arXiv:2303.01877v4 [quant-ph] 22 Mar 2025

Quantum Merlin-Arthur proof systems for synthesizing quantum states

Hugo Delavenne[1,2], François Le Gall[1], Yupan Liu[1], and Masayuki Miyamoto[1]

[1]Graduate School of Mathematics, Nagoya University
[2]ENS Paris-Saclay, Université Paris-Saclay

Complexity theory typically focuses on the difficulty of solving computational problems with classical inputs and outputs, even with a quantum computer. In the quantum world, it is natural to apply a different notion of complexity, namely the complexity of synthesizing quantum states. We investigate a state-synthesizing counterpart of the class NP, referred to as stateQMA, which is concerned with preparing certain quantum states through a polynomial-time quantum verifier with the aid of a single quantum message from an all-powerful but untrusted prover. This is a subclass of the class stateQIP recently introduced by Rosenthal and Yuen (ITCS 2022), which permits polynomially many interactions between the prover and the verifier. Our main result consists of error reduction of this class and its variants with an exponentially small gap or bounded space, as well as how this class relates to other fundamental state-synthesizing classes, i.e., states generated by uniform polynomial-time quantum circuits (stateBQP) and space-uniform polynomial-space quantum circuits (statePSPACE). Furthermore, we establish that the family of UQMA witnesses, considered as one of the most natural candidates for stateQMA containments, is in stateQMA. Additionally, we demonstrate that stateQCMA achieves perfect completeness.

1 Introduction

Classical and quantum complexity theory typically concentrates on the computational difficulty of solving problems with *classical* inputs and outputs. However, quantum computers have the ability to handle not only classical problems, but also quantum tasks, such as synthesizing quantum states. The most famous example is preparing ground states of a physical system [Llo96, PW09], which even dates back to Feynman's original ideas [Fey82]. Analogous tasks are also commonplace in quantum cryptography and generalized notions of the pseudorandomness, such as quantum money [Aar09] and pseudorandom quantum states [JLS18]. This motivates the study of complexity of synthesizing quantum states.

In [Aar16], Aaronson investigated the concept on quantum state complexity, leading to the *state synthesizing problem*. This problem involves generating a quantum state ρ from the all-zero state based on a quantum circuit with a succinct description acting on n qubits (with the depth up to exponential). The resulting state ρ is supposed to be close to the designated *target state* $|\psi\rangle$.[1] This problem is solvable in (quantum) polynomial space (PSPACE), i.e., a quantum computer running in exponential time but using polynomially many (possibly ancillary) qubits can generate a state that well approximates the target state.

[1]We measure the closeness between ρ and $|\psi\rangle$ by the trace distance, see Section 2.1 for the definition.

Quantum computers are seemingly not capable of solving any PSPACE problem in polynomial time, while *polynomially many* messages interactive protocols with the help of an all-powerful and *untrusted* prover (known as *interactive proofs*, IP) captures the full computational power of polynomial-space computation, referred to as the celebrated IP = PSPACE theorem [LFKN92, Sha92]. A recent line of works [RY22, MY23] initializes the study on the *interactive* state synthesizing problem. Rosenthal and Yuen [RY22] denote the polynomial-space-preparable state families as statePSPACE[2] and show that such state families are preparable by *polynomial-message* interactive synthesis protocols, which belongs to the class stateQIP. Recently, Metger and Yuen [MY23] managed to prove the equivalence between state families that are preparable using polynomial space and those generated by interactive synthesis protocols, that is, stateQIP = statePSPACE, which is the state-synthesizing counterpart of the IP = PSPACE theorem (and its quantum analogue [JJUW11]). Very recently (after our work was released), Rosenthal [Ros24] strengthened the inclusion statePSPACE $\subseteq$ stateQIP by presenting a *constant-message* stateQIP protocol. This result, combined with the other direction, can be considered as a parallelization technique counterpart for stateQIP, highlighting that the behavior of stateQIP aligns more closely with QIP than IP.

However, there is currently a lack of fine-grained characterizations of computationally easier state families, viz., state families that are efficiently preparable (e.g., efficiently simulating view of quantum statistical zero-knowledge [Wat02]), or state families that are synthesizable via simply one-message interactive protocols (e.g., efficient verification of pure quantum states in the adversarial scenario [ZH19]). This opens up opportunities for our main results.

1.1 Main results

In this work, we are particularly interested in state families that are preparable by a *one-message* protocol, denoted as stateQMA, which is obviously a subclass of stateQIP. Let us first define stateQMA informally (see Section 3.2 for a formal definition). A state family in stateQMA is a family $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ indexed by *binary strings* in the corresponding language $\mathcal{L}$ such that there is a verifier that has the following properties, verifying whether the target state $|\psi_x\rangle$ corresponding to a given input $x \in \mathcal{L}$ can be well-approximated by the resulting state of this verifier. The verifier's computation, which is a polynomial-size *unitary* quantum circuit,[3] takes a quantum-proof state $|w\rangle$ (with no limitations on the preparation method) and ancillary qubits in the state $|\bar{0}\rangle$ as input. After performing the verification circuit, a designated output qubit will be measured on the computational basis, and the verifier accepts if the measurement outcome is 1. If the verifier accepts, the verification circuit has prepared the resulting state $\rho_{x,w}$ on the remaining qubits that is a good approximation of the target state $|\psi_x\rangle$ (if the verifier rejects, the resulting state could be anything). The acceptance probability is called *the success probability* for approximately preparing $|\psi_x\rangle$.

More precisely, the state family is in the class $\mathsf{stateQMA}_\delta[c,s]$ for some $0 \le s < c \le 1$ and $\delta \ge 0$, if the resulting state $\rho_{x,w}$ is δ-close to the target state $|\psi_x\rangle$ provided that the verifier accepts with probability at least s (soundness condition); and additionally there exists a quantum witness that makes the verifier accept with probability at least c (completeness condition).

It is pretty evident that $\mathsf{stateQMA}_\delta[c,s] \subseteq \mathsf{stateQMA}_{\delta'}[c',s']$ if $c' \le c$, $s' \ge s$ and $\delta' \ge$

[2]The definition of statePSPACE is a bit subtle: although all quantum states can be well-approximated by an exponentially long gate sequence owing to the Solovay-Kitaev theorem [Kit97], this exponential gate sequence is not necessarily *space-uniform*.

[3]In particular, extending to general quantum circuits does not change the class stateQMA owing to the principle of deferred measurement. However, such extensions do not immediately work for the space-bounded counterpart, namely $\mathsf{stateQMA}_\cup\mathsf{PSPACE}^{\mathsf{off}}$, see Remark 3.4.

δ. However, how crucially does $\mathsf{stateQMA}_\delta[c,s]$ depend on its parameters? For commonplace complexity classes, viz. BQP, QMA, QIP, etc., the dependence on such parameters is very weak: the class remains the same so long as the completeness c and soundness s differ by at least some inverse polynomial of $n := |x|$ where $x \in \mathcal{L}$. This is known as *error reduction*, which typically involves performing the verification circuit in parallel and taking the majority vote.

However, error reduction for stateQMA requires a more nuanced approach. A simple parallel repetition of the verification circuit ends with a tensor product of the resulting state that evidently differs from the original state family. Therefore, error reduction for stateQMA does need to preserve not only the quantum witness state $|w\rangle$, but also the resulting state $\rho_{x,w}$, referred to as the *doubly-preserving error reduction* (ending with negligible errors):

Theorem 1.1 (Doubly-preserving error reduction for stateQMA, informal version of Theorem 5.1)**.** *For any $c(n) - s(n) \geq 1/\mathrm{poly}(n)$ and $0 \leq c(n), s(n) \leq 1$, we have*

$$\mathsf{stateQMA}_\delta[c,s] \subseteq \mathsf{stateQMA}_\delta[1-\mathrm{negl}, \mathrm{negl}].$$

Nevertheless, applying Theorem 1.1 to a *polynomial-space-bounded* variant of $\mathsf{stateQMA}_\delta[c,s]$, which we denote by $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$,[4] will result in *exponential* space. To address this, we generalize Theorem 1.1 in a manner that preserves the polynomial space complexity, as presented in Theorem 1.2. Here in the class $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$, the verifier's computation stays polynomially space-bounded but may take *exponential time* and the gap between the completeness c and the soundness s is at least some inverse-exponential of $n := |x|$.

Theorem 1.2 (Doubly-preserving error reduction for $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$, informal version of Theorem 5.2)**.** *For any $c(n) - s(n) \geq \exp(-\mathrm{poly}(n))$ and $0 \leq c(n), s(n) \leq 1$, we have*

$$\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}_\delta[c,s] \subseteq \mathsf{stateQMA_UPSPACE}^{\mathsf{off}}_\delta[1-\mathrm{negl}, \mathrm{negl}].$$

We note that Theorem 1.1 is a state-synthesizing counterpart of the witness-preserving error reduction for QMA [MW05, NWZ09]. Likewise, Theorem 1.2 shares similarities with error reduction for unitary quantum computations [FKL+16] in the context of synthesizing states. Along the line of Marriott and Watrous [MW05], we demonstrate that logarithmic-size quantum witness states are useless for stateQMA (this variant is referred to as stateQMA[log]), as shown in Corollary 1.3. Here stateBQP is defined as a subclass of statePSPACE with only polynomially many gates.

Corollary 1.3 (Informal version of Theorem 5.5)**.** $\mathsf{stateQMA}_\delta[\log] = \mathsf{stateBQP}_\delta$.

Resembling the approach of Fefferman and Lin [FL16], we demonstrate that a variant of stateQMA that admits an exponentially small gap between completeness and soundness, known as statePreciseQMA, is contained in statePSPACE:

Corollary 1.4 (Informal version of Theorem 5.7)**.** $\mathsf{statePreciseQMA}_\delta \subseteq \mathsf{statePSPACE}_\delta$.

Surprisingly, Corollary 1.4 shows that the distance parameter δ remains *unchanged*, while a similar statePSPACE containment following from [MY23] will worsen the distance parameter δ, namely $\mathsf{stateQMA}_\delta \subseteq \mathsf{statePSPACE}_{\delta+1/\mathrm{poly}}$.

Furthermore, we demonstrate a natural instance of stateQMA that illustrates the state family of UQMA witnesses, as described in Theorem 1.5. It is noteworthy that we concentrate on UQMA witnesses rather than QMA witnesses because stateQMA comprises *state families* whereas QMA witnesses typically correspond to *a subspace*, such as the ground space $\mathcal{S}_H$ of a local Hamiltonian H with a dimension $\dim(\mathcal{S}_H) > 1$.

[4] We emphasize that $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$ is not a state-synthesizing counterpart of the class NPSPACE, where "off" indicates *offline* access to the witness state. See Remark 3.8 for details.

Theorem 1.5 (UQMA witness family is in stateQMA, informal version of Theorem 6.1)**.** *For any promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, we have*

- *If $\mathcal{L} \in$ UQMA, the family of witness states $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to yes instances is in $\mathsf{stateQMA}_{1/\text{poly}}$;*
- *If $\mathcal{L} \in \mathsf{PreciseUQMA}_{1-1/\exp}$ (PreciseUQMA with $1/\exp$ completeness error), the family of witness states $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to yes instances is in $\mathsf{statePreciseQMA}_{1/\exp}$.*

In addition, we prove that stateQCMA, which is a variant of stateQMA in which only classical witnesses (i.e., binary strings) are considered for both completeness and soundness conditions, can achieve perfect completeness:

Theorem 1.6 (stateQCMA achieves perfect completeness, informal version of Theorem 7.1)**.** *For any $c(n) - s(n) \geq 1/\text{poly}(n)$ and $0 \leq c(n), s(n) \leq 1$, we have*

$$\mathsf{stateQCMA}_\delta[c, s] \subseteq \mathsf{stateQCMA}_\delta[1, s']$$

for some s' such that $1 - s'(n) \geq 1/\text{poly}(n)$.

This result is analogous to the $\mathsf{QCMA} = \mathsf{QCMA}_1$ theorem [JN11, JKNN12] for synthesizing quantum states. In addition, it is worth noting that Theorem 1.6 also straightforwardly extends to statePreciseQCMA.

1.2 Proof techniques

The proof of Theorem 1.1 and Theorem 1.2 employs the quantum linear algebra techniques developed by Gilyén, Su, Low, and Wiebe [GSLW19], specifically the quantum singular value discrimination.

Error reduction for stateQMA by manipulating singular values. To elaborate on the intuition, we begin by briefly reviewing the witness-preserving error reduction for QMA [MW05, NWZ09]. Consider a QMA verification circuit V_x that takes a quantum witness state $|w\rangle$ (on the register W) and ancillary qubits in the state $|\bar{0}\rangle$ as input. The corresponding acceptance probability is $\||1\rangle\langle 1|_{\text{out}} V_x |w\rangle|\bar{0}\rangle\|_2^2$, which is equal to a quadratic form $\langle w|M_x|w\rangle$ where the matrix $M_x := \langle\bar{0}|V_x^\dagger|1\rangle\langle 1|_{\text{out}} V_x|\bar{0}\rangle$. It is not hard to see the maximum acceptance probability of V_x is the largest eigenvalue of M_x. We then view $M_x = \Pi_{\text{in}}\Pi\Pi_{\text{in}}$ as a product of Hermitian projectors Π_{in} and Π where $\Pi_{\text{in}} = I_{\mathsf{W}} \otimes |\bar{0}\rangle\langle\bar{0}|$ and $\Pi = V_x^\dagger|1\rangle\langle 1|_{\text{out}} V_x$. Remarkably, there exists an orthogonal decomposition of the Hilbert space, which the projectors Π_{in} and Π act on, into *one-dimensional* and *two-dimensional* common invariant subspaces. This elegant decomposition property is referred as to the Jordan lemma [Jor75].[5] Marriott and Watrous [MW05] then take advantage of the Jordan lemma and present error reduction for QMA that preserves the quantum witness state.

However, this error reduction technique does not automatically preserve the resulting state, as required in stateQMA, we thus need a more sophisticated technique, namely the quantum singular value transformation [GSLW19]. This technique generalizes the qubitization technique introduced by Low and Chuang [LC19] that was inspired by the aforementioned decomposition property. Moving on to the maximum acceptance probability of a stateQMA verifier V_x, it corresponds to the square root of the largest singular value of the matrix $A_x = \Pi_{\text{out}} V_x \Pi_{\text{in}}$ where $\Pi_{\text{out}} := |1\rangle\langle 1|_{\text{out}}$ is the final measurement. In Section 3.2 of [GSLW19], the authors extend the Jordan lemma to the singular value scenarios. In particular, $\text{Img}(\Pi_{\text{in}})$ and $\text{Img}(\Pi_{\text{out}})$ can be

[5] See [Reg06] for the detailed statement of the Jordan lemma, as well as a simple proof.

decomposed into one-dimensional or two-dimensional common invariant subspaces. Now let us focus on the specific case of stateQMA, we notice that the right singular vectors of A_n correspond to the quantum witness state $|w\rangle$, and the left singular vectors correspond to the resulting state $\rho_{x,w}$. Therefore, we obtain *doubly-preserving error reduction* for stateQMA (Theorem 1.1) by manipulating the singular values accordingly.[6]

It is noteworthy that Theorem 1.1 differs from Theorem 38 in [GSLW19] since our construction is based on the *projected unitary encoding* (e.g., the presented matrix A_n) instead of the block-encoding. Furthermore, for establishing Theorem 1.2, we make use of an *exponential-degree* approximation polynomial of the sign function where all coefficients are computable in PSPACE to within *exponential precision* [MY23]. We additionally observe that the proof techniques in [MY23] can be straightforwardly adapted to *projected unitary encodings* instead of the block-encodings originally utilized in their work.

Applications of error reduction for stateQMA. Along the line of Theorem 3.13 in [MW05], which states QMA[log] = BQP, with Theorem 1.1, it seems to straightforwardly make for Corollary 1.3. Nevertheless, we need a careful analysis on the resulting state to achieve the statement. Specifically, utilizing the error reduction for stateQMA, we begin with a verifier with completeness $1 - 2^{-p(n)}$ and soundness $2^{-p(n)}$ where p is a polynomial of $n := |x|$. Then we replace the short quantum witness state $|w\rangle$ with a completely mixed state $I_{\mathsf{W}}/\dim(I_{\mathsf{W}})$, which gives us a computation meeting the soundness condition such that the soundness s is preserved and the gap between the completeness and the soundness shrinks to some inverse-polynomial of $n := |x|$. Although the new resulting state $\rho_{I_{\mathsf{W}}}$ may greatly differ from $\rho_{x,w}$, the definition of stateQMA guarantees that $\rho_{I_{\mathsf{W}}}$ is also close to the target state because the acceptance probability of the verifier with I_{W} is greater than the soundness s. This proof also easily extends to Corollary 1.4 employing Theorem 1.2. In addition, it is noteworthy that stateBQP achieves perfect completeness with a worsening distance parameter δ'. By incorporating error techniques for both stateBQP and $\mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}$, the difference between the new distance parameter δ' and the original one can be made *exponentially small*. Furthermore, we remark that stateBQP is contained in stateQMA.[7] We therefore complete the other direction in Corollary 1.3.

UQMA witness family is in stateQMA. To establish Theorem 1.5, we start by employing a weighted circuit-to-Hamiltonian construction [BC18, BCNY19] to generate a ground state (also known as the history state) that provides a δ_1-close approximation of the output state produced by a UQMA verifier V_x with maximum acceptance probability $1-\nu$. The resulting Hamiltonian $H^{(x)}$ possesses several crucial properties: the ground energy of $H^{(x)}$ is ν, and the spectral gap satisfies $\Delta(H^{(x)}) \geq q(\nu\delta_1/T^3)$ for some polynomial q, where T is the size of V_x.

Next, we construct a $\mathsf{stateQMA}_{\delta}[c', s']$ verifier primarily based on the one-bit precision phase estimation [Kit95], often referred to as Hadamard test [AJL09]. Through a fairly complicated analysis, we demonstrate that the promise gap $c' - s' \geq q'(v\delta_1 t/T^3) - 2\epsilon$ for some polynomial q' and the distance parameter $\delta \leq O(\max\{(1-\cos\nu)/2, \delta_1, q(\nu\delta_1 t/T^3)\})$. Here, ϵ represents the implementation error of $\exp(-iH^{(x)}t)$ guaranteed by space-efficient Hamiltonian simulation [FL18, Theorem 12]. We then achieve Theorem 1.5 by appropriately choosing parameters.

[6]Concretely speaking, the analysis of error reduction based on majority votes essentially corresponds to obtaining tail bounds for the Binomial distribution. By leveraging the central limit theorem, it becomes sufficient to estimate tail bounds for the normal distribution, referred to as the error function $\mathrm{erf}(x)$. The approximation polynomials of the sign function in [LC17] then achieve this task.

[7]See Section 3.2 (in particular, Proposition 3.9) for a detailed elaboration.

stateQCMA achieves perfect completeness. Our proof of Theorem 1.6 takes inspiration from [JN11, JKNN12], but it requires several modifications. Note that our concern in stateQCMA is not only the maximum acceptance probability but also the resulting state after performing the verification circuit and the final measurement. To meet these requirements, we must choose a specific universal gateset $\mathcal{S}$ such that $\mathcal{S}$ can generate a dense subgroup of $\mathrm{SU}(2^n)$ where n is the number of qubits utilized in the quantum circuit, and all quantum states generated by these gates in $\mathcal{S}$ have rational entries. For this reason, we opt for the "Pythagorean gateset"[8] [JN11, CK24]. To ensure that the resulting state is indeed close to the target state, we slightly adjust the construction outlined in [JKNN12].

1.3 Related works

In addition to the state-synthesizing complexity classes explored in prior works [RY22, INN+22, MY23] and the present study, there are other investigations focusing on the quantum state synthesizing problem from diverse perspectives, including cryptography and distributed computing. From a cryptographic standpoint, a recent work [CGK21] examines non-interactive zero-knowledge (NIZK) proofs for quantum states, with a relevance to the setting of stateQCMA. Another concurrent study [CMS23] addresses zero-knowledge proofs for quantum states, considering scenarios that pertinent to both stateQMA and stateQIP scenarios. On the other hand, in the realm of distributed computing, another recent work [LMN23] delves into quantum state synthesizing through the utilization of distributed quantum Merlin-Arthur protocols.

1.4 Discussion and open problems

Reduction and completeness in state-synthesizing complexity theory. In the context of state-synthesizing complexity theory, including prior works [INN+22, MY23, RY22] and our own, the concepts of *reduction* and *completeness* have not been defined. However, these concepts hold significant importance in (quantum) complexity theory. The immediate challenge lies in appropriately defining these concepts, such as reduction, in a manner that ensures the resulting states exhibit reasonable behavior before and after the application of the reduction. Nevertheless, a very recent work [BEM+23] introduced notions of reduction and completeness within the context of *unitary-synthesising* complexity theory.

The computational power of statePreciseQMA. Although Corollary 1.4 establishes that a statePSPACE containment of statePreciseQMA, the reverse inclusion, namely statePSPACE $\subseteq$ statePreciseQMA, remains an open problem. The main challenge lies in adapting existing proof techniques that demonstrate PSPACE $\subseteq$ PreciseQMA [FL16, FL18, Li22], as these techniques heavily rely on notions of *completeness* or *reduction* for the class PSPACE.

2 Preliminaries

In this paper we assume the reader is familiar with the basic concepts and notions of quantum computation (see, e.g., [NC10] for the reference). We begin by introducing some useful linear-algebraic notations. Let M be an Hermitian matrix, and we denote the largest eigenvalue of M as $\lambda_{\max}(M)$, as well as the largest singular value of M as $\sigma_{\max}(M)$. Also, I_k is the identity matrix of size $2^k \times 2^k$. In addition, we will employ three Schatten norms of matrices in this paper, which include:

[8] See Remark 7.2 for the details.

- Trace norm $\|M\|_1 \coloneqq \mathrm{Tr}\sqrt{M^\dagger M}$;
- Frobenius norm $\|M\|_2 \coloneqq \sqrt{\mathrm{Tr}(M^\dagger M)}$;
- Operator norm $\|M\|_\infty \coloneqq \sigma_{\max}(M) = \sqrt{\lambda_{\max}(M^\dagger M)}$.

2.1 Distances for quantum states

For any (in general mixed) quantum states ρ_0 and ρ_1, we measure the closeness between these states by the *trace distance* $\mathrm{td}(\rho_0, \rho_1) \coloneqq \frac{1}{2}\|\rho_0 - \rho_1\|_1$. Moreover, we will employ the following properties of the trace distance, which are explained in detail in Section 9.2.1 of [NC10]:

Contractivity For any quantum channel Φ, we have $\mathrm{td}(\Phi(\rho_0), \Phi(\rho_1)) \leq \mathrm{td}(\rho_0, \rho_1)$;

Convexity For any non-negative coefficients $\{p_i\}_i$ such that $\sum_i p_i = 1$, we have

$$\mathrm{td}(\rho_0, \textstyle\sum_i p_i \rho_1^{(i)}) \leq \sum_i p_i \mathrm{td}(\rho_0, \rho_1^{(i)}).$$

In addition, we utilize the (Uhlmann) *fidelity* defined as *fidelity* $\mathrm{F}(\rho_0, \rho_1) \coloneqq \mathrm{Tr}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$. Importantly, when considering a pure state $\rho_0 \coloneqq |\psi_0\rangle\langle\psi_0|$ and a mixed state ρ_1, the fidelity simplifies to $\mathrm{F}(\rho_0, \rho_1) = \sqrt{\langle\psi_0|\rho_1|\psi_0\rangle}$. Furthermore, the well-known Fuchs-van de Graaf inequality [FvdG99] states the following:

Lemma 2.1 (Trace distance vs. Fidelity,[FvdG99])**.** *For any quantum states ρ_0 and ρ_1,*

$$1 - \mathrm{F}(\rho_0, \rho_1) \leq \mathrm{td}(\rho_0, \rho_1) \leq \sqrt{1 - \mathrm{F}^2(\rho_0, \rho_1)}.$$

2.2 Gatesets matter for synthesizing quantum states

A *gateset* is a finite set of unitary matrices each of which acts on a finite-dimensional quantum system. A gateset $\mathcal{S}$ is *universal* if the subgroup generated by $\mathcal{S}$ is dense in $\mathrm{SU}(2^n)$ for large enough n. We mainly use the common universal gateset $\{\mathrm{CNOT}, \textsc{Hadamard}, \mathrm{T}\}$ for convenience, and further note that complexity classes remain unchanged for all reasonable choices of gatesets that all entries are algebraic numbers,[9] owing to the Solovay-Kitaev theorem [Kit97] and its space-efficient variant [vMW12].

Additionally, to achieve perfect completeness, we require a particular *"Pythagorean" gateset* in Section 7, introduced by Jordan and Nagaj[JN11], which consists of CNOT and "Pythagorean" gates $\frac{1}{5}\left(\begin{smallmatrix} 4 & -3 \\ 3 & 4 \end{smallmatrix}\right)$ and $\frac{1}{5}\left(\begin{smallmatrix} 4 & 3i \\ 3i & 4 \end{smallmatrix}\right)$.[10]

We end with Lemma 2.2 which states changing the gateset of a family of quantum circuits that prepares a certain family of quantum states will make the resulting state negligibly far from the target state. Lemma 2.2 highlights the robustness of the state-synthesizing procedure with respect to the choice of gateset. For convenience, we will define $\psi \coloneqq |\psi\rangle\langle\psi|$.

Lemma 2.2 (Changing gateset worsens the distance parameter)**.** *Consider a family of (verification) circuits $\{Q_x\}_{x\in\mathcal{L}}$ that prepares the corresponding family of resulting states $\{\rho_x\}_{x\in\mathcal{L}}$.*[11] *Then there exists a circuit family $\{Q'_x\}_{x\in\mathcal{L}}$ that prepares $\{\rho'_x\}_{x\in\mathcal{L}}$, using a designated universal*

[9] For a comprehensive explanation of the conditions on choosing gatesets, see Theorem 2.10 in [Kup15].

[10] An analogous gateset is also utilized in [CK24] with a slightly different "Pythagorean" gate.

[11] In particular, we first perform the (verification) circuit Q_x on the input state, which is not necessarily the all-zero state, then we measure the designated output qubit. If the measurement outcome is 1, we obtain the resulting state corresponding to Q_x on the remaining qubits.

gateset $\mathcal{G}$ that is closed under adjoint, such that $\mathrm{td}(\rho_x, \rho'_x) \leq \exp(-\mathrm{poly}(n))$ *where* $n := |x|$*. In particular, the deterministic algorithm that constructs* $\{Q'_x\}_{x\in\mathcal{L}}$ *runs in polynomial time and polynomial space.*

Proof. Consider a quantum channel $\Phi(\rho) := \frac{\Pi_{\mathrm{out}}\rho\Pi_{\mathrm{out}}}{\mathrm{Tr}(\Pi_{\mathrm{out}}\rho\Pi_{\mathrm{out}})}$ where $\Pi_{\mathrm{out}} := |1\rangle\langle 1|_{\mathrm{out}}$ that post-selects the output qubit to be 1, and let $|w\rangle$ be a (quantum) witness,[12] we have derived that

$$\begin{aligned}
\mathrm{td}(\rho_x, \rho'_x) &= \mathrm{td}\left(\Phi\left(Q_x(|w\rangle\langle w| \otimes |\bar{0}\rangle\langle\bar{0}|)Q_x^\dagger\right), \Phi\left(Q'_x(|w\rangle\langle w| \otimes |\bar{0}\rangle\langle\bar{0}|)(Q'_x)^\dagger\right)\right) \\
&\leq \mathrm{td}\left(Q_x(|w\rangle\langle w| \otimes |\bar{0}\rangle\langle\bar{0}|)Q_x^\dagger, Q'_x(|w\rangle\langle w| \otimes |\bar{0}\rangle\langle\bar{0}|)(Q'_x)^\dagger\right) \\
&= \sqrt{1 - \left|\langle w|\langle\bar{0}|Q_x^\dagger Q'_x|w\rangle|\bar{0}\rangle\right|^2} \\
&\leq \|Q_x|w\rangle|\bar{0}\rangle - Q'_x|w\rangle|\bar{0}\rangle\|_2^2 \\
&= \|Q_x - Q'_x\|_\infty^2 \||w\rangle|\bar{0}\rangle\|_2^2,
\end{aligned}$$

with the second line owing to the contractive property, and the fourth line due to the fact that $(\langle\psi|\phi\rangle - 1)^\dagger(\langle\psi|\phi\rangle - 1) \geq 0$ for any pure states $|\psi\rangle$ and $|\phi\rangle$.

Note that the gates of $\mathcal{G}$ are closed under adjoint. By a space-efficient Solovay-Kitaev theorem (i.e., Theorem 4.3 in [vMW12]), we can construct Q'_x such that $\|Q_x - Q'_x\|_\infty \leq \epsilon$ by a deterministic algorithm running in time $\mathrm{poly}\log(1/\epsilon)$ and space $O(\log(1/\epsilon))$. By choosing $\epsilon^2 = \exp(-\mathrm{poly}(n))$, we thus obtain $\mathrm{td}(\rho_x, \rho'_x) \leq \|Q_x - Q'_x\|_\infty^2 \leq \exp(-\mathrm{poly}(n))$ as desired. □

2.3 Unique-witness QMA

Definition 2.3 (Unique Quantum Merlin-Arthur, UQMA, adapted from [ABBS22, JKK+12])**.** *A promise problem* $\mathcal{L} = (\mathcal{L}_{\mathrm{yes}}, \mathcal{L}_{\mathrm{no}})$ *is in* $\mathsf{UQMA}[c, r, s]$ *if there exists a uniformly generated polynomial-size quantum circuit* $\{V_x\}_{x\in\mathcal{L}}$ *having* $k(n)$ *qubits for the witness register and requiring* $m(n)$ *ancillary qubits initialized to* $|0^m\rangle$*, where* k *and* m *are polynomials of* $n := |x|$ *such that*

- **Completeness**. *If* $x \in \mathcal{L}_{\mathrm{yes}}$*, then there exists a witness* $|w\rangle$ *such that* $\Pr[V_x \text{ accepts } |w\rangle] \geq c(n)$*. Furthermore, for all states* $|\phi\rangle$ *orthogonal to* $|w\rangle$*,* $\Pr[V_x \text{ accepts } |\phi\rangle] \leq r(n)$*.*
- **Soundness**. *If* $x \in \mathcal{L}_{\mathrm{no}}$*, then for all states* $|\phi\rangle$*,* $\Pr[V_x \text{ accepts } |\phi\rangle] \leq s(n)$*.*

Here, $c, r, s\colon \mathbb{N} \to [0, 1]$ *are efficiently computable functions such that* $c(n) > \max\{r(n), s(n)\}$*.*

Following the witness-preserving error reduction for QMA by Marriott and Watrous [MW05], we know that UQMA admits error reduction.

Theorem 2.4 (Error reduction for UQMA, [JKK+12, Theorem 3.6])**.** *Consider* $x \in \mathcal{L}$ *where* $\mathcal{L} \in \mathsf{UQMA}$*. Let* $c, r, s\colon \mathbb{N} \to [0, 1]$ *be efficiently computable functions such that* $c(n) > \max\{r(n), s(n)\} + 1/q(n)$ *for some polynomial* q *of* $n := |x|$*. Then for any polynomial* $l(n)$*, we have that*

$$\mathsf{UQMA}[c, r, s] \subseteq \mathsf{UQMA}\left[1 - 2^{-l}, 2^{-l}, 2^{-l}\right].$$

The witness length of the new UQMA *verifier remains preserved.*

Furthermore, we can similarly define a variant of UQMA that corresponds to a promise gap, specifically $c - \max\{r, s\}$, exponentially approaching zero. This variant is denoted as

[12] If Q_x and Q'_x are not verification circuits, then this witness state is simply the all-zero state.

PreciseUQMA. Additionally, we introduce the notations $\mathsf{UQMA}_{1-\nu}$ and $\mathsf{PreciseUQMA}_{1-\nu}$ when the completeness error of these classes is ν:

$$\mathsf{UQMA}_{1-\nu} \coloneqq \cup_{1-\nu-\max\{r(n),s(n)\}\geq 1/\mathrm{poly}(n)} \mathsf{UQMA}[1-\nu, r, s],$$
$$\mathsf{PreciseUQMA}_{1-\nu} \coloneqq \cup_{1-\nu-\max\{r(n),s(n)\}\geq \exp(-\mathrm{poly}(n))} \mathsf{UQMA}[1-\nu, r, s].$$

In particular, if ν is exponentially small (negligible), we use the notations $\mathsf{UQMA}_{1-\mathrm{negl}}$ and $\mathsf{PreciseUQMA}_{1-\mathrm{negl}}$.

2.4 Tools from random walks on graphs

In this subsection, we recapitulate several useful lemmas concerning random walks on an undirected path graph $G = (V, E)$ and their associated spectral properties. These lemmas have been employed in weighted circuit-to-Hamiltonian constructions, such as [BC18] and [BCNY19, Section 6]. A random walk on such a graph corresponds to a reversible Markov chain (Ω, P, π) on the state space $\Omega = V$ with a stationary distribution π and a transition matrix P. For detailed definitions of these terminologies, we refer to [LP17, Chapter 1].

Lemma 2.5 (Adapted from [BC18, Lemma 4])**.** *Consider a $(T+1)$-node path graph $G = (V, E)$ and a strictly positive probability distribution π on V.*[13] *There exists a Markov chain (V, P, π) with Metropolis transition probabilities P that is reversible with respect to the given stationary distribution π as below:*

- *For $0 < t < T$, $P_{t,t+1} \coloneqq \frac{1}{4}\min\{1, \frac{\pi_{t+1}}{\pi_t}\}$, $P_{t+1,t} \coloneqq \frac{1}{4}\min\{1, \frac{\pi_{t-1}}{\pi_t}\}$, and $P_{t,t} \coloneqq 1 - P_{t,t+1} - P_{t+1,t}$;*
- *For $t = 0$, $P_{0,1} \coloneqq \frac{1}{2}\min\{1, \frac{\pi_1}{\pi_0}\}$, $P_{0,-1} \coloneqq 0$, and $P_{0,0} \coloneqq 1 - P_{0,1}$;*
- *For $t = T$, $P_{T,T-1} \coloneqq \frac{1}{2}\min\{1, \frac{\pi_{T-1}}{\pi_T}\}$, $P_{T,T+1} \coloneqq 0$, and $P_{T,T} \coloneqq 1 - P_{T,T-1}$.*

Furthermore, we have a corresponding stoquastic frustration-free[14] *$O(\log n)$-local Hamiltonian $H^{(T)}_{\mathrm{path}} \coloneqq \sum_{t=0}^{T} H_{\mathrm{path}}(t)$ such that the spectral gap $\Delta(H^{(T)}_{\mathrm{path}})$ is the same as the spectral gap Δ_P.*[15] *Here, the local term $H_{\mathrm{path}}(t)$ for any $0 \leq t \leq T$ is defined as:*

$$H_{\mathrm{path}}(t) \coloneqq (1 - P_{t,t})|t\rangle\langle t| - \frac{\sqrt{\pi_t}}{\sqrt{\pi_{t-1}}} P_{t,t-1}|t\rangle\langle t-1| - \frac{\sqrt{\pi_{t-1}}}{\sqrt{\pi_t}} P_{t-1,t}|t-1\rangle\langle t|$$

Proof. Our construction and the analysis closely parallel the proof of [BC18, Lemma 4]. Through a direct calculation, we can establish that the matrix P satisfies the condition of being a transition matrix: $\sum_{t=0}^{T} \pi_t P_{t,t'} = \pi_{t'}$. Additionally, the constructed Markov chain is reversible as the transition probabilities satisfy $\pi_t P_{t,t'} = \pi_{t'} P_{t',t}$ for all $0 \leq t, t' \leq T$.

According to the equivalent conditions for a reversible Markov chain (see [SJ89]), this construction gives rise to a symmetric matrix $A \coloneqq D^{1/2} P D^{-1/2}$, where $D \coloneqq \mathrm{diag}(\pi_0, \pi_1, \cdots, \pi_T)$. Since we obtain A by applying a similarity transformation to P, all eigenvalues of A coincide with those of P. Consequently, we arrive at $H^{(T)}_{\mathrm{path}} = I - A$ where I is a $(T+1) \times (T+1)$ identity matrix. Notably, $H^{(T)}_{\mathrm{path}}$ is both stoquastic and frustration-free because P is entry-wise non-negative and the largest eigenvalue of P is 1. □

[13] A probability distribution π is *strictly positive* if all components π_t are positive.

[14] We say that a Hamiltonian is *stoquastic* if all off-diagonal entries in the corresponding Hermitian matrix are real and non-positive. Additionally, we say that a Hamiltonian is *frustration-free* if its ground energy is zero, and the ground states of the Hamiltonian $H = \sum_i H_i$ are also ground states of all local terms H_i.

[15] Specifically, $\Delta(H^{(T)}_{\mathrm{path}})$ is the difference between the second smallest eigenvalue of $H^{(T)}_{\mathrm{path}}$ and the smallest eigenvalue, whereas Δ_P is the difference between the largest eigenvalue of P and the second largest eigenvalue.

Then we will provide a lower bound for the spectral gap Δ_P based on the *conductance* of the underlying graph $G = (V, E)$, which characterizes the graph's connectivity. In particular, for any nonempty subset $S \subseteq V$, we define the conductance as $\Phi_G(S) \coloneqq \frac{1}{\min\{\pi(S),\pi(\bar{S})\}} \sum_{x\in S, y\in\bar{S}} \pi_x P_{x,y}$, and the conductance of the graph G is denoted by $\Phi_G \coloneqq \min_{S\subseteq V} \Phi(S)$. The well-known Cheeger's inequality demonstrates a spectral gap lower bound as follows.

Lemma 2.6 (Cheeger's inequality, adapted from [SJ89, Lemma 3.3])**.** *For a reversible Markov chain with the underlying (weighted) graph G, the spectral gap Δ_P of the transition matrix P satisfies $\frac{1}{2}\Phi_G^2 \leq \Delta_P$.*

2.5 Space-efficient Hamiltonian simulation

We adopt the following definition of *efficient encodings* of matrices adapted from [FL18]:

Definition 2.7 (Efficient encodings, adapted from [FL18, Definition 10])**.** *Let M be a $2^{k(n)} \times 2^{k(n)}$ matrix, and let $\mathcal{A}$ be a classical algorithm (e.g., a Turing machine) specified using n bits. We say that $\mathcal{A}$ provides an efficient encoding of M if, given an input $i \in \{0,1\}^{k(n)}$, $\mathcal{A}$ outputs the indices and contents of the nonzero entries of the i-th row, using at most $\mathrm{poly}(n)$ time and $O(k)$ workspace (excluding the output size). Consequently, M has at most $\mathrm{poly}(n)$ nonzero entries in each row.*

In the following scenario, we will specify a matrix M in the input by providing an efficient encoding of M, where the size of the encoding is the input size denoted by n.

We now proceed with a Hamiltonian simulation procedure achieving exponential precision with only polynomial space. The techniques come from [BCC+14, BCC+15, BCK15], with an observation on the space complexity made in [FL18].

Lemma 2.8 (Adapted from [FL18, Theorem 12])**.** *Consider the size-n efficient encoding of a $2^{k(n)} \times 2^{k(n)}$ Hermitian matrix H as an input, and treat this matrix H as a Hamiltonian. Then the time evolution $\exp(-iHt)$ can be simulated using $\mathrm{poly}(n, k, \|H\|_\infty, t, \log(1/\epsilon))$ operations and $O(k + \log(t/\epsilon))$ space, where ϵ is the error in operator norm.*

3 Basic state-synthesizing complexity classes

In this section, we will define state-synthesizing complexity classes involved in this paper.

3.1 State-synthesizing complexity classes with bounded time or space

We begin with two crucial notations on circuit families. A family of quantum circuits $\{Q_x\}_{x\in\mathcal{L}}$ associated with the language $\mathcal{L} \subseteq \{0,1\}^*$ is *uniformly generated* if there exists a deterministic polynomial-time Turing machine (and thus polynomially space-bounded) that on input $x \in \mathcal{L}$ outputs the description of Q_x. Likewise, a family of quantum circuits $\{Q_x\}_{x\in\mathcal{L}}$ is *space-uniformly generated* if Q_x acts on polynomially many qubits and there exists a deterministic polynomial-space Turing machine that on input $x \in \mathcal{L}$ outputs the description of Q_x. Then we move on to the class that captures efficiently preparable quantum state families.

Definition 3.1 ($\mathsf{stateBQP}_\delta[\gamma]$)**.** *A family of quantum states $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ is in $\mathsf{stateBQP}_\delta[\gamma]$ if each $|\psi_x\rangle$ is an n-qubit state where $n \coloneqq |x|$, and there exists a uniformly generated quantum circuit family $\{Q_x\}_{x\in\mathcal{L}}$, which takes no inputs, such that for all $x \in \mathcal{L}$:*

- *The circuit Q_x outputs a (in general mixed) quantum state ρ_x satisfying $\mathrm{td}(\rho_x, \psi_x) \leq \delta(n)$ if Q_x succeeds. Here, we define the success of circuit Q_x as the measurement outcome of the designated output qubit being 1.*

- *The success probability of Q_x is at least γ.*

For convenience, we define $\mathsf{stateBQP}_\delta := \mathsf{stateBQP}_\delta[2/3]$. Similarly, we define $\mathsf{stateBQP}$ with exponentially small success probability in Definition 3.2.

Definition 3.2 ($\mathsf{statePreciseBQP}_\delta$)**.** $\mathsf{statePreciseBQP}_\delta := \cup_{\gamma \geq \exp(-\mathrm{poly}(n))} \mathsf{stateBQP}_\delta[\gamma]$.

Afterwards, we consider a state-synthesizing counterpart of unitary quantum polynomial space $\mathsf{BQ_UPSPACE}$ in [FL18]. In particular, we define $\mathsf{statePSPACE}$ in terms of *unitary quantum computation*, denoted as $\mathsf{state_UPSPACE}$.

Definition 3.3 ($\mathsf{state_UPSPACE}_\delta[\gamma]$)**.** *A family of quantum states $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ is in $\mathsf{state_UPSPACE}_\delta[\gamma]$ if each $|\psi_x\rangle$ is an n-qubit state where $n := |x|$, and there exists a space-uniform family of unitary quantum circuits $\{Q_x\}_{x\in\mathcal{L}}$, which takes no inputs, such that for all $x \in \mathcal{L}$:*

- *The circuit Q_x outputs a (in general mixed) quantum state ρ_x satisfying $\mathrm{td}(\rho_x, \psi_x) \leq \delta(n)$ if Q_x succeeds. Here, we define the success of circuit Q_x as the measurement outcome of the designated output qubit being 1.*

- *The success probability of Q_x is at least γ.*

We denote $\mathsf{state_UPSPACE}_\delta := \mathsf{state_UPSPACE}_\delta[2/3]$. It is worth noting that there are three differences between our definition $\mathsf{state_UPSPACE}$ and $\mathsf{statePSPACE}$ as defined in [RY22, MY23]: 1) our definition only admits unitary quantum computation whereas $\mathsf{statePSPACE}$ also permits general quantum circuits (see Remark 3.4); 2) our definition does not assume perfect completeness, even though this property is always achievable for our definition with a worsening distance parameter; and 3) our definition merely deals with pure state families, while $\mathsf{statePSPACE}$ in [MY23] also accommodates mixed state families.

Remark 3.4 (Synthesizing states by general quantum circuits)*.* General quantum circuits allow not only unitary quantum gates but also intermediate measurements and resetting qubits. Because of the principle of deferred measurement, admitting intermediate measurements does not make the time-efficient class more powerful. Recent developments on eliminating intermediate measurements in quantum logspace [FR21, GRZ21, GR22] improve this to the space-efficient scenario. Nevertheless, these new techniques in [FR21, GRZ21] do not automatically extend to state-synthesizing classes since they do not (even approximately) preserve the resulting state, and another result [GR22] only apply to a subclass of general quantum computation.

$\mathsf{stateBQP}$ and $\mathsf{state_UPSPACE}$ achieve perfect completeness. It is worth noting that the family of states constructed by the simulator used in quantum statistical zero-knowledge [Wat02] is an instance of $\mathsf{stateBQP}$. Interestingly, one can assume that the corresponding simulator achieves perfect completeness with a worsening distance parameter δ'.[16] To achieve this, one can simply replace the designated output qubit of the QSZK simulator, or a $\mathsf{stateBQP}$ circuit in general, with a qubit in state $|1\rangle$. This technique applies to any state-synthesizing complexity class with bounded time or space, including $\mathsf{stateBQP}$ and $\mathsf{state_UPSPACE}$:

[16] To be specific, this fact is demonstrated in the QSZK-hardness proof of the Quantum State Distinguishability Problem, as presented in Theorem 6 in [Wat02].

Proposition 3.5. *For any $0 \leq \delta(n), \gamma(n) \leq 1$, choosing $\delta' := \gamma\delta + 1 - \gamma$, then*

$$\mathsf{stateBQP}_{\delta}[\gamma] \subseteq \mathsf{stateBQP}_{\delta'}[1] \text{ and } \mathsf{state_UPSPACE}_{\delta}[\gamma] \subseteq \mathsf{state_UPSPACE}_{\delta'}[1].$$

Moreover, we note that achieving perfect completeness has little effect on the distance parameter when combined with the error reduction techniques employed by the aforementioned classes. Specifically, the new distance parameter δ' can be made *exponentially close* to δ.

Proof of Proposition 3.5. Let ρ be the resulting state upon acceptance with respect to either a stateBQP circuit or a state$_U$PSPACE circuit, denoted as Q_x, and similarly let ρ_* be the resulting state upon rejection. Also, let $\hat{\rho}$ be the resulting state when we replace the output qubit with a qubit in state $|1\rangle$. Let γ' be the exact success probability of Q_x. Recall that $|\psi_x\rangle$ is the target state that Q_x aims to approximate, then we obtain:

$$\begin{aligned}
\mathrm{td}(|\psi_x\rangle\langle\psi_x|, \hat{\rho}) &= \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \gamma' \cdot \rho + (1-\gamma') \cdot \rho_*) \\
&\leq \gamma' \cdot \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \rho) + (1-\gamma') \cdot \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \rho_*) \\
&= \gamma \cdot \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \rho) + (\gamma' - \gamma) \cdot \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \rho) + (1-\gamma') \cdot \mathrm{td}(|\psi_x\rangle\langle\psi_x|, \rho_*) \\
&\leq \gamma\delta + 1 - \gamma.
\end{aligned}$$

Here, the second line follows from the convexity of the trace distance, and the last line holds because $\mathrm{td}(\psi_x, \rho) \leq \delta(n)$, with the trace distance bounded by 1. □

3.2 Quantum Merlin-Arthur proof systems for synthesizing quantum states

We will now discuss stateQMA, which is a state-synthesizing counterpart of the class NP. Moreover, it is a natural subclass of stateQIP, as defined [RY22], since we merely admit one message from the prover to the verifier. It is worth noting that quantum state-synthesizing complexity classes can be viewed as quantum analogs of classical function classes, such as TFNP,[17] which do not contain *no* instances.

Definition 3.6 ($\mathsf{stateQMA}_{\delta}[c, s]$)**.** *Consider efficiently computable functions $c(n), s(n), \delta(n)$ satisfying $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, $0 \leq s(n) < c(n) \leq 1$, and $0 \leq \delta(n) \leq 1$. A family of quantum states $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ is in $\mathsf{stateQMA}_{\delta}[c, s]$ if each $|\psi_x\rangle$ is an n-qubit state where $n := |x|$, and there is a uniformly generated polynomial-size unitary quantum circuits family $\{V_x\}_{x\in\mathcal{L}}$ acting on $m+k$ qubits, where m is the number of workspace qubits and k is the number of ancillary qubits where both $m(n)$ and $k(n)$ are polynomials of n, such that the following conditions hold:*

- **Completeness.** *There is an m-qubit state $|w\rangle$ such that $\Pr[V_x \text{ accepts } |w\rangle] \geq c(n)$.*
- **Soundness.** *For any m-qubit state $|w\rangle$ such that $\mathrm{td}(\rho_{x,w}, |\psi_x\rangle\langle\psi_x|) \geq \delta(n)$, we have $\Pr[V_x \text{ accepts } |w\rangle] \leq s(n)$, where $\rho_{x,w}$ is the resulting state of V_x on the input $|w\rangle|0^k\rangle$ conditioned on the measurement outcome of the output qubit being 1. Here, we allow the verifier to trace out some qubits in the resulting state for convenience.*

In addition, we use the notation $\mathsf{stateQMA}_{\delta}[l, c, s]$ to represent stateQMA with witness states of bounded length, where $l(n)$ is the number of qubits employed by the witness states. If $l(n)$ is a polynomial function of $n := |x|$, we will omit the parameter l.

[17] The class TFNP consists of function problems of the following form: given an input x and a polynomial predicate $F(x, y)$, output any y such that $F(x, y)$ holds, with the promise that such a y exists.

We define $\mathsf{stateQMA}_\delta := \mathsf{stateQMA}_\delta[2/3, 1/3]$. Additionally, we also define the variant of stateQMA with exponentially small promise gap[18] and the variant of stateQMA with a logarithmic-length witness in Definition 3.7.

Definition 3.7 (stateQMA with tiny promise gap and short-length witness)**.**

$$\mathsf{statePreciseQMA}_\delta := \cup_{c-s\geq \exp(-\mathrm{poly}(n))}\mathsf{stateQMA}_\delta[c,s].$$
$$\mathsf{stateQMA}_\delta[\log, c, s] := \cup_{l(n)\leq O(\log n)}\mathsf{stateQMA}_\delta[l, c, s].$$

Furthermore, we need to define $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$, a polynomial-space-bounded variant of stateQMA, which corresponds to state families that are preparable by a polynomial-space-uniform unitary quantum circuit family $\{V_x\}_{x\in\mathcal{L}}$. In particular, we utilize circuit families outlined in Definition 3.3 as verification circuits, where an $m(n)$-qubit witness state and $k(n)$ ancillary qubits (instead of the all-zero state) serve as input, with the witness length $m(n)$ polynomial in n. It is noteworthy that $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$ is not a state-synthesizing counterpart of NPSPACE, as explained in Remark 3.8.

Remark 3.8 (Online vs. offline access to quantum witness state). Online and offline access to a classical witness in the class NP are equivalent, but the models significantly differs in space-bounded classical computation and so do quantum counterparts.[19] The class NPSPACE has online access to an *exponential-length* classical witness, whereas $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$ has offline access to a *polynomial-length* quantum witness, suggesting $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$ is not a state-synthesizing analogue of NPSPACE.

By restricting witnesses for both completeness and soundness conditions in Definition 3.6 to be classical (i.e., binary strings), we obtain the class stateQCMA, and similarly for the precise variant statePreciseQCMA that has an exponentially small promise gap. Likewise, we define $\mathsf{stateQCMA}_\delta := \mathsf{stateQCMA}_\delta[2/3, 1/3]$.

Relation between stateBQP and stateQMA. Finally, we remark that while $\mathsf{stateBQP}_\delta[\gamma]$ is trivially contained in $\mathsf{stateQMA}_\delta[\gamma, \gamma]$ by letting the verifier simply trace out the witness state, proving inclusion in $\mathsf{stateQMA}_\delta[\gamma, \gamma']$ with $\gamma(n) - \gamma'(n) \geq 1/\mathrm{poly}(n)$ is more complicated. In particular, we measure the input quantum state of Q_x (also viewed as a quantum witness state for a stateQMA verifier) on the computational basis, and reject if the outcome is not an all-zero string. We now proceed with a formal statement with a proof:

Proposition 3.9. *For any* $1/\mathrm{poly}(n) \leq \gamma(n) \leq 1$ *and* $0 \leq \delta \leq 1$, $\mathsf{stateBQP}_\delta[\gamma] \subseteq \mathsf{stateQMA}_\delta[\gamma, \gamma']$ *for some* $\gamma'(n) > 0$ *such that* $\gamma(n) - \gamma'(n) \geq 1/\mathrm{poly}(n)$.

Proof. For any given $\mathsf{stateBQP}_\delta[\gamma]$ circuit C_x with $m(n)$ workspace qubits, we construct a new stateQMA verification circuit V_x. We first introduce a new register W for the $m(n)$-qubit witness state $|w\rangle$, and the remaining is the given stateBQP circuit. Then the construction of V_x follows from Algorithm 1.

It suffices to analyze this protocol. For the completeness condition, it is evident that the optimal witness is 0^m. Then guaranteed by the given stateBQP circuit, we obtain $\Pr[V_x \text{ accepts } 0^m] \geq$

[18] To be specific, the gap between the acceptance probability in completeness and soundness is inverse-exponential.

[19] See Section 5.3.1 in [Gol08] for elaborations on space-bounded classical computation. Regarding quantum scenarios, recent advancements in [GR23] signifies that quantum analogues of NPSPACE with online access to an exponential-length witness are more powerful than the offline-access variant QMAPSPACE defined in [FR21], implying a quantum analogue of Savitch's theorem is unlikely to hold.

Algorithm 1: stateQMA verification circuit V_x

1. Perform the stateBQP circuit C_x without the final measurement;
2. Measure all qubits in W (the witness state $|w\rangle$) on the computational basis. Reject if the measurement outcome is not 0^m;
3. Measure the designated output qubit in the stateBQP circuit. Accept and produce the resulting state if the measurement outcome is 1, otherwise reject.

γ. For the soundness condition, since any witness $|w\rangle$ that is orthogonal to $|0^m\rangle$ will be simply rejected, then we have derived that

$$\Pr[V_x \text{ accepts } |w\rangle] = |\langle w|0^m\rangle|^2 \cdot \Pr[C_x \text{ accepts}] \geq \gamma |\langle w|0^m\rangle|^2.$$

Therefore, for any witness state $|w\rangle$, we conclude that $\Pr[V_x \text{ accepts } |w\rangle] > 0$, and the resulting state $\rho_{x,w}$ satisfies $\mathrm{td}(\rho_{x,w}, |\psi_x\rangle\langle\psi_x|) = \mathrm{td}(\rho_{x,0^m}, |\psi_x\rangle\langle\psi_x|) \leq \delta$ as desired. □

4 Quantum singular value discrimination, revisited

In this section, we aim to prove Theorem 4.1, which serves as a "meta theorem" for singular value discrimination using different approximation polynomials with varying parameters. Our approach differs from Theorem 3.2.9 in [Gil19] as we employ the *projected unitary encoding* with an *odd polynomial* to preserve the output of the verification circuit, as specified in Definition 3.6.

We will start by defining a *projected unitary encoding*. We say that U is an ε-projected unitary encoding of linear operator A if $\|A - \tilde{\Pi}U\Pi\|_\infty \leq \varepsilon$ where orthogonal projectors $\tilde{\Pi}$ and Π may also act on some ancillary qubits. In particular, we refer to U as an exact projected unitary encoding of A when $\varepsilon = 0$.

Theorem 4.1 (Singular value discrimination with bounded time and space)**.** *Consider $0 \leq a < b \leq 1$ and an exact projected unitary encoding $A := \tilde{\Pi}U\Pi$, where U acts on $s_1(n)$ qubits. Let $|\psi\rangle$ be an unknown quantum state, a right singular vector of A with a singular value either below a or above b. Suppose there exists a degree-d odd polynomial S satisfying $|S(x) - \mathrm{sgn}(x)| \leq \epsilon$ for all $x \in [-1,1] \setminus (-\delta, \delta)$, where $d = O\left(\delta^{-1}\log(1/\epsilon)\right)$ and δ linearly depends on $b - a$. We can implement the QSVT associated with the polynomial S to distinguish between the two cases, ensuring that the singular value of the given right singular vector $|\psi\rangle$ is either below a or above b, with error probability at most ϵ.*
In particular, the description of quantum circuit implementation (classical prepossessing) can be computed in deterministic time $\mathrm{poly}(d)$ *and space $s_2(n)$, and the circuit implementation takes* $\mathrm{poly}(d)$ *quantum gates and acts on at most $s_1(n) + O(\log d) + 1$ qubits, where $s_2(n)$ is decided by the construction of S.*

Our construction is heavily influenced by [GSLW19] (and Lemma 4.7 taken from [MY23]) and we utilize specific statements from [Gil19] for ease of use. We will show that, for any ϵ equal to $1/\mathrm{poly}(n)$ or $1/\exp(-\mathrm{poly}(n))$, when equipped with different approximation polynomials for the sign function, the space complexity parameters $s_1(n)$ and $s_2(n)$ remain $\mathrm{poly}(n)$ whereas the time complexity parameter $t(n)$ may differ greatly.

4.1 A general framework

Let us now define the singular value decomposition for projected unitary encodings.

Lemma 4.2 (Singular value decomposition of a projected unitary, adapted from Definition 2.3.1 in [Gil19])**.** *Consider a projected unitary encoding of A, denoted by U, associated with orthogonal projectors Π and $\tilde{\Pi}$ on a finite-dimensional Hilbert space $\mathcal{H}_U$. Namely, $A = \tilde{\Pi}U\Pi$. Then there exist orthonormal bases of Π_i and $\tilde{\Pi}_i$ as follows: for Π_i, the orthonormal basis of the subspace $\mathrm{Img}(\Pi_i)$ is $\{|\psi_i\rangle : i \in [d]\}$, where $d \coloneqq \mathrm{rank}(\Pi)$. Similarly, for $\tilde{\Pi}_i$, the orthonormal basis of the subspace $\mathrm{Img}(\tilde{\Pi}_i)$ is $\{|\tilde{\psi}_i\rangle : i \in [\tilde{d}]\}$, where $\tilde{d} \coloneqq \mathrm{rank}(\tilde{\Pi})$. These bases ensure that there is a singular value decomposition $A = \sum_{i=1}^{\min\{d,\tilde{d}\}} \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$, where singular values $\sigma_i > \sigma_j$ for any $i < j \in [\min\{d, \tilde{d}\}]$.*

With these definitions in place, we present the alternating phase modulation as Lemma 4.3, which serves as the key ingredient for implementing quantum singular value transformations. It is worth noting that Lemma 4.3 deviates from Theorem 2.3.7 in [Gil19] due to our assumption that the sequence of rotation angles is already provided. The rotation angles Φ in this context correspond to the polynomial P and will be utilized in computing the descriptions of quantum circuits implementing QSVT corresponding to P.

Lemma 4.3 (QSVT by alternating phase modulation, adapted from Theorem 2.3.7 in [Gil19])**.** *Let $P \in \mathbb{C}[x]$ be an odd polynomial, and let $\Phi \in \mathbb{R}^n$ be the corresponding sequence of rotation angles. There exists an explicit implementation of $P^{(\mathrm{SV})}(\tilde{\Pi}U\Pi) = \tilde{\Pi}U_\Phi\Pi$ when n is odd, using a single ancillary qubit. Specifically, U_Φ represents a quantum circuit that implements the QSVT associated with P, using the corresponding rotation angles specified by Φ. Moreover, the notation $P^{(\mathrm{SV})}(A)$ indicates that the polynomial P is applied to the singular values of the matrix A, rather than to its eigenvalues.*

We will now proceed with proving Theorem 4.1.

Proof of Theorem 4.1. Given an exact projected unitary encoding $\tilde{\Pi}U\Pi$, with a singular value decomposition $W\Sigma V^\dagger = \tilde{\Pi}U\Pi$, and using with Lemma 4.3, it suffices to construct an odd polynomial P associated with a sequence of angles $\Phi \in \mathbb{R}^m$, where $m = O(\delta^{-1}\log(1/\varepsilon))$. The goal is to ensure that the following conditions hold:

$$\|\tilde{\Pi}_{\geq t+\delta}U_\Phi\Pi_{\geq t+\delta} - I \otimes \sum_{i:\sigma_i \geq t+\delta} |\tilde{\psi}_i\rangle\langle\psi_i|\| \leq \varepsilon \text{ and } \|(\langle+| \otimes \tilde{\Pi}_{\leq t-\delta})U_\Phi(|+\rangle \otimes \Pi_{\leq t-\delta}) - 0\| \leq \varepsilon.$$

Next, we define singular value threshold projectors as $\Pi_{\geq\delta} \coloneqq \Pi V\Sigma_{\geq\delta}V^\dagger\Pi$, and similarly $\Pi_{\leq\delta} \coloneqq \Pi V\Sigma_{\leq\delta}V^\dagger\Pi$. In the same way, we define $\tilde{\Pi}_{\geq\delta} \coloneqq \Pi U\Sigma_{\geq\delta}U^\dagger\Pi$ and $\tilde{\Pi}_{\leq\delta} \coloneqq \Pi U\Sigma_{\leq\delta}U^\dagger\Pi$. Using these constructions, we apply an ϵ-approximate singular value projector by choosing $t = (a+b)/2$ and $\delta = (b-a)/2$. Then, we measure $|+\rangle\langle+| \otimes \Pi$:

- If the final state lies in $\mathrm{Img}(|+\rangle\langle+| \otimes \Pi)$, there exists a singular value σ_i above b;
- Otherwise, all singular values σ_i must be below a.

The remaining task is to implement singular value threshold projectors. It is noteworthy that U_Φ can be implemented using a single ancillary qubit, which requires m uses of U,$U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and single qubit gates.

Implementing singular value threshold projectors. We begin by constructing an odd polynomial $P \in \mathbb{R}[x]$ of degree $m = O(\log(1/\epsilon^2)/\delta)$, which approximates the function

$$\frac{1}{2}[(1-\epsilon)\cdot\mathrm{sgn}(x+t) + (1-\epsilon)\cdot\mathrm{sgn}(x-t) + 2\epsilon\cdot\mathrm{sgn}(x)]$$

with $\epsilon^2/4$ precision on the interval $[-1,1] \setminus (-t-\delta, -t+\delta) \cup (t-\delta, t+\delta)$.

This construction of P is based on the degree-d approximation polynomial $S(x)$, which is specified in the statement of the theorem. This polynomial $S(x)$ satisfies the condition:

$$\forall x \in [-1,1] \setminus (-\delta,\delta), |S(x) - \mathrm{sgn}(x)| \leq \epsilon, \text{ where } d = O(\delta^{-1}\log(1/\epsilon)).$$

In addition, it holds that $|P(x)| \leq 1$ for any $-1 \leq x \leq 1$, with the following properties:

$$(-1)^z P(x) \in [0,\epsilon] \text{ when } (-1)^z x \in [0, t-\delta],$$
$$(-1)^z P(x) \in [1-\epsilon, 1] \text{ when } (-1)^z \in [t+\delta, 1], \text{ for } z \in \{0,1\}.$$

Finally, it remains to construct a projected unitary encoding U such that

$$\|\tilde{\Pi} U_\Phi \Pi - P^{(\mathrm{SV})}(\tilde{\Pi} U \Pi)\| \leq \epsilon.$$

This task can be accomplished using Lemma 4.3, provided that the rotation angles Φ, corresponding to $P(x)$, can be computed in deterministically $\mathrm{poly}(d)$ time and $s_2(n)$ space. Furthermore, the gate complexity follows from Lemma 2.3.9 in [Gil19], which provides an explicit implementation and analysis of the gate complexity for the alternating phase modulation procedure described in Lemma 4.3. □

4.2 Scenarios in time-efficient and space-bounded

Equipped with Theorem 4.1, utilizing a polynomial approximation of the sign function in Corollary 6 of [LC17], as well as the angle finding algorithms in Theorems 2.2.1-2.2.3 of [Gil19], we conclude the time-efficient singular value discrimination.

Theorem 4.4 (Time-efficient singular value discrimination)**.** *Consider $0 \leq a, b \leq 1$ and an exact projected unitary encoding $A := \tilde{\Pi} U \Pi$. Let $|\psi\rangle$ be an unknown state, a right singular vector of A with a singular value either below a or above b such that $b - a \geq 1/\mathrm{poly}(n)$. Employing the quantum singular value transform (QSVT) with a degree-$O(\frac{\log 1/\epsilon}{b-a})$ odd polynomial, one can distinguish the two cases with error probability at most ϵ. Moreover, the time complexity of implementing this QSVT is $\mathrm{poly}\log(1/\epsilon) \cdot \mathrm{poly}(1/(b-a))$. We can also compute the description of this quantum circuit implementation in deterministic time $\mathrm{poly}\log(1/\epsilon) \cdot \mathrm{poly}(1/(b-a))$.*

Proof Sketch. It suffices to construct a degree-d approximation polynomial of the sign function and to find the rotation angles used in Lemma 4.3 in deterministic time $\mathrm{poly}\log(1/\epsilon) \cdot \mathrm{poly}(1/(b-a))$. Lastly, the construction of the approximation polynomial is provided in [GSLW19, Gil19], along with Proposition 4.5.

Proposition 4.5 (Polynomial approximation of the sign function, Corollary 6 in [LC17])**.** *For all $\delta > 0$, $\epsilon \in (0, 1/2)$, there exists an efficiently computable odd polynomials $P \in \mathbb{R}[x]$ of degree $n = O(\log(1/\epsilon)/\delta)$ s.t. $\forall x \in [-2,2], |P(x)| \leq 1$ and $\forall x \in [-2,2] \setminus (-\delta,\delta) : |P(x) - \mathrm{sgn}(x)| \leq \epsilon$.*

Regarding finding angles, this is achievable in time $\tilde{O}(d^3 \mathrm{poly}\log(1/\epsilon))$ using the recent developments [Haa19, CDG+20]. This results in a quantum circuit implementing the desired QSVT, and the description of this quantum circuit implementation can be computed in P. □

Now we move to *the space-bounded scenario*, stated in Theorem 4.6.

Theorem 4.6 (Space-bounded singular value discrimination)**.** *Consider $0 \leq a, b \leq 1$ and an exact projected unitary encoding $A := \tilde{\Pi} U \Pi$. Let $|\psi\rangle$ be an unknown state, a right singular vector of A with a singular value either below a or above b such that $b - a \geq \exp(-\mathrm{poly}(n))$. Employing the quantum singular value transform (QSVT) with a degree-$O(\frac{\log 1/\epsilon}{b-a})$ odd polynomial, one can distinguish the two cases with error probability at most ϵ. In addition, quantum circuits implementing this QSVT utilize $\mathrm{poly}(n)$ qubits, and we can compute the description of this quantum circuit implementation in* PSPACE.

The proof of Theorem 4.6 is closely derived from the *space-bounded* quantum singular value transformation techniques in [MY23, Lemma 3.13]. This is because their proof techniques can be straightforwardly adapted to the context of projected unitary encodings. In addition, we require the following lemma to proceed with the proof:

Lemma 4.7 (Exponentially good approximation to the sign function, adapted from Lemma 2.10 in [MY23])**.** *For any $\epsilon \geq 2^{-\mathrm{poly}(n)}$, there exists a degree $d = O(\epsilon^{-1}\log(1/\epsilon)) = O(2^{\mathrm{poly}(n)})$ and* PSPACE*-computable coefficients $c_0, \cdots, c_d$ such that $\forall x \in [-1,1]\backslash[-\epsilon,\epsilon]$, $|\mathrm{sgn}(x) - P_d^{\mathrm{sgn}}(x)| \leq \epsilon$ where $P_d^{\mathrm{sgn}} := \sum_{i=0}^{d} c_i T_i$ and $T_i(x)$ is the Chebyshev polynomial (of the first kind).*[20] *Furthermore, the coefficient vector $c = (c_1, \cdots, c_d)$ has norm bounded by $\|c\|_1 \leq O(\log d)$.*

We now outline the proof sketch of Theorem 4.6:

Proof Sketch of Theorem 4.6. Similar to the time-efficient scenario (e.g., Theorem 4.4), it suffices to implement the QSVT corresponding to the sign function, provided that we have an exponentially good (bounded) polynomial approximation of the sign function, as stated in Lemma 4.7.

However, instead of directly constructing the sequence of rotation angles in the time-efficient scenario, we employ the linear combination of unitaries (LCU) technique [BCC+14]. This technique can be readily adapted to space-bounded scenarios (as demonstrated in Lemma 3.6 in [MY23]) and is also applicable to projected unitary encodings. Next, we focus on implementing the quantum singular value transformation (QSVT) for the Chebyshev polynomials $T_i(x)$ with odd $i \in [1,d]$ utilized in Lemma 4.7. To achieve this, we examine the proof of Lemma 2.2.7 in [Gil19], which specifies the rotation angles corresponding to Chebyshev polynomials, and directly adapt it to the context of projected unitary encodings. Consequently, implementing an exponential-degree QSVT corresponding to the sign function requires polynomially many qubits, and the description of this circuit implementation can be computed in PSPACE. □

5 Doubly-preserving error reduction for state-synthesizing classes

In this section, we will present error reduction for stateQMA and its variants which preserves not only *the (quantum) witness state* but also *the resulting state* that well-approximates the target state.

5.1 Doubly-preserving error reduction for stateQMA and more

We start by stating error reduction for stateQMA, this leads to

$$\mathsf{stateQMA}_{\delta} = \cup_{c-s\geq 1/\mathrm{poly}(n)}\mathsf{stateQMA}_{\delta}[c,s].$$

Theorem 5.1 (Error reduction for stateQMA)**.** *For any efficiently computable $c(n), s(n), \delta(n)$ such that $0 \leq s(n) < c(n) \leq 1$, $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, we have that for any polynomial $l(n)$,*

$$\mathsf{stateQMA}_{\delta}[c,s] \subseteq \mathsf{stateQMA}_{\delta}[1-2^{-l}, 2^{-l}].$$

It is noteworthy that the proof of Theorem 5.1 can be understood as a sequential repetition of the original stateQMA verifier in a clever manner. In particular, the number of repetitions is $O(l/(\sqrt{c}-\sqrt{s}))$, implying that the circuit size of the resultant stateQMA verifier remains polynomial as long as promise gap $c-s$ is at least polynomially small.

Proof of Theorem 5.1. Our proof closely relates to Theorem 38 in [GSLW19] besides an additional analysis on resulting states.

[20] The Chebyshev polynomials (of the first kind) $T_k(x)$ are defined via the following recurrence relation: $T_0(x) = 1$, $T_1(x) = x$, and $T_{k+1}(x) = 2xT_k(x) - T_{k-1}(x)$. For $x \in [-1,1]$, an equivalent definition is $T_k(\cos\theta) = \cos(k\theta)$.

Amplifying the promise gap by QSVT. Note that the acceptance probability of a stateQMA verifier V_x taking $|w\rangle$ as a quantum witness is $\Pr[V_x \text{ accepts } |\psi\rangle] = \||1\rangle\langle 1|_{\text{out}} V_x |0^k\rangle|w\rangle\|_2^2 \geq c$ or $\leq s$. Then consider a projected unitary encoding $M_x := \Pi_{\text{out}} V_x \Pi_{\text{in}}$ such that $\|M_x\| \geq \sqrt{c}$ or $\sqrt{s}$ where $\Pi_{\text{in}} := (|0\rangle\langle 0|^{\otimes k} \otimes I_m)$ and $\Pi_{\text{out}} := |1\rangle\langle 1|_{\text{out}} \otimes I_{m+k-1}$. Since $\|M_x\| = \sigma_{\max}(M_x)$ where $\sigma_{\max}(M_x)$ is the largest singular value of M_x, it suffices to distinguish the cases where the largest singular value of M_x is either below $\sqrt{s}$ or above $\sqrt{c}$. By setting $a = \sqrt{s}, b = \sqrt{c}$, and $\varepsilon = 2^{-l(n)}$, this task is a straightforward corollary of the time-efficient singular value discrimination (Theorem 4.4).

QSVT preserves both the witness state and the resulting state. Utilizing notations of Lemma 4.2, we notice that the construction in the proof of Theorem 4.4 essentially maps $M_x = \sum_i \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$ to $f(M_x) = \sum_i f(\sigma_i)|\tilde{\psi}_i\rangle\langle\psi_i|$, for an odd polynomial f, such that $f(x) \in [1-\varepsilon, 1]$ if $x \geq b$ and $f(x) \in [0, \varepsilon]$ if $x \leq a$ for any $0 \leq x \leq 1$. Since both left and right singular vectors are invariant in $f(M_x)$, the resulting state and the witness state are clearly preserved after reducing errors. □

Using the space-bounded quantum singular value discrimination (Theorem 4.6), we will now improve Theorem 5.1 to $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$, which may have *exponential precision*. This is partially analogous to [FKL+16] since Theorem 4.6 works merely for *polynomial space*.[21]

Theorem 5.2 (Error reduction for $\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}$)**.** *Given any efficiently computable functions $c(n)$ and $s(n)$, also $\delta(n)$ such that $0 \leq s(n) < c(n) \leq 1$ and $c(n) - s(n) \geq \exp(-\mathrm{poly}(n))$, then for any polynomial $l(n)$,*

$$\mathsf{stateQMA_UPSPACE}^{\mathsf{off}}_{\delta}[c, s] \subseteq \mathsf{stateQMA_UPSPACE}^{\mathsf{off}}_{\delta}[1 - 2^{-l}, 2^{-l}].$$

In addition, by forcing the input state of the "verification circuit" to be an all-zero state in the proof of Theorem 5.1, namely replacing the projector $\Pi_{\text{in}} := (|0\rangle\langle 0|^{\otimes k} \otimes I_m)$ with $\Pi'_{\text{in}} := |0\rangle\langle 0|^{\otimes k+m}$, we will straightforwardly result in error reduction for $\mathsf{stateBQP}$.

Theorem 5.3 (Error reduction for $\mathsf{stateBQP}$)**.** *For any polynomials $p(n)$ such that $1/p(n) \leq \gamma(n) < 1$, we have that for any polynomial $l(n)$,*

$$\mathsf{stateBQP}_{\delta}[\gamma] \subseteq \mathsf{stateBQP}_{\delta}[1 - 2^{-l}].$$

Theorem 5.3 implies that $\mathsf{stateBQP}_{\delta} = \cup_{1 \leq \gamma^{-1} \leq \mathrm{poly}(n)} \mathsf{stateBQP}_{\delta}[\gamma]$. Also, combining with Proposition 3.5, $\mathsf{stateBQP}$ achieves perfect completeness with a slightly modified distance parameter δ'. Particularly, $\mathsf{stateBQP}_{\delta}[\gamma] \subseteq \mathsf{stateBQP}_{\delta'}[1]$ where $\delta'(n) := \delta(n) + \exp(-\mathrm{poly}(n))$.

Likewise, together with the projector $\Pi'_{\text{in}} := |0\rangle\langle 0|^{\otimes k+m}$ and the space-bounded quantum singular value discrimination (Theorem 4.6), we will deduce error reduction for $\mathsf{state_UPSPACE}$.

Theorem 5.4 (Error reduction for $\mathsf{state_UPSPACE}$)**.** *For any efficiently computable functions $\gamma(n)$ and $\delta(n)$ such that $\exp(-\mathrm{poly}(n)) \leq \gamma(n) \leq 1$, we have that for any polynomial $l(n)$,*

$$\mathsf{state_UPSPACE}_{\delta}[\gamma] \subseteq \mathsf{state_UPSPACE}_{\delta}[1 - 2^{-l}].$$

A direct consequence of Theorem 5.4 is that $\mathsf{state_UPSPACE}_{\delta} = \cup_{\gamma \geq 2^{-\mathrm{poly}(n)}} \mathsf{state_UPSPACE}_{\delta}[\gamma]$. Similarly, by utilizing Proposition 3.5, we can also conclude that

$$\mathsf{state_UPSPACE}_{\delta}[\gamma] \subseteq \mathsf{state_UPSPACE}_{\delta'}[1] \text{ where } \delta'(n) = \delta(n) + \exp(-\mathrm{poly}(n)).$$

[21] To achieve a state-synthesizing analog of error reduction for unitary quantum logspace [FKL+16], a *space-efficient* version of Theorem 4.6 is necessary. Such a space-efficient variant of QSVT [LLW23] became available only after our work. By replacing Theorem 4.6 with this technique in the proof of Theorem 5.2 and Theorem 5.4, we can establish error reduction for state-synthesizing unitary quantum *logspace* classes $\mathsf{stateBQ_UL}_{\delta}$ and $\mathsf{stateQMA_UL}^{\mathsf{off}}_{\delta}$, as well as the equivalence $\mathsf{stateQMA_UL}^{\mathsf{off}}_{\delta} = \mathsf{stateBQ_UL}_{\delta}$, which is fully analogous to [FKL+16].

5.2 Application 1: stateQMA with a short message is as weak as stateBQP

Recall that $\mathsf{stateQMA}_{\log}$ is a variant of stateQMA where the witness state is logarithmic-size. Analogous to Theorem 3.10 in [MW05], a short message is also useless for stateQMA.

Theorem 5.5 (A short message is useless for stateQMA)**.** *For any $0 \leq s(n) < c(n) \leq 1$ and $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, there exists a polynomial $q(n)$ such that*

$$\mathsf{stateQMA}_{\delta}[\log, c, s] \subseteq \mathsf{stateBQP}_{\delta}[1/q].$$

Proof. Consider a state family $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ that is in $\mathsf{stateQMA}_{\delta}[\log, c, s]$, we then notice that this state family is also in $\mathsf{stateQMA}_{\delta}[\log, 1-2^{-p}, 2^{-p}]$ where $p(n)$ is a polynomial of $n := |x|$ after performing error reduction (Theorem 5.1). Now let $\{V_x\}_{x\in\mathcal{L}}$ be the family of quantum verifiers with negligible errors.

Removing the witness by a "random-guess" state. Now consider a stateBQP algorithm that applies V_x with the witness being a completely mixed state $\tilde{I}_m := 2^{-m} I_m$ on $m(n) = O(\log n)$ qubits. It accepts iff V_x accepts. For the analysis, we define $M_x := (|1\rangle\langle 1|_{\text{out}} \otimes |0\rangle\langle 0|^{\otimes m+k-1}) V_x (I_m \otimes |0\rangle\langle 0|^{\otimes k})$. Then $\Pr[V_x \text{ accepts}|w\rangle] = \|M_x|w\rangle\|_2^2$, which implies that the acceptance probability of the stateBQP algorithm is

$$\Pr[V_x \text{ accepts } \tilde{I}_m] = \mathrm{Tr}(M_x^\dagger M_x 2^{-m} I_m) = 2^{-m}\mathrm{Tr}(M_x^\dagger M_x) = 2^{-m}\lambda_{\max}(M_x^\dagger M_x), \tag{1}$$

where $\lambda_{\max}(M_x^\dagger M_x)$ is the largest eigenvalue of $M_x^\dagger M_x$. For the completeness, there exists $|w\rangle$ such that $\lambda_{\max}(M_x^\dagger M_x) \geq \Pr[V_x \text{ accepts } |w\rangle] \geq 1 - 2^{-p(n)}$. Plugging it into Equation (1), we have $\Pr\left[V_x \text{ accepts } \tilde{I}_m\right] \geq 2^{-m(n)}(1-2^{-p(n)}) \geq 1/q(n)$, where $q(n) := 2^{O(m(n))}$ is a polynomial of $n := |x|$. For the soundness, we obtain $\Pr\left[V_x \text{ accepts } \tilde{I}_m\right] \geq 2^{-p(n)}$, it guarantees that $\mathrm{td}(\rho_{\tilde{I}_m}, \psi_x) \leq \delta$ owing to Definition 3.6. □

We remark that Theorem 5.5 straightforwardly adapts to any stateQMA verifier with witness states of polynomial-size, which is a state-synthesizing counterpart of $\mathsf{QMA} \subseteq \mathsf{PP}$ [Vya03, MW05].

Proposition 5.6 ("stateQMA ⊆ statePP")**.** $\mathsf{stateQMA}_{\delta} \subseteq \mathsf{statePreciseBQP}_{\delta}$.

Proof. Consider a family of quantum states $\{|\psi_x\rangle\}_{n\in\mathbb{N}} \in \mathsf{stateQMA}_m[c, s, \delta]$ where $m(n)$ is the size of the witness state. Analogous to Theorem 5.5, we have derived that

$$\mathsf{stateQMA}_{\delta}[m, c, s] \subseteq \mathsf{stateQMA}_{\delta}[m, 1-2^{-m'}, 2^{-m'}] \subseteq \mathsf{stateBQP}_{\delta}[2^{-m}],$$

where $m'(n) = m(n) \cdot n^2$. □

5.3 Application 2: statePreciseQMA is in statePSPACE

Finally, we provide a state-synthesizing analogue of $\mathsf{PreciseQMA} \subseteq \mathsf{BQPSPACE}$ [FL16, FL18].

Theorem 5.7. $\mathsf{statePreciseQMA}_{\delta} \subseteq \mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}_{\delta}$.

Proof. Consider a family of quantum states $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ that is in $\mathsf{statePreciseQMA}_{\delta}[m, c, s]$ where $m(n)$ is the size of witness state. We begin by observing that

$$\mathsf{statePreciseQMA}_{\delta}[m, c, s] \subseteq \mathsf{stateQMA}_{\mathsf{U}}\mathsf{PSPACE}^{\mathsf{off}}_{\delta}[m, c, s].$$

Then we replace the witness with a "random-guess" state analogous to the proof of Theorem 5.5. Utilizing error reduction for $\mathsf{stateQMA}_{\mathsf{U}}\mathsf{PSPACE}^{\mathsf{off}}$ (Theorem 5.2), we have derived that

$$\mathsf{statePreciseQMA}_{\delta}[m, c, s] \subseteq \mathsf{stateQMA}_{\mathsf{U}}\mathsf{PSPACE}^{\mathsf{off}}_{\delta}[m, 1-2^{-m'}, 2^{-m'}] \subseteq \mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}_{\delta}[2^{-m}],$$

where $m'(n) = m(n) \cdot n^2$. Employing error reduction for $\mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}$ (Theorem 5.2), we conclude that

$$\mathsf{statePreciseQMA}_{\delta}[m, c, s] \subseteq \mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}_{\delta}[2^{-m}] \subseteq \mathsf{state}_{\mathsf{U}}\mathsf{PSPACE}_{\delta}[1 - 2^{-l}],$$

where $l(n)$ is a polynomial of $n \coloneqq |x|$. This completes the proof. □

6 UQMA witness family is in stateQMA

In this section, we will provide a natural example of stateQMA state families. Specifically, the family of *yes*-instance witness states of verifiers corresponding to $\mathcal{L}_{\text{yes}}$, where $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \mathsf{UQMA}$, is in stateQMA:

Theorem 6.1 ($\mathsf{UQMA}_{1-\nu}$ witness family is in stateQMA)**.** *For any promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ that is in $\mathsf{UQMA}_{1-\nu}$, the family of unique witness states $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to yes instances is in $\mathsf{stateQMA}_{\delta}[c', s']$, where $c' = (1+\cos\nu)/2 - \epsilon$, $s' = (1+\cos(\lambda_1 t))(2+\cos(\nu t) - \cos(\lambda_1 t))/4 + \epsilon$, and $\delta = O(\max\{(1-\cos\nu)/2, \delta_1, q(\nu\delta_1 t/T^3)\})$ for some polynomial q. Here, let $H^{(x)}$ be the Hamiltonian corresponding to a UQMA verifier V_x with the parameter δ_1 specified in Lemma 6.4, λ_1 is the second smallest eigenvalue of $H^{(x)}$ respectively, T is the size of verification circuit V_x, as well as t satisfies that $\lambda_{\max}(H^{(x)})t \leq \pi$, and ϵ is the implementation error of $\exp(-iH^{(x)}t)$.*

By employing Theorem 6.1, we can determine that the promise gap of the new stateQMA verifier is given by

$$c' - s' = (1 - \cos(\lambda_1 t))(\cos(\nu t) - \cos(\lambda_1 t)) - 2\epsilon \geq q'(\nu\delta_1 t/T^3) - 2\epsilon.$$

Here, q' represents a polynomial due to the bound $\Delta(H^{(x)}) = \lambda_1 - \nu \geq \Omega(\nu\delta_1/T^3)$ stated in Lemma 6.4. According to Lemma 2.8, we know that the implementation error ϵ is exponentially small. Consequently, by utilizing UQMA error reduction (Theorem 2.4), we establish $\mathsf{UQMA} \subseteq \mathsf{UQMA}_{1/\text{poly}}$ and thus Theorem 6.1 implies Corollary 6.2 by choosing $\delta_1 = 1/\text{poly}(n)$:

Corollary 6.2 (UQMA witness family is in stateQMA)**.** *For any promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ in UQMA, the family of unique witness states $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to yes instances is in $\mathsf{stateQMA}_{\delta}$, where $\delta(n) = 1/\text{poly}(n)$.*

Similarly, Theorem 6.1 implies Corollary 6.3 by setting $\delta_1 = \exp(-\text{poly}(n))$:

Corollary 6.3 ($\mathsf{PreciseUQMA}_{1-\text{negl}}$ witness family is in statePreciseQMA)**.** *For any promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ in $\mathsf{PreciseUQMA}_{1-\text{negl}}$, the family of unique witness states $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to yes instances is in $\mathsf{statePreciseQMA}_{\delta}$, where $\delta(n) = \exp(-\text{poly}(n))$.*

6.1 Proof of Theorem 6.1

To establish Theorem 6.1, we begin with a weighted circuit-to-Hamiltonian construction [BC18, BCNY19], as stated in Lemma 6.4, where the resulting ground state (also known as the history state) provides a good approximation of the output state produced by the UQMA verifier. The proof of Lemma 6.4 can be found in Section 6.2.

Lemma 6.4 (Weighted circuit-to-Hamiltonian construction)**.** *For any $x \in \mathcal{L}_{\text{yes}}$, where $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ is a promise problem that is in UQMA, there exists an $O(\log n)$-local Hamiltonian $H^{(x)}$ with ground energy ν from the UQMA verifier family $\{V_x\}_{x\in\mathcal{L}}$ with maximum acceptance*

probability $1-\nu$*, along with the corresponding unique witness state family* $\{|w_x\rangle\}_{x\in\mathcal{L}}$*. This unique ground state of* $H^{(x)}$ *is given by*

$$|\Omega_x\rangle = \sum_{t=0}^{T-1} \frac{\sqrt{\delta_1}}{\sqrt{T}}|t\rangle \otimes U_t \cdots U_1|w_x\rangle + \sqrt{1-\delta_1}|T\rangle \otimes U_T \cdots U_1|w_x\rangle.$$

Here T *denotes the number of quantum gates utilized by* V_x*. Furthermore, the spectral gap of* $H^{(x)}$ *satisfies* $\Delta(H^{(x)}) \geq \Omega(\nu\delta_1/T^3)$*.*

With Lemma 6.4 established, we proceed to prove the main theorem in this section.

Proof of Theorem 6.1. We begin by constructing a stateQMA verifier V'_x. Let $H^{(x)}$ be the $O(\log n)$-local Hamiltonian, which is obtained by applying Lemma 6.4 to a UQMA verifier V_x with the unique witness $|w_x\rangle$. Our construction is primarily relies on the one-bit precision phase estimation [Kit95], often referred to as Hadamard test [AJL09], as illustrated in Algorithm 2.

Algorithm 2: stateQMA verification circuit V'_x

1. Apply one-bit precision phase estimation on registers O, W, and C. Here, register O is the control qubit, while registers W and C are the target qubits. Specifically, (clock) register C consists of $\lceil \log T \rceil$ qubits, and the number of qubits in register W matches the number of qubits that V_x acts on;
2. Apply the circuit $V_x^\dagger$ to register W;
3. Measure the designated output qubit, and we say that V'_x accepts $|\psi\rangle$ if the final measurement outcome is 0;
4. If V'_x accepts, trace out all qubits in C. The resulting state, denoted as ρ_ψ, is located in register W

Here, we choose the parameter $t = \frac{\pi}{p(n)\max_{s,t}|H^{(x)}(s,t)|} \leq \frac{\pi}{\|H^{(x)}\|_\infty}$ such that all eigenvalues of $H^{(x)}t$ is in $[0,\pi]$. The corresponding circuit implementation has demonstrated in Figure 1.

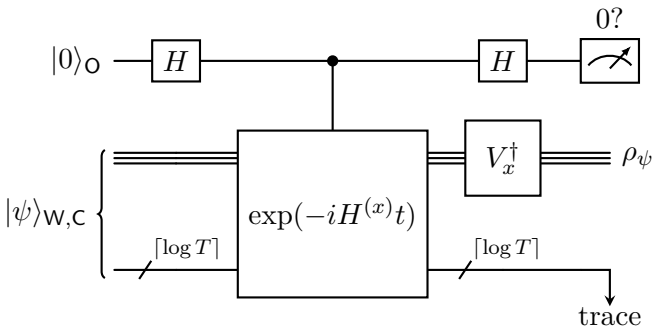

Figure 1: stateQMA verification circuit V'_x

Through direct calculation, we can express the acceptance probability as follows:

$$p'_{\text{acc}} \coloneqq \Pr\left[V'_x \text{ accepts } |\psi\rangle\right] = \frac{1}{4}\|V_x^\dagger(I+e^{-iH^{(x)}t})|\psi\rangle\|_2^2 = \frac{1}{2} + \frac{1}{2}\operatorname{Re}(\langle\psi|e^{-iH^{(x)}t}|\psi\rangle).$$

We denote the resulting state by ρ_ψ when $\exp(-iH^{(x)}t)$ is perfectly implemented, whereas the resulting state is ρ'_ψ if the implementation error ϵ of $\exp(-iH^{(x)}t)$ is considered (e.g., Lemma 2.8). Simultaneously, ρ_ψ is given by $\rho_\psi \coloneqq \frac{1}{4p'_{\text{acc}}} V_x^\dagger \operatorname{Tr}_{\mathsf{C}}\Big((I+e^{-iH^{(x)}t})|\psi\rangle\langle\psi|(I+e^{iH^{(x)}t})\Big) V_x$.

Completeness. We first prove that this stateQMA verifier V'_x meets the completeness condition.

Consider the unique ground state $|\Omega_x\rangle$ of the Hamiltonian $H^{(x)}$ specified in Lemma 6.4 as a witness state of V'_x, and let $\lambda_0 := \lambda_{\min}(H^{(x)}) = 1 - p_{\text{acc}} = \nu$ be the ground energy of $H^{(x)}$ corresponding to the maximum acceptance probability p_{acc} of V_x. Consequently, we obtain the following by combining with the implementation error ϵ of $\exp(-H^{(x)}t)$ specified in Lemma 2.8:

$$\Pr\left[V'_x \text{ accepts } |\Omega_x\rangle\right] = \frac{1+\cos(\nu t)}{2} \text{ and } c'(n) = \frac{1+\cos(\nu t)}{2} - \epsilon.$$

Soundness. For the soundness condition, we consider a quantum state $|\psi\rangle = \alpha_0|\Omega_x\rangle + \sum_{1\leq j<N}\alpha_j|\Phi_x^{(j)}\rangle$, where the coefficients $\{\alpha_j\}_{0\leq j<N}$ satisfies that $\sum_{0\leq j<N}|\alpha_j|^2 = 1$ and $|\Phi_x^{(j)}\rangle$ is the j-th excited state of $H^{(x)}$, as a witness state of the stateQMA verifier V'_x, we thus obtain the corresponding acceptance probability p'_{acc} and the resulting state ρ_ψ, respectively:

$$p'_{\text{acc}} = \Pr\left[V'_x \text{ accepts } |\psi\rangle\right] = |\alpha_0|^2\cdot\frac{1+\cos(\lambda_0)}{2} + \sum_{1\leq j<N}|\alpha_j|^2\cdot\frac{1+\cos(\lambda_j t)}{2} \geq s(n), \tag{2}$$

$$\begin{aligned}\rho_\psi = \frac{1}{4p'_{\text{acc}}}V_x^\dagger \text{Tr}_{\mathsf{C}}\Bigg(&\Big(\alpha_0(1+e^{-i\lambda_0 t})|\Omega_x\rangle + \sum_{1\leq j<N}\alpha_j(1+e^{-i\lambda_j t})|\Phi_x^{(j)}\rangle\Big)\\ &\Big(\alpha_0^*(1+e^{i\lambda_0 t})\langle\Omega_x| + \sum_{1\leq j<N}\alpha_j^*(1+e^{i\lambda_j t})\langle\Phi_x^{(j)}|\Big)\Bigg)V_x.\end{aligned} \tag{3}$$

Here, λ_j $(1\leq j<N)$ is the j-th excited[22] energy corresponding to j-th excited state $|\Phi_x^{(j)}\rangle$ such that $\lambda_1 \leq \cdots \leq \lambda_{N-1} \leq \pi$. It is noteworthy that the fidelity (overlap) between the resulting state ρ_ψ and the unique witness state $|w_x\rangle\langle w_x|$ is mostly decided by $|\alpha_0|^2$. To upper-bound $\text{td}(\rho_\psi, |w_x\rangle\langle w_x|)$, it suffices to minimize $|\alpha_0|^2$ amongst all quantum states $|\psi\rangle$ such that V'_x accepts $|\psi\rangle$ with probability at least $s(n)$. Accordingly, we need to maximize $|\alpha_1|^2$ because $\exp(-i\lambda_1 t)$ contributes the largest possible weight amongst all eigenvalues of $H^{(x)}$ except for λ_0. Meanwhile, we can without loss of generality assume that $\alpha_2 = \cdots = \alpha_{N-1} = 0$, then we obtain the following derived from Equation (2):

$$p'_{\text{acc}} = |\alpha_0|^2\cdot\frac{1+\cos(\lambda_0 t)}{2} + (1-|\alpha_0|^2)\cdot\frac{1+\cos(\lambda_1 t)}{2} \geq s'(n). \tag{4}$$

Furthermore, we can assume that $(1+\cos(\lambda_1 t)/2) \leq s'(n) \leq (1+\cos(\lambda_0 t))/2$, otherwise $|\psi\rangle$ will be orthogonal to $|\Omega_x\rangle$ which means that $|\alpha_0|^2 = 0$. By adapting ρ_ψ in Equation (3) according to the choice of $\{\alpha_i\}_{2\leq i<N}$ with $\lambda_0 = \nu$, we have derive that:

$$\begin{aligned}\text{F}^2(\rho_\psi, |w_x\rangle\langle w_x|) &= \langle w_x|\rho_\psi|w_x\rangle\\ &\geq \frac{1}{4p'_{\text{acc}}}\langle w_x|V_x^\dagger\text{Tr}_{\mathsf{C}}\big(|\alpha_0|^2(1+e^{-i\nu t})|\Omega_x\rangle\langle\Omega_x|(1+e^{i\nu t})\big)V_x|w_x\rangle\\ &\geq \frac{|\alpha_0|^2}{p'_{\text{acc}}}\cdot\frac{(1+\cos(\nu t))^2}{4}\cdot(1-\delta_1)\\ &:= \frac{|\alpha_0|^2}{p'_{\text{acc}}}\cdot(1-\delta_0)^2\cdot(1-\delta_1)\end{aligned} \tag{5}$$

Here, the third line is because of $\langle w_x|V_x^\dagger\text{Tr}_{\mathsf{C}}(|\Omega_x\rangle\langle\Omega_x|)V_x|w_x\rangle \geq 1-\delta_1$, and the last line

[22] It is noteworthy that the j-th excited energy of a Hamiltonian corresponds to the $(j+1)$-th smallest eigenvalue of H, where H is viewed as an Hermitian matrix. Similarly, the j-th excited state of a Hamiltonian H corresponds to the eigenvector associated with the $(j+1)$-th smallest eigenvalue of H.

defines $\delta_0 := (1-\cos(\nu t))/2$. By employing Lemma 2.1 on Equation (5), we obtain:

$$\mathrm{td}(\rho_\psi, |w_x\rangle\langle w_x|) \leq 1 - \mathrm{F}(\rho_\psi, |w_x\rangle\langle w_x|) = 1 - (1-\delta_0)\cdot\sqrt{1-\delta_1}\cdot\frac{|\alpha_0|}{p'_{\mathrm{acc}}}. \tag{6}$$

We then establish a lower bound of $|\alpha_0|^2/p'_{\mathrm{acc}}$ and the corresponding soundness parameter s' in Proposition 6.5, and the proof will be deferred.

Proposition 6.5. *$|\alpha_0|^2/p'_{\mathrm{acc}} \geq 1 - q(\nu\delta_1 t/T^3)$ for some polynomial q. Moreover, the choice of parameters implies that $s'(n) = \frac{1}{4}\big((1+\cos(\lambda_1 t)\big)\big(2+\cos(\nu t)-\cos(\lambda_1 t)\big) + \epsilon$.*

Plugging Proposition 6.5 into Equation (6) with $\delta' := \max\{\delta_0, \delta_1, q(\nu\delta_1 t/T^3)\}$, we obtain:

$$\mathrm{td}(\rho_\psi, |w_x\rangle\langle w_x|) \leq 1 - (1-\delta_0)\sqrt{(1-\delta_1)(1-q(\nu\delta_1 t/T^3))} \leq 1 - (1-\delta')^2 = 2\delta' - (\delta')^2 \leq 2\delta'.$$

By utilizing Lemma 2.8, we note that the implementation error ϵ of $\exp(-H^{(x)}t)$ is exponentially small, and thus finish the proof by noticing $\mathrm{td}(\rho'_\psi, |w_x\rangle\langle w_x|) \leq O(\delta')$. □

At the end of this subsection, we provide the proof of Proposition 6.5.

Proof of Proposition 6.5. We establish a lower bound for $|\alpha_0|^2/p'_{\mathrm{acc}}$ by a direct calculation:

$$\begin{aligned}
\frac{|\alpha_0^2|}{p'_{\mathrm{acc}}} &= \frac{|\alpha_0|^2}{|\alpha_0|^2\cdot\frac{1+\cos(\lambda_0 t)}{2} + (1-|\alpha_0|^2)\cdot\frac{1+\cos(\lambda_1 t)}{2}} := f(|\alpha_0|^2) \\
&\geq \frac{(2s(n)-1)-\cos(\lambda_1 t)}{s(n)\cdot(\cos(\lambda_0 t)-\cos(\lambda_1 t))} \\
&= \frac{2\xi}{1+\xi\cos(\lambda_0 t)+(1-\xi)\cos(\lambda_1 t)} := g(\xi) \\
&\geq \frac{2}{1+\cos(\lambda_1 t)}\cdot\xi - \frac{2(\cos(\lambda_0 t)-\cos(\lambda_1 t))}{(1+\cos(\lambda_1 t)^2)}\cdot\xi^2.
\end{aligned}$$

Here, the second line is due to the fact that the function $f(|\alpha_0|^2)$ is monotonically increasing on the interval $[0,1]$, and the minimum achieves when $|\alpha_0|^2 = \frac{(2s(n)-1)-\cos(\lambda_1 t)}{\cos(\lambda_0 t)-\cos(\lambda_1 t)}$ following from Equation (4). The third line owing to choose $s := \xi\cdot\frac{1+\cos(\lambda_0)}{2} + (1-\xi)\cdot\frac{1+\cos(\lambda_1 t)}{2}$ for $0 \leq \xi \leq 1$, and the last line is because of truncated Taylor series of the function $g(\xi)$.

By choosing $\xi = (1+\cos(\lambda_1 t))/2$ and utilizing the bound $\Delta(H^{(x)}) = \lambda_1 - \lambda_0 = \lambda_1 - \nu \geq \Omega(\nu\delta_1/T^3)$ in Lemma 6.4, we have the following for some polynomial q:

$$\frac{2}{1+\cos(\lambda_1 t)}\cdot\xi - \frac{2(\cos(\nu t)-\cos(\lambda_1 t))}{(1+\cos(\lambda_1 t)^2)}\cdot\xi^2 = 1 - \frac{\cos(\nu t)-\cos(\lambda_1 t)}{2} \geq 1 - q\Big(\frac{\nu\delta_1 t}{T^3}\Big).$$

Accordingly, we obtain the soundness parameter s by combining the implementation error ϵ of $\exp(-iH^{(x)}t)$ specified in Lemma 2.8: $s'(n) = \big((1+\cos(\lambda_1 t)\big)\big(2+\cos(\nu t)-\cos(\lambda_1 t)\big)/4+\epsilon$. □

6.2 Weighted circuit-to-Hamiltonian construction, revisited

Finally, we demonstrate the weighted circuit-to-Hamiltonian construction with a spectral gap lower bound, along the line of [BC18, BCNY19].

Proof of Lemma 6.4. We consider an UQMA verifier V_x with maximum acceptance probability $1-\nu$, where the verification circuit consists of a sequence of local quantum gates $U_1, \cdots, U_T$. To begin, we specify a weighted circuit-to-Hamiltonian construction $H^{(x)} := H^{(x)}_{\mathrm{prop}} + H_{\mathrm{in}} +$

H_{out} proposed in [BC18].[23] Here, $H_{\mathrm{in}} := |\bar{0}\rangle\langle\bar{0}| \otimes \Pi_{\mathrm{in}}$ and $H_{\mathrm{out}} := |T\rangle\langle T| \otimes \Pi_{\mathrm{out}}$ correspond to input and output constraints, respectively. It is straightforward to see that the ground energy of $H^{(x)}$ is $1-(1-\nu)=\nu$. This construction closely resembles the standard circuit-to-Hamiltonian construction [KSV02], except for the weighted ground state resulting from the distinct propagation term $H^{(x)}_{\mathrm{prop}}$.

Constructing the propagation term. Next, we proceed to construct the propagation term $H^{(x)}\mathrm{prop}$ for the given weights, specifically a probability distribution π. We define the ground state of $H^{(x)}$ as $|\Omega_x\rangle := \sum_{t=0}^{T}\sqrt{\pi_t}|t\rangle \otimes (U_t \cdots U_1)|w_x\rangle$, where $|w_x\rangle$ represents the unique witness state of V_x, and $\pi = (\delta_1/T, \cdots, \delta_1/T, 1-\delta_1)$ is a probability distribution on $[T] = \{0, 1, \cdots, T\}$.

Our construction of the propagation term is based on the transition matrix P of random walks on a $(T+1)$-node path with the stationary distribution π. Here, the specific form of the matrix P is provided in Lemma 2.5 for the given π. By employing Lemma 2.5, we obtain an $O(\log n)$-local stoquastic frustration-free Hamiltonian $H^{(T)}_{\mathrm{path}}$ derived from P. Let us consider a unitary operator $W_x := \sum_{t=0}^{T}|t\rangle\langle t| \otimes U_t \cdots U_1$ associated with the given V_x. By combining $H^{(T)}_{\mathrm{path}}$ with Lemma 2 in [BC18], we arrive at the expression for the propagation term $H^{(x)}_{\mathrm{prop}}$:

$$\begin{aligned} H^{(x)}_{\mathrm{prop}} &= W_x(H^{(T)}_{\mathrm{path}} \otimes I)W_x^{\dagger} \\ &= \sum_{t=0}^{T}(1-P_{t,t})|t\rangle\langle t| \otimes I - \sum_{t=0}^{T}\left(\tfrac{\sqrt{\pi_t}}{\sqrt{\pi_{t-1}}}P_{t,t-1}|t\rangle\langle t-1| \otimes U_t + \tfrac{\sqrt{\pi_{t-1}}}{\sqrt{\pi_t}}P_{t-1,t}|t-1\rangle\langle t| \otimes U_t^{\dagger}\right). \end{aligned}$$

Lower-bounding the spectral gap. It is left to establish a lower bound for the spectral gap $\Delta(H^{(x)})$. By applying Cheeger's inequality (Lemma 2.6), we obtain $\Delta(H^{(x)}_{\mathrm{prop}}) = \Delta_P \geq \frac{1}{2}\Phi_G^2$, where Φ_G is the conductance of the underlying $(T+1)$-node path graph G. Notably, the weights in G are primarily concentrated on the $(T+1)$-th node since δ_1 is tiny. The minimum conductance $\Phi_G = \min_{S\subseteq[T]}\Phi_G(S)$ is thus achieved at the subset $S = [T-1] := \{0, 1, \cdots, T-1\}$. Consequently, we can deduce:

$$\Phi_G = \Phi_G([T-1]) = \frac{1}{\pi_{[T-1]}}\pi_{T-1}P_{T-1,T} = \frac{1}{\delta_1}\cdot\pi_{T-1}\cdot\frac{1}{4}\min\left\{1, \frac{\pi_T}{\pi_{T-1}}\right\} = \frac{1}{4T}. \tag{7}$$

From Equation (7), we infer that $\Delta(H^{(x)}\mathrm{prop}) \geq \Omega(T^{-2})$.

Now, let $C(\tau, T)$ be the set of quantum circuits of size T that achieve the maximum acceptance probability τ amongst states satisfying the input and output constraints Π_{in} and Π_{out}, respectively. In particular, $C(\tau,T) := \{U_1, \cdots, U_T : \max_{|\xi\rangle\in\ker(\Pi_{\mathrm{in}}),|\eta\rangle\in\ker(\Pi_{\mathrm{out}})}|\langle\xi|U_1\cdots U_T|\eta\rangle|^2 = \tau\}$. By employing Lemma 3 in [BC18], we obtain the following when $\tau = 1-\nu$:

$$\begin{aligned} \Delta(H^{(x)}) &\geq \min_{U:=U_1,\cdots,U_T\in C(1-\nu,T)}\left(\lambda_{\min}(H^{(U)}) - \lambda_{\min}(H^{(U)}_{\mathrm{prop}})\right) \\ &\geq \Delta(H^{(T)}_{\mathrm{path}})\cdot\frac{1-\sqrt{1-\nu}}{4}\cdot\min\{\pi_0, \pi_T\} \\ &= \Omega\left(\frac{\nu\delta_1}{T^3}\right). \end{aligned} \tag{8}$$

Here, the last line is because $\sqrt{1-x} \leq 1 - x/2$ when $0 \leq x \leq 1$. As Equation (8) establishes the desired spectral gap lower bound, this thus finishes the proof. □

[23] We note that by utilizing a spacetime circuit-to-Hamiltonian construction outlined in [BCNY19], we can achieve a constantly improved distance parameter δ.

7 stateQCMA achieves perfect completeness

In this section, we will present a state-synthesizing analogue of the $\mathsf{QCMA} = \mathsf{QCMA}_1$ theorem [JKNN12].

Theorem 7.1 (stateQCMA is closed under perfect completeness)**.** *For any efficiently computable functions $c(n)$, $s(n)$ and $\delta(n)$ such that $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\mathsf{stateQCMA}_{\delta}[c, s] \subseteq \mathsf{stateQCMA}_{\delta'}[1, s'],$$

where $s' = \frac{1}{2}\left(\frac{s}{c}\right)^3 - 2\left(\frac{s}{c}\right)^2 + \frac{5}{2}\left(\frac{s}{c}\right)$ and $\delta'(n) = \delta(n) + \exp(-\mathrm{poly}(n))$.

Furthermore, for any stateQCMA *verifier utilizing the "Pythagorean" gateset, we have $\delta' = \delta$.*

It is noteworthy that while error reduction for stateQCMA (a corollary of Theorem 5.1) preserves the distance between the resulting state and the target state, this distance-preserving property in Theorem 7.1 is *gateset-dependent* since changing gatesets will worsen the distance parameter (Lemma 2.2). This is because the key insight from [JKNN12], that the maximum acceptance probability of a QCMA (or stateQCMA) verifier can be expressed with polynomially many bits, only applies to certain gatesets, elaborating in Remark 7.2.

Remark 7.2 (On choices of the gateset). For state-synthesizing complexity classes, we require to deal with not only the maximum acceptance probability but also the resulting states after the computation. To well-approximate any quantum states with a designated gateset $\mathcal{S}$, this gateset S must generate a dense subgroup of $\mathrm{SU}(2^n)$ for large enough n. However, this does not hold for the gateset used in [JKNN12].[24] We then use the "Pythagorean" gateset in [JN11] where real and imaginary parts of all matrix entries are rational numbers.

Analogous to [JKNN12], to achieve perfect completeness, we also utilize the quantum rewinding lemma [Wat09] with a single iteration. As stated in Lemma 7.4, it suffices to construct a new stateQCMA verifier that the acceptance probability is exactly 1/2 for the completness condition.

Our construction of the new stateQCMA verifier with perfect completeness tightly follows the construction for QCMA (i.e., Figure 1 in [JKNN12]). The only difference is that the unitary transformation Q since the original construction in [JKNN12] cannot preserve the resulting states, which also leads to a slightly different analysis for the soundness condition.

We begin with two lemmas that are crucial for our analysis.

Lemma 7.3 (Acceptance probabilities from the "Pythagorean" gateset are rational, adapted from [JN11])**.** *For all unitary transform U on an n-qubit system that consists of $l(n)$ gates from the "Pythagorean" gateset where l is a polynomial, the probability p_{acc} that the first qubit of $U|0^n\rangle$ is found in the state $|1\rangle$ (i.e., the measurement on the computational basis) is expressed as $p_{acc} = \frac{k}{5^{l(n)}}$ where k is an integer from the range $[0, 5^{l(n)}]$.*

Lemma 7.4 (Success probability of the quantum rewinding, adapted from Lemma 8 in [Wat09])**.** *Let Q be a quantum circuit such that $Q|\psi\rangle = \sqrt{p(\psi)}|0\rangle|\psi_0\rangle + \sqrt{1-p(\psi)}|1\rangle|\psi_1\rangle$, and $p := p(\psi) \in (0,1)$ is constant over all choices of the input $|\psi\rangle$. Then the probability of producing $|\psi_0\rangle$ within t iterations is $1 - (1-p)(1-2p)^{2t}$.*

Particularly, the probability of producing $|\psi_0\rangle$ by the single-iteration quantum rewinding of Q is $p + 4p(1-p)^2$, as well as this achieves the perfect success probability when $p = 1/2$.

Now we proceed with the actual proof.

[24] To be specific, the proof of Theorem 3.2 in [Shi03] indicates that the gateset consists of Toffoli and Hadamard merely generates a dense subgroup of SO(8).

Proof of Theorem 7.1. Let $V_{x,w}$ be a $\mathsf{stateQCMA}_{\delta}[c,s]$ verification circuit with a classical witness w of size $m(n)$ where $n := |x|$ and $c(n)$ is a sufficiently large constant.[25] Using Lemma 2.2, we first convert $V_{x,w}$ to another circuit that utilizes a polynomial number of gates from the gateset $\mathcal{G}$. Note that while we can assume that the completeness parameter $c(n)$ does not increase by this conversion, the trace distance error increases to $\delta'(n) := \delta(n) + \exp(-\mathrm{poly}(n))$ owing to the triangle inequality. In the rest of the proof, we use $V_{x,w}$ as the converted circuit. So $V_{x,w}$ is assumed to be a $\mathsf{stateQCMA}_{\delta'}[c,s]$ circuit. Utilizing Lemma 7.3, the acceptance probability of each $V_{x,w}$ is expressed as $k_{x,w}/5^{l(n)}$ for some integer $k_{x,w} \in \{0,1,\cdots,5^{l(n)}\}$ and polynomial l which represents the size of the circuit $V_{x,w}$.

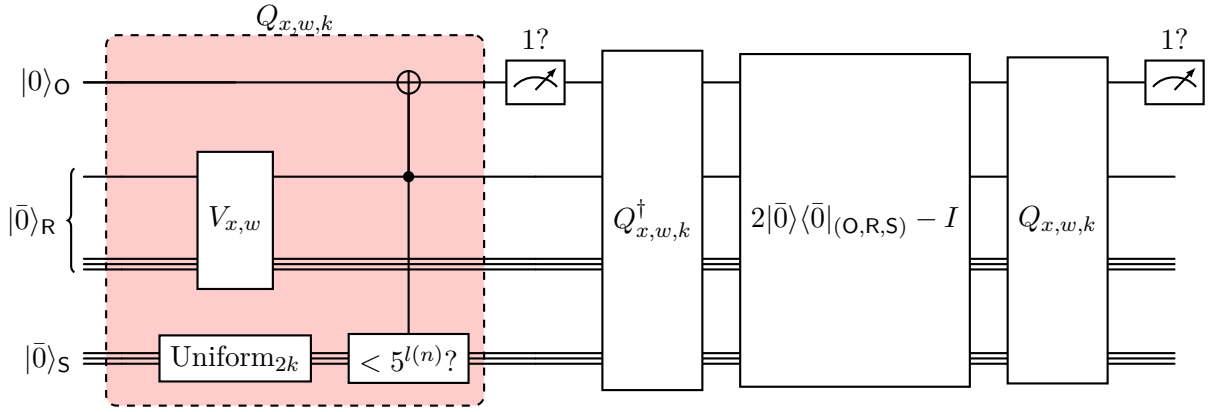

Figure 2: The new verification circuit $\tilde{V}_{x,w}$

Now we construct a $\mathsf{stateQCMA}_{\delta'}[1,s']$ verifier such that the verification circuit $\tilde{V}_{x,w}$ is the single-iteration quantum rewinding of $Q_{x,w,k}$ with a pre-processing, where the unitary transformation $Q_{x,w,k}$ is shown in Algorithm 3. To be precise, $\tilde{V}_{x,w}$ will simply reject if $k/5^{l(n)} < c(n)$,[26] then $\tilde{V}_{x,w}$ will perform the construction in Figure 2.

Algorithm 3: Unitary Transformation $Q_{x,w,k}$

1. Prepare the uniform superposition $\frac{1}{\sqrt{2k}} \sum_{z\in\{0,1,\cdots,2k-1\}} |z\rangle$ in S ;
2. Apply $V_{x,w}$ on R;
3. Apply a Toffoli gate that targets at O, and the first control qubit is the designated output qubit in R, as well as the second control qubit is decided by whether the integer in S at most $5^{l(n)}$.

In Algorithm 3, all registers $\mathsf{O},\mathsf{R},\mathsf{S}$ are assumed to be initialized to all-zero state, where O is a single-qubit register, and R is the $(q(n)+n)$-qubit register for some polynomial q, on which the verification circuit $V_{x,w}$ acts (and the last n-qubit of R is assumed to contain the output), as well as S is a t-qubit register where t is the minimum integer satisfying $2^t \geq 5^{l(n)}$. Moreover, the first step in Algorithm 3 can be implemented by exact amplitude amplification.[27] We then show that the unitary transformation $Q_{x,w,k}$ indeed preserves the resulting states of the verification circuit $V_{x,w}$ as Proposition 7.5, whose proof is deferred to the last part of this section.

[25] This is achievable by first applying error reduction on the given $\mathsf{stateQCMA}$ verifier.

[26] The claimed maximum acceptance probability $k/5^{l(n)}$ are supposed to correspond to *legal* witnesses.

[27] Note that any integer in $[0,5^{l(n)}-1]$ can be decomposed into a product of some power of 2 and some odd integer. Then we can employ with the construction in Figure 12 in [BGB+18].

Proposition 7.5. *For the unitary transformation $Q_{x,w,k}$ specified in Algorithm 3, the success probability is* $\Pr[Q_{x,w,k} \text{ accepts}] := \|\Pi_{\text{acc}} Q_{x,w,k}|\bar{0}\rangle_{(\mathsf{O},\mathsf{R},\mathsf{S})}\|^2 = k_{x,w}/(2k)$ *where* $\Pi_{\text{acc}} := |1\rangle\langle 1|_{\mathsf{O}} \otimes I_{(\mathsf{R},\mathsf{S})}$. *Moreover, $Q_{x,w,k}$ preserves the state synthesized by $V_{x,w}$.*

Plugging Proposition 7.5 into Lemma 7.4, we obtain that

$$\Pr\left[\tilde{V}_{x,w} \text{ accepts }\right] = \frac{1}{2}\left(\frac{k_{x,w}}{k}\right)^3 - 2\left(\frac{k_{x,w}}{k}\right)^2 + \frac{5}{2}\left(\frac{k_{x,w}}{k}\right) := g\left(\frac{k_{x,w}}{k}\right), \tag{9}$$

as guaranteed that $k \geq c(n) \cdot 2^{l(n)}$. We further notice the following fact:[28]

Fact 7.6. *For $0 \leq t \leq 1$, $g(t)$ defined in Equation (9) is monotonically increasing.*

It is thus left to analyze the maximum acceptance probability of $\tilde{V}_{x,w}$.

- For the completeness condition, equipped with Fact 7.6, the maximum achieves if $t := k_{x,w}/k = 1$. Namely, the claimed maximum acceptance probability k of $V_{x,w}$ is indeed the maximum acceptance probability $k_{x,w}$.
- For the soundness condition, we observe below for any illegal witness $w \in \{0,1\}^{m(n)}$:

  $$\frac{k_{x,w}}{k} \leq \frac{s(n) \cdot 5^{l(n)}}{c(n) \cdot 5^{l(n)}} = \frac{s(n)}{c(n)}.$$

  Since $k_{x,w}/k \leq s(n)/c(n)$, this indicates that the acceptance probability of $V_{x,w}$ is $s'(n) \leq g(s(n)/c(n))$. By Fact 7.6, $\Pr[V_{x,w} \text{ accepts }] \leq s'(n)$ holds for any choice of k as long as the witness w is illegal. Note that c is a constant and the promise gap $c(n) - s(n) \geq 1/p(n)$ where $p(n)$ is a polynomial of n, this deduces that

  $$s'(n) \leq g\left(1 - \frac{c(n)}{p(n)}\right) = 1 - \frac{1}{2}\left[\left(\frac{c(n)}{p(n)}\right)^2 + \left(\frac{c(n)}{p(n)}\right)^3\right] := 1 - \frac{1}{q(n)}. \tag{10}$$

We complete the proof by noticing $q(n)$ is a polynomial of n. □

In the remaining of this section, we complete the proof of Proposition 7.5.

Proof of Proposition 7.5. Let $V_{x,w}|\bar{0}\rangle_{\mathsf{R}} = |0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle$ be the quantum state just before the final measurement of the verification circuit $V_{x,w}$ where $n := |x|$. This deduces that

$$\Pr[V_{x,w} \text{ accepts }] = \||1\rangle\langle 1|_{\text{out}} V_{x,w}|\bar{0}\rangle_{\mathsf{R}}\|_2^2 = \langle\phi_1|\phi_1\rangle = k_{x,w}/5^{l(n)}.$$

The output state conditioned on accepting is then defined as the state we obtain by tracing out all but the last n-qubit of the density matrix $\frac{5^{l(n)}}{k_{x,w}}|\phi_1\rangle\langle\phi_1|$. The quantum state in $(\mathsf{O},\mathsf{R},\mathsf{S})$ before the last step in Algorithm 3 is then

$$|0\rangle_{\mathsf{O}} \otimes \left[|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle\right]_{\mathsf{R}} \otimes \frac{1}{\sqrt{2k}} \sum_{0 \leq z < 2k} |z\rangle_{\mathsf{S}}$$

and therefore the state after applying Algorithm 3 is $Q_{x,w,k}|\bar{0}\rangle_{(\mathsf{O},\mathsf{R},\mathsf{S})}$ as below:

$$|0\rangle_{\mathsf{O}} \otimes |0\rangle|\phi_0\rangle_{\mathsf{R}} \otimes \frac{1}{\sqrt{2k}} \sum_{z=0}^{2k-1} |z\rangle_{\mathsf{S}} + |0\rangle_{\mathsf{O}} \otimes |1\rangle|\phi_1\rangle_{\mathsf{R}} \otimes \frac{1}{\sqrt{2k}} \sum_{z=5^{l(n)}}^{2k-1} |z\rangle_{\mathsf{S}} + |1\rangle_{\mathsf{O}} \otimes |1\rangle|\phi_1\rangle_{\mathsf{R}} \otimes \frac{1}{\sqrt{2k}} \sum_{z=0}^{5^{l(n)}-1} |z\rangle_{\mathsf{S}}$$

[28] Fact 7.6 follows from the facts that $t = 1$ and $t = 5/3$ are roots of $g'(t) = 0$, as well as $g'(0) > 0$.

We thus conclude that

$$\Pr\left[Q_{x,w,k} \text{ accepts}\right] = \langle\phi_1|\phi_1\rangle \cdot \left\| \frac{1}{\sqrt{2k}} \sum_{z=0}^{5^{l(n)}-1} |z\rangle_{\mathsf{S}} \right\|_2^2 = \frac{k_{x,w}}{5^{l(n)}} \cdot \frac{5^{l(n)}}{2k} = \frac{k_{x,w}}{2k}.$$

Furthermore, we notice that the resulting state of $Q_{x,w,k}$ is

$$(|1\rangle\langle 1| \otimes (|\phi_1\rangle\langle\phi_1|)_{\mathsf{R}} \otimes \left(|0\rangle\langle 0| \otimes |+\rangle\langle +|^{\otimes l(n)}\right)_{\mathsf{S}}.$$

By tracing out S and all but the last n-qubit of R, we get the resulting state of $V_{x,w}$. □

Acknowledgments

We are grateful to Henry Yuen and Chinmay Nirkhe for insightful discussions and for bringing [BCNY19] to our attention. We also thank Gregory Rosenthal for suggesting the motivation behind defining the quantum state-synthesizing classes by drawing a comparison with classical function classes. Additionally, YL thanks Naixu Guo for helpful discussions on quantum singular value transformations. Furthermore, we express our gratitude to anonymous reviewers for providing detailed and helpful comments.

The authors were supported by JSPS KAKENHI Grants Nos. JP19H04066, JP20H00579, JP20H05966, JP20H04139, JP21H04879 and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grants Nos. JPMXS0118067394 and JPMXS0120319794. MM was also supported by JST, the establishment of University fellowships towards the creation of science technology innovation, Grant No. JPMJFS2120. Circuit diagrams were drawn by the Quantikz package [Kay18].

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity*. pages 229–242. IEEE. 2009. doi:10.1109/CCC.2009.42. arXiv:1110.5353. Appearances: 1

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: from quantum money to black holes. *arXiv preprint*. 2016. arXiv:1607.05256. Appearances: 1

[ABBS22] Dorit Aharonov, Michael Ben-Or, Fernando GSL Brandao, and Or Sattath. The pursuit of uniqueness: Extending Valiant-Vazirani theorem to the probabilistic and quantum settings. *Quantum*. 6:668. 2022. doi:10.22331/q-2022-03-17-668. arXiv:0810.4840. Appearances: 8

[AJL09] Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the Jones polynomial. *Algorithmica*. 55(3):395–421. 2009. doi:10.1007/s00453-008-9168-0. Preliminary version in *STOC 2006*. arXiv:quant-ph/0511096. Appearances: 5, 21

[BC18] Johannes Bausch and Elizabeth Crosson. Analysis and limitations of modified circuit-to-Hamiltonian constructions. *Quantum*. 2:94. 2018. doi:10.22331/q-2018-09-19-94. arXiv:1609.08571. Appearances: 5, 9, 20, 23, 24

[BCC+14] Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma. Exponential improvement in precision for simulating sparse Hamiltonians. In *Proceedings of the forty-sixth annual ACM Symposium on Theory of Computing*. pages 283–292. 2014. doi:10.1145/2591796.2591854. arXiv:1312.1414. Appearances: 10, 17

[BCC+15] Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. *Physical Review Letters*. 114(9):090502. 2015. doi:10.1103/PhysRevLett.114.090502. arXiv:1412.4687. Appearances: 10

[BCK15] Dominic W Berry, Andrew M Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science*. pages 792–809. IEEE. 2015. doi:10.1109/FOCS.2015.54. arXiv:1501.01715. Appearances: 10

[BCNY19] Thomas C Bohdanowicz, Elizabeth Crosson, Chinmay Nirkhe, and Henry Yuen. Good approximate quantum LDPC codes from spacetime circuit Hamiltonians. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. pages 481–490. 2019. doi:10.1145/3313276.3316384. arXiv:1811.00277. Appearances: 5, 9, 20, 23, 24, 28

[BEM+23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the Uhlmann transformation problem. *arXiv preprint*. 2023. arXiv:2306.13073. Appearances: 6

[BGB+18] Ryan Babbush, Craig Gidney, Dominic W Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. Encoding electronic spectra in quantum circuits with linear T complexity. *Physical Review X*. 8(4):041015. 2018. doi:10.1103/PhysRevX.8.041015. arXiv:1805.03662. Appearances: 26

[CDG+20] Rui Chao, Dawei Ding, Andras Gilyen, Cupjin Huang, and Mario Szegedy. Finding angles for quantum signal processing with machine precision. *arXiv preprint*. 2020. arXiv:2003.02831. Appearances: 16

[CGK21] Léo Colisson, Frédéric Grosshans, and Elham Kashefi. Non-destructive zero-knowledge proofs on quantum states, and multi-party generation of authorized hidden GHZ states. *arXiv preprint*. 2021. arXiv:2104.04742. Appearances: 6

[CK24] Marcos Crichigno and Tamara Kohler. Clique Homology is QMA_1-hard. *Nature Communications*. 15(1):9846. 2024. doi:10.1038/s41467-024-54118-z. arXiv:2209.11793. Appearances: 6, 7

[CMS23] Léo Colisson, Garazi Muguruza, and Florian Speelman. Oblivious transfer from zero-knowledge proofs - or how to achieve round-optimal quantum oblivious transfer and zero-knowledge proofs on quantum states. In *Advances in Cryptology – ASIACRYPT 2023 : 29th International Conference on the Theory and Application of Cryptology and Information Security*. volume 14445. pages 3–38. Springer. 2023. doi:10.1007/978-981-99-8742-9_1. arXiv:2303.01476. Appearances: 6

[Fey82] Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*. 21(6-7):467–488. 1982. doi:10.1201/9780429500459-11. Appearances: 1

[FKL+16] Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, and Harumichi Nishimura. Space-efficient error reduction for unitary quantum computations. In *43rd International Colloquium on Automata, Languages, and Programming*. volume 55. page 14. 2016. doi:10.4230/LIPIcs.ICALP.2016.14. arXiv:1604.08192. Appearances: 3, 18

[FL16] Bill Fefferman and Cedric Lin. Quantum Merlin Arthur with exponentially small gap. *arXiv preprint*. 2016. arXiv:1601.01975. Appearances: 3, 6, 19

[FL18] Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. In *9th Innovations in Theoretical Computer Science Conference*. volume 94. page 4. 2018. doi:10.4230/LIPIcs.ITCS.2018.4. arXiv:1604.01384. Appearances: 5, 6, 10, 11, 19

[FvdG99] Christopher A Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*. 45(4):1216–1227. 1999. doi:10.1109/18.761271. arXiv:quant-ph/9712042. Appearances: 7

[FR21] Bill Fefferman and Zachary Remscrim. Eliminating intermediate measurements in space-bounded quantum computation. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. pages 1343–1356. 2021. doi:10.1145/3406325.3451051. arXiv:2006.03530. Appearances: 11, 13

[Gil19] András Gilyén. *Quantum singular value transformation & its algorithmic applications*. PhD thesis. University of Amsterdam. 2019. URL: https://hdl.handle.net/11245.1/20e9733e-6014-402d-afa9-20f3cc4a0568. Appearances: 14, 15, 16, 17

[Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press. 2008. doi:10.1017/CBO9780511804106. Appearances: 13

[GR22] Uma Girish and Ran Raz. Eliminating intermediate measurements using pseudorandom generators. In *13th Innovations in Theoretical Computer Science Conference*. volume 215. pages 76:1–76:18. 2022. doi:10.4230/LIPIcs.ITCS.2022.76. arXiv:2106.11877. Appearances: 11

[GR23] Sevag Gharibian and Dorian Rudolph. Quantum space, ground space traversal, and how to embed multi-prover interactive proofs into unentanglement. In *14th Innovations in Theoretical Computer Science Conference*. volume 251. pages 53:1–53:23. 2023. doi:10.4230/LIPIcs.ITCS.2023.53. arXiv:2206.05243. Appearances: 13

[GRZ21] Uma Girish, Ran Raz, and Wei Zhan. Quantum logspace algorithm for powering matrices with bounded norm. In *48th International Colloquium on Automata, Languages, and Programming*. volume 198. pages 73:1–73:20. 2021. doi:10.4230/LIPIcs.ICALP.2021.73. arXiv:2006.04880. Appearances: 11

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. pages 193–204. 2019. doi:10.1145/3313276.3316366. arXiv:1806.01838. Appearances: 4, 5, 14, 16, 17

[Haa19] Jeongwan Haah. Product decomposition of periodic functions in quantum signal processing. *Quantum*. 3:190. 2019. doi:10.22331/q-2019-10-07-190. arXiv:1806.10236. Appearances: 16

[INN+22] Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. Quantum search-to-decision reductions and the state synthesis problem. In *Proceedings of the 37th Computational Complexity Conference*. pages 1–19. 2022. doi:10.4230/LIPIcs.CCC.2022.5. arXiv:2111.02999. Appearances: 6

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Journal of the ACM*. 58(6):1–27. 2011. doi:10.1145/2049697.2049704. Preliminary version in *STOC 2010*. arXiv:0907.4737. Appearances: 2

[JKK+12] Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath, and Shengyu Zhang. On the power of a unique quantum witness. *Theory of Computing*. 8(1):375–400. 2012. doi:10.4086/toc.2012.v008a017. Preliminary version in *ICS 2010*. arXiv:0906.4425. Appearances: 8

[JKNN12] Stephen P Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information & Computation*. 12(5-6):461–471. 2012. doi:10.26421/QIC12.5-6-7. arXiv:1111.5306. Appearances: 4, 6, 25

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference*. pages 126–152. Springer. 2018. doi:10.1007/978-3-319-96878-0_5. arXiv:1711.00385. Appearances: 1

[JN11] Stephen P Jordan and Daniel Nagaj. QCMA with one-sided error equals QCMA with two-sided error. *arXiv preprint*. 2011. arXiv:1111.5306v1. Appearances: 4, 6, 7, 25

[Jor75] Camille Jordan. Essai sur la géométrie á n dimensions. *Bulletin de la Société mathématique de France*. 3:103–174. 1875. doi:10.24033/bsmf.90. Appearances: 4

[Kay18] Alastair Kay. Tutorial on the quantikz package. *arXiv preprint*. 2018. arXiv:1809.03842. Appearances: 28

[Kit95] Alexei Yu Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXiv preprint*. 1995. arXiv:quant-ph/9511026. Appearances: 5, 21

[Kit97] Alexei Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*. 52(6):1191. 1997. doi:10.1070/rm1997v052n06abeh002155. Appearances: 2, 7

[KSV02] Alexei Y. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and quantum computation*. volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society. 2002. doi:10.1090/gsm/047. Appearances: 24

[Kup15] Greg Kuperberg. How hard is it to approximate the Jones polynomial? *Theory of Computing*. 11(1):183–219. 2015. doi:10.4086/toc.2015.v011a006. arXiv:0908.0512. Appearances: 7

[LC17] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by uniform spectral amplification. *arXiv preprint*. 2017. arXiv:1707.05391. Appearances: 5, 16

[LC19] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*. 3:163. 2019. doi:10.22331/q-2019-07-12-163. arXiv:1610.06546. Appearances: 4

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*. 39(4):859–868. 1992. doi:10.1145/146585.146605. Preliminary version in *FOCS 1990*. Appearances: 2

[Li22] Yulong Li. A simple proof of PreciseQMA = PSPACE. *arXiv preprint*. 2022. arXiv:2206.09230. Appearances: 6

[Llo96] Seth Lloyd. Universal quantum simulators. *Science*. 273(5278):1073–1078. 1996. doi:10.1126/science.273.5278.1073. Appearances: 1

[LLW23] François Le Gall, Yupan Liu, and Qisheng Wang. Space-bounded quantum state testing via space-efficient quantum singular value transformation. *arxiv preprint*. 2023. arXiv:2308.05079. Appearances: 18

[LMN23] François Le Gall, Masayuki Miyamoto, and Harumichi Nishimura. Distributed Merlin-Arthur synthesis of quantum states and its applications. In *48th International Symposium on Mathematical Foundations of Computer Science*. volume 272. pages 63:1–63:15. 2023. doi:10.4230/LIPIcs.MFCS.2023.63. arXiv:2210.01389. Appearances: 6

[LP17] David A Levin and Yuval Peres. *Markov chains and mixing times*. volume 107. American Mathematical Society. 2017. doi:10.1090/mbk/107. Appearances: 9

[vMW12] Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*. 8(1):1–51. 2012. doi:10.4086/toc.2012.v008a001. Preliminary version in arXiv:0712.2545. Appearances: 7, 8

[MW05] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *computational complexity*. 14(2):122–152. 2005. doi:10.1007/s00037-005-0194-x. Preliminary version in *CCC 2004*. arXiv:cs/0506068. Appearances: 3, 4, 5, 8, 19

[MY23] Tony Metger and Henry Yuen. stateQIP = statePSPACE. In *Proceedings of the 64th Annual IEEE Symposium on Foundations of Computer Science*. pages 1349–1356. IEEE. 2023. doi:10.1109/FOCS57990.2023.00082. arXiv:2301.07730. Appearances: 2, 3, 5, 6, 11, 14, 17

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press. 2010. doi:10.1017/CBO9780511976667. Appearances: 6, 7

[NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information & Computation*. 9(11):1053–1068. 2009. doi:10.26421/QIC9.11-12-8. arXiv:0904.1549. Appearances: 3, 4

[PW09] David Poulin and Pawel Wocjan. Preparing ground states of quantum many-body systems on a quantum computer. *Physical Review Letters*. 102(13):130503. 2009. doi:10.1103/PhysRevLett.102.130503. arXiv:0809.2705. Appearances: 1

[Reg06] Oded Regev. Witness-preserving amplification of QMA. https://cims.nyu.edu/~regev/teaching/quantum_fall_2005/ln/qma.pdf. 2006. Appearances: 4

[Ros24] Gregory Rosenthal. Efficient quantum state synthesis with one query. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms*. pages 2508–2534. SIAM. 2024. doi:10.1137/1.9781611977912.89. arXiv:2306.01723. Appearances: 2

[RY22] Gregory Rosenthal and Henry Yuen. Interactive proofs for synthesizing quantum states and unitaries. In *13th Innovations in Theoretical Computer Science Conference*. volume 215. pages 112:1–112:4. 2022. doi:10.4230/LIPIcs.ITCS.2022.112. arXiv:2108.07192. Appearances: 2, 6, 11, 12

[Sha92] Adi Shamir. IP = PSPACE. *Journal of the ACM*. 39(4):869–877. 1992. doi:10.1145/146585.146609. Preliminary version in *FOCS 1990*. Appearances: 2

[Shi03] Yaoyun Shi. Both toffoli and controlled-not need little help to do universal quantum computing. *Quantum Information & Computation*. 3(1):84–92. 2003. doi:10.26421/QIC3.1-7. arXiv:quant-ph/0205115. Appearances: 25

[SJ89] Alistair Sinclair and Mark Jerrum. Approximate counting, uniform generation and rapidly mixing markov chains. *Information and Computation*. 82(1):93–133. 1989. doi:10.1016/0890-5401(89)90067-9. Preliminary version in *WG 1987*. Appearances: 9, 10

[Vya03] Mikhail Vyalyi. QMA = PP implies that PP contains PH. In *Electronic Colloquium on Computational Complexity*. Citeseer. 2003. ECCC:TR03-021. Appearances: 19

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*. pages 459–468. IEEE. 2002. doi:10.1109/SFCS.2002.1181970. arXiv:quant-ph/0202111. Appearances: 2, 11

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*. 39(1):25–58. 2009. doi:10.1137/060670997. Preliminary version in *STOC 2006*. arXiv:quant-ph/0511020. Appearances: 25

[ZH19] Huangjun Zhu and Masahito Hayashi. Efficient verification of pure quantum states in the adversarial scenario. *Physical Review Letters*. 123(26):260504. 2019. doi:10.1103/PhysRevLett.123.260504. arXiv:1909.01900. Appearances: 2