable function f that identifies a Clifford circuit of circuit size $\mathcal{O}(n^2/\log(n))$, which is sufficient to represent any Clifford unitary [82].

A set of n -qubit unitaries appearing in a *one-dimensional local random quantum circuit (1D LRC)* with $\mathcal{O}(\text{poly}(n))$ depth is also an important instance of a set with a computationally efficient description. A 1D LRC repeats two layers of two-qubit unitaries organized in a brickwork fashion. In the first layer, two-qubit gates, each randomly and independently drawn from a fixed gate set \mathcal{G} , are applied to odd-even qubits in parallel. Similarly, in the second layer, random and independent two-qubit gates from \mathcal{G} are applied to even-odd qubits. To specify each quantum circuit generated in this way, we need $\mathcal{O}(\{\# \text{ of gates}\} \log_2 |\mathcal{G}|)$ bits, where $|\mathcal{G}|$ is the cardinality of the gate set \mathcal{G} . The number of gates is $\mathcal{O}(\text{poly}(n))$ whenever the depth is $\mathcal{O}(\text{poly}(n))$. In a standard case, $|\mathcal{G}|$ is constant, but even if $|\mathcal{G}| \in \mathcal{O}(\exp(n))$, each quantum

circuit generated in this way can be specified by $\text{poly}(n)$ bits (in the latter case, we need to assume that each gate in \mathcal{G} has a constant-size description). This is also the case for local random quantum circuits on any graph in which the graph describes the two qubits to which a two-qubit gate is applied.

Other important sets of unitaries are those generated by Hamiltonian dynamics. When a Hamiltonian H satisfies certain conditions, it is known that the corresponding time evolution e^{-itH} can be simulated efficiently in terms of the time t by quantum circuits with small error (see, e.g., Ref. [83]). Hence, by sampling discrete times $t_j \in [0, \text{poly}(n)]$ ($j = 1 \dots, K$ with $K \in \Theta(2^{\text{poly}(n)})$) in an efficiently computable manner, we can define a set $\{e^{-iH_j t_j}\}_{j=1}^K$ of unitaries with computationally efficient descriptions. This type of set of unitaries may be of particular interest in numerical or experimental approaches to the emergent designs in quantum many-body systems [38, 51, 72–76]. Note that in numerical or experimental settings, continuous degrees of freedom typically must be discretized and, hence, it is natural to consider discrete choices of time. Instead of discrete times, one may also consider a set of Hamiltonians $\{H_j\}_{j=1}^K$ and one may define $\{e^{-iH_j t}\}_{j=1}^K$ at a fixed time $t \in \mathcal{O}(\text{poly}(n))$. This set also has a computationally efficient description as far as the Hamiltonian dynamics can be simulated efficiently by quantum circuits.

We also introduce a *set of state vectors with a computationally efficient description*. It is a set of state vectors generated by applying a set of unitaries with a computationally efficient description to a fixed initial state vector that can be prepared in a quantum polynomial time, such as a computational-basis state.

B. Quantum algorithm for computing frame potentials

Propositions 1 and 2 imply that we can check if a given set of unitaries or states is a unitary or state design by computing their frame potentials. This motivates us to first provide quantum algorithms for estimating the unitary and state frame potentials. The idea behind the quantum algorithm comes from the fact that the frame potentials are defined by a sum of inner products between state vectors or unitaries. By “encoding” all the inner products into a single quantum state, we can compute the frame potential.

In Fig. 1, we provide a key quantum circuit of our quantum algorithm, which is based on a multiqubit controlled unitary $\text{ctrl-}U_n$ constructed from the set U_n of unitaries to be investigated. In the case of state vectors, U_n is a set of unitaries that generates the state vectors. Let us denote $U_n = \{U_j\}_{j=1, \dots, K_n}$, and let A be a κ_n -qubit system ($\kappa_n := \log K_n$) and B_m be an n -qubit system ($m = 1, \dots, t$). We define the controlled unitary $\text{ctrl}^A\text{-}U_n^{B_m}$ as

$$\text{ctrl}^A\text{-}U_n^{B_m} := \sum_{j=1}^{K_n} |j\rangle\langle j|^A \otimes U_j^{B_m}. \quad (26)$$

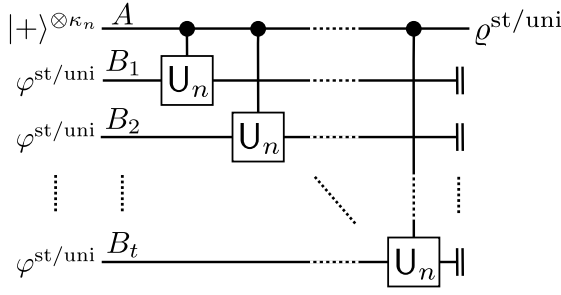


FIG. 1. A key quantum circuit for estimating the state or unitary frame potentials of degree t . The system A consists of $\kappa_n = \log K_n$ qubits, initially prepared in $|+\rangle^{\otimes \kappa_n}$. Each B_m ($m = 1, \dots, t$) is an n -qubit system and is initially prepared in $\varphi^{st} := |0\rangle\langle 0|^{\otimes n}$ and $\varphi^{uni} := I/2^n$ for computing the state and unitary frame potentials, respectively. Each multiqubit-controlled unitary applies U_j onto B_m when A is in $|j\rangle$. The value of the state or unitary frame potential can be obtained from the purity of the output state $\varrho^{st/uni}$ on A .

Note that when U_n has a computationally efficient description, the controlled unitary $\text{ctrl-}U_n$ can be efficiently implemented by quantum circuits obtained from classically controlling the Boolean function f that classically specifies the $\text{poly}(n)$ -sized quantum circuit. Denoting $B_1 \dots B_t$ simply by B , which is a (tn) -qubit system in total, we define

$$\text{ctrl}^A\text{-}U_n^B := \prod_{m=1}^t \text{ctrl}^A\text{-}U_n^{B_m}. \quad (27)$$

Denoting $|+\rangle^{\otimes \kappa_n}$ by $|+_{\kappa_n}\rangle$, $|0\rangle^{\otimes n}$ by $|0_n\rangle$, and a maximally entangled state between B_m and R_m by $|\Phi_n\rangle^{B_m R_m}$, we introduce

$$|\varrho_{st}\rangle^{AB} = \text{ctrl}^A\text{-}U_n^B \left(|+_{\kappa_n}\rangle^A \bigotimes_{m=1}^t |0_n\rangle^{B_m} \right), \quad (28)$$

$$|\varrho_{uni}\rangle^{ABR} = \text{ctrl}^A\text{-}U_n^B \left(|+_{\kappa_n}\rangle^A \bigotimes_{m=1}^t |\Phi_n\rangle^{B_m R_m} \right). \quad (29)$$

Note that the former is the output state of the circuit in Fig. 1, when the initial states in B_m are φ^{st} , and the latter is a purification of the output state of the circuit in Fig. 1, when the initial states in B_m are φ^{uni} , where $R = R_1 \dots R_t$ is the purifying system.

We then have the following lemma about the frame potentials.

Lemma 1. Let ϱ_{st}^A and ϱ_{uni}^A be the reduced density matrix in A of $|\varrho_{st}\rangle^{AB}$ and $|\varrho_{uni}\rangle^{ABR}$, respectively. Then, the state frame potential of $S_n = \{U_j|0_n\rangle\}_{j=1, \dots, K_n}$ and the unitary

frame potential of U_n are given by

$$F_t(S_n) = \text{Tr}[(\varrho_{st}^A)^2], \quad F_t(U_n) = 2^{2nt} \text{Tr}[(\varrho_{uni}^A)^2], \quad (30)$$

respectively.

Lemma 1 implies that the frame potentials can be evaluated by the purities of the corresponding quantum states, which can be achieved by, e.g., the SWAP test or an amplitude-estimation algorithm. This leads to the following theorem.

Theorem 2. Let U_n be a set of n -qubit unitaries with a computationally efficient description, the cardinality of which is K_n , and let S_n be a set of n -qubit state vectors with a computationally efficient description that is generated by applying the U_n to a computational zero state $|0_n\rangle$. The following hold:

- (1) For $\eta \in (\max\{d_t^{-1}, K_n^{-1}\}, 1]$ and $\epsilon \in (0, \eta - K_n^{-1})$, it takes tM_{st} queries to $\text{ctrl-}U_n$ and its inverse to determine whether $F_t(S_n) \geq \eta$ or $F_t(S_n) \leq \eta - \epsilon$ with success probability at least $2/3$, where

$$M_{st} := \mathcal{O}\left(\frac{1}{\epsilon} \min\left\{\sqrt{\eta K_n - 1}, 1\right\}\right). \quad (31)$$

- (2) For $\eta \in (\max\{t!, 2^{2nt} K_n^{-1}\}, 2^{2nt}]$ and $\epsilon \in (0, \eta - 2^{2nt} K_n^{-1})$, it takes tM_{uni} queries to $\text{ctrl-}U_n$ and its inverse to determine whether $F_t(U_n) \geq \eta$ or $F_t(U_n) \leq \eta - \epsilon$ with success probability at least $2/3$, where

$$M_{uni} := \mathcal{O}\left(\frac{2^{nt}}{\epsilon} \min\left\{\sqrt{\eta K_n - 2^{2nt}}, 2^{nt}\right\}\right). \quad (32)$$

The details of Lemma 1 and Theorem 2 are provided in Appendix B.

For a set of state vectors, the complexity of this quantum algorithm is determined merely by the required accuracy ϵ . This is because the algorithm uses $\kappa_n = \log K_n$ ancillary qubits and tM_{st} queries to $\text{ctrl-}U$, both of which are efficient if a set of state vectors has a computationally efficient description. Also, M_{st} is at most $\mathcal{O}(\epsilon^{-1})$. Thus, one can estimate the state frame potential with $1/\text{poly}(n)$ accuracy in $\text{poly}(n)$ time for sets of n -qubit state vectors with computationally efficient descriptions. On the other hand, the algorithm fails to estimate the state frame potential with $1/\exp(n)$ accuracy in polynomial time. We will see below that improving this algorithm is unlikely to be possible.

In contrast, this algorithm fails to compute the unitary frame potential in polynomial time even for, e.g., constant accuracy. This is merely due to the factor 2^{nt} in Eq. (32), which can be further traced back to the fact that $\text{Tr}[(\varrho_{uni}^A)^2]$ should be evaluated with at least exponential accuracy for estimating $F_t(U)$ with constant accuracy [see Eq. (30)].

C. Complexity of computing frame potentials

To address the question of whether the quantum algorithm can be improved, we formulate and investigate the problems of computing the frame potentials in a complexity-theoretic manner. We first formulate the problem of computing the state frame potential as $\text{compSFP}(t)$.

Problem 1 ($\text{compSFP}(t)$).

Input:

- (1) a set S_n of state vectors of n qubits with a computationally efficient description
- (2) $t \in \mathbb{Z}^+$ (degree)

Output: the state frame potential $F_t(S_n)$ of degree t .

In the definition of $\text{compSFP}(t)$, we do not put any assumption on the structure of S_n . However, since our primary concern is a state t -design, we mainly deal with candidate sets of designs and do not consider any sets that are apparently not a state t -design. For instance, if the cardinality of a given set after removing the multiplicity is substantially smaller than $K_{\text{st}}(2^n, t, \delta)$, the set is clearly not a δ -approximate state t -design due to property (5) in Proposition 1. Such sets are out of our interest.

In the definition of $\text{compSFP}(t)$, we do not include these assumptions on S_n , simply to keep the problem as minimal as possible. When necessary, we explicitly mention that we consider only candidate sets of designs. This remark applies to all computational problems that we introduce below.

We can show that, for any constant $t \in \mathbb{Z}^+$, $\text{compSFP}(t)$ can be solved by using a single query to a $\#\text{P}$ oracle and is $\#\text{P}$ -hard. For the proofs, see Sec. IV A.

Theorem 3. For any constant $t \in \mathbb{Z}^+$, $\text{compSFP}(t) \in \text{FP}^{\#\text{P}}$.

Theorem 4. For any constant $t \in \mathbb{Z}^+$, $\text{compSFP}(t)$ is $\#\text{P}$ -hard. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t, 0)$.

From Theorems 3 and 4, we observe a gap between the inclusion and the hardness of $\text{compSFP}(t)$. This is merely due to the fact that the answer to $\text{compSFP}(t)$ is a non-negative *real number* but answers to the problems in $\#\text{P}$ are non-negative *integers*. This gap can be closed by restricting the class of state vectors and by considering a normalized frame potential. The corresponding computational problem, defined similarly to $\text{compSFP}(t)$, can be shown to be in $\#\text{P}$ for any constant $t \in \mathbb{Z}^+$. For the complete statement, see Theorem 17 in Sec. IV.

We next consider the problem of computing the unitary frame potential $\text{compUFP}(t)$. When one is concerned with unitary designs, one may additionally put assumptions on the set.

Problem 2 ($\text{compUFP}(t)$).

Input:

- (1) a set U_n of unitaries on n qubits with a computationally efficient description
- (2) $t \in \mathbb{Z}^+$ (degree)

Output: the unitary frame potential $F_t(U_n)$.

We obtain the results similar to those for $\text{compSFP}(t)$. The proofs are given in Sec. IV B.

Theorem 5. For any constant $t \in \mathbb{Z}^+$, $\text{compUFP}(t) \in \text{FP}^{\#\text{P}}$.

Theorem 6. For any constant $t \in \mathbb{Z}^+$, $\text{compUFP}(t)$ is $\#\text{P}$ -hard. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{uni}}(2^n, t, 0)$.

D. Promise problems on frame potentials

From the results in the previous section, it follows that an efficient general algorithm, whether classical or quantum, for exactly computing frame potentials, is unlikely to exist. It is then natural to consider approximate computation. One approach to address this question is to formulate it as a promise problem.

We introduce the state frame potential problem $\text{SFP}(t, \epsilon)$ as follows.

Problem 3 ($\text{SFP}(t, \epsilon)$).

Input:

- (1) a set S_n of K_n n -qubit state vectors with a computationally efficient description
- (2) $t \in \mathbb{Z}^+$ (degree)
- (3) $\alpha > \beta \geq \max\{1/d_t, 1/K_n\}$ such that $\alpha - \beta > \epsilon > 0$.

Promise: the state frame potential $F_t(S_n)$ is either $\geq \alpha$ or $\leq \beta$.

Output: decide which is the case.

From the definition of $\text{SFP}(t, \epsilon)$ as a promise problem, the frame potential $F_t(S_n)$ is guaranteed to either be $\geq \alpha$ or $\leq \beta$, where $\alpha > \beta$. The difference between α and β is characterized by ϵ , which is called a *promise gap*. Note that we have assumed $\beta \geq \max\{1/d_t, 1/K_n\}$ simply to avoid a trivial situation. See property (2) in Proposition 1.

An algorithm for solving $\text{SFP}(t, \epsilon)$ would allow us to approximately compute the frame potential by, e.g., a binary search with logarithmic overhead.

In Sec. III B, we have already provided a polynomial-time quantum algorithm for computing the state frame potential within the inverse-polynomial accuracy (see Theorem 2). In terms of the computational complexity, this implies the following.

Theorem 7. For any constant $t \in \mathbb{Z}^+$, $\text{SFP}(t, \epsilon) \in \text{BQP}$ if $\epsilon \in \Omega(1/\text{poly}(n))$.

We can further show that $\text{SFP}(t, \epsilon)$ is **BQP-hard** even if ϵ is constant. For the proof, see Sec. [VA](#).

Theorem 8. For any constant $t \in \mathbb{Z}^+$, there exists a constant ϵ such that $\text{SFP}(t, \epsilon)$ is **BQP-hard**. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t, 0)$.

Combining these two, we conclude that, for any constant $t \in \mathbb{Z}^+$, $\text{SFP}(t, \Omega(1/\text{poly}(n)))$ is **BQP-complete**.

The inverse-polynomial accuracy of the state frame potential is, however, not sufficient for checking whether or not a given set is a state design. In fact, properties (3) and (4) in Proposition 1 imply that an inverse-exponential accuracy is needed to decide which is the case. For this reason, we investigate $\text{SFP}(t, \epsilon)$ for exponentially small ϵ and show the following. For the proof, see Sec. [VB](#).

Theorem 9. For any constant $t \in \mathbb{Z}^+$, $\text{SFP}(t, \epsilon) \in \text{PP}$ if $\epsilon \in \Omega(2^{-\text{poly}(n)})$.

Theorem 10. For any constant $t \in \mathbb{Z}^+$, $\text{SFP}(t, \epsilon)$ is **PP-hard** if $\epsilon \in \mathcal{O}(1/(K_n^2 2^n))$, where K_n is the cardinality of the set. This is the case even if $K_n \geq K_{\text{st}}(2^n, t, 0)$.

Note that $K_n \in \mathcal{O}(2^{\text{poly}(n)})$ for a set of state vectors with a computationally efficient description. Hence Theorems 9 and 10 imply that $\text{SFP}(t, \Theta(2^{-\text{poly}(n)}))$ is **PP-complete** for any constant $t \in \mathbb{Z}^+$.

We can similarly formulate the unitary frame potential problem $\text{UFP}(t, \epsilon)$.

Problem 4 ($\text{UFP}(t, \epsilon)$).

Input:

- (1) a set U_n of K_n n -qubit unitaries with a computationally efficient description
- (2) $t \in \mathbb{Z}^+$ (degree)
- (3) $\alpha > \beta \geq \max\{t!, 2^{2nt}/K_n\}$ such that $\alpha - \beta > \epsilon > 0$

Promise: the unitary frame potential $F_t(U_n)$ is either $\geq \alpha$ or $\leq \beta$.

Output: decide which is the case.

The lower bound on β is for avoiding trivial situations [see property (2) in Proposition 2].

We obtain the following results about the complexity class of $\text{UFP}(t, \epsilon)$. For the proofs, see Sec. [VC](#).

Theorem 11. For any constant $t \in \mathbb{Z}^+$, $\text{UFP}(t, \epsilon) \in \text{PP}$ if $\epsilon \in \Omega(2^{-\text{poly}(n)})$.

Theorem 12. For any constant $t \in \mathbb{Z}^+$, $\text{UFP}(t, \mathcal{O}(2^{2(t-1)n}/K_n^2))$ is **PP-hard**, where K_n is the cardinality of the set. This is the case even if $K_n \geq K_{\text{uni}}(2^n, t, 0)$.

In Theorem 12, the required promise gap is $\mathcal{O}(2^{2(t-1)n}/K_n^2)$, which can be large if the cardinality K_n is small. However, when one is concerned with a set of unitaries that is a candidate of a unitary t -design, its cardinality should be at least $K_{\text{uni}} \approx 2^{2m}$. In this case, the required promise gap is $\mathcal{O}(2^{-\text{poly}(n)})$. That is, it is, in general, hard to compute the unitary frame potential for a candidate set of unitary designs with exponential accuracy.

These results imply that it is unlikely to drastically improve the quantum algorithm in the previous section. A general algorithm, whether quantum or classical, that computes the state frame potential with exponential accuracy in polynomial time is highly unlikely to exist.

E. Promise problems about designs

So far, we have considered problems related to frame potentials. We can also consider a problem of deciding whether a given set is a good approximation to a design. This problem directly captures the main computational complexity of designs, as it is natural to expect that more fine-grained problems related to quantum designs are at least as difficult.

To this end, we introduce the state design problem $\text{StDes}(t, t', \delta, \delta')$ for a set of state vectors as follows.

Problem 5 ($\text{StDes}(t, t', \delta, \delta')$).

Input:

- (1) a set S_n of K_n n -qubit state vectors with a computationally efficient description
- (2) $t \leq t' \in \mathbb{Z}^+$ (degree)
- (3) $0 \leq \delta < \delta'$

Promise: S_n is either a δ -approximate state t -design or not a δ' -approximate state t' -design. Only one of the two is the case.

Output: decide which is the case.

The problem $\text{StDes}(t, t', \delta, \delta')$ has four parameters (t, t', δ, δ') , which can be split to two different types. One is a pair (t, t') , corresponding to the degree of designs, and the other is (δ, δ') , corresponding to the approximation accuracy. We propose the problem with four parameters $t, t', \delta,$ and δ' so as to deal with these different notions in a unified manner. For the conceptual visualization of the problem, see Fig. 2.

Due to the mixture of two conceptually different types of parameters in $\text{StDes}(t, t', \delta, \delta')$, we need to explicitly state that the promise is *exclusive*. Without this exclusive promise, both could be the case, as a set of state vectors

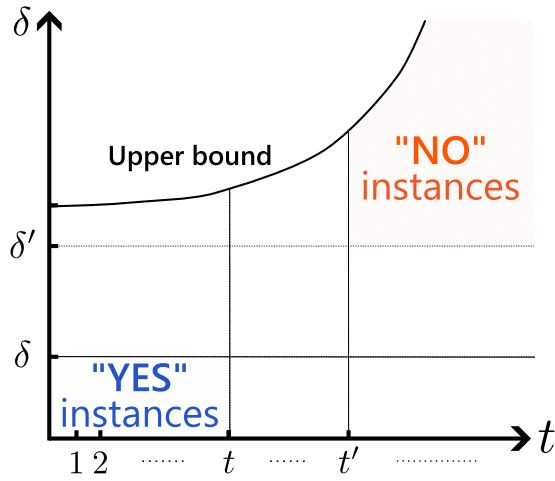


FIG. 2. A conceptual visualization of $\text{StDes}(t, t', \delta, \delta')$ and $\text{UniDes}(t, t', \delta, \delta')$. The “yes” instances, namely, δ -approximate t -designs, are indicated by a blue box and the “no” instances, i.e., the sets that are not δ' -approximate t' -design, are indicated by a red box. They form boxes because, e.g., a δ -approximate t -design is a δ -approximate \tilde{t} -design for any $\tilde{t} \leq t$. Note that the “yes” and “no” instances are not exclusive in general, but in $\text{StDes}(t, t', \delta, \delta')$ and $\text{UniDes}(t, t', \delta, \delta')$, it is promised that a given instance belongs to only one of the “yes” or “no” instances. See the text. The upper bound in the figure is given by approximately d_t for StDes and approximately 2^{2nt} for UniDes . In particular, we show that $\text{StDes}(t, t', \delta, \delta')$ and $\text{UniDes}(t, t', \delta, \delta')$ with $t' = t + 1$, $\delta \in \Theta(2^{-cn})$, and $\delta' \in \Theta(1)$ is PP-hard, where $c = 1$ for StDes and $c = 2$ for UniDes .

could be a good approximate t -design *and* a bad approximate t' -design at the same time, making the problem ill defined.

When $t = t'$, we can use the computational complexity of $\text{SFP}(t, \epsilon)$ for showing that $\text{StDes}(t, t, \delta, \delta')$ is in PP if the promise gap is not too small.

Theorem 13. For any constant $t \in \mathbb{Z}^+$ and $\delta'^2 - d_t \delta^2 \in \Omega(2^{-\text{poly}(n)})$, $\text{StDes}(t, t, \delta, \delta') \in \text{PP}$.

In contrast, we can obtain the hardness result for any $t \leq t'$.

Theorem 14. For any constant $t \leq t' \in \mathbb{Z}^+$, $\delta \in \Omega(2^{-\text{poly}(n)})$, and δ' that satisfies

$$\delta' - \delta \in \begin{cases} \Theta(2^{(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-n}\delta), & \text{for } t = t', \end{cases} \quad (33)$$

$\text{StDes}(t, t', \delta, \delta')$ is PP-hard under polynomial-time mapping reductions. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t', 0)$.

Note that Eq. (33) implies that $\delta' \in \Theta(2^{(t'-t)n}\delta)$ for any $t \leq t'$. For the proofs of Theorems 13 and 14, see Sec. VIA.

As a direct corollary of Theorem 14, it follows that, for any $t \in \mathbb{Z}^+$ and $\delta \in \Omega(2^{-\text{poly}(n)})$, it is PP-hard to determine whether a given set of state vectors is a δ -approximate state t -design or not a $\Theta(2^n\delta)$ -approximate state $(t+1)$ -design. If the latter is the case, the set is not a δ -approximate state t -design due to the promise. Hence an efficient general algorithm is unlikely to exist to decide if a given set is an exponentially accurate approximation to a state t -design or a worse-than-constant approximation to a state $(t+1)$ -design that fails to form an accurate t -design.

This inherent difficulty of distinguishing good designs from bad designs highlights the computational hardness of general verification methods of state designs. Hence, in practical applications of state designs, developing a verification technique specifically tailored to the method that generated the set of state vectors is of crucial importance. Our result may also find applications in adversarial scenarios such as quantum cryptography, because it implies that an adversary can easily cheat by preparing a bad $(t+1)$ -design instead of a good t -design. This may potentially offer a new cryptographic primitive but we leave a concrete application as a problem for future research.

We similarly formulate the unitary design problem $\text{UniDes}(t, t', \delta, \delta')$ for a set of unitaries and show similar results. For the proofs, see Sec. VIB.

Problem 6 ($\text{UniDes}(t, t', \delta, \delta')$).

Input:

- (1) a set U_n of K_n n -qubit unitaries with a computationally efficient description
- (2) $t \leq t' \in \mathbb{Z}^+$ (degree)
- (3) $0 \leq \delta < \delta'$

Promise: U_n is either a δ -approximate unitary t -design or not a δ' -approximate unitary t' -design. Only one of the two is the case.

Output: decide which is the case.

The same remarks as those for $\text{StDes}(t, t', \delta, \delta')$ apply to $\text{UniDes}(t, t', \delta, \delta')$. Specifically, the problem has two types of parameter (t, t') and (δ, δ') and the *exclusive* promise is also important.

Theorem 15. For any constant $t \in \mathbb{Z}^+$ and $\delta'^2 - 2^{2nt}\delta^2 \in \Omega(2^{-\text{poly}(n)})$, $\text{UniDes}(t, t, \delta, \delta') \in \text{PP}$.

Theorem 16. For any constant $t \leq t' \in \mathbb{Z}^+$, $\delta \in \Omega(2^{-\text{poly}(n)}) \cap o(2^{2(t-1)n})$, and δ' that satisfies

$$\delta' - \delta \in \begin{cases} \Theta(2^{(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-2n}\delta), & \text{for } t = t', \end{cases} \quad (34)$$

$\text{UniDes}(t, t', \delta, \delta')$ is PP-hard under polynomial-time mapping reductions. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{uni}}(2^n, t', 0)$.

By setting $t' = t + 1$, Theorem 16 implies that it is computationally hard to decide whether a given set of unitaries is a δ -approximate unitary t -design or not a $\Theta(2^{2n}\delta)$ -approximate unitary $(t + 1)$ -design. The exclusive promise further guarantees that if the latter is the case, the set is not a δ -approximate unitary t -design. Thus, similarly to a state design, an efficient algorithm is unlikely to exist for distinguishing a good approximate unitary t -design from a bad approximate unitary $(t + 1)$ -design that fails to form a good approximate t -design. This also has implications to verifying unitary designs in practical applications and to future applications in adversarial situations.

F. Implications of our results

Our approach is based on computational complexity theory. Due to its broad applicability, our results have immediate implications for the topics related to unitary or state designs. Below, we outline three such implications along with a brief overview of the literature.

1. Variational approach to constructing designs

Generating δ -approximate unitary t -designs is of fundamental importance. In Ref. [60], the first efficient circuit construction has been proposed, which uses $\mathcal{O}(tn^2(tn + \log 1/\delta))$ gates if $t \in \mathcal{O}(n/\log n)$ and $t \leq 2^{n/50}$ [84]. Later, the number of gates has been improved to $\mathcal{O}(t^{4+o(1)}n(tn + \log 1/\delta))$ for any t by local random circuits [64] and to $(t + 1)n^2 + n \log 1/\delta + \mathcal{O}(n)$ for $t \in o(\sqrt{n})$ by phase-Hadamard-cocktail random circuits [62], where the term “phase-Hadamard-cocktail” has been proposed in Ref. [85]. Recently, structured random circuits with $\mathcal{O}(tn(\log n + \log 1/\delta))$ gates have been shown to suffice [69,70]. Due to the substantial importance of designs and related concepts, more and more circuit constructions have been proposed [65–69].

These results have been obtained first by proposing specific quantum circuits, such as local random circuits or phase-Hadamard-cocktail random circuits, and then by analyzing their design properties.

An alternative approach is a variational method, explored in Ref. [71], to construct a design with small cardinality. The variational method is based on a variational ansatz set \mathbf{A} with computationally efficient descriptions and an update protocol, such as gradient descent, and may proceed as follows:

- (1) Initialize an ansatz set \mathbf{A} .
- (2) Compute the frame potential of \mathbf{A} and its derivative.
- (3) Update the ansatz set \mathbf{A} to reduce its frame potential.
- (4) Repeat steps (2) and (3) until the frame potential approaches its minimum sufficiently closely.

Such a variational method performs well in small systems [71]. Moreover, Theorem 7 indicates that, for state

vectors, this method may work well on quantum computers until the frame potential approaches its minimum with an accuracy of $\Omega(1/\text{poly}(n))$. However, achieving higher accuracy for state vectors, such as $\mathcal{O}(2^{-\text{poly}(n)})$, and dealing with a set of unitaries requires careful consideration. In fact, Theorems 9–12 immediately imply the following.

Corollary 1. If the ansatz set \mathbf{A} can represent arbitrary sets with computationally efficient description, there is no variational method that outputs an approximate t -design in quantum and classical polynomial time, assuming that $\text{PP} \neq \text{BQP}$ and $\text{PP} \neq \text{BPP}$, respectively.

Our results, therefore, highlight that it is essential to restrict the representability of the ansatz set \mathbf{A} for the variational approach to scale up to a large system.

2. Computational complexity of chaos via OTOCs

The unitary frame potential is closely related to OTOCs, which are widely used as diagnostics for quantum chaotic dynamics in many-body systems. A $2t$ -point OTOC is defined for an n -qubit state ρ , an n -qubit unitary U , and $2t$ n -qubit observables $\{O_j\}_{j=1,\dots,2t}$ as follows:

$$\begin{aligned} \text{OTOC}_{2t}(\rho, U, \{O_j\}_j) \\ = \text{Tr}[(O_{2t}O_{2t-1}(U) \dots O_2O_1(U)) \rho], \end{aligned} \quad (35)$$

where $O_j(U) = U^\dagger O_j U$. Note that the unitary is applied only to operators with odd indexes. The OTOCs are important quantities for characterizing chaotic behavior in quantum many-body systems, where ρ is a thermal state of a given Hamiltonian H , $U = e^{-iHT}$ with T being time, and observables are commonly chosen to be single-qubit Pauli operators. Under these settings, the OTOCs typically decrease as time T increases and the speed of the decrease characterizes quantum chaotic dynamics in terms of the Lyapunov exponent [36].

Reference [37] has shown that the OTOCs are closely related to the frame potential. To explain this, let us set ρ to be the completely mixed state π , corresponding to the infinite temperature, and let us take the average of the OTOCs over a given set \mathbf{U}_n of n -qubit unitaries. By summing each observable O_j over an operator basis \mathbf{B}_n , such as a set of all n -qubit Pauli operators, we can define an average $2t$ -point OTOC at infinite temperature as

$$\begin{aligned} \text{OTOC}_{2t}(\mathbf{U}) \\ = \frac{1}{2^{4nt}} \sum_{\{O_j\}_j \in \mathbf{B}_n^{2t}} \mathbb{E}_{U \sim \mathbf{U}_n} |\text{OTOC}_{2t}(\pi, U, \{O_j\}_j)|^2. \end{aligned} \quad (36)$$

This quantity is shown to be equivalent to the unitary frame potential of \mathbf{U}_n of degree t , namely,

$$\text{OTOC}_{2t}(\mathbf{U}_n) = \frac{1}{2^{2(t+1)n}} F_t(\mathbf{U}_n). \quad (37)$$

From Eq. (37) and Theorems 5 and 6, it directly follows that computing the average $2t$ -point OTOCs at infinite temperature is hard for any constant $t \in \mathbb{Z}^+$.

Corollary 2. For any constant $t \in \mathbb{Z}^+$, computing $\text{OTOC}_{2t}(\mathcal{U}_n)$ for a set \mathcal{U}_n of unitaries with a computationally efficient description is in $\text{FP}^{\#\text{P}}$ and $\#\text{P}$ -hard.

This indicates that verifying quantum chaotic dynamics via OTOCs is, in general, computationally hard in large systems, which characterizes the complex nature of chaotic dynamics from the computational complexity perspective.

3. Verification of emergent state designs

The concepts of unitary and state designs have also been applied to investigate higher-order properties of thermalization and ergodicity in quantum many-body systems.

Let H be a Hamiltonian on a composite system AB of $n + m$ qubits, where n and m are the number of qubits in A and B , and let $|\Psi(T)\rangle = e^{-iHT}|0\rangle^{\otimes(n+m)}$ be the state vector in AB at time T . By measuring the subsystem B in the computational basis, the following ensemble \mathcal{P} of pure states is realized in A :

$$\mathcal{P} = \{p_j, |\Psi_j(T)\rangle\}_{j=1, \dots, 2^m}, \quad (38)$$

where $|\Psi_j(T)\rangle := (I^A \otimes \langle j|^B)|\Psi(T)\rangle / \sqrt{p_j}$ with $p_j = |(I^A \otimes \langle j|^B)|\Psi(T)\rangle|^2$. This ensemble is called a *projected state ensemble*. It is conjectured, with supporting numerical evidence, that if the Hamiltonian H is chaotic and lacks conservation laws, the projected state ensemble obtained by measuring a sufficiently large subsystem B after long-time evolution forms an approximate state t -design [38,51]. By leveraging the connection between state designs, thermalization, and ergodicity, this insight has been extensively applied to the study of complex quantum many-body systems [29,30,39,40,72–76]. Novel concepts in quantum many-body physics through the framework of designs, such as *deep thermalization* [29,30] and *complete Hilbert-space ergodicity* [39,40], have also emerged.

The conjecture has been analytically addressed in a few solvable models in the thermodynamic limit [74,75] but numerical approaches are crucial for the further studies. While general numerical simulations of a projected state ensemble are difficult, as they have to compute the measurement probability distributions, there may exist a class of Hamiltonians for which this is also computationally tractable. Even in such cases, our results highlight the importance of developing numerical methods that account for the specific dynamics governed by the Hamiltonian H and the measurement. In particular, the following corollary is obtained from Theorem 14.

Corollary 3. Let \mathcal{P} be a projected state ensemble of n qubits obtained by measuring the $(n + m)$ -qubit state

generated by Hamiltonian dynamics with Hamiltonian H after time T , which has a computationally efficient description. Assuming that $\text{PP} \neq \text{BQP}$ for the quantum case and that $\text{PP} \neq \text{BPP}$ for the classical case, there is no general quantum or classical polynomial-time algorithm that can check whether \mathcal{P} is a δ -approximate state t -design or not a δ' -approximate state t' -design if $\delta' - \delta \in \Theta(2^{(t'-t)n}\delta)$ for $t < t'$ and $\delta' - \delta \in \Theta(2^{-n}\delta)$ for $t = t'$.

Corollary 3 particularly implies that, toward the proof of the conjecture in general situations, it is of crucial importance to develop an algorithm that is specifically tailored to exploit problem-specific properties, such as the property of Hamiltonian dynamics by H , or additional constraints beyond the general case.

G. Proof sketch

Below, we provide a brief overview of our proof methods. We first focus on the inclusion results and then explain the methods that we use for proving the hardness results.

1. Methods for the inclusion results

Our strategy to obtain the inclusion results is to begin with quantum algorithms, which are not necessarily efficient, and to dequantize them. The inclusion results for compSFP and compUFP are obtained by dequantizing the quantum algorithm based on Lemma 1, which is achieved by a similar technique in Ref. [86]. For SFP and UFP , we propose variants of the quantum algorithm. In this case, the dequantization step follows from the equivalence that $\text{PQP} = \text{PP}$ [79].

From these inclusion results of the computational problems related to frame potentials, the inclusion results of StDes and UniDes can be immediately obtained as frame potentials characterize designs.

2. Methods for the hardness results

Proving hardness results is less straightforward. To establish those results, we employ a technique that we call “hide a hard instance in a set.” This consists of three steps. First, we choose a computationally hard instance relevant to the desired proof. Second, we embed the hard instance in state vectors or unitaries and, finally, we hide them in a set of state vectors or unitaries with known properties.

The specific hard instance depends on the statement to be shown. For the $\#\text{P}$ -hardness of compSFP and compUFP , we use a $\#\text{P}$ -complete problem $\#\text{SAT}$. For the PP -hardness of SFP and UFP with suitable parameters, a PP -complete problem MAJ-SAT is used. For the BQP -hardness of $\text{SFP}(t, \Omega(1/\text{poly}(n)))$, we use a quantum circuit that solves a BQP -complete problem.

These problems are embedded in a pair of state vectors or unitaries with a computationally efficient description. This embedding is such that the solution of the problems

is given by the inner product of the pair. The pairs are then “hidden” in a set of state vectors or unitaries that we know the details of. In the case of the computational problems related to frame potentials, this is enough for obtaining the hardness result: as the frame potential is a function of inner products, the frame potential of the resulting set should contain the information about the solution of the hard instance. That is, if one can evaluate the frame potential of the resulting set, one can use the same method to obtain the solution of the hard instance. This provides a polynomial-time reduction from a complete problem to the corresponding computational problem.

This “hide-a-hard-instance-in-a-set” technique is also useful for proving the hardness results of **StDes** and **UniDes**, in which the main concern is to evaluate the approximation accuracy of a given set to a design. In the proofs, we similarly use the MAJ-SAT problem and embed it into a pair of state vectors or unitaries. We then hide the pair in an approximate design. Although these steps are similar to those in the proof of the problems related to frame potentials, the proofs are more intricate due to the following two challenges.

First, unlike the frame potential, it is not immediately obvious if the approximation accuracy of the set is directly related to the inner product. Note that it is the inner product of the hidden pair that contains the solution of MAJ-SAT. Through careful evaluations of matrix norms, we explicitly compute the approximation accuracy of the resulting set and show that it is given as a function of the inner product of the hidden pair. This evaluation is tight, which is also crucial, as the tightness is the key factor to guarantee that any Boolean function can be embedded into **StDes** and **UniDes** while keeping their exclusive promise.

The second difficulty is that, in general, hiding even a single pair of state vectors or unitaries in approximate designs significantly degrades their approximation accuracy. This imposes a substantial restriction on the parameter δ in **StDes**(t, t', δ, δ') and **UniDes**(t, t', δ, δ'), preventing us from dealing with accurate designs in the problems. That is, we cannot choose, e.g., $\delta \in \mathcal{O}(2^{-\text{poly}(n)})$. We circumvent this limitation by using the multiplicity degree of freedom of approximate designs. Specifically, we use the fact that the multiplicity of approximate designs can be arbitrarily increased without changing the approximation accuracy. By hiding hard instances into a *sufficiently large* set, we can control the restriction on the approximation of the set after hiding and can remove the restriction on δ .

IV. ANALYSIS OF COMPLEXITY OF **compSFP** AND **compUFP**

In this section, we investigate the computational complexity of **compSFP** and **compUFP** and provide proofs for Theorems 3 to 6. We address **compSFP** in Sec. IV A and **compUFP** in Sec. IV B.

A. Complexity of **compSFP**

We prove Theorem 3 by explicitly constructing a classical algorithm to compute the state frame potential that uses a single query to a $\#\text{P}$ oracle. The algorithm is based on the quantum algorithm in Lemma 1.

Theorem 3 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{compSFP}(t) \in \text{FP}^{\#\text{P}}$.

Proof of Theorem 3. From Lemma 1, we have $F_t(\mathcal{S}_n) = \text{Tr}[(\varrho_{\text{st}}^A)^2]$, where ϱ_{st}^A is the marginal state of $|\varrho_{\text{st}}\rangle^{AB}$, defined in Eq. (28). Let A' and B' be isomorphic to A and B , respectively, and denote by $\mathbb{F}^{AA'} = \sum_{ij} |ij\rangle\langle ji|^{AA'}$ the SWAP operator between A and A' , where $\{|j\rangle\}_j$ is an orthonormal basis. The state frame potential can be rephrased as

$$\begin{aligned} F_t(\mathcal{S}_n) &= \left(\langle \varrho_{\text{st}} |^{AB} \otimes \langle \varrho_{\text{st}} |^{A'B'} \right) (\mathbb{F}^{AA'} \otimes I^{BB'}) \left(|\varrho_{\text{st}}\rangle^{AB} \otimes |\varrho_{\text{st}}\rangle^{A'B'} \right). \end{aligned} \quad (39)$$

Below, we simply denote the right-hand-side by $\langle \varrho_{\text{st}} |^{\otimes 2} (\mathbb{F}^{AA'} \otimes I^{BB'}) | \varrho_{\text{st}} \rangle^{\otimes 2}$. The statement of Theorem 3 follows from the fact that this expectation value is obtained by counting the number of satisfying instances of an appropriate Boolean function that is computable in classical polynomial time. We show this by using a technique similar to the one used in Ref. [86].

We first map the state $|\varrho_{\text{st}}\rangle^{\otimes 2}$ to the one that is generated by a quantum circuit consisting only of the Hadamard and Toffoli gates. To this end, let $\sum_{\alpha} (x_{\alpha} + iy_{\alpha}) |\alpha\rangle$ ($x_{\alpha}, y_{\alpha} \in \mathbb{R}$) be an expansion of $|\varrho_{\text{st}}\rangle^{\otimes 2}$ in the computational basis. Using this notation and Eq. (39), the frame potential is given as

$$F_t(\mathcal{S}_n) = \langle \varrho_{\text{st}} |^{\otimes 2} (\mathbb{F}^{AA'} \otimes I^{BB'}) | \varrho_{\text{st}} \rangle^{\otimes 2} \quad (40)$$

$$= \sum_{\alpha, \beta} (x_{\beta} - iy_{\beta})(x_{\alpha} + iy_{\alpha}) h(\alpha, \beta) \quad (41)$$

$$= \sum_{\alpha, \beta} (x_{\alpha} x_{\beta} + y_{\alpha} y_{\beta}) h(\alpha, \beta), \quad (42)$$

where $h(\alpha, \beta) = \langle \beta | (\mathbb{F} \otimes I) | \alpha \rangle$. In the last line, we have used the fact that $h(\alpha, \beta) = h(\beta, \alpha)$, which is either 0 or 1.

We now introduce one more ancillary qubit and define $|\bar{\varrho}_{\text{st}}^{\otimes 2}\rangle$ by

$$|\bar{\varrho}_{\text{st}}^{\otimes 2}\rangle = \sum_{\alpha} |\alpha\rangle \otimes (x_{\alpha} |0\rangle + y_{\alpha} |1\rangle). \quad (43)$$

This is a state on $2(\kappa_n + nt) + 1$ qubits, where $\kappa_n = \log K_n$, and K_n is the cardinality of \mathcal{S}_n . When $|\varrho_{\text{st}}\rangle^{\otimes 2}$ can be efficiently generated by a quantum circuit, which is the case in

our problem, it is known that $|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle$ can also be efficiently generated from the computational zero state only by using the Hadamard and Toffoli gates [87]. Furthermore, it holds that

$$\langle \bar{\rho}_{\text{st}}^{\otimes 2} | (\mathbb{F}^{AA'} \otimes I^{BB'} \otimes I) | \bar{\rho}_{\text{st}}^{\otimes 2} \rangle = \sum_{\alpha, \beta} (x_\alpha x_\beta + y_\alpha y_\beta) h(\alpha, \beta), \quad (44)$$

which is equal to the frame potential $F_t(\mathcal{S}_n)$ due to Eq. (42). Hence the state frame potential can be obtained as an expectation value by the state $|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle$ that is generated by the quantum circuit consisting only of the Hadamard and Toffoli gates. Below, we denote by M the total number of gates in the quantum circuit generating $|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle$ and by h the number of Hadamard gates in the circuit. The number of Toffoli gates is $M - h$.

Let \tilde{H} be a ‘‘rescaled’’ Hadamard gate $\sqrt{2}H$, where H is the Hadamard gate. Denoting by G_m the unitary on $(2(\kappa_n + nt) + 1)$ qubits corresponding to a single \tilde{H} or a Toffoli gate in the quantum circuit, we can rewrite $|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle$ as follows:

$$|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle = 2^{-h/2} G_M G_{M-1} \dots G_1 |0\rangle^{\otimes 2(\kappa_n + nt) + 1}. \quad (45)$$

By substituting the identity $I = \sum_\alpha |\alpha\rangle\langle\alpha|$ after each G_m , where $|\alpha\rangle$ are the computational basis states, we obtain

$$|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle = 2^{-h/2} \sum_{\alpha_1, \dots, \alpha_M} \prod_{m=1}^M g_m(\alpha_m, \alpha_{m-1}) |\alpha_M\rangle, \quad (46)$$

where $g_m(\alpha_m, \alpha_{m-1}) = \langle \alpha_m | G_m | \alpha_{m-1} \rangle$, and $|\alpha_0\rangle = |0\rangle^{\otimes 2(\kappa_n + nt) + 1}$. Since $|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle$ is a state on $2(\kappa_n + nt) + 1$ qubits, $\alpha_m \in \{0, 1\}^{2(\kappa_n + nt) + 1}$. Below, we use the notation $g(\vec{\alpha}) = \prod_{m=1}^M g_m(\alpha_m, \alpha_{m-1})$ for $\vec{\alpha} = (\alpha_1, \dots, \alpha_M)$. With this notation, we have

$$|\bar{\rho}_{\text{st}}^{\otimes 2}\rangle = 2^{-h/2} \sum_{\vec{\alpha}} g(\vec{\alpha}) |\alpha_M\rangle \quad (47)$$

and

$$F_t(\mathcal{S}_n) = 2^{-h} \sum_{\vec{\alpha}, \vec{\beta}} g(\vec{\alpha}, \vec{\beta}) \bar{h}(\alpha_M, \beta_M), \quad (48)$$

where $g(\vec{\alpha}, \vec{\beta}) = g(\vec{\alpha})g(\vec{\beta})$, and $\bar{h}(\alpha_M, \beta_M) = \langle \beta_M | (\mathbb{F}^{AA'} \otimes I^{BB'} \otimes I) | \alpha_M \rangle \in \{0, 1\}$.

Since G_m is a unitary corresponding to either single \tilde{H} or a single Toffoli gate, $g_m(\alpha_m, \alpha_{m-1})$ is computable in classical polynomial time. This further implies that $g(\vec{\alpha})$ is also computable in classical polynomial time, and so is $g(\vec{\alpha}, \vec{\beta})$. Clearly, $\bar{h}(\alpha_M, \beta_M)$ is also computable in classical polynomial time.

We now define a Boolean function $f : \{0, 1\}^{L+1} \rightarrow \{0, 1\}$, where $L = 2M(2(\kappa_n + nt) + 1)$, by

$$f(\vec{\alpha}, \vec{\beta}, b) = \begin{cases} 1, & \text{if } g(\vec{\alpha}, \vec{\beta}) \bar{h}(\alpha_M, \beta_M) \geq b, \\ 0, & \text{otherwise.} \end{cases} \quad (49)$$

As both $g(\vec{\alpha}, \vec{\beta})$ and $\bar{h}(\alpha_M, \beta_M)$ are computable in classical polynomial time, so is $f(\vec{\alpha}, \vec{\beta}, b)$.

We claim that

$$F_t(\mathcal{S}_n) = 2^{-h} (s(f) - 2^L), \quad (50)$$

where $s(f) = |\{(\vec{\alpha}, \vec{\beta}, b) \in \{0, 1\}^{L+1} : f(\vec{\alpha}, \vec{\beta}, b) = 1\}|$. This claim implies that the state frame potential can be computed by counting the number $s(f)$ of satisfying instances of an efficiently computable Boolean function f . As counting $s(f)$ is in $\#\mathbf{P}$, one can compute the state frame potential by a single access to a $\#\mathbf{P}$ oracle.

To show Eq. (50), let s_\pm and s_0 be the number of $(\vec{\alpha}, \vec{\beta})$ such that

$$g(\vec{\alpha}, \vec{\beta}) \bar{h}(\alpha_M, \beta_M) = \pm 1, 0, \quad (51)$$

respectively. As the left-hand side is either ± 1 or 0 for any $\vec{\alpha}$ and $\vec{\beta}$, $s_- + s_0 + s_+ = 2^L$. It also follows from Eq. (48) that $F_t(\mathcal{S}_n) = 2^{-h}(s_+ - s_-)$.

By definition, the number of $(\vec{\alpha}, \vec{\beta})$ such that $f(\vec{\alpha}, \vec{\beta}, 0) = 1$ and the number of those satisfying $f(\vec{\alpha}, \vec{\beta}, 1) = 1$ are $s_+ + s_0$ and s_+ , respectively. This implies that $s(f) = 2s_+ + s_0$. As $s_- + s_0 + s_+ = 2^L$, we have $s(f) = 2^L + s_+ - s_-$. This implies Eq. (50). ■

We next show the hardness of compSFP , i.e., Theorem 4. To this end, we provide a polynomial-time reduction from $\#\text{SAT}$ to compSFP .

Theorem 4 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{compSFP}(t)$ is $\#\mathbf{P}$ -hard. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t, 0)$.

Proof of Theorem 4. For a Boolean function f that is computable in classical polynomial time, consider a set of quantum circuits on n qubits that generates the set $\mathcal{S}_n = \{|f\rangle, |p\rangle\} \cup \{|\psi_j\rangle\}_{j=1}^{K_n-2}$, where

$$|f\rangle = 2^{-(n-2)/2} \sum_{x \in \{0, 1\}^{n-2}} |x\rangle |f(x)\rangle |0\rangle, \quad (52)$$

$$|p\rangle = |+\rangle^{\otimes n-2} |1\rangle |0\rangle, \quad (53)$$

$$|\psi_j\rangle = |\varphi_j\rangle |1\rangle. \quad (54)$$

Here, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $\mathcal{S}_\varphi := \{|\varphi_j\rangle\}_{j=1}^{K_n-2}$ is any set of $(n-1)$ -qubit state vectors with a computationally

efficient description such that $F_t(\mathcal{S}_\varphi)$ can be computed in classical polynomial time.

The set \mathcal{S}_n constructed in this way also has a computationally efficient description. In fact, one can obtain the description of \mathcal{S}_n by adding one bit to the computationally efficient description of \mathcal{S}_φ and by using the added degree of freedom for conditioning if we generate either $|f\rangle$ or $|p\rangle$, or some state in \mathcal{S}_φ .

Since $\langle f|p\rangle = 2^{-(n-2)}s(f)$ and $\langle f|\psi_j\rangle = \langle p|\psi_j\rangle = 0$ for all $j = 1, \dots, K_n - 2$, the state frame potential $F_t(\mathcal{S}_n)$ is directly computed as

$$F_t(\mathcal{S}_n) = \left(1 - \frac{2}{K_n}\right)^2 F_t(\mathcal{S}_\varphi) + \frac{2}{K_n^2} \left[1 + \left(\frac{s(f)}{2^{n-2}}\right)^{2t}\right]. \quad (55)$$

Since $F_t(\mathcal{S}_\varphi)$ is polynomial-time computable by assumption, this equation directly yields a polynomial-time reduction from a #P-complete problem, #SAT, to compSFP. ■

In the proof of Theorem 4, we have used a set \mathcal{S}_φ of $(n-1)$ -qubit state vectors with a computationally efficient description, for which we can compute the state frame potential in polynomial time. For completeness, below we provide three instances of such a set.

The first one works when $K_n - 2 \leq 2^{n-1}$. In this case, we can trivially use any orthonormal basis $\{|e_j\rangle\}_{j=1, \dots, K_n-2}$. The frame potential $F_t(\mathcal{S}_\varphi)$ is simply $1/(K_n - 2)$.

A more nontrivial choice of \mathcal{S}_φ is

$$|\varphi_j\rangle = \frac{|0\rangle + e^{2ij\pi/(K_n-2)}|1\rangle}{\sqrt{2}} \otimes |0^{n-2}\rangle. \quad (56)$$

Let $K := K_n - 2$ and assume that $K > t$. The frame potential $F_t(\mathcal{S}_\varphi)$ can be computed as

$$F_t(\mathcal{S}_\varphi) = \frac{1}{K^2} \sum_{j,k=1}^K |\langle \varphi_j | \varphi_k \rangle|^{2t} \quad (57)$$

$$= \frac{1}{K^2} \sum_{j,k=1}^K \cos^{2t} \left(\frac{k-j}{K} \pi \right) \quad (58)$$

$$= \frac{1}{K^2} \sum_{j=1-K}^{K-1} (K - |j|) \cos^{2t} \left(\frac{j}{K} \pi \right) \quad (59)$$

$$= \frac{2}{K^2} \sum_{j=0}^{K-1} (K - j) \cos^{2t} \left(\frac{j}{K} \pi \right) - \frac{1}{K} \quad (60)$$

$$= \frac{1}{K} \sum_{j=0}^{K-1} \cos^{2t} \left(\frac{j}{K} \pi \right), \quad (61)$$

where, in the last line, we have used the following:

$$\begin{aligned} & 2 \sum_{j=0}^{K-1} (K - j) \cos^{2t} \left(\frac{j}{K} \pi \right) \\ &= \sum_{j=0}^{K-1} (K - j) \cos^{2t} \left(\frac{j}{K} \pi \right) + \sum_{j=0}^K j \cos^{2t} \left(\frac{K-j}{K} \pi \right) \end{aligned} \quad (62)$$

$$= \sum_{j=0}^{K-1} (K - j) \cos^{2t} \left(\frac{j}{K} \pi \right) + \sum_{j=0}^{K-1} j \cos^{2t} \left(\frac{j}{K} \pi \right) + K \quad (63)$$

$$= K \left[1 + \sum_{j=0}^{K-1} \cos^{2t} \left(\frac{j}{K} \pi \right) \right]. \quad (64)$$

Moreover, we can further simplify Eq. (61) by using Ref. [88, Theorem 2.1], which results in

$$F_t(\mathcal{S}_\varphi) = 2^{1-2t} \binom{2t-1}{t-1}. \quad (65)$$

For any constant t , Eq. (65) can be computed in classical constant time. Note that by using this set, we can vary the cardinality K_n without changing the frame potential $F_t(\mathcal{S}_\varphi)$.

We may also generalize Eq. (56) to

$$|\varphi_j\rangle = \left(\frac{|0\rangle + e^{2ij\pi/(K_n-2)}|1\rangle}{\sqrt{2}} \right)^{\otimes m} \otimes |0^{n-m-1}\rangle \quad (66)$$

for any natural number $1 \leq m \leq n-1$. By a similar calculation, the frame potential can be shown to be

$$2^{1-2mt} \binom{2mt-1}{mt-1}. \quad (67)$$

This value can be dependent on the number n of qubits if we choose m as a function of n .

From Theorems 3 and 4, we conclude that compSFP \in $\mathbb{FP}^{\#P}$ and is #P-hard. Although there is a gap between the result about the inclusion and the hardness, this is merely due to the fact that the answer to compSFP is a real number, while the answer to #P problems is a non-negative integer. One way to close the gap is to restrict a set of state vectors and consider a “rescaled” frame potential. A possible example is a set $\mathcal{S}_\mathcal{X}$ of state vectors on n qubits in the form of

$$|\psi_j\rangle = \chi^{-1/2} \sum_{x \in \mathcal{X}} (-1)^{a_{jx}} |x\rangle, \quad (68)$$

where $\mathcal{X} \subseteq \{0, 1\}^n$ with cardinality $\chi := |\mathcal{X}|$, and $a_{jx} \in \{0, 1\}$. We call this type of state a *subset phase state*. The

subset phase states and their relations to a state design have been studied in a general context from the viewpoint of entanglement and thermalization phenomena [89]. In recent years, special types of subset phase states have also been of particular interest in quantum cryptography because the state reduces to a phase-random state [54,90,91] when $\chi = 2^n$ and each $a_{j\bar{x}}$ is randomly chosen, and to a random subset state [92,93] when \mathcal{X} is randomly chosen and $a_{j\bar{x}} = 0$. Both are known to be useful as quantum cryptographic primitives.

For the subset phase states, we can show that computing a rescaled state frame potential is in #P.

Theorem 17. Let $S_{\mathcal{X}}$ be a set of n -qubit subset phase states, with $a_{j\bar{x}}$ being efficiently computable in classical polynomial time, and let $K_n := |S_{\mathcal{X}}|$ be its cardinality. For any constant $t \in \mathbb{Z}^+$, computing

$$\frac{\chi^{2t} K_n^2}{2} (1 - F_t(S_{\mathcal{X}})) \quad (69)$$

is in #P. This is the case even if $K_n \geq K_{\text{st}}(2^n, t, 0)$.

Proof of Theorem 17. The frame potential of degree t for $S_{\mathcal{X}}$ is given by

$$\begin{aligned} F_t(S_{\mathcal{X}}) &= \frac{1}{\chi^{2t} K_n^2} \sum_{j,k=1}^{K_n} \left| \sum_{x \in \mathcal{X}} (-1)^{a_{j\bar{x}} + a_{k\bar{x}}} \right|^{2t} \quad (70) \\ &= \frac{1}{\chi^{2t} K_n^2} \sum_{j,k=1}^{K_n} \sum_{\bar{x} \in \mathcal{X}^{2t}} (-1)^{|a_{j\bar{x}} + a_{k\bar{x}}|}, \quad (71) \end{aligned}$$

where $a_{j\bar{x}} = (a_{j\bar{x}_1}, \dots, a_{j\bar{x}_{2t}})$ and $|a_{j\bar{x}} + a_{k\bar{x}}| := \sum_{m=1}^{2t} (a_{j\bar{x}_m} + a_{k\bar{x}_m})$, with all the addition taken as exclusive-OR (XOR).

For simplicity, we introduce a $(K_n \times \chi)$ matrix $A = (a_{j\bar{x}})_{j\bar{x}}$ and define a Boolean function $f_A(j, k, \bar{x})$ from $\{0, 1\}^{2(\log K_n + t \log \chi)}$ to $\{0, 1\}$, such as

$$f_A(j, k, \bar{x}) = |a_{j\bar{x}} + a_{k\bar{x}}|. \quad (72)$$

As we have assumed that $a_{j\bar{x}}$ are efficiently computable in classical polynomial time, $f_A(j, k, \bar{x})$ is also computable in classical polynomial time. Using $s(f_A) = \sum_{j,k,\bar{x}} f_A(j, k, \bar{x})$, which is the number of inputs satisfying $f_A(j, k, \bar{x}) = 1$, it follows that

$$F_t(S_{\mathcal{X}}) = \frac{1}{\chi^{2t} K_n^2} \sum_{j,k=1}^{K_n} \sum_{\bar{x} \in \mathcal{X}^{2t}} (-1)^{f_A(j,k,\bar{x})} \quad (73)$$

$$= \frac{\chi^{2t} K_n^2 - 2s(f_A)}{\chi^{2t} K_n^2}, \quad (74)$$

which further implies that

$$s(f_A) = \frac{\chi^{2t} K_n^2}{2} (1 - F_t(S_{\mathcal{X}})). \quad (75)$$

Thus, computing Eq. (69) is in #P. ■

B. Complexity of compUFP

We now turn to compUFP. Both the inclusion and the hardness of compUFP can be shown in a similar way to compSFP.

Theorem 5 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{compUFP}(t) \in \text{FP}^{\#\text{P}}$.

The proof of Theorem 5 is almost the same as that of Theorem 3, except for the point that, instead of using $|\varrho_{\text{st}}\rangle$, we simply use $|\varrho_{\text{uni}}\rangle$, which is defined in Eq. (29).

We next prove Theorem 6.

Theorem 6 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{compUFP}(t)$ is #P-hard. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{uni}}(2^n, t, 0)$.

Proof of Theorem 6. Let $f : \{0, 1\}^{n-2} \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time. Consider a set $\mathbf{U}_n = \{U_f, U_p\} \cup \{U_j\}_{j=1}^{K_n-2}$ of unitaries, where

$$U_f = (I_{n-1} - 2|f\rangle\langle f|) \otimes Z, \quad (76)$$

$$U_p = (I_{n-1} - 2|p\rangle\langle p|) \otimes Z, \quad (77)$$

$$U_j = V_j \otimes I, \quad (78)$$

where I_{n-1} is the identity operator on $(n-1)$ qubits, $|f\rangle = 2^{-(n-2)/2} \sum_{x \in \{0,1\}^{n-2}} |x\rangle \otimes |f(x)\rangle$ and $|p\rangle = |+\rangle^{\otimes(n-2)} \otimes |1\rangle$ are the states on $(n-1)$ qubits, Z is the one-qubit Pauli-Z operator, and $\mathbf{V}_{n-1} = \{V_j\}_{j=1}^{K_n-2}$ is any set of unitaries on $(n-1)$ qubits with a computationally efficient description, the frame potential of which, of degree t , can be computed in classical polynomial time. As \mathbf{V}_{n-1} has a computationally efficient description, so does the set \mathbf{U}_n .

A straightforward calculation leads to

$$F_t(\mathbf{U}_n) = 2^{2t} \left(1 - \frac{2}{K_n}\right)^2 F_t(\mathbf{V}_{n-1}) + \frac{2}{K_n^2} [2^{2nt} + g_t(s(f))], \quad (79)$$

where $g_t(x) = (2^n - 8 + 2^{-2n+7} x^2)^{2t}$ and $s(f) = \sum_{x \in \{0,1\}^{n-2}} f(x)$.

Since we have assumed that $F_t(\mathbf{V}_{n-1})$ is computable in classical polynomial time, this equation yields a polynomial-time reduction from a #P-complete problem, #SAT, to compUFP. ■

Similarly to the comment after the proof of Theorem 4, we can choose various sets V_{n-1} with a computationally efficient description as far as its unitary frame potential can be computed in classical polynomial time.

V. ANALYSIS OF COMPLEXITY OF SFP and UFP

In this section, we explain our results about the promise problems SFP and UFP in detail. In Secs. VA and VB, we consider SFP with the promise gap $\Omega(1/\text{poly}(n))$ and $\mathcal{O}(1/\text{exp}(n))$, respectively. The unitary case, UFP, is investigated in Sec. VC.

A. Complexity of SFP with a promise gap $\Omega(1/\text{poly}(n))$

Theorem 8 (restated). For any constant $t \in \mathbb{Z}^+$, there exists a constant ϵ such that SFP(t, ϵ) is BQP-hard. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t, 0)$.

This result is obtained by providing a reduction from a BQP-complete problem to SFP.

Proof of Theorem 8. We denote the length of a bit string x by $|x|$.

Let $L = (L_{\text{yes}}, L_{\text{no}}) \subseteq \{0, 1\}^*$ be a BQP-complete problem. By definition, for $x \in L$, there exists a unitary U_x corresponding to a polynomial-sized quantum circuit on $m \in \text{poly}(|x|)$ many qubits such that the probability

$$q_1(x) := \langle 0^m | U_x^\dagger (|1\rangle\langle 1| \otimes I^{\otimes m-1}) U_x | 0^m \rangle \quad (80)$$

of measuring the first qubit in state $|1\rangle$ satisfies:

- (1) if $x \in L_{\text{yes}}$, then $q_1(x) \geq \frac{2}{3}$
- (2) if $x \in L_{\text{no}}$, then $q_1(x) \leq \frac{1}{3}$

We assume $m \geq 2$ without loss of generality. We define $V_x := (U_x^\dagger \otimes H) \text{CZ}_{1,m+1} (U_x \otimes H)$, with $\text{CZ}_{1,m+1}$ and H being the controlled-Z (CZ) gate applied on the first and $(m+1)$ th qubits and the Hadamard gate, respectively. As shown in Ref. [94], $q_1(x) = |\langle 0^m 1 | V_x | 0^{m+1} \rangle|$ holds.

We consider the set $\{|v_j\rangle, |a_j\rangle\}_{j=1}^K$ of state vectors, where

$$|v_j\rangle := V_x | 0^{m+1} \rangle \otimes \frac{|0\rangle + e^{2ij\pi/K} |1\rangle}{\sqrt{2}}, \quad (81)$$

$$|a_j\rangle := |0^m\rangle \otimes |1\rangle \otimes \frac{|0\rangle + e^{2ij\pi/K} |1\rangle}{\sqrt{2}}, \quad (82)$$

and K is set to be larger than t . Since $\{U_x\}_x$ is a uniform family of polynomial-sized quantum circuits, this is a multiset of state vectors with a computationally efficient description. For simplicity, let $|\varphi_j\rangle := (|0\rangle + e^{2ij\pi/K} |1\rangle) / \sqrt{2}$ for all $1 \leq j \leq K$.

The state frame potential of degree t for the above set is

$$\frac{1}{4K^2} \sum_{j,k=1}^K (|\langle v_j | v_k \rangle|^{2t} + |\langle a_j | a_k \rangle|^{2t} + 2|\langle a_j | v_k \rangle|^{2t}) \quad (83)$$

$$= \frac{1 + q_1(x)^{2t}}{2} \left(\frac{1}{K^2} \sum_{j,k=1}^K |\langle \varphi_j | \varphi_k \rangle|^{2t} \right) \quad (84)$$

$$= \frac{1 + q_1(x)^{2t}}{4^t} \binom{2t-1}{t-1}, \quad (85)$$

where we have used Eq. (65) to derive the last equation. From Eq. (85), we can solve the BQP-complete problem by deciding whether the frame potential is at least

$$\frac{\binom{2t-1}{t-1}}{4^t} + \frac{\binom{2t-1}{t-1}}{9^t} \quad (86)$$

or at most

$$\frac{\binom{2t-1}{t-1}}{4^t} + \frac{\binom{2t-1}{t-1}}{36^t}. \quad (87)$$

Therefore, the promise gap ϵ is

$$\left(\frac{1}{9^t} - \frac{1}{36^t} \right) \binom{2t-1}{t-1}, \quad (88)$$

and hence, it is constant. \blacksquare

B. Complexity of SFP with a promise gap $\mathcal{O}(1/\text{exp}(n))$

Theorem 9 (restated). For any constant $t \in \mathbb{Z}^+$, SFP(t, ϵ) \in PP if $\epsilon \in \Omega(2^{-\text{poly}(n)})$.

Our proof of Theorem 9 is based on the complexity class PQP, i.e., is a quantum analog of PP.

Proof of Theorem 9. Consider the following algorithm:

- (1) With probability $p = 2/(2 + \alpha + \beta)$, proceed to the next step. With the remaining probability, output “reject.”
- (2) Choose i and j from $\{1, 2, \dots, K_n\}$ uniformly at random.
- (3) Perform the SWAP test for $|\psi_i\rangle^{\otimes t}$ and $|\psi_j\rangle^{\otimes t}$, where $|\psi_i\rangle, |\psi_j\rangle \in \mathcal{S}_n$. If the outcome is 0 (1), output “accept” (“reject”).

Note that the second step, choosing i and j , can be done in $\text{poly}(n)$ time since we consider a set with a computationally efficient description, the cardinality of which is $K_n \in \mathcal{O}(2^{\text{poly}(n)})$.

The acceptance probability of this algorithm is

$$\frac{p}{K_n^2} \sum_{ij=1}^{K_n} \frac{1 + |\langle \psi_i | \psi_j \rangle|^{2t}}{2} = p \frac{1 + F_t(\mathbf{S}_n)}{2}. \quad (89)$$

Therefore, the acceptance probability is either

$$\geq p \frac{1 + \alpha}{2} = \frac{1}{2} + \frac{\alpha - \beta}{2(2 + \alpha + \beta)} \quad (90)$$

or

$$\leq p \frac{1 + \beta}{2} = \frac{1}{2} - \frac{\alpha - \beta}{2(2 + \alpha + \beta)}. \quad (91)$$

This means that $\text{SFP}(t, \epsilon)$ is in PQP if $\alpha - \beta > \epsilon \in \Omega(2^{-\text{poly}(n)})$. The proof is completed by the fact that $\text{PQP} = \text{PP}$. ■

This proof also provides an alternative proof of Theorem 7, stating that $\text{SFP}(t, \epsilon) \in \text{BQP}$ when $\epsilon \in \Omega(1/\text{poly}(n))$.

We next provide the proof of the hardness of SFP for sufficiently small promise gaps.

Theorem 10 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{SFP}(t, \epsilon)$ is PP -hard if $\epsilon \in \mathcal{O}(1/(K_n^2 2^n))$, where K_n is the cardinality of the set. This is the case even if $K_n \geq K_{\text{st}}(2^n, t, 0)$.

To show Theorem 10, we provide a polynomial-time reduction from a PP -complete problem, MAJ-SAT , to SFP . Below, we prove Theorem 10 by explicitly embedding the quantity $s(f)$ in MAJ-SAT to the state frame potential $F_t(\mathbf{S}_n)$.

Proof of Theorem 10. Let $f : \{0, 1\}^{n-2} \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time. Consider the same set \mathbf{S}_n defined by Eqs. (52) to (54), which has a computationally efficient description. As in Eq. (55), the state frame potential F_t of degree t for \mathbf{S}_n is given by

$$F_t(\mathbf{S}_n) = \left(1 - \frac{2}{K_n}\right)^2 F_t(\mathbf{S}_\varphi) + \frac{2}{K_n^2} \left[1 + \left(\frac{s(f)}{2^{n-2}}\right)^{2t}\right]. \quad (92)$$

We set α and β as

$$\alpha := \left(1 - \frac{2}{K_n}\right)^2 F_t(\mathbf{S}_\varphi) + \frac{2}{K_n^2} [1 + 2^{-2t}], \quad (93)$$

$$\beta := \left(1 - \frac{2}{K_n}\right)^2 F_t(\mathbf{S}_\varphi) + \frac{2}{K_n^2} \left[1 + \left(\frac{2^{n-3} - 1}{2^{n-2}}\right)^{2t}\right]. \quad (94)$$

It suffices for solving MAJ-SAT to determine either $F_t(\mathbf{S}_n) \geq \alpha$ or $\leq \beta$. As MAJ-SAT is PP -complete (Theorem 1), $\text{SFP}(t, \alpha - \beta)$ is PP -hard.

The promise gap, i.e., $\alpha - \beta$, is evaluated as

$$\alpha - \beta = \frac{1}{2^{2t-1} K_n^2} \left[1 - \left(1 - \frac{1}{2^{n-3}}\right)^{2t}\right] \quad (95)$$

$$\geq \frac{t}{2^{2t-1} K_n^2 (2^{n-4} + t)}, \quad (96)$$

where we have used $(1 - \epsilon)^m \leq (1 + m\epsilon)^{-1}$. ■

C. Complexity of UFP

In a similar way to SFP , we can clarify the computational complexity class of UFP .

Theorem 11 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{UFP}(t, \epsilon) \in \text{PP}$ if $\epsilon \in \Omega(2^{-\text{poly}(n)})$.

Proof of Theorem 11. Let $\alpha' := \alpha/2^{2m}$ and $\beta' := \beta/2^{2m}$. We run the following algorithm:

- (1) With probability $p = 2/(2 + \alpha' + \beta')$, proceed to the next step. With the remaining probability, output “reject.”
- (2) Select i and j from $\{1, 2, \dots, K_n\}$ uniformly at random.
- (3) Let $|\Phi\rangle = (1/\sqrt{2^n}) \sum_{k=0}^{2^n-1} |kk\rangle$ be a maximally entangled state. Perform the SWAP test for

$$|\Psi_i\rangle := ((I^{\otimes n} \otimes U_i) |\Phi\rangle)^{\otimes t} \quad (97)$$

and

$$|\Psi_j\rangle := ((I^{\otimes n} \otimes U_j) |\Phi\rangle)^{\otimes t}, \quad (98)$$

where $U_i, U_j \in \mathcal{U}_n$. If the outcome is 0 (1), output “accept” (“reject”).

The acceptance probability of this algorithm is

$$\frac{p}{K_n^2} \sum_{ij=1}^{K_n} \frac{1 + |\langle \Psi_i | \Psi_j \rangle|^2}{2} = p \frac{1 + F_t(\mathbf{U}_n)/2^{2m}}{2}, \quad (99)$$

which is either

$$\geq p \frac{1 + \alpha'}{2} = \frac{1}{2} + \frac{\alpha' - \beta'}{2(2 + \alpha' + \beta')} \quad (100)$$

or

$$\leq p \frac{1 + \beta'}{2} = \frac{1}{2} - \frac{\alpha' - \beta'}{2(2 + \alpha' + \beta')}. \quad (101)$$

This implies that $\text{UFP}(t, \epsilon)$ is in PQP . The fact that $\text{PQP} = \text{PP}$ completes the proof. ■

Unlike the case of $\text{SFP}(t, \epsilon)$, this proof does not imply that $\text{UFP}(t, \epsilon)$ is in BQP even if $\epsilon \in \Omega(1/\text{poly}(n))$. This is due to the factor 2^{-2m} in α' and β' .

Theorem 12 (restated). For any constant $t \in \mathbb{Z}^+$, $\text{UFP}(t, \mathcal{O}(2^{2(t-1)n}/K_n^2))$ is PP -hard, where K_n is the cardinality of the set. This is the case even if $K_n \geq K_{\text{uni}}(2^n, t, 0)$.

Proof of Theorem 12. We provide a polynomial-time reduction from a PP -complete problem, MAJ-SAT , to $\text{UFP}(t, \epsilon)$. Let $f : \{0, 1\}^{n-2} \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time. Consider the same set U_n defined by Eqs. (76)–(78), of unitaries on n qubits, which has a computationally efficient description. As in Eq. (79), the unitary frame potential for U_n is

$$F_t(U_n) = 2^{2t} \left(1 - \frac{2}{K_n}\right)^2 F_t(V_{n-1}) + \frac{2}{K_n^2} [2^{2nt} + g_t(s(f))], \quad (102)$$

where $g_t(x) = (2^n - 8 + 2^{-2n+7}x^2)^{2t}$.

We set α and β such as

$$\alpha := 2^{2t} \left(1 - \frac{2}{K_n}\right)^2 F_t(V_{n-1}) + \frac{2}{K_n^2} [2^{2nt} + g_t(2^{n-3})], \quad (103)$$

$$\beta := 2^{2t} \left(1 - \frac{2}{K_n}\right)^2 F_t(V_{n-1}) + \frac{2}{K_n^2} [2^{2nt} + g_t(2^{n-3} - 1)]. \quad (104)$$

If one can determine whether $F_t(U_n) \geq \alpha$ or $\leq \beta$, one can also determine if $M < 2^{n-3}$ or $M \geq 2^{n-3}$. Since the latter is MAJ-SAT and PP -complete due to Theorem 1, the former is PP -hard.

The promise gap $\epsilon = \alpha - \beta$ is computed as

$$\epsilon \geq \frac{2t(2^n - 6)^{2t} (1 + \mathcal{O}(2^{-n}))}{K_n^2 [2^{n-6}(2^n - 6) + t]} \in \Theta(2^{2(t-1)n}/K_n^2). \quad (105)$$

This concludes the proof. \blacksquare

VI. ANALYSIS OF COMPLEXITY OF StDes AND UniDes

We investigate the complexity class of StDes in Sec. VIA and that of UniDes in Sec. VIB.

A. Complexity of StDes

The fact that StDes is in PP if δ' and δ satisfy a certain condition directly follows from Theorem 9, i.e., from the statement that $\text{SFP}(t, \epsilon) \in \text{PP}$ if ϵ is not too small.

Theorem 13 (restated). For any constant $t \in \mathbb{Z}^+$ and $\delta^2 - d_t \delta^2 \in \Omega(2^{-\text{poly}(n)})$, $\text{StDes}(t, t, \delta, \delta') \in \text{PP}$.

Proof of Theorem 13. Due to the promise of the problem, it is guaranteed that a given set S_n is either a δ -approximate or not a δ' -approximate state t -design. If the former is the case, $F_t(S_n) \leq 1/d_t + \delta^2/d_t$ and, if the latter is the case, $F_t(S_n) > 1/d_t + \delta^2/d_t^2$. Since $(1/d_t + \delta^2/d_t^2) - (1/d_t + \delta^2/d_t) \in \Omega(2^{-\text{poly}(n)})$ by assumption, checking which is the case is in PP due to Theorem 9. Hence $\text{StDes}(t, t, \delta, \delta') \in \text{PP}$. \blacksquare

We next show the hardness of StDes . The following is the restatement of Theorem 14.

Theorem 14 (restated). For any constant $t \leq t' \in \mathbb{Z}^+$, $\delta \in \Omega(2^{-\text{poly}(n)})$, and δ' that satisfies

$$\delta' - \delta \in \begin{cases} \Theta(2^{(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-n}\delta), & \text{for } t = t', \end{cases} \quad (33a)$$

$\text{StDes}(t, t', \delta, \delta')$ is PP -hard under polynomial-time mapping reductions. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{st}}(2^n, t', 0)$.

Proof of Theorem 14. In the proof, we use the notation $d = 2^n$ for simplicity. Let $f : \{0, 1\}^{n-1} \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time, and let $|f\rangle$ and $|p\rangle$ be n -qubit state vectors given by, respectively,

$$|f\rangle = \sqrt{\frac{2}{d}} \sum_{x \in \{0, 1\}^{n-1}} |x\rangle |f(x)\rangle, \quad (106)$$

$$|p\rangle = |+\rangle^{\otimes n-1} |1\rangle. \quad (107)$$

Let δ_0 be such that $\delta_0 \in o(\delta/d)$, and $D_{t'}$ be a set of n -qubit state vectors with a computationally efficient description that forms an exact state 1-design and a δ_0 -approximate state t' -design. Such designs exist as $\delta \in \Omega(2^{-\text{poly}(n)})$. For instance, it can be generated by first applying Pauli operators uniformly at random to a fixed state and then applying a local random circuit with $\text{poly}(n)$ depth. The first application of Pauli operators guarantees that the generated states form an exact state 1-design. We denote by D the cardinality of $D_{t'}$.

We define a multiset $S_n(f)$ of state vectors by

$$S_n(f) = \{|f\rangle, |p\rangle\}^{\oplus m} \cup D_{t'}, \quad (108)$$

where $\oplus m$ implies the multiplicity $m \in \mathbb{Z}^+$. A key quantity in the proof is D/m , which we will later choose appropriately depending on δ . Here, we note that D/m can be an arbitrary positive rational number because we can choose

arbitrarily large positive integers m and D . Note that this is the case for D since, given a δ_0 -approximate state t' -design with some cardinality, one can increase its cardinality by changing the multiplicity of each state vector. The resulting multiset is a δ_0 -approximate state t' -design with cardinality that is an integer multiple of the original one.

For $\tau \in \{1, t, t'\}$, the set $S_n(f)$ is a $\delta_\tau(f)$ -approximate state τ -design, where

$$\delta_\tau(f) := d_\tau \left\| \Delta_{S_n(f)}^{(\tau)} \right\|_\infty \quad (109)$$

with

$$\Delta_{S_n(f)}^{(\tau)} := \frac{\Pi_{\text{sym}}^{(\tau)}}{d_\tau} - \mathbb{E}_{|\varphi\rangle \sim S_n(f)} [|\varphi\rangle\langle\varphi|^{\otimes\tau}]. \quad (110)$$

Here, $\Pi_{\text{sym}}^{(\tau)}$ is the projection onto the symmetric subspace $\mathcal{H}_{\text{sym}}^{(\tau)}$, $d_\tau = \text{Tr} \left[\Pi_{\text{sym}}^{(\tau)} \right]$, and

$$\begin{aligned} & \mathbb{E}_{|\varphi\rangle \sim S_n(f)} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] \\ & := \frac{1}{2m+D} \left[m(|f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau}) \right. \\ & \quad \left. + D \mathbb{E}_{|\varphi\rangle \sim D_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] \right]. \end{aligned} \quad (111)$$

Below, we compute $\delta_\tau(f)$.

We begin by checking the eigenvalues of $|f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau}$. By expanding $|f\rangle\langle f|^{\otimes\tau}$ as $\alpha_\tau |p\rangle\langle p|^{\otimes\tau} + \sqrt{1-\alpha_\tau^2} |q\rangle\langle q|^{\otimes\tau}$, where

$$\alpha_\tau = \langle p|f\rangle^\tau = \left(\frac{2s(f)}{d} \right)^\tau, \quad (112)$$

with $s(f) = \sum_{x \in \{0,1\}^{n-1}} f(x)$, and $|q\rangle$ orthogonal to $|p\rangle^{\otimes\tau}$, we have

$$|f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau} = \begin{pmatrix} 1 + \alpha_\tau^2 & \alpha_\tau \sqrt{1 - \alpha_\tau^2} \\ \alpha_\tau \sqrt{1 - \alpha_\tau^2} & 1 - \alpha_\tau^2 \end{pmatrix} \quad (113)$$

where the matrix representation is in terms of $\{|p\rangle^{\otimes\tau}, |q\rangle\}$. Hence the eigenvalues are $1 \pm \alpha_\tau$. Below, we denote the corresponding eigenvectors by $|\alpha_{\tau,\pm}\rangle$.

When $\tau = 1$, we can use the fact that $D_{t'}$ is an exact state 1-design. That is,

$$\mathbb{E}_{|\varphi\rangle \sim D_{t'}} [|\varphi\rangle\langle\varphi|] = \frac{I}{d}. \quad (114)$$

Also, $\Pi_{\text{sym}}^{(1)} = I$ and $d_1 = d$. Hence it follows that

$$\delta_1(f) = \frac{m}{2m+D} \|2I - d(|f\rangle\langle f| + |p\rangle\langle p|)\|_\infty \quad (115)$$

$$= \frac{1}{D/m+2} (d + 2s(f) - 2), \quad (116)$$

where we have used that the eigenvalues of $|f\rangle\langle f| + |p\rangle\langle p|$ are $1 \pm \alpha_1$, which is $1 \pm 2s(f)/d$.

When $\tau > 1$, we derive an upper and a lower bound on $\delta_\tau(f)$. Using the eigenvectors $|\alpha_{\tau,\pm}\rangle$, a lower bound on $\delta_\tau(f)$ is given as

$$\begin{aligned} & d_\tau \max \left\{ \left| \langle \alpha_{\tau,+} | \Delta_{S_n(f)}^{(\tau)} | \alpha_{\tau,+} \rangle \right|, \left| \langle \alpha_{\tau,-} | \Delta_{S_n(f)}^{(\tau)} | \alpha_{\tau,-} \rangle \right| \right\} \\ & \leq \delta_\tau(f), \end{aligned} \quad (117)$$

which turns out to be

$$d_\tau |\langle \alpha_{\tau,+} | \Delta_{S_n(f)}^{(\tau)} | \alpha_{\tau,+} \rangle| \leq \delta_\tau(f). \quad (118)$$

As $|\alpha_{\tau,+}\rangle \in \mathcal{H}_{\text{sym}}^{(\tau)}$, we have

$$\begin{aligned} \langle \alpha_{\tau,+} | \Delta_{S_n(f)}^{(\tau)} | \alpha_{\tau,+} \rangle & = \frac{1}{d_\tau} - \frac{1}{2m+D} (m(1 + \alpha_\tau) \\ & \quad + D \langle \alpha_{\tau,+} | \mathbb{E}_{|\varphi\rangle \sim D_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] | \alpha_{\tau,+} \rangle). \end{aligned} \quad (119)$$

Hence,

$$\begin{aligned} \delta_\tau(f) & \geq \left| 1 - \frac{d_\tau}{2m+D} (m(1 + \alpha_\tau) \right. \\ & \quad \left. + D \langle \alpha_{\tau,+} | \mathbb{E}_{|\varphi\rangle \sim D_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] | \alpha_{\tau,+} \rangle) \right|. \end{aligned} \quad (120)$$

Moreover, as $\tau \in \{1, t, t'\}$ and $t \leq t'$, $D_{t'}$ is a δ_0 -approximate state τ -design. This implies that

$$\frac{1 - \delta_0}{d_\tau} \leq \langle \alpha_{\tau,+} | \mathbb{E}_{|\varphi\rangle \sim D_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] | \alpha_{\tau,+} \rangle \leq \frac{1 + \delta_0}{d_\tau}. \quad (121)$$

From Eqs. (120) and (121), we obtain a lower bound on $\delta_\tau(f)$, which reads as

$$\frac{1}{D/m+2} \left[(1 + \alpha_\tau) d_\tau - 2 - \frac{D}{m} \delta_0 \right] \leq \delta_\tau(f). \quad (122)$$

Remember that $\alpha_\tau = (2s(f)/d)^\tau$. For the later convenience, we introduce a real-valued function $L_\tau(q, x)$ as

$$L_\tau(q, x) := \frac{1}{q+2} \left\{ \left[1 + \left(\frac{2x}{d} \right)^\tau \right] d_\tau - 2 - q\delta_0 \right\}. \quad (123)$$

Using this notation, we can rephrase the lower bound as $L_\tau(D/m, s(f)) \leq \delta_\tau(f)$.

It is easy to obtain an upper bound on $\delta_\tau(f)$. From the triangle inequality, we obtain

$$\delta_\tau(f) \leq d_\tau \left\| \frac{\Pi_{\text{sym}}^{(\tau)}}{d_\tau} - \frac{D}{2m+D} \mathbb{E}_{|\varphi\rangle \sim \mathcal{D}_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] \right\|_\infty + \frac{md_\tau}{2m+D} \left\| |f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau} \right\|_\infty. \quad (124)$$

As $\mathcal{D}_{t'}$ is a δ_0 -approximate state τ -design, it holds that

$$\left\| \frac{\Pi_{\text{sym}}^{(\tau)}}{d_\tau} - \frac{D}{2m+D} \mathbb{E}_{|\varphi\rangle \sim \mathcal{D}_{t'}} [|\varphi\rangle\langle\varphi|^{\otimes\tau}] \right\|_\infty \leq \left(1 - \frac{D}{2m+D}\right) \frac{1}{d_\tau} + \frac{D}{2m+D} \frac{\delta_0}{d_\tau}. \quad (125)$$

We also have

$$\left\| |f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau} \right\|_\infty = 1 + \alpha_\tau, \quad (126)$$

from the diagonalization of $|f\rangle\langle f|^{\otimes\tau} + |p\rangle\langle p|^{\otimes\tau}$. Hence we obtain

$$\delta_\tau(f) \leq \frac{1}{D/m+2} \left[(1 + \alpha_\tau)d_\tau + 2 + \frac{D}{m}\delta_0 \right]. \quad (127)$$

Similarly to the lower bound, we introduce a real-valued function $U_\tau(q, x)$ as

$$U_\tau(q, x) := \frac{1}{q+2} \left\{ \left[1 + \left(\frac{2x}{d} \right)^\tau \right] d_\tau + 2 + q\delta_0 \right\}, \quad (128)$$

and write the upper bound as $\delta_\tau(f) \leq U_\tau(D/m, s(f))$.

To summarize so far, we have obtained

$$\delta_1(f) = \frac{d + 2s(f) - 2}{D/m + 2}, \quad (129)$$

and for $\tau > 1$, a lower and an upper bound on $\delta_\tau(f)$:

$$L_\tau\left(\frac{D}{m}, s(f)\right) \leq \delta_\tau(f) \leq U_\tau\left(\frac{D}{m}, s(f)\right). \quad (130)$$

Importantly, for any fixed $q \geq 0$, both $L_\tau(q, x)$ and $U_\tau(q, x)$ are monotonically increasing in x when $x \geq 0$.

We now choose D/m . For our purpose, we specifically use D/m that approximately satisfies the following:

if $t = 1$,

$$\frac{d + 2s_0 - 2}{D/m + 2} = \delta, \quad (131)$$

with $s_0 = d/4 - 2/3$, and if $t > 1$,

$$L_t\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right) = \delta. \quad (132)$$

As L_t is defined as Eq. (123), the latter equation is explicitly given by

$$\frac{1}{D/m + 2} \left[\left\{ 1 + \left(\frac{1}{2} - \frac{4}{3d} \right)^t \right\} d_t - 2 \right] - \frac{D/m}{D/m + 2} \delta_0 = \delta. \quad (133)$$

As D/m can be an arbitrary positive rational number by choosing the appropriate cardinality D of $\mathcal{D}_{t'}$ and multiplicity m of $\{|f\rangle, |p\rangle\}$ in $\mathcal{S}_n(f)$, the solutions of these equations can be approximated by D/m with arbitrary precision.

With this choice of D/m , we set δ' as follows. If $t' = 1$,

$$\delta' = \frac{d + 2s_1 - 2}{D/m + 2}, \quad (134)$$

with $s_1 = d/4 - 1/3$, and if $t' > 1$,

$$\delta' := U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) \quad (135)$$

$$= \frac{1}{D/m + 2} \left[\left\{ 1 + \left(\frac{1}{2} - \frac{2}{3d} \right)^{t'} \right\} d_{t'} + 2 \right] + \frac{D/m}{D/m + 2} \delta_0. \quad (136)$$

From simple calculations and using $\delta_0 \in o(\delta/d)$, it follows that

$$\delta' \in \Theta(d^{t'-t}\delta). \quad (137)$$

Clearly, $\delta' - \delta \in \Theta(\delta') = \Theta(d^{t'-t}\delta)$ for $t < t'$. When $t = t'$, it is also straightforward to see that $\delta' - \delta \in \Theta(\delta/d)$.

Below, we show that MAJ-SAT can be solved by a single use of the algorithm \mathcal{A} for solving $\text{StDes}(t, t', \delta, \delta')$. By definition, the algorithm \mathcal{A} can determine whether $\mathcal{S}_n(f)$ satisfies

$$\delta_{t'}(f) > \delta' \quad \text{or} \quad \delta_{t'}(f) \leq \delta, \quad (138)$$

under the exclusive assumption that only one of the two holds.

We begin by checking that, for any Boolean function $f : \{0, 1\}^{n-1} \rightarrow \{0, 1\}$, the corresponding set $\mathcal{S}_n(f)$ must exclusively satisfy one of the two conditions in Eq. (138).

We check this condition separately for three cases. The first case is $t = t' = 1$, the second case is $t = 1 < t'$, and the last case is $1 < t \leq t'$.

In the first case, in which $t = t' = 1$, we observe from Eqs. (129), (131), and (134) that

$$\delta_1(f) \leq \delta \iff s(f) \leq s_0 = \frac{d}{4} - \frac{2}{3}, \quad (139)$$

$$\delta_1(f) > \delta' \iff \frac{d}{4} - \frac{1}{3} = s_1 < s(f). \quad (140)$$

As $s(f)$ is a non-negative integer, these cases are equivalent to

$$\delta_1(f) \leq \delta \iff s(f) \leq \frac{d}{4} - 1, \quad (141)$$

$$\delta_1(f) > \delta' \iff \frac{d}{4} \leq s(f). \quad (142)$$

It is clear that all Boolean functions must exclusively satisfy one of the two.

In the second case, in which $t = 1 < t'$, as shown above, $\delta_1(f) \leq \delta$ is equivalent to $s(f) \leq d/4 - 1$. On the other hand, if $\delta_{t'}(f) > \delta'$, it follows from Eqs. (130) and (135) that

$$U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) = \delta' < \delta_{t'}(f) \leq U_{t'}\left(\frac{D}{m}, s(f)\right). \quad (143)$$

As $U_{t'}(q, x)$ is monotonically increasing in x for any fixed $q \geq 0$, this implies that $s(f) > d/4 - 1/3$. As $s(f)$ is a non-negative integer, we conclude that $\delta_{t'}(f) > \delta'$ implies that $s(f) \geq d/4$. We also show that if $s(f) \geq d/4$, then $\delta_{t'}(f) > \delta'$. That is, $\delta_{t'}(f) > \delta'$ is equivalent to $s(f) \geq d/4$. We show the contraposition of this statement. To this end, it is crucial to note that

$$U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) < L_{t'}\left(\frac{D}{m}, \frac{d}{4}\right), \quad (144)$$

which is obtained by the direct calculation using $1 < t'$, and the fact that $D_{t'}$ is a δ_0 -approximate state t' -design with $\delta_0 \in o(\delta/d)$. As δ' for $t' > 1$ is defined as Eq. (135), this implies that

$$\delta' < L_{t'}\left(\frac{D}{m}, \frac{d}{4}\right). \quad (145)$$

Thus, if $\delta_{t'}(f) \leq \delta'$, we obtain, by using Eq. (130),

$$L_{t'}\left(\frac{D}{m}, s(f)\right) \leq \delta_{t'}(f) \leq \delta' < L_{t'}\left(\frac{D}{m}, \frac{d}{4}\right). \quad (146)$$

Using the monotonicity of $L_{t'}(q, x)$, this reduces to $s(f) < d/4$. That is, $\delta_{t'}(f) \leq \delta'$ implies that $s(f) < d/4$. Taking the contraposition of this, we obtain that $s(f) \geq d/4$ implies that $\delta_{t'}(f) > \delta'$.

All together, in the case of $t = 1 < t'$, we have

$$\delta_1(f) \leq \delta \iff s(f) \leq \frac{d}{4} - 1, \quad (147)$$

$$\delta_{t'}(f) > \delta' \iff \frac{d}{4} \leq s(f). \quad (148)$$

Clearly, all Boolean functions must exclusively satisfy one of the two.

Finally, when $1 < t \leq t'$, we begin by rephrasing $\delta_t(f) \leq \delta$ in terms of $s(f)$. If $\delta_t(f) \leq \delta$, we have, from Eqs. (130) and (132),

$$L_t\left(\frac{D}{m}, s(f)\right) \leq \delta_t(f) \leq \delta = L_t\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right). \quad (149)$$

As $L_t(q, x)$ is monotonically increasing in x for any fixed $q \geq 0$, together with the fact that $s(f)$ is a non-negative integer, this implies that $s(f) \leq d/4 - 1$. We can also show that $d/4 - 1 \geq s(f)$ implies that $\delta_t(f) \leq \delta$. To this end, we consider the contraposition. The crucial observation is

$$U_t\left(\frac{D}{m}, \frac{d}{4} - 1\right) \leq L_t\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right), \quad (150)$$

which can be shown using $1 < t$ and the fact that D_t is a δ_0 -approximate state t -design with $\delta_0 \in o(\delta/d)$. Note that $t \leq t'$. From Eq. (132), this implies that

$$U_t\left(\frac{D}{m}, \frac{d}{4} - 1\right) \leq \delta. \quad (151)$$

Hence, if $\delta_t(f) > \delta$, then

$$U_t\left(\frac{D}{m}, \frac{d}{4} - 1\right) \leq \delta < \delta_t(f) \leq U_t\left(\frac{D}{m}, s(f)\right), \quad (152)$$

where we have used Eq. (130). Using the monotonicity of $U_t(q, x)$, this further implies that $d/4 - 1 < s(f)$. By taking the contraposition, we obtain that $d/4 - 1 \geq s(f)$ implies that $\delta_t(f) \leq \delta$.

Therefore, when $1 < t \leq t'$, we have

$$\delta_t(f) \leq \delta \iff s(f) \leq \frac{d}{4} - 1, \quad (153)$$

$$\delta_{t'}(f) > \delta' \iff \frac{d}{4} \leq s(f). \quad (154)$$

Note that the latter follows from Eq. (148). Thus, also in the case of $1 < t \leq t'$, all Boolean functions must exclusively satisfy one of the two conditions in Eq. (138).

We finally show that the algorithm \mathcal{A} for solving $\text{StDes}(t, t', \delta, \delta')$ can be used to solve MAJ-SAT. We simply apply the algorithm \mathcal{A} to the set $S_n(f)$ constructed from

a Boolean function f . As we have shown, $S_n(f)$ satisfies the exclusive promise of $\text{StDes}(t, t', \delta, \delta')$ and, hence, the algorithm \mathcal{A} can determine which of the following two is the case:

$$\delta_{t'}(f) > \delta' \quad \text{or} \quad \delta_t(f) \leq \delta. \quad (155)$$

From Eqs. (141), (142), (147), (148), (153), and (154), it is clear that, for any $t \leq t'$, the algorithm \mathcal{A} can decide

$$s(f) \geq \frac{d}{4} = 2^{n-2}, \quad \text{or} \quad s(f) \leq \frac{d}{4} - 1 = 2^{n-2} - 1. \quad (156)$$

Hence one can efficiently solve MAJ-SAT with one query to \mathcal{A} . \blacksquare

B. Complexity of UniDes

The same proof technique as for Theorems 13 and 14 can be applied to proving Theorems 15 and 16, respectively.

Theorem 15 (restated). For any constant $t \in \mathbb{Z}^+$ and $\delta^2 - 2^{2t}\delta^2 \in \Omega(2^{-\text{poly}(n)})$, $\text{UniDes}(t, t, \delta, \delta') \in \text{PP}$.

Proof of Theorem 15. Due to the promise of the problem, it is guaranteed that a given set U_n is either a δ -approximate or not a δ' -approximate unitary t -design. If the former is the case, $F_t(U_n) \leq t! + \delta^2$ and, if the latter is the case, $F_t(U_n) > t! + \delta'^2/2^{2t}$. Since $(t! + \delta'^2/2^{2t}) - (t! + \delta^2) \in \Omega(2^{-\text{poly}(n)})$ by assumption, checking which is the case is in PP due to Theorem 11. Hence $\text{UniDes}(t, t, \delta, \delta') \in \text{PP}$. \blacksquare

Below is a restatement of Theorem 16 for clarity.

Theorem 16 (restated). For any constant $t \leq t' \in \mathbb{Z}^+$, $\delta \in \Omega(2^{-\text{poly}(n)}) \cap o(2^{2(t-1)n})$, and δ' that satisfies

$$\delta' - \delta \in \begin{cases} \Theta(2^{2(t'-t)n}\delta), & \text{for } t < t', \\ \Theta(2^{-2n}\delta), & \text{for } t = t', \end{cases} \quad (34a)$$

$\text{UniDes}(t, t', \delta, \delta')$ is PP-hard under polynomial-time mapping reductions. This is the case even if the cardinality K_n of the set satisfies $K_n \geq K_{\text{uni}}(2^n, t', 0)$.

Proof of Theorem 16. The proof is almost in parallel with that of StDes , though we make use of unitaries instead of state vectors. Let $f : \{0, 1\}^{n-1} \rightarrow \{0, 1\}$ be a Boolean function that is computable in classical polynomial time and let $|f\rangle$ and $|p\rangle$ be n -qubit state vectors given

by, respectively,

$$|f\rangle = \sqrt{\frac{2}{d}} \sum_{x \in \{0, 1\}^{n-1}} |x\rangle |f(x)\rangle, \quad (157)$$

$$|p\rangle = |+\rangle^{\otimes n-1} |1\rangle. \quad (158)$$

Using these states, we define unitaries as

$$V_f = I - 2|f\rangle\langle f|, \quad \text{and} \quad V_p = I - 2|p\rangle\langle p|. \quad (159)$$

Let δ_0 be such that $\delta_0 \in O(\delta^2/d^{2t})$ and let $D_{t'}$ be a δ_0 -approximate unitary t' -design of n qubits with a computationally efficient description, which can be generated by, e.g., local random circuits with $\text{poly}(n)$ depth. We denote by D the cardinality of $D_{t'}$.

We define a multiset $U_n(f)$ of unitaries by

$$U_n(f) = \{V_f, V_p\}^{\oplus m} \cup D_{t'}, \quad (160)$$

where $\oplus m$ implies the multiplicity $m \in \mathbb{Z}^+$. Later, we determine D and m depending on δ such that D/m is appropriately set for our purpose. Note that D/m can be an arbitrary positive rational number.

Let $\tau \in \{t, t'\}$. The set $U_n(f)$ is a $\delta_\tau(f)$ -approximate unitary τ -design, where

$$\delta_\tau(f) := \left\| M_{U_n(f)}^{(\tau)} - M_{\text{H}}^{(\tau)} \right\|_1. \quad (161)$$

Here, $M_\mu^{(\tau)} = \mathbb{E}_{U \sim \mu}[U^{\otimes \tau} \otimes \bar{U}^{\otimes \tau}]$ is the moment operator. Below, we compute a lower and an upper bound on $\delta_\tau(f)$.

The moment operator of the Haar measure is a projector onto the irreducible representation of $\pi_\tau : U \mapsto U^{\otimes \tau} \otimes \bar{U}^{\otimes \tau}$. Denoting the projector by $\Pi_{\text{irrep}}^{(\tau)}$, the moment operator of the uniform measure on $U_n(f)$ is in the form of

$$M_{U_n(f)}^{(\tau)} = \Pi_{\text{irrep}}^{(\tau)} + \Pi_{\text{irrep}}^{(\tau)\perp} M_{U_n(f)}^{(\tau)} \Pi_{\text{irrep}}^{(\tau)\perp}, \quad (162)$$

where $\Pi_{\text{irrep}}^{(\tau)\perp} = I - \Pi_{\text{irrep}}^{(\tau)}$. Note that we have used the irreducibility. Hence,

$$\delta_\tau(f) = \left\| \Pi_{\text{irrep}}^{(\tau)\perp} M_{U_n(f)}^{(\tau)} \Pi_{\text{irrep}}^{(\tau)\perp} \right\|_1, \quad (163)$$

with

$$M_{U_n(f)}^{(\tau)} = \mathbb{E}_{U \sim U_n(f)}[\pi_\tau(U)] \quad (164)$$

$$= \frac{1}{D + 2m} \left[m(\pi_\tau(V_f) + \pi_\tau(V_p)) + DM_{D_{t'}}^{(\tau)} \right]. \quad (165)$$

From the triangle inequality, we have that

$$\begin{aligned} & \frac{1}{D + 2m} |mA - DB| \\ & \leq \delta_\tau(f) \leq \frac{1}{D + 2m} (mA + DB), \end{aligned} \quad (166)$$

where

$$A = \left\| \Pi_{\text{irrep}}^{(\tau)\perp} (\pi_\tau(V_f) + \pi_\tau(V_p)) \Pi_{\text{irrep}}^{(\tau)\perp} \right\|_1 \quad (167)$$

$$B = \left\| \Pi_{\text{irrep}}^{(\tau)\perp} M_{D'}^{(\tau)} \Pi_{\text{irrep}}^{(\tau)\perp} \right\|_1 \leq \delta_0. \quad (168)$$

Note that the upper bound on B follows from the fact that D' is a δ_0 -approximate τ -design as $\tau \in \{t, t'\}$ and $t \leq t'$.

To compute A , we use the expansion that

$$\begin{aligned} & \pi_\tau(V_f) + \pi_\tau(V_p) \\ &= 2\Pi_{\text{irrep}}^{(\tau)} + \Pi_{\text{irrep}}^{(\tau)\perp} (\pi_\tau(V_f) + \pi_\tau(V_p)) \Pi_{\text{irrep}}^{(\tau)\perp} \end{aligned} \quad (169)$$

and the fact that the first and the remaining term in the right-hand side have orthogonal support. Hence, using $\tau! = \text{Tr} \left[\Pi_{\text{irrep}}^{(\tau)} \right]$, we obtain

$$\begin{aligned} & \left\| \pi_\tau(V_f) + \pi_\tau(V_p) \right\|_1 \\ &= \left\| \Pi_{\text{irrep}}^{(\tau)\perp} (\pi_\tau(V_f) + \pi_\tau(V_p)) \Pi_{\text{irrep}}^{(\tau)\perp} \right\|_1 + 2\tau!. \end{aligned} \quad (170)$$

In Appendix C, we show that

$$\left\| \pi_\tau(V_f) + \pi_\tau(V_p) \right\|_1 = \Lambda_\tau(s(f)). \quad (171)$$

Here, $\Lambda_\tau(x)$ is defined for $x \in [0, d/2]$ as

$$\begin{aligned} & \Lambda_\tau(x) \\ &:= 2 \sum_{s=0}^{2\tau} \binom{2\tau}{s} (d-2)^{2\tau-s} \sum_{r=0}^s \binom{s}{r} \left| T_{|2r-s|} \left(\frac{2x}{d} \right) \right| \end{aligned} \quad (172)$$

and $T_m(z) = \cos m\theta$, where $z = \cos \theta$, are the Chebyshev polynomials of the first kind. Hence,

$$A = \Lambda_\tau(s(f)) - 2\tau!. \quad (173)$$

Substituting A and B into Eq. (166), we obtain

$$\begin{aligned} & \frac{1}{D/m+2} \left(\Lambda_\tau(s(f)) - 2\tau! - \frac{D}{m}\delta_0 \right) \\ & \leq \delta_\tau(f) \leq \frac{1}{D/m+2} \left(\Lambda_\tau(s(f)) - 2\tau! + \frac{D}{m}\delta_0 \right). \end{aligned} \quad (174)$$

In the lower bound, we have assumed that δ_0 is sufficiently small. We will check this condition later.

For later convenience, we introduce functions $U_\tau(q, x)$ and $L_\tau(q, x)$ by

$$U_\tau(q, x) = \frac{1}{q+2} (\Lambda_\tau(x) - 2\tau! + q\delta_0) \quad (175)$$

$$L_\tau(q, x) = \frac{1}{q+2} (\Lambda_\tau(x) - 2\tau! - q\delta_0), \quad (176)$$

using which we have

$$L_\tau \left(\frac{D}{m}, s(f) \right) \leq \delta_\tau(f) \leq U_\tau \left(\frac{D}{m}, s(f) \right). \quad (177)$$

Importantly, for any fixed $q \geq 0$, these functions are monotonically increasing as x increases for sufficiently large d . Indeed, the leading-order expansion of $\Lambda_\tau(x)$ is given by

$$\Lambda_\tau(x) = 2d^{2\tau} - 8\tau d^{2\tau-1} \left(1 - \frac{2x}{d} \right) + \mathcal{O}(d^{2\tau-2}), \quad (178)$$

as shown in Appendix C. Thus, if d is sufficiently large, $\Lambda_\tau(x)$ is monotonically increasing in x , and so are $U_\tau(q, x)$ and $L_\tau(q, x)$ for a fixed $q \geq 0$.

We now choose D and m such that D/m satisfies

$$L_t \left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3} \right) = \delta. \quad (179)$$

From the order estimation of $\Lambda_t(x)$ and the facts that $\delta_0 \in \mathcal{O}(\delta^2/d^{2t})$ and $\delta \in o(d^{2(t-1)})$, which implies that $\delta \in o(d^{2t})$, we have $D/m \in \Theta(d^{2t}/\delta)$. We also check the assumption on δ_0 in Eq. (174), which is that δ_0 is sufficiently small such that $L_\tau(D/m, s(f)) \geq 0$. As $D/m \in \Theta(d^{2t}/\delta)$, this condition is satisfied when $\delta_0 \in \mathcal{O}(\delta^2/d^{2t})$, which we have assumed. We also set δ' as

$$\delta' = U_{t'} \left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3} \right) \in \Theta(d^{2(t'-t)}\delta). \quad (180)$$

Clearly, $\delta' - \delta \in \Theta(d^{2(t'-t)}\delta)$ for $t < t'$. When $t = t'$, we need more careful analysis based on Eq. (178), from which it turns out that $\delta' - \delta \in \Theta(d^{-2}\delta)$ for $t = t'$.

With this choice of D/m , we below show that an algorithm \mathcal{A} to solve $\text{UniDes}(t, t', \delta, \delta')$ can be used to solve MAJ-SAT. By definition, the algorithm can determine

$$\delta_{t'}(f) > \delta', \quad \text{or} \quad \delta_t(f) \leq \delta, \quad (181)$$

under the exclusive promise that only one of the two holds.

Let us first check if $U_n(f)$ constructed from any Boolean function $f : \{0, 1\}^{n-1} \rightarrow \{0, 1\}$ satisfies the exclusive promise. To this end, we show that

$$\delta_{t'}(f) > \delta' \iff s(f) \geq \frac{d}{4}, \quad (182)$$

$$\delta_{t'}(f) \leq \delta \iff s(f) \leq \frac{d}{4} - 1. \quad (183)$$

From these two, it is clear that all Boolean functions must exclusively satisfy one of the two conditions $\delta_{t'}(f) \leq \delta$ or $\delta_{t'}(f) > \delta'$.

To show Eq. (182), we begin by assuming that $\delta_{t'}(f) > \delta'$. If this is satisfied, it follows from Eqs. (177) and (180) that

$$U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) = \delta' < \delta_{t'}(f) \leq U_{t'}\left(\frac{D}{m}, s(f)\right). \quad (184)$$

Using the monotonicity of $U_{t'}(q, x)$ in x , we have $d/4 - 1/3 < s(f)$. Moreover, $s(f)$ is a non-negative integer, leading to $d/4 \leq s(f)$.

On the other hand, if $d/4 \leq s(f)$, $\delta_{t'}(f) > \delta'$. To show this, we use the fact that, for sufficiently large d ,

$$U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) < L_{t'}\left(\frac{D}{m}, \frac{d}{4}\right), \quad (185)$$

which is shown in Appendix D using the assumption that $\delta \in o(d^{2(t'-1)})$. Hence, if $\delta_{t'}(f) \leq \delta'$, it follows from Eqs. (177) and (180) that

$$\begin{aligned} L_{t'}\left(\frac{D}{m}, s(f)\right) &\leq \delta_{t'}(f) \leq \delta' \\ &= U_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3}\right) < L_{t'}\left(\frac{D}{m}, \frac{d}{4}\right). \end{aligned} \quad (186)$$

From the monotonicity of $L_{t'}(q, x)$ in x , we conclude that $\delta_{t'}(f) \leq \delta'$ implies that $s(f) < d/4$. Taking the contraposition, we obtain that if $s(f) \geq d/4$, then $\delta_{t'}(f) > \delta'$.

To show Eq. (183), if $\delta_{t'}(f) \leq \delta$, we have, from Eqs. (177) and (179), that

$$L_{t'}\left(\frac{D}{m}, s(f)\right) \leq \delta_{t'}(f) \leq \delta = L_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right). \quad (187)$$

Using the monotonicity of $L_{t'}(q, x)$ in x and the fact that $s(f)$ is a non-negative integer, this implies that $s(f) \leq d/4 - 1$. To show that $s(f) \leq d/4 - 1$ implies that $\delta_{t'}(f) \leq \delta$, we consider its contraposition. A key observation is

$$U_{t'}\left(\frac{D}{m}, \frac{d}{4} - 1\right) < L_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right), \quad (188)$$

shown in Appendix D, using the assumption that $\delta \in o(d^{2(t'-1)})$. Hence, if $\delta_{t'}(f) > \delta$, we have, from Eqs. (177)

and (179), that

$$\begin{aligned} U_{t'}\left(\frac{D}{m}, \frac{d}{4} - 1\right) &< L_{t'}\left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3}\right) = \delta \\ &< \delta_{t'}(f) \leq U_{t'}\left(\frac{D}{m}, s(f)\right). \end{aligned} \quad (189)$$

From the monotonicity, we have $d/4 - 1 < s(f)$. By taking the contraposition, we obtain that $s(f) \leq d/4 - 1$ implies that $\delta_{t'}(f) \leq \delta$.

We finally show how the algorithm \mathcal{A} for solving $\text{UniDes}(t, t', \delta, \delta')$ can be used to solve MAJ-SAT. As $U_n(f)$ satisfies the exclusive promise of $\text{UniDes}(t, t', \delta, \delta')$ for any Boolean function f , the algorithm is capable of determining whether $U_n(f)$ satisfies

$$\delta_{t'}(f) > \delta' \quad \text{or} \quad \delta_{t'}(f) \leq \delta. \quad (190)$$

From Eqs. (182) and (183), this implies that \mathcal{A} can determine

$$s(f) \geq \frac{d}{4} = 2^{n-2}, \quad \text{or} \quad s(f) \leq \frac{d}{4} - 1 = 2^{n-2} - 1. \quad (191)$$

Hence one can efficiently solve MAJ-SAT with one query to \mathcal{A} . \blacksquare

VII. CONCLUSIONS AND DISCUSSION

In this paper, we have initiated computational complexity-theoretic analyses about the problems related to unitary and state designs and have paved the way to understanding randomness in quantum systems from the complexity perspective. We have begun with an explicit quantum algorithm for computing the state and unitary frame potentials and then clarified the complexity classes of exactly computing the frame potentials, $\text{compSFP}(t)$ and $\text{compUFP}(t)$, which have been shown to be $\#\text{P}$ -hard and to be achievable by a single query to a $\#\text{P}$ oracle.

We have then introduced promise problems, $\text{SFP}(t, \epsilon)$ and $\text{UFP}(t, \epsilon)$, to decide whether the frame potential is larger than or smaller than certain values with a promise gap ϵ . These problems are important to address the complexity of approximately computing the frame potentials. For $\text{SFP}(t, \epsilon)$, we have proven that the problem is BQP -complete for $\epsilon \in \Theta(1/\text{poly}(n))$, but is PP -complete for $\epsilon \in \Theta(2^{-\text{poly}(n)})$. The latter has been shown to be the case for $\text{UFP}(t, \epsilon)$.

We have finally addressed promise problems that are directly related to state and unitary designs: whether a given set is a δ -approximate t -design or not a δ' -approximate t' -design, under the promise that only one of the two is the case. We have shown that these problems, $\text{StDes}(t, t', \delta, \delta')$ and $\text{UniDes}(t, t', \delta, \delta')$, are in **PP** if $t = t'$ and the gap between δ and δ' is not too small. We have also shown the hardness result. Specifically, these problems are **PP**-hard if the gap is $\delta' - \delta \in \Theta(2^{c(t'-t)n}\delta)$ for $t < t'$ and $\delta' - \delta \in \Theta(2^{-cn}\delta)$ for $t = t'$, where $c = 1$ for $\text{StDes}(t, t', \delta, \delta')$ and $c = 2$ for $\text{UniDes}(t, t', \delta, \delta')$. We would like to emphasize that these results imply the computational hardness of deciding if a given set is an exponentially accurate approximation to a t -design or a constant-away approximation to a $(t + 1)$ -design that is not an accurate t -design, highlighting the computationally hard nature of checking design properties.

These results have far-reaching implications, owing to the broad applicability of complexity theory and the universal significance of designs. Specifically, we have demonstrated their relevance to variational constructions of designs, the characterization of quantum chaos via the average OTOC, and the emergence of designs in Hamiltonian systems. Notably, our results imply that, for algorithms addressing these problems to scale efficiently to large systems, it is crucial to tailor them to leverage the specific structure of the underlying problems.

While we have thoroughly investigated the computational complexity classes of the introduced problems, the complexity in some parameter regions, such as $\text{UFP}(t, \epsilon)$ for $\epsilon \in \Omega(1/\text{poly}(n))$, remains open. Investigating these cases is an important future work. While it is natural to expect that $\text{UFP}(t, \epsilon)$ with inverse-polynomial or constant ϵ is computationally easy, showing this is not straightforward, at least in our approach. The difficulty is intrinsic in our approach, where we start with a quantum algorithm to compute the purity of a quantum state that encodes all the information of the unitary frame potential. This approach inevitably introduces the prefactor 2^{-2nt} between the unitary frame potential and the purity. Therefore, for estimating the frame potential with constant approximation in our approach, it is necessary to evaluate the purity with exponential accuracy, which is, in general, computationally intractable. This is, however, the difficulty specific to our approach, and it is open if $\text{UFP}(t, \epsilon)$ with inverse-polynomial or constant ϵ is computationally feasible. Developing a new approach toward this is an interesting open problem.

Regarding $\text{StDes}(t, t', \delta, \delta')$ and $\text{UniDes}(t, t', \delta, \delta')$, it is of great interest to further investigate the problems when $t = t'$. In this case, we have succeeded in proving the hardness only with small gap $\delta' - \delta$. To this end, however, our methods, i.e., to hide a hard instance in a set, may not work. It may also be interesting to consider the computational problems related to other definitions of unitary

designs, such as the one based on the diamond norm. As different definitions do not lead to significant differences in applications, this is not practically important but may still be of theoretical interest. In this case, the key is to tightly compute the approximation accuracy as we have done for proving the **PP**-hardness of UniDes in terms of the moment operators.

Our results, showing the computationally hard nature of checking design properties, indicate that there may exist *pseudo*- t -designs, namely, a set of state vectors or unitaries that is not a t -design but is indistinguishable from t -designs in polynomial time. This direction may be of interest in regard to the recent progress in computationally secure quantum cryptography based on pseudorandom states or unitaries. We expect that our results, that good t -design cannot be efficiently distinguished from bad $(t + 1)$ -design that fails to be a good t -design, could offer an interesting starting point toward this direction.

From a more practical viewpoint, it will also be important to consider restricted sets of state vectors or unitaries, for which the problems that we have introduced in this work become solvable in classical or quantum polynomial time. This direction is of significant importance for developing the practical variational ansatz for constructing designs or algorithms for studying emergent designs in Hamiltonian systems.

ACKNOWLEDGMENTS

We would like to thank Özgün Kum for discussions on computational complexity theory and Masaki Owari for discussions about the algorithms for computing the frame potential. Y.N. is supported by Japan Society for the Promotion of Science (JSPS) KAKENHI Grant No. JP22K03464, Ministry of Education, Culture, Sports, Science and Technology (MEXT)–KAKENHI Grant-in-Aid for Transformative Research Areas (A) “Extreme Universe” Grants No. JP21H05182 and No. JP21H05183, Japan Science and Technology Agency (JST) CREST Grant No. JPMJCR23I3, and JST PRESTO Grant No. JPMJPR2456. Y.T. is partially supported by JST Moonshot R&D—MILLENNIA Program Grant No. JPMJMS2061. M.K. is supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) within the Emmy Noether program (Grant No. 441423094) and Fujitsu Germany GmbH as part of the endowed professorship “Quantum Inspired and Quantum Optimization.” A.D. is supported by MEXT-KAKENHI Grant-in Aid for Transformative Research Areas (A) “Extreme Universe” Grant No. 21H05183.

DATA AVAILABILITY

No data were created or analyzed in this study.

APPENDIX A: PROOFS OF PROPOSITIONS 1 AND 2

1. Proof of Proposition 1

Here, we provide a proof of Proposition 1 for completeness. Note that we assume that $t \leq d$, but similar statements hold even for $t > d$.

Proposition 1 (restated). Let $d, t \in \mathbb{Z}^+$ be such that $t \leq d$, and $d_t = \binom{d+t-1}{t}$. The following hold for the state frame potential of degree t :

- (1) $F_t(\mathbb{H}) = 1/d_t$.
- (2) For any probability measure μ on a nonempty set of state vectors,

$$F_t(\mu) \in [1/d_t, 1], \quad (7a)$$

where equality of the lower bound holds if and only if it is an exact state t -design. For the uniform measure on a finite set \mathbb{S} with cardinality K ,

$$F_t(\mathbb{S}) \in [\max\{1/d_t, 1/K\}, 1]. \quad (8a)$$

- (3) If a finite set \mathbb{S} of state vectors is a δ -approximate state t -design, then

$$F_t(\mathbb{S}) \leq \frac{1}{d_t} + \frac{\delta^2}{d_t}. \quad (9a)$$

- (4) If a finite set \mathbb{S} of state vectors satisfies

$$F_t(\mathbb{S}) \leq \frac{1}{d_t} + \frac{\delta^2}{d_t^2}, \quad (10a)$$

then \mathbb{S} is a δ -approximate state t -design.

- (5) For a finite set \mathbb{S} of state vectors to be a δ -approximate state t -design, it has to contain at least $K_{\text{st}}(d, t, \delta)$ state vectors, where

$$K_{\text{st}}(d, t, \delta) := \frac{d_t}{1 + \delta^2}. \quad (11a)$$

Proof of Proposition 1. The state frame potential for a uniformly distributed state can be calculated directly using Eqs. (3) and (5).

To show the second statement, we begin with the fact that the support of the state $\sum_{j=1}^K |\psi_j\rangle\langle\psi_j|^{\otimes t}/K$ is the symmetric subspace, as it is a probabilistic mixture of symmetric states. The frame potential is defined by the squared Hilbert-Schmidt norm of the state and its minimum $1/d_t$ is attained by the completely mixed state on the subspace, which corresponds to a state averaged over an exact state t -design. The upper bound follows from the simple facts that $|\langle\phi|\psi\rangle| \leq 1$ for any state vectors $|\phi\rangle$ and $|\psi\rangle$. For

the uniform probability measure over a finite set \mathbb{S} with cardinality K , the frame potential further satisfies

$$F_t(\mathbb{S}) = \frac{1}{K^2} \sum_{i,j=1}^K |\langle\psi_i|\psi_j\rangle|^{2t} \quad (A1)$$

$$\geq \frac{1}{K^2} \sum_{j=1}^K |\langle\psi_j|\psi_j\rangle|^{2t} \quad (A2)$$

$$= \frac{1}{K}. \quad (A3)$$

To show the third statement, we start with the definition of a state design. If a set \mathbb{S} is a δ -approximate state t -design, Eq. (2) holds. Since $\|\cdot\|_2 \leq \sqrt{\text{rank}(\cdot)}\|\cdot\|_\infty$, we have

$$\left\| \frac{1}{K} \sum_{j=1}^K |\psi_j\rangle\langle\psi_j|^{\otimes t} - \frac{\Pi_{\text{sym}}(n, t)}{d_t} \right\|_2 \leq \frac{\delta}{\sqrt{d_t}}, \quad (A4)$$

where we have used Eq. (3). By direct calculation and Eq. (5), the left-hand side satisfies

$$\left\| \frac{1}{K} \sum_{j=1}^K |\psi_j\rangle\langle\psi_j|^{\otimes t} - \frac{\Pi_{\text{sym}}(n, t)}{d_t} \right\|_2^2 = F_t(\mathbb{S}) - \frac{1}{d_t}. \quad (A5)$$

Hence the third statement holds.

The fourth statement is shown as follows. Suppose that a set $\mathbb{S} = \{|\psi_j\rangle\}_{j=1, \dots, K}$ satisfies $F_t(\mathbb{S}) \leq 1/d_t + \delta^2/d_t^2$. A direct calculation leads to

$$\left\| \frac{1}{K} \sum_{j=1}^K |\psi_j\rangle\langle\psi_j|^{\otimes t} - \frac{\Pi_{\text{sym}}(n, t)}{d_t} \right\|_2 \leq \delta/d_t. \quad (A6)$$

As $\|\cdot\|_\infty \leq \|\cdot\|_2$, we obtain

$$\left\| \frac{1}{K} \sum_{j=1}^K |\psi_j\rangle\langle\psi_j|^{\otimes t} - \frac{\Pi_{\text{sym}}(n, t)}{d_t} \right\|_\infty \leq \delta/d_t, \quad (A7)$$

which implies that \mathbb{S} is a δ -approximate state t -design.

Finally, suppose that the cardinality K of a set $\mathbb{S} = \{|\psi_j\rangle\}_{j=1, \dots, K}$ is less than $d_t/(1 + \delta^2)$. Together with Eq. (A3), we have

$$F_t(\mathbb{S}) \geq \frac{1}{K} > \frac{1}{d_t} + \frac{\delta^2}{d_t}. \quad (A8)$$

Due to the contraposition of the third statement, this implies that \mathbb{S} is not a δ -approximate state t -design. ■

2. Proof of Proposition 2

We next show Proposition 2. Similarly to the state frame potential, we assume that $t \leq d$ just for simplicity. Similar statements hold even for $t > d$.

Proposition 2 (restated). Let $d, t \in \mathbb{Z}^+$ be such that $t \leq d$. The following hold for the unitary frame potential:

- (1) $F_t(\mathbb{H}) = t!$.
- (2) For any probability measure μ on a nonempty set in $\mathbb{U}(d)$,

$$F_t(\mu) \in [t!, d^{2t}], \quad (19a)$$

where equality of the lower bound holds if and only if it is an exact unitary t -design. For the uniform measure on a finite set \mathbb{U} with cardinality K ,

$$F_t(\mathbb{U}) \in [\max\{t!, d^{2t}/K\}, d^{2t}]. \quad (20a)$$

- (3) If a finite set \mathbb{U} of unitaries is a δ -approximate unitary t -design, then

$$F_t(\mathbb{U}) \leq t! + \delta^2. \quad (21a)$$

- (4) If a finite set \mathbb{U} of unitaries satisfies

$$F_t(\mathbb{U}) \leq t! + \frac{\delta^2}{d^{2t}}, \quad (22a)$$

then \mathbb{U} is a δ -approximate unitary t -design.

- (5) For a finite set \mathbb{U} of unitaries to be a δ -approximate unitary t -design, it has to contain at least $K_{\text{uni}}(d, t, \delta)$ unitaries, where

$$K_{\text{uni}}(d, t, \delta) := \frac{d^{2t}}{t! + \delta^2}. \quad (23a)$$

- (6) Let $\mathcal{G}_\mu^{(t)}$ be the superoperator defined by Eq. (15) for a probability measure μ on $\mathbb{U}(d)$. For a finite set \mathbb{U} of unitaries, it satisfies

$$\begin{aligned} d^{-t} \sqrt{F_t(\mathbb{U}) - F_t(\mathbb{H})} &\leq \left\| \mathcal{G}_\mathbb{U}^{(t)} - \mathcal{G}_\mathbb{H}^{(t)} \right\|_{\diamond} \\ &\leq d^t \sqrt{F_t(\mathbb{U}) - F_t(\mathbb{H})}. \end{aligned} \quad (24a)$$

Proof of Proposition 2. The unitary frame potential for the Haar measure is given by the number of trivial irreducible representations of $U \mapsto U^{\otimes t} \otimes \bar{U}^{\otimes t}$, which is $t!$ when $t \leq 2^n$. This is the first statement.

For the second statement, since the Haar measure is the left- and right-unitary invariant measure,

$$\left\| M_{\mathbb{H}}^{(t)} - M_{\mu}^{(t)} \right\|_2^2 = F_t(\mu) - F_t(\mathbb{H}), \quad (A9)$$

for any probability measure μ on $\mathbb{U}(d)$. As the left-hand side is non-negative, $F_t(\mathbb{H}) \leq F_t(\mu)$. Also, using the first

property, we have $t! \leq F_t(\mu)$. The upper bound is obtained from the fact that $\text{Tr}[U^\dagger V] \leq d$ for any unitary $U, V \in \mathbb{U}(d)$. For the uniform probability measure on a finite set \mathbb{U} with cardinality K , the frame potential satisfies

$$F_t(\mathbb{U}) = \frac{1}{K^2} \sum_{i,j=1}^K \left| \text{Tr}[U_i^\dagger U_j] \right|^{2t} \quad (A10)$$

$$\geq \frac{1}{K^2} \sum_{j=1}^K \left| \text{Tr}[U_j^\dagger U_j] \right|^{2t} \quad (A11)$$

$$= \frac{d^{2t}}{K}. \quad (A12)$$

If a set \mathbb{U} is a δ -approximate unitary t -design, it satisfies

$$\left\| M_{\mathbb{H}}^{(t)} - M_{\mathbb{U}}^{(t)} \right\|_1 \leq \delta. \quad (A13)$$

Since $\|\cdot\|_2 \leq \|\cdot\|_1$, the first statement and Eq. (A9) lead to $F_t(\mathbb{U}) \leq t! + \delta^2$.

Suppose that a set \mathbb{U} satisfies $F_t(\mathbb{U}) \leq t! + \delta^2/d^{2t}$. From the first statement and Eq. (A9), it follows that

$$\left\| M_{\mathbb{H}}^{(t)} - M_{\mathbb{U}}^{(t)} \right\|_2 \leq \delta/d^t. \quad (A14)$$

As $\|\cdot\|_1 \leq \sqrt{\text{rank}(\cdot)} \|\cdot\|_2$, we obtain $\left\| M_{\mathbb{H}}^{(t)} - M_{\mathbb{U}}^{(t)} \right\|_1 \leq \delta$. That is, \mathbb{U} is a δ -approximate unitary t -design.

Finally, suppose that the cardinality K of a set $\mathbb{U} = \{U_j\}_{j=1,\dots,K}$ of unitaries is less than $d^{2t}/(t! + \delta^2)$. Together with Eq. (A12), the frame potential satisfies

$$F_t(\mathbb{U}) \geq \frac{d^{2t}}{K} > t! + \delta^2. \quad (A15)$$

Due to the contraposition of the third statement, \mathbb{S} is not a δ -approximate unitary t -design.

To show the last statement, we use the Choi-Jamiołkowski representation of a superoperator. For \mathcal{T} , it is given by $\mathfrak{J}(\mathcal{T}) := \mathcal{T} \otimes \text{id}(|\Phi\rangle\langle\Phi|)$, where $|\Phi\rangle$ is a maximally entangled state. It is known that $\|\mathfrak{J}(\mathcal{T})\|_1 \leq \|\mathcal{T}\|_{\diamond} \leq d \|\mathfrak{J}(\mathcal{T})\|_1$, where d is the dimension of the input Hilbert space. Using this relation, we have

$$\begin{aligned} \left\| \mathfrak{J} \left(\mathcal{G}_\mathbb{U}^{(t)} - \mathcal{G}_\mathbb{H}^{(t)} \right) \right\|_1 &\leq \left\| \mathcal{G}_\mathbb{U}^{(t)} - \mathcal{G}_\mathbb{H}^{(t)} \right\|_{\diamond} \\ &\leq d^t \left\| \mathfrak{J} \left(\mathcal{G}_\mathbb{U}^{(t)} - \mathcal{G}_\mathbb{H}^{(t)} \right) \right\|_1. \end{aligned} \quad (A16)$$

We further use the vectorization of an operator: $\mathcal{O} = \sum_{j,k} c_{jk} |j\rangle\langle k| \mapsto |o\rangle = \sum_{j,k} c_{jk} |j\rangle \otimes |\bar{k}\rangle$, where $\bar{\cdot}$ represents the complex conjugate in a fixed orthonormal basis. This map preserves the Hilbert-Schmidt norm, i.e., $\|\mathcal{O}\|_2 = \||o\rangle\|_2$. We consider the vectorization of

$\mathfrak{J}(\mathcal{G}_U^{(t)} - \mathcal{G}_H^{(t)})$. For simplicity, let A be denoted by the d^t -dimensional input Hilbert space of $\mathcal{G}_\mu^{(t)}$ ($\mu \in \{U, H\}$), and B, C , and D by the systems isomorphic to A . Denoting the systems on which operators act by superscripts, the vectorization is given by

$$(M_U^{(t)AB} - M_H^{(t)AB}) |\Phi\rangle^{AC} \otimes |\Phi\rangle^{BD}. \quad (\text{A17})$$

A direct calculation shows that the Hilbert-Schmidt norm of this vector is $d^{-t} \sqrt{F_t(U) - F_t(H)}$. Thus, we have

$$\|\mathfrak{J}(\mathcal{G}_U^{(t)} - \mathcal{G}_H^{(t)})\|_2 = \frac{1}{d^t} \sqrt{F_t(U) - F_t(H)}. \quad (\text{A18})$$

The desired statement is obtained by combining Eq. (A16), this equality, and the relations between norms given in Eq. (1). ■

APPENDIX B: ANALYSIS OF QUANTUM ALGORITHM FOR COMPUTING FRAME POTENTIALS

Here, we provide proofs of Lemma 1 and Theorem 2.

Lemma 1 (restated). Let ρ_{st}^A and ρ_{uni}^A be the reduced density matrix in A of $|\rho_{\text{st}}\rangle^{AB}$ and $|\rho_{\text{uni}}\rangle^{ABR}$, respectively. Then, the state frame potential of $\mathcal{S}_n = \{U_j|0_n\rangle\}_{j=1, \dots, K_n}$ and the unitary frame potential of U_n are given by

$$F_t(\mathcal{S}_n) = \text{Tr}[(\rho_{\text{st}}^A)^2], \quad F_t(U_n) = 2^{2nt} \text{Tr}[(\rho_{\text{uni}}^A)^2], \quad (\text{30a})$$

respectively.

Note that the states $|\rho_{\text{st}}\rangle^{AB}$ and $|\rho_{\text{uni}}\rangle^{ABR}$ are defined by

$$|\rho_{\text{st}}\rangle^{AB} = \text{ctrl}^A \cdot U_n^B \left(|+\kappa_n\rangle^A \bigotimes_{m=1}^t |0_n\rangle^{B_m} \right), \quad (\text{B1})$$

$$|\rho_{\text{uni}}\rangle^{ABR} = \text{ctrl}^A \cdot U_n^B \left(|+\kappa_n\rangle^A \bigotimes_{m=1}^t |\Phi_n\rangle^{B_m R_m} \right), \quad (\text{B2})$$

respectively. The controlled unitary is given by Eq. (27).

Proof of Lemma 1. By a direct calculation, it can be shown that

$$\rho_{\text{st}}^A = \frac{1}{K_n} \sum_{i,j=1}^{K_n} \left(\langle 0_n | U_j^\dagger U_i | 0_n \rangle \right)^t |i\rangle \langle j|^A, \quad (\text{B3})$$

$$\rho_{\text{uni}}^A = \frac{1}{2^{nt} K_n} \sum_{i,j=1}^{K_n} \left(\text{Tr} [U_j^\dagger U_i] \right)^t |i\rangle \langle j|^A. \quad (\text{B4})$$

This implies Eq. (30). ■

We next show Theorem 2.

Theorem 2 (restated). Let U_n be a set of n -qubit unitaries with a computationally efficient description, the cardinality of which is K_n , and let \mathcal{S}_n be a set of n -qubit state vectors with a computationally efficient description that is generated by applying the U_n to a computational zero state $|0_n\rangle$. The following hold:

- (1) For $\eta \in (\max\{d_t^{-1}, K_n^{-1}\}, 1]$ and $\epsilon \in (0, \eta - K_n^{-1})$, it takes tM_{st} queries to $\text{ctrl}\text{-}U_n$ and its inverse to determine whether $F_t(\mathcal{S}_n) \geq \eta$ or $F_t(\mathcal{S}_n) \leq \eta - \epsilon$ with success probability at least $2/3$, where

$$M_{\text{st}} := \mathcal{O} \left(\frac{1}{\epsilon} \min \left\{ \sqrt{\eta K_n - 1}, 1 \right\} \right). \quad (\text{31a})$$

- (2) For $\eta \in (\max\{t!, 2^{2nt} K_n^{-1}\}, 2^{2nt}]$ and $\epsilon \in (0, \eta - 2^{2nt} K_n^{-1})$, it takes tM_{uni} queries to $\text{ctrl}\text{-}U_n$ and its inverse to determine whether $F_t(U_n) \geq \eta$ or $F_t(U_n) \leq \eta - \epsilon$ with success probability at least $2/3$, where

$$M_{\text{uni}} := \mathcal{O} \left(\frac{2^{nt}}{\epsilon} \min \left\{ \sqrt{\eta K_n - 2^{2nt}}, 2^{nt} \right\} \right). \quad (\text{32a})$$

To show this, we refer to a quantum algorithmic result for computing the Hilbert-Schmidt distance between two states [95].

Theorem B1 (Quantum algorithm for ℓ^2 -closeness with purified query access [95]). Given $\epsilon, \nu \in (0, 1)$ and mixed states ρ and σ on a D -dimensional system, the purified states of which can be generated by U_ρ and U_σ , respectively, it takes

$$\mathcal{O} \left(\min \left\{ \frac{\sqrt{D}}{\epsilon}, \frac{1}{\epsilon^2} \right\} \frac{1}{\nu} \right) \quad (\text{B5})$$

queries to $U_\rho, U_\rho^\dagger, U_\sigma, U_\sigma^\dagger$ to decide whether $\|\rho - \sigma\|_2 \geq \epsilon$ or $\|\rho - \sigma\|_2 \leq (1 - \nu)\epsilon$ with success probability at least $2/3$.

The former query complexity in Theorem B1, i.e., $\mathcal{O}(\sqrt{D}/(\epsilon\nu))$, is achieved by using block encoding and the latter by combining the SWAP test and amplitude estimation.

Proof of Theorem 2. For our purpose, we may estimate $\|\rho_{\text{st}/\text{uni}}^A - \pi^A\|_2$ instead of $\text{Tr}[(\rho_{\text{st}/\text{uni}}^A)^2]$, where π^A is the

completely mixed state on A , since

$$\|\varrho_{\text{st/uni}}^A - \pi^A\|_2^2 \quad (\text{B6})$$

$$= \text{Tr}[(\varrho_{\text{st/uni}}^A - \pi^A)^2] \quad (\text{B7})$$

$$= \text{Tr}[(\varrho_{\text{st/uni}}^A)^2] - 2\text{Tr}[\varrho_{\text{st/uni}}^A \pi^A] + \text{Tr}[(\pi^A)^2] \quad (\text{B8})$$

$$= \text{Tr}[(\varrho_{\text{st/uni}}^A)^2] - \frac{1}{K_n}. \quad (\text{B9})$$

Using Eq. (30), we obtain

$$F_t(\mathbf{S}_n) = \|\varrho_{\text{st}}^A - \pi^A\|_2^2 + \frac{1}{K_n}, \quad (\text{B10})$$

$$F_t(\mathbf{U}_n) = 2^{2nt} \left(\|\varrho_{\text{uni}}^A - \pi^A\|_2^2 + \frac{1}{K_n} \right). \quad (\text{B11})$$

From this fact, it is easy to obtain Theorem 2. \blacksquare

APPENDIX C: DERIVATION OF EQ. (171)

We show $\|\pi_\tau(V_f) + \pi_\tau(V_p)\|_1 = \Lambda_\tau(s(f))$, where π_τ is a representation given by $U \mapsto U^{\otimes 2\tau} \otimes \tilde{U}^{\otimes \tau}$, $V_w = I - 2|w\rangle\langle w|$ for $w = f, p$ with $|f\rangle$ and $|p\rangle$ defined by Eqs. (157) and (158), respectively, and

$$\begin{aligned} \Lambda_\tau(x) \\ = 2 \sum_{s=0}^{2\tau} \binom{2\tau}{s} (d-2)^{2\tau-s} \sum_{r=0}^s \binom{s}{r} \left| T_{|2r-s|} \left(\frac{2x}{d} \right) \right|. \end{aligned} \quad (\text{C1})$$

Here, $T_m(z) = \cos m\theta$ with $z = \cos \theta$ are the Chebyshev polynomials of the first kind.

We first decompose the Hilbert space $\mathcal{H}_d = (\mathbb{C}^2)^{\otimes n}$ to a two-dimensional (2D) subspace \mathcal{H}_2 spanned by $|f\rangle$ and $|p\rangle$, and the remaining one \mathcal{H}_{d-2} . We also fix the orthonormal basis of \mathcal{H}_2 as $\{|p\rangle, |p^\perp\rangle\}$, where $|p^\perp\rangle$ is orthogonal to $|p\rangle$ such that $\langle f|p^\perp\rangle \in \mathbb{R}$. Under this decomposition, we can write V_w for $w = f, p$ as $\tilde{w} \oplus I_{d-2}$. The 2×2 matrix \tilde{w} is given by $I_2 - 2|w\rangle\langle w|$ or, more explicitly,

$$\tilde{f} = \begin{pmatrix} 1 - 2\alpha^2 & -2\alpha\beta \\ -2\alpha\beta & 1 - 2\beta^2 \end{pmatrix}, \quad \text{and} \quad \tilde{p} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (\text{C2})$$

in our fixed basis, where $\alpha = \langle f|p\rangle = 2s(f)/d$, and $\beta = \sqrt{1 - \alpha^2}$.

Using this notation, we have

$$\pi_\tau(V_w) = V_w^{\otimes 2\tau} \quad (\text{C3})$$

$$= (\tilde{w} \oplus I_{d-2})^{\otimes 2\tau} \quad (\text{C4})$$

$$= \bigoplus_{s=0}^{2\tau} \bigoplus_{\text{sym}} (\tilde{w}^{\otimes s} \otimes I_{d-2}^{\otimes (2\tau-s)}), \quad (\text{C5})$$

where

$$\bigoplus_{\text{sym}} (\tilde{w}^{\otimes s} \otimes I_{d-2}^{\otimes (2\tau-s)}) := \overbrace{(\tilde{w}^{\otimes s} \otimes I_{d-2}^{\otimes (2\tau-s)}) \oplus (\tilde{w}^{\otimes s-1} \otimes I_{d-2} \otimes \tilde{w} \otimes I_{d-2}^{\otimes (2\tau-s-1)}) \oplus \dots \oplus (I_{d-2}^{\otimes (2\tau-s)} \otimes \tilde{w}^{\otimes s})}^{(2\tau)\text{ terms}} \quad (\text{C6})$$

is a full symmetrization of the tensor product. As this holds both for $w = f, p$, we have

$$\pi_\tau(V_f) + \pi_\tau(V_p) = \bigoplus_{s=0}^{2\tau} \bigoplus_{\text{sym}} ((\tilde{f}^{\otimes s} + \tilde{p}^{\otimes s}) \otimes I_{d-2}^{\otimes (2\tau-s)}). \quad (\text{C7})$$

Hence we have

$$\begin{aligned} \|\pi_\tau(V_f) + \pi_\tau(V_p)\|_1 \\ = \sum_{s=0}^{2\tau} \binom{2\tau}{s} (d-2)^{2\tau-s} \|\tilde{f}^{\otimes s} + \tilde{p}^{\otimes s}\|_1. \end{aligned} \quad (\text{C8})$$

To compute $\|\tilde{f}^{\otimes s} + \tilde{p}^{\otimes s}\|_1$, we note that both \tilde{f} and \tilde{p} are unitary and use the unitary invariance of the trace norm. This leads to

$$\|\tilde{f}^{\otimes s} + \tilde{p}^{\otimes s}\|_1 = \left\| (\tilde{f}\tilde{p})^{\otimes s} + I_2^{\otimes s} \right\|_1, \quad (\text{C9})$$

where I_2 is the 2×2 identity matrix. From the matrix representation of \tilde{f} and \tilde{p} given in Eq. (C2), we have

$$\tilde{f}\tilde{p} = \begin{pmatrix} 2\alpha^2 - 1 & -2\alpha\beta \\ 2\alpha\beta & 1 - 2\beta^2 \end{pmatrix}. \quad (\text{C10})$$

The eigenvalues of this unitary are $e^{\pm i\theta}$ with $\theta = \arccos(2\alpha^2 - 1)$. Hence,

$$\left\| \tilde{f}^{\otimes s} + \tilde{p}^{\otimes s} \right\|_1 = \left\| \left(\tilde{f} \tilde{p} \right)^{\otimes s} + I_2^{\otimes s} \right\|_1 \quad (\text{C11})$$

$$= \sum_{r=0}^s \binom{s}{r} \left| e^{ir\theta} e^{-i(s-r)\theta} + 1 \right| \quad (\text{C12})$$

$$= \sum_{r=0}^s \binom{s}{r} \left| e^{i(2r-s)\theta} + 1 \right| \quad (\text{C13})$$

$$= 2 \sum_{r=0}^s \binom{s}{r} \left| \cos(2r-s) \frac{\theta}{2} \right| \quad (\text{C14})$$

$$= 2 \sum_{r=0}^s \binom{s}{r} \left| \cos |2r-s| \frac{\theta}{2} \right|. \quad (\text{C15})$$

Using the Chebyshev polynomials of the first kind, we have $\cos |2r-s| \frac{\theta}{2} = T_{|2r-s|}(\cos \theta/2)$. It further turns out that $\cos \theta/2 = \pm \alpha$. Using the fact that $|T_m(\pm x)| = |T_m(x)|$, we have

$$\left\| \tilde{f}^{\otimes s} + \tilde{p}^{\otimes s} \right\|_1 = 2 \sum_{r=0}^s \binom{s}{r} |T_{|2r-s|}(\alpha)|. \quad (\text{C16})$$

Substituting this into Eq. (C8) completes the derivation.

We next show that, for $x \in [0, d/2]$, $\Lambda_\tau(x)$ is given by

$$\Lambda_\tau(x) = 2d^{2\tau} - 8\tau d^{2\tau-1} \left(1 - \frac{2x}{d} \right) + \mathcal{O}(d^{2\tau-2}), \quad (\text{C17})$$

to the second leading order of d .

From the definition of $\Lambda_\tau(x)$, an expansion up to the second leading order is obtained by expanding the summation over s up to $s = 1$, such as

$$\begin{aligned} \Lambda_{t'} \left(\frac{d}{4} \right) - \Lambda_{t'} \left(\frac{d}{4} - \frac{1}{3} \right) &= 8t'(d-2)^{2t'-1} \left(\left| T_1 \left(\frac{1}{2} \right) \right| - \left| T_1 \left(\frac{1}{2} - \frac{2}{3d} \right) \right| \right) \\ &+ 2 \sum_{s=2}^{2t'} \binom{2t'}{s} (d-2)^{2t'-s} \sum_{r=0}^s \binom{s}{r} \left(\left| T_{|2r-s|} \left(\frac{1}{2} \right) \right| - \left| T_{|2r-s|} \left(\frac{1}{2} - \frac{2}{3d} \right) \right| \right). \end{aligned} \quad (\text{D4})$$

As $T_1(x) = \cos(\arccos x) = x$,

$$\left| T_1 \left(\frac{1}{2} \right) \right| - \left| T_1 \left(\frac{1}{2} - \frac{2}{3d} \right) \right| = \frac{2}{3d}. \quad (\text{D5})$$

From the Taylor expansion of the Chebyshev polynomials $T_n(x)$ around $x = 1/2$, we have

$$T_n \left(\frac{1}{2} - \varepsilon \right) = \cos \left(\frac{\pi n}{3} \right) + \frac{2\sqrt{3}n}{3} \sin \left(\frac{\pi n}{3} \right) \varepsilon + \mathcal{O}(\varepsilon^2). \quad (\text{D6})$$

$$\Lambda_\tau(x)/2 = (d-2)^{2\tau} + 4\tau(d-2)^{2\tau-1} \left| T_1 \left(\frac{2x}{d} \right) \right|. \quad (\text{C18})$$

The Chebyshev polynomials of the first kind can be explicitly given by

$$T_0 \left(\frac{2x}{d} \right) = 1, \quad (\text{C19})$$

$$T_1 \left(\frac{2x}{d} \right) = \cos \left(\arccos \left(\frac{2x}{d} \right) \right) = \frac{2x}{d}. \quad (\text{C20})$$

Substituting these results in Eq. (C17).

APPENDIX D: DERIVATIONS OF EQS. (185) AND (188)

We show that, for sufficiently large d ,

$$U_{t'} \left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3} \right) < L_{t'} \left(\frac{D}{m}, \frac{d}{4} \right), \quad (\text{D1})$$

$$U_{t'} \left(\frac{D}{m}, \frac{d}{4} - 1 \right) < L_{t'} \left(\frac{D}{m}, \frac{d}{4} - \frac{2}{3} \right), \quad (\text{D2})$$

which are used in the analysis of UniDes(t, t', δ, δ'). These functions are defined by Eqs. (175) and (176).

For the former, a direct calculation leads to

$$\begin{aligned} \text{RHS} - \text{LHS} &= \frac{1}{D/m+2} \left[\Lambda_{t'} \left(\frac{d}{4} \right) - \Lambda_{t'} \left(\frac{d}{4} - \frac{1}{3} \right) \right] \\ &- \frac{2D/m}{D/m+2} \delta_0. \end{aligned} \quad (\text{D3})$$

We also have

This leads to

$$\begin{aligned} & \left| \left(\left| T_{|2r-s|} \left(\frac{1}{2} \right) \right| - \left| T_{|2r-s|} \left(\frac{1}{2} - \frac{2}{3d} \right) \right| \right) \right| \\ & \leq \frac{4\sqrt{3}|2r-s|}{9d} + \mathcal{O}(d^{-2}) \leq \frac{8\sqrt{3}t'}{9d} + \mathcal{O}(d^{-2}). \end{aligned} \quad (\text{D7})$$

Note that we have used the fact that $s, r \in [0, 2t']$. Hence it holds that

$$\begin{aligned} & \Lambda_{t'} \left(\frac{d}{4} \right) - \Lambda_{t'} \left(\frac{d}{4} - \frac{1}{3} \right) \\ & \geq \frac{16t'}{3} d^{2t'-2} + \mathcal{O}(d^{2t'-3}) \\ & \quad - \frac{16\sqrt{3}t'}{9d} \sum_{s=2}^{2t'} \binom{2t'}{s} (d-2)^{2t'-s} \sum_{r=0}^s \binom{s}{r} \end{aligned} \quad (\text{D8})$$

$$= \frac{16t'}{3} d^{2t'-2} + \mathcal{O}(d^{2t'-3}). \quad (\text{D9})$$

All together, we obtain

RHS – LHS

$$\geq \frac{1}{D/m+2} \left(\frac{16t'}{3} d^{2t'-2} + \mathcal{O}(d^{2t'-3}) \right) - \frac{2D/m}{D/m+2} \delta_0. \quad (\text{D10})$$

As $D/m \in \Theta(d^{2t}/\delta)$ and $\delta_0 \in \mathcal{O}(\delta^2/d^{2t})$, this reduces to

$$\text{RHS} - \text{LHS} \geq \frac{\delta}{d^{2t}} \left(\frac{16t'c}{3} d^{2t'-2} - c'\delta \right), \quad (\text{D11})$$

with some positive constants c and c' , to leading order. Hence, as far as $\delta \in o(d^{2(t'-1)})$ that follows from the assumption $\delta \in o(d^{2(t'-1)})$ of the theorem, the leading term is positive. That is, for sufficiently large d , we have

$$U_{t'} \left(\frac{D}{m}, \frac{d}{4} - \frac{1}{3} \right) < L_{t'} \left(\frac{D}{m}, \frac{d}{4} \right). \quad (\text{D12})$$

The latter inequality can be similarly shown. In this case,

$$\begin{aligned} & \text{RHS} - \text{LHS} \\ & = \frac{1}{D/m+2} \left[\Lambda_{t'} \left(\frac{d}{4} - \frac{2}{3} \right) - \Lambda_{t'} \left(\frac{d}{4} - 1 \right) \right] \\ & \quad - \frac{2D/m}{D/m+2} \delta_0. \end{aligned} \quad (\text{D13})$$

The right-hand side of this equation is exactly the same as that of Eq. (D10), since

$$\left| T_1 \left(\frac{1}{2} - \frac{4}{3d} \right) \right| - \left| T_1 \left(\frac{1}{2} - \frac{2}{d} \right) \right| = \frac{2}{3d}, \quad (\text{D14})$$

which has the same value as Eq. (D5), and

$$\begin{aligned} & \left| \left(\left| T_{|2r-s|} \left(\frac{1}{2} - \frac{4}{3d} \right) \right| - \left| T_{|2r-s|} \left(\frac{1}{2} - \frac{2}{d} \right) \right| \right) \right| \\ & \leq \frac{8\sqrt{3}t'}{9d} + \mathcal{O}(d^{-2}), \end{aligned} \quad (\text{D15})$$

which is the same as Eq. (D7). Thus, the difference between the left-hand side (LHS) and the right-hand side (RHS) in this case is the same as previously, implying that $\text{RHS} - \text{LHS}$ is positive as well, to leading order.

-
- [1] A. Ambainis and A. Smith, in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. RANDOM APPROX 2004 2004*, Lecture Notes in Computer Science, edited by K. Jansen, S. Khanna, J. D. P. Rolim, and D. Ron (Springer, Berlin, Heidelberg, 2004), Vol. 3122.
 - [2] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, *Commun. Math. Phys.* **250**, 371 (2004).
 - [3] W. Kretschmer, in *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)* (Schloss Dagstuhl—Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021), Vol. 197, pp. 2:1–2:20.
 - [4] T. Morimae and T. Yamakawa, in *Advances in Cryptology—CRYPTO 2022* (Springer Nature Switzerland, Cham, 2022), pp. 269–295.
 - [5] P. Ananth, L. Qian, and H. Yuen, in *Advances in Cryptology—CRYPTO 2022* (Springer Nature Switzerland, Cham, 2022), pp. 208–236.
 - [6] P. Sen, in *21st Annual IEEE Conference on Computational Complexity (CCC'06)* (IEEE, Prague, 2006), pp. 14–287.
 - [7] F. G. S. L. Brandão and M. Horodecki, Exponential quantum speed-ups are generic, *Quantum Inf. Comput.* **13**, 901 (2013).
 - [8] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nat. Phys.* **14**, 595 (2018).
 - [9] F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
 - [10] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, *Nat. Phys.* **15**, 159 (2019).
 - [11] R. Kueng, H. Rauhut, and U. Terstiege, Low rank matrix recovery from rank one measurements, *Appl. Comput. Harmon. Anal.* **42**, 88 (2017).
 - [12] S. Kimmel and Y.-K. Liu, in *2017 International Conference on Sampling Theory and Applications (SampTA)* (IEEE, Tallinn, Estonia, 2017), pp. 345–349.
 - [13] R. Kueng, H. Zhu, and D. Gross, Distinguishing quantum states using Clifford orbits, [arXiv:1609.08595](https://arxiv.org/abs/1609.08595) [quant-ph].
 - [14] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, and M. Lewenstein, Random bosonic states for robust quantum metrology, *Phys. Rev. X* **6**, 041044 (2016).

- [15] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, *IEEE Trans. Inf. Theory* **51**, 44 (2005).
- [16] I. Devetak and A. Winter, Relating quantum privacy and quantum coherence: An operational approach, *Phys. Rev. Lett.* **93**, 080501 (2004).
- [17] B. Groisman, S. Popescu, and A. Winter, Quantum, classical, and total amount of correlations in a quantum state, *Phys. Rev. A* **72**, 032317 (2005).
- [18] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, The mother of all protocols: Restructuring quantum information's family tree, *Proc. R. Soc. A* **465**, 2537 (2009).
- [19] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, One-shot decoupling, *Commun. Math. Phys.* **328**, 251 (2014).
- [20] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, Decoupling with unitary approximate two-designs, *New J. Phys.* **15**, 053022 (2013).
- [21] M. Horodecki, J. Oppenheim, and A. Winter, Partial quantum information, *Nature* **436**, 673 (2005).
- [22] M. Horodecki, J. Oppenheim, and A. Winter, Quantum state merging and negative information, *Commun. Math. Phys.* **269**, 107 (2007).
- [23] Y. Nakata, E. Wakakuwa, and H. Yamasaki, One-shot quantum error correction of classical and quantum information, *Phys. Rev. A* **104**, 012408 (2021).
- [24] E. Wakakuwa and Y. Nakata, One-shot triple-resource trade-off in quantum channel coding, *IEEE Trans. Inf. Theory* **69**, 2400 (2023).
- [25] S. Popescu, A. J. Short, and A. Winter, Entanglement and the foundations of statistical mechanics, *Nat. Phys.* **2**, 754 (2006).
- [26] N. Linden, S. Popescu, A. J. Short, and A. Winter, Quantum mechanical evolution towards thermal equilibrium, *Phys. Rev. E* **79**, 061103 (2009).
- [27] L. del Rio, A. Hutter, R. Renner, and S. Wehner, Relative thermalization, *Phys. Rev. E* **94**, 022104 (2016).
- [28] K. Kaneko, E. Iyoda, and T. Sagawa, Characterizing complexity of many-body quantum dynamics by higher-order eigenstate thermalization, *Phys. Rev. A* **101**, 042126 (2020).
- [29] M. Ippoliti and W. W. Ho, Solvable model of deep thermalization with distinct design times, *Quantum* **6**, 886 (2022).
- [30] T. Bhore, J.-Y. Desaulles, and Z. Papić, Deep thermalization in constrained quantum systems, *Phys. Rev. B* **108**, 104317 (2023).
- [31] P. Hayden and J. Preskill, Black holes as mirrors: Quantum information in random subsystems, *J. High Energy Phys.* **2007**, 120 (2007).
- [32] Y. Nakata, E. Wakakuwa, and M. Koashi, Black holes as clouded mirrors: The Hayden-Preskill protocol with symmetry, *Quantum* **7**, 928 (2023).
- [33] Y. Nakata, T. Matsuura, and M. Koashi, Decoding general error correcting codes and the role of complementarity, *npj Quantum Inf.* **11**, 4 (2025).
- [34] Y. Sekino and L. Susskind, Fast scramblers, *J. High Energy Phys.* **2008**, 065 (2008).
- [35] N. Lashkari, D. Stanford, M. Hastings, T. Osborne, and P. Hayden, Towards the fast scrambling conjecture, *J. High Energy Phys.* **2013**, 22 (2013).
- [36] J. Maldacena, S. H. Shenker, and D. Stanford, A bound on chaos, *J. High Energy Phys.* **2016**, 106 (2016).
- [37] D. A. Roberts and B. Yoshida, Chaos and complexity by design, *J. High Energy Phys.* **2017**, 121 (2017).
- [38] J. S. Cotler, D. K. Mark, H.-Y. Huang, F. Hernández, J. Choi, A. L. Shaw, M. Endres, and S. Choi, Emergent quantum state designs from individual many-body wave functions, *PRX Quantum* **4**, 010311 (2023).
- [39] 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, *Phys. Rev. X* **14**, 041051 (2024).
- [40] S. Pilatowsky-Cameo, I. Marvian, S. Choi, and W. W. Ho, Hilbert-space ergodicity in driven quantum systems: Obstructions and designs, *Phys. Rev. X* **14**, 041059 (2024).
- [41] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, *J. Opt. B: Quantum Semiclass. Opt.* **7**, S347 (2005).
- [42] E. Knill *et al.*, Randomized benchmarking of quantum gates, *Phys. Rev. A* **77**, 012307 (2008).
- [43] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and robust randomized benchmarking of quantum processes, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [44] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, *Phys. Rev. A* **85**, 042311 (2012).
- [45] J. Kelly *et al.*, Optimal quantum control using randomized benchmarking, *Phys. Rev. Lett.* **112**, 240504 (2014).
- [46] S. Sheldon, L. S. Bishop, E. Magesan, S. Filipp, J. M. Chow, and J. M. Gambetta, Characterizing errors on qubit operations via iterative randomized benchmarking, *Phys. Rev. A* **93**, 012301 (2016).
- [47] S. Garion, N. Kanazawa, H. Landa, D. C. McKay, S. Sheldon, A. W. Cross, and C. J. Wood, Experimental implementation of non-Clifford interleaved randomized benchmarking with a controlled-S gate, *Phys. Rev. Res.* **3**, 013204 (2021).
- [48] E. Onorati, A. H. Werner, and J. Eisert, Randomized benchmarking for individual quantum gates, *Phys. Rev. Lett.* **123**, 060501 (2019).
- [49] J. Helsen, I. Roth, E. Onorati, A. Werner, and J. Eisert, General framework for randomized benchmarking, *PRX Quantum* **3**, 020357 (2022).
- [50] M. Heinrich, M. Kliesch, and I. Roth, General guarantees for randomized benchmarking with random quantum circuits, [arXiv:2212.06181](https://arxiv.org/abs/2212.06181) [quant-ph].
- [51] J. Choi, A. L. Shaw, I. S. Madjarov, X. Xie, R. Finkelstein, J. P. Covey, J. S. Cotler, D. K. Mark, H.-Y. Huang, A. Kale, H. Pichler, F. G. S. L. Brandão, S. Choi, and M. Endres, Preparing random states and benchmarking with many-body quantum chaos, *Nature* **613**, 468 (2023).
- [52] D. K. Mark, J. Choi, A. L. Shaw, M. Endres, and S. Choi, Benchmarking quantum simulators using ergodic quantum dynamics, *Phys. Rev. Lett.* **131**, 110601 (2023).
- [53] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2010), 10th ed.
- [54] Z. Ji, Y. Liu, and F. Song, in *Advances in Cryptology—CRYPTO 2018* (Springer International Publishing, Cham, 2018), pp. 126–152.

- [55] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Pseudorandom unitaries with non-adaptive security, [arXiv:2402.14803 \[quant-ph\]](#).
- [56] P. Delsarte, J. Goethals, and J. Seidel, Bounds for systems of lines, and Jacobi polynomials, *Philips Res. Rep.* **30**, 91 (1975).
- [57] P. Delsarte, J. M. Goethals, and J. J. Seidel, Spherical codes and designs, *Geom. Dedicata* **6**, 363 (1977).
- [58] E. Bannai, Y. Nakata, T. Okuda, and D. Zhao, Explicit construction of exact unitary designs, *Adv. Math.* **405**, 108457 (2022).
- [59] Y. Nakata *et al.*, Quantum circuits for exact unitary t -designs and applications to higher-order randomized benchmarking, *PRX Quantum* **2**, 030339 (2021).
- [60] A. W. Harrow and R. A. Low, in *Proc. RANDOM'09*, Lecture Notes in Computer Science (Springer, Berlin, 2009), pp. 548–561.
- [61] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Commun. Math. Phys.* **346**, 397 (2016).
- [62] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Efficient quantum pseudorandomness with nearly time-independent Hamiltonian dynamics, *Phys. Rev. X* **7**, 021006 (2017).
- [63] E. Onorati, O. Buerschaper, M. Kliesch, W. Brown, A. H. Werner, and J. Eisert, Mixing properties of stochastic quantum Hamiltonians, *Commun. Math. Phys.* **355**, 905 (2017).
- [64] J. Haferkamp, Random quantum circuits are approximate unitary t -designs in depth $O(nr^{5+o(1)})$, *Quantum* **6**, 795 (2022).
- [65] A. W. Harrow and S. Mehraban, Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates, *Commun. Math. Phys.* **401**, 1531 (2023).
- [66] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Efficient unitary designs with a system-size independent number of non-Clifford gates, *Commun. Math. Phys.* **397**, 995 (2023).
- [67] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Simple constructions of linear-depth t -designs and pseudorandom unitaries, [arXiv:2404.12647 \[quant-ph\]](#).
- [68] C.-F. Chen, J. Docter, M. Xu, A. Bouland, F. G. S. L. Brandão, and P. Hayden, in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (Chicago, IL, USA, 2024), pp. 476–484.
- [69] N. LaRacuente and F. Leditzky, in *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2025), Vol. 325, pp. 69:1–69:2.
- [70] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, *Science* **389**, 92 (2025).
- [71] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, *J. Math. Phys.* **48**, 052104 (2007).
- [72] A. Chan and A. D. Luca, Projected state ensemble of a generic model of many-body quantum chaos, *J. Phys. A: Math. Theor.* **57**, 405001 (2024).
- [73] W.-K. Mok, T. Haug, A. L. Shaw, M. Endres, and J. Preskill, *Phys. Rev. Lett.* **134**, 180403 (2025).
- [74] W. W. Ho and S. Choi, Exact emergent quantum state designs from quantum chaotic dynamics, *Phys. Rev. Lett.* **128**, 060601 (2022).
- [75] M. Ippoliti and W. W. Ho, Dynamical purification and the emergence of quantum state designs from the projected ensemble, *PRX Quantum* **4**, 030322 (2023).
- [76] S. Pilatowsky-Cameo, C. B. Dag, W. W. Ho, and S. Choi, Complete Hilbert-space ergodicity in quantum dynamics of generalized Fibonacci drives, *Phys. Rev. Lett.* **131**, 250401 (2023).
- [77] A. Ambainis and J. Emerson, in *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (IEEE, San Diego, CA, USA, 2007), pp. 129–140.
- [78] O. Goldreich, in *Theoretical Computer Science: Essays in Memory of Shimon Even*, edited by O. Goldreich, A. L. Rosenberg, and A. L. Selman (Springer-Verlag, Berlin, 2006), pp. 254–290.
- [79] J. Watrous, *Encyclopedia of Complexity and Systems Science* (Springer, New York, 2009).
- [80] J. T. Gill, in *Proceedings of the Sixth Annual ACM Symposium on Theory of Computing*, STOC '74 (Association for Computing Machinery, New York, 1974), pp. 91–95.
- [81] J. L. Cox and T. Pay, An overview of some semantic and syntactic complexity classes, [arXiv:1806.03501 \[cs.CC\]](#).
- [82] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, *Phys. Rev. Appl.* **70**, 052328 (2004).
- [83] A. M. Childs, Y. Su, M. C. Tran, N. Wiebe, and S. Zhu, Theory of Trotter error with commutator scaling, *Phys. Rev. X* **11**, 011020 (2021).
- [84] A. Brodsky and S. Hoory, Simple permutations mix even better, *Random Struct. Algorithms* **32**, 274 (2008).
- [85] W. Kretschmer, L. Qian, M. Sinha, and A. Tal, in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023 (Association for Computing Machinery, New York, 2023), pp. 1589–1602.
- [86] N. Schuch, M. M. Wolf, F. Verstraete, and J. I. Cirac, Computational complexity of projected entangled pair states, *Phys. Rev. Lett.* **98**, 140506 (2007).
- [87] Strictly speaking, the state generated by the quantum circuit composed only of the Hadamard and Toffoli gates is exponentially close to the original state. We ignore this approximation error, as it can be made arbitrarily small within the order of $\Theta(1/\exp(n))$.
- [88] C. M. da Fonseca, M. L. Glasser, and V. Kowalenko, Basic trigonometric power sums with applications, *Ramanujan J.* **42**, 401 (2017).
- [89] Y. Nakata, P. S. Turner, and M. Murao, Phase-random states: Ensembles of states with fixed amplitudes and uniformly distributed phases in a fixed basis, *Phys. Rev. A* **86**, 012301 (2012).
- [90] Z. Brakerski and O. Shmueli, in *Theory of Cryptography, TCC 2019, Lecture Notes in Computer Science*, edited by D. Hofheinz and A. Rosen (Springer, Cham, 2019), Vol. 11891.
- [91] P. Ananth, A. Gulati, L. Qian, and H. Yuen, in *Theory of Cryptography: 20th International Conference, TCC 2022, Chicago, IL, USA, November 7–10, 2022, Proceedings*,

- Part I* (Springer-Verlag, Berlin, Heidelberg, 2022), pp. 237–265.
- [92] T. Giurgica-Tiron and A. Bouland, Pseudorandomness from subset states, [arXiv:2312.09206](#) [quant-ph].
- [93] F. G. Jeronimo, N. Magrafta, and P. Wu, Pseudorandom and pseudoentangled states from subset states, [arXiv:2312.15285](#) [quant-ph].
- [94] D. Aharonov and A. Green, A quantum inspired proof of $P^{\#P} \subseteq IP$, [arXiv:1710.09078](#) [quant-ph].
- [95] A. Gilyén and T. Li, in *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2020), Vol. 151, pp. 25:1–25:19.