Quantum Signal Processing and Quantum Singular Value Transformation on $U(N)$

Xi Lu[1], Yuan Liu[2,3] and Hongwei Lin[1]
[1] *School of Mathematical Science, Zhejiang University, Hangzhou, 310027, China*
[2] *Department of Electrical and Computer Engineering,*
North Carolina State University, Raleigh, NC 27606, USA
[3] *Department of Computer Science, North Carolina State University, Raleigh, NC 27606, USA*

Quantum signal processing and quantum singular value transformation are powerful tools to implement polynomial transformations of block-encoded matrices on quantum computers, and has achieved asymptotically optimal complexity in many prominent quantum algorithms. We propose a framework of quantum signal processing and quantum singular value transformation on $U(N)$, which realizes multiple polynomials simultaneously from a block-encoded input, as a generalization of those on $U(2)$ in the original frameworks. We also perform a comprehensive analysis on achievable polynomials and give a recursive algorithm to construct the quantum circuit that gives the desired polynomial transformation. As an example application, the new framework is used to construct the quantum amplitude estimation algorithm with asymptotically optimal query complexity. Based on this framework, we also propose a framework to realize multi-variate polynomial functions for commutative variables.

I. INTRODUCTION

Quantum Signal Processing (QSP) is a powerful tool for building quantum algorithms, capable of unifying many other existing algorithms [1–3]. QSP can be conceptualized as a framework of polynomial transformation of matrices, which maps a set of phase angles to a polynomial function to approximate a wide range of target functions. Quantum Singular Value Trandformatoin (QSVT) [2], another framework derived from QSP, extends the application to polynomial singular value transformations of matrices, which can be even non-square. Asymptotic analyses of QSP-based quantum algorithms indicate their potential to achieve optimal complexity in various tasks, such as Hamiltonian simulation [1, 4, 5], linear system solving [6], ground state preperation [7], fixed-point quantum search [8]. QSP is also used to improve and simplify algorithms for quantum amplitude estimation (QAE) [9], which is a fundamental task in quantum metrology [10–12] and has direct applications in numerical integration [13], quantum tomography [14–18], overlap and expectation value estimation in quantum simulation [19–23], Gibbs sampling [24], variational quantum algorithms and quantum machine learning [25–28]. Recent research in QSP theories has focused on efficient realization of block encoding [29, 30], classical evaluation of phase angles [31–33], and generalization [34–38].

Meanwhile, the original framework of QSP has some restrictions that limit its applicability. On the mathematical side, the original framework utilizes a series of tunable $U(2)$ elements to realize a class of polynomial transformations, i.e., to construct a unitary transformation that is a block encoding of the target polynomial $P(U)$ given input U. It is a natural question whether we can realize more than one polynomials at the same time if we use a sequence of tunable $U(N)$ elements instead. On the practical side, the idea of realizing multiple target functions lies in the core of some quantum algorithms like the quantum phase estimation (QPE) and quantum amplitude estimation (QAE) algorithms [39]. In addition, by expanding the toolkit in manipulating matrices in quantum computers, QSP and QSVT on $U(N)$ can also helps us in more complicated taks like the multi-variate generalization of QSP, which is much less understood than the uni-variate one, and known to have significant difficulties brought by its exponentially large target space and the commuting relations between different variables [37, 38].

During the preparation of this paper, another paper [34] by Lorenzo Laneve came out, which studies the generalization of QSP over $SU(N)$ that can prepare the state $\sum_m P_m(z)\left|m\right\rangle$ from $\left|0\right\rangle$ by a similar construction, and its application in quantum phase estimation. In comparison, his result [34] can be viewed as a special case of our Theorem 3, in which a $N \times 1$ polynomial block $\boldsymbol{P}$ is encoded. Compared to QSP and QSVT in $U(2)$, establishing theories in $U(N)$ requires understanding the quantum circuits from a different perspective and more theoretical results from algebraic geometry.

In this paper, we establish a complete theory of QSP and QSVT on $U(N)$ that has multiple outputs block encoded in a unitary, in the sense that given any mathematically permissible set of target polynomials, one can find a sequence of $U(N)$ elements in the quantum circuits, evaluated by a recursive procedure, to realize them. As examples of application, we first show how our theory helps to give resource bound in QAE problem and construct asympotically optimal QAE algorithms, then have a discussion on its potential application towards multi-variate QSP. A graphical summary of the contributions of our paper is given in FIG. 1.

The structure of this paper is organized as follows. In Sec. II, we first review fundamental results on single block encoding of uni-variate QSP, then define the generalization on $U(N)$ for two types of QSP algorithms, namely QSP for unitary and QSVT, introduce and prove the main theories on achievable polynomial sets. As the first

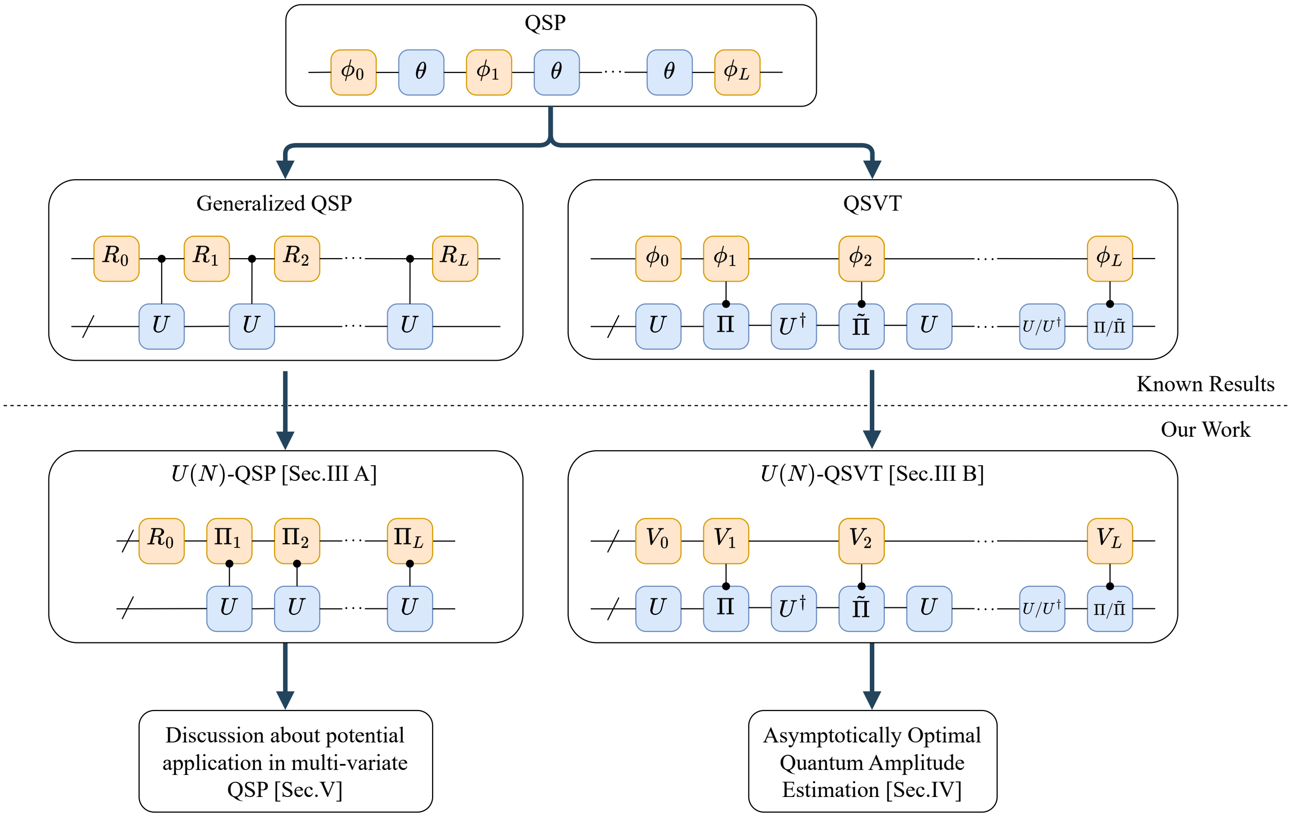

FIG. 1: A summary of our contributions in the paper. The orange quantum gates are for tunnable parameterized unitaries or projectors, while the blue gates are for fixed input variables.

application, in Sec. III we show that any measurement output of a QAE circuit can be regarded as a polynomial transformation of the amplitude on $U(N)$, and using numerical optimization on achievable polynomials we can obtain and achieve the optimal accuracy of QAE in different measures. Next, we also show that $U(N)$-QSP can be used to perform multi-variate quantum signal processing (MQSP) with a wider range of achievable polynomials than $U(2)$-QSP in Sec. IV. Finally, we make conclusions and discuss outlooks in Sec. V.

II. THEORY OF QSP AND QSVT ON $U(N)$

In this section, we first briefly review the fundamental results about QSP in Sec. II A. Then, in Sec. II B and Sec. II C, we first define the generalization on $U(N)$, then construct a quantum circuit with tunable parts that help achieving different target functions, and finally state and prove the achievable polynomial sets by the circuit.

A. Review of Quantum Signal Processing

To block-encode any matrix A in a quantum operation, an ancilla system is used to construct a unitary U such that,

$$U|\mathbf{0}\rangle|\psi\rangle = |\tilde{\mathbf{0}}\rangle A|\psi\rangle + \cdots, \text{ or } U = \begin{pmatrix} A & * \\ * & * \end{pmatrix}, \quad (1)$$

in which both $|\mathbf{0}\rangle$ and $|\tilde{\mathbf{0}}\rangle$ are qubits all set to zero, and we use different notations here to indicate that the number of qubits in them can be different, so that the block encoding can also be well defined for non-square matrix A.

In this paper, we focus on two algorithms in the QSP family, namely the QSP for unitrary matrices and quantum singular value transformation (QSVT) for general matrices. In QSP-U, one use several controlled-U operations to construct a block encoding of polynomials of U of the form $P(U) = \sum_j c_j U^j$ [33, 40]. A fundamental result in QSP-U is as follows.

Theorem 1 (Theorem 3 and 4 in [40]) *Given any polynomial $P(z)$ of degree L s.t. $|P(z)| \leq 1, \forall |z| = 1$. Then one can block-encode $P(U)$ using L calls to controlled-U for any unitary matrix input U.*

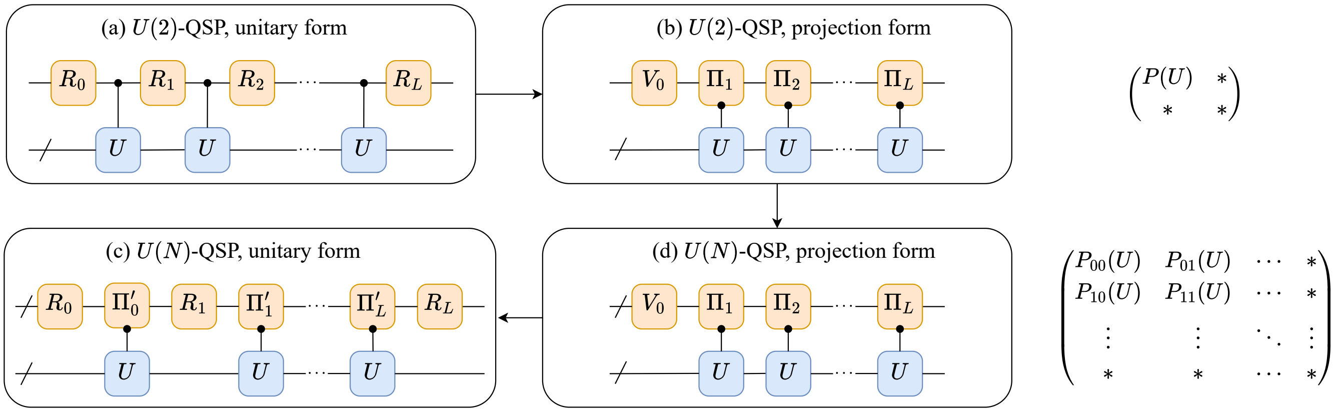
(a) $U(2)$-QSP, unitary form
R_0 R_1 R_2 R_L U
(b) $U(2)$-QSP, projection form
V_0 Π_1 Π_2 Π_L U
(c) $U(N)$-QSP, unitary form
R_0 Π'_0 R_1 Π'_1 Π'_L R_L U
(d) $U(N)$-QSP, projection form
V_0 Π_1 Π_2 Π_L U
$\begin{pmatrix} P(U) & * \\ * & * \end{pmatrix}$
$\begin{pmatrix} P_{00}(U) & P_{01}(U) & \cdots & * \\ P_{10}(U) & P_{11}(U) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix}$

FIG. 2: Comparison between QSP on $U(2)$ and $U(N)$, in which Π_k are projection operators, and a gate connecting a projector Π with a unitary U is for the multi-qubit controlled gate $C_\Pi(U) := \Pi \otimes U + (I - \Pi) \otimes I$.

In QSVT, however, one uses U and $U^\dagger$ alternatively to construct a block encoding of singular-value polynomial transformations of A, which is defined as,

$$P^{(SV)}(A) = \begin{cases} \sum_j P(\lambda_j)\,|\psi_j\rangle\langle\psi_j|\,, & \text{if } L \text{ is even},\\ \sum_j P(\lambda_j)\,\left|\psi_j\right\rangle\left\langle\tilde{\psi}_j\right|, & \text{if } L \text{ is odd},\end{cases} \tag{2}$$

where L is the number of calls to U and $U^\dagger$ in total, and $A = \sum_j \lambda_j \left|\psi_j\right\rangle\left\langle\tilde{\psi}_j\right|$ for two orthogonal sets $\{|\psi_j\rangle\}, \{\left|\tilde{\psi}_j\right\rangle\}$ and $\lambda_j \in \mathbb{R}$, and P naturally subjects to the parity condition that $P(-x) = (-1)^L P(x)$. When A is Hermitian, one can write $A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ with $\lambda_j \in \mathbb{R}$, then the singular value polynomial transformation is equal to the matrix polynomial. But in general they can be different. A milestone result in the original framework of QSVT is as follows.

Theorem 2 (Corollary 8 and 10 in [41]) *Given a pair of polynomials $P(z)$ satisfying,*

1. $\deg(P) \le L$;
2. *P has parity $L \bmod 2$;*
3. $\forall x \in [-1, 1]$, $|P(x)| \le 1$;

and a general matrix A block-encoded by a unitary U, one can block-encode $P^{(SV)}(A)$ using L calls to U and U^{-1} in total.

Compared to QSP-U, it has inherit restrictions on parity, since singular value transformation (SVT) by polynomials without definite parity is not well-defined in Eq. (2) and can give unexpected results. One exception is that for Hermitian input, the SVT by polynomials without definite parity since the left and right singular vector spaces share the same basis and is identical to the common polynomial transformation. In this case SVT with complex-valued polynomials is also well-defined. To tackle with the two problems we can utilize the linear combination of unitaries (LCU, also introduced in Lemma 6 in this paper) [42], given additional access to controlled U and U^{-1}.

B. $U(N)$-Quantum Signal Processing

Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z) = \{P_{jk}(z)\}$, by $U(N)$-QSP we hope to construct the unitary transformation,

$$\begin{pmatrix} P_{00}(U) & P_{01}(U) & \cdots & * \\ P_{10}(U) & P_{11}(U) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix}. \tag{3}$$

For this task we construct a quantum circuit in FIG. 2(d), with $\{\Pi_k\}$ being tunable projection operators. The $U(2)$-QSP was first written in the form in FIG. 2(a), with $\{R_k\}$ being tunable single-qubit unitary operators,

$$R(\theta, \phi, \lambda) = \begin{pmatrix} e^{i(\lambda+\phi)}\cos\theta & e^{i\phi}\sin\theta \\ e^{i\lambda}\sin\theta & -\cos\theta \end{pmatrix}. \tag{4}$$

To see the relationship between (a) and (d) in FIG. 2, we can write the circuit (a), in which all U are controlled by the projector $|1\rangle\langle 1|$ in the first register, into an equivalent form in (b) with controlling projectors $\Pi_1, \cdots, \Pi_k$ and an initial unitary V_0 by,

$$\begin{cases} V_0 = R_0 R_1 \cdots R_L, \\ \Pi_k = R_L^\dagger \cdots R_k^\dagger\, |1\rangle\langle 1|\, R_k \cdots R_L. \end{cases} \tag{5}$$

From (b) to (d), the number of ancilla qubits is generalized from one to many, V_0 can take value from $U(N)$, and each Π_k is a projector of arbitrary subspace of the N-dimensional Hilbert space, where N equals 2 to the power of the number of ancilla qubits. If we write $\Pi_k = \sum_{l=0}^{r_k-1} |\psi_{k,l}\rangle\langle\psi_{k,l}|$, where $r_k \in \{0, \cdots, N\}$ is the rank of Π_k, we can further write (d) as an equivalent unitary form in (c) with tunable unitaries V_k and controlled projectors $\Pi'_k = \sum_{l=0}^{r_k-1} |l\rangle\langle l|$, by

$$\begin{cases} R_k = \left(\sum_{l=0}^{r_k-1} |l\rangle\langle\psi_{k,l}|\right) R_L^\dagger \cdots R_{k+1}^\dagger, \ (k = L, \cdots, 1) \\ R_0 = V_0 R_L^\dagger \cdots R_1^\dagger. \end{cases} \tag{6}$$

We characterize the achievable polynomials of $U(N)$-QSP in FIG. 2(d) by the following lemmas and theorems.

Lemma 1 ($U(N)$-QSP, forward) *Using L calls to a unitary U, the quantum circuit in FIG. 2(d) implements the unitary operation,*

$$\begin{pmatrix} P_{00}(U) & P_{01}(U) & \cdots & P_{0,N-1}(U) \\ P_{10}(U) & P_{11}(U) & \cdots & P_{1,N-1}(U) \\ \vdots & \vdots & \ddots & \vdots \\ P_{N-1,0}(U) & P_{N-1,1}(U) & \cdots & P_{N-1,N-1}(U) \end{pmatrix}. \tag{7}$$

for a matrix of complex-valued polynomials $\{P_{jk}(z)\}$ of degrees no more than L, denoted as $\boldsymbol{P}(z)$.

Proof of Lemma 1. The proof is straightforward by induction on L. For $L = 0$, the target unitary is $V_0 \otimes I$, indicating that P_{jk} is simply the constant function equal to the (j, k)-th entry of V_0.

If the lemma holds for $L-1$, i.e., the part of the circuit before the last controlled-U implements the unitary operation $\boldsymbol{P}(U) = \sum_{l=0}^{L-1} \tilde{P}_l \otimes U^l$ for some constant matrices $\{\tilde{P}_l\}$. Then,

$$C_{\Pi_L}(U)\boldsymbol{P}(U) = \sum_{l=0}^{L-1} \Pi_L \tilde{P}_l \otimes U^{l+1} + (I - \Pi_L)\tilde{P}_l \otimes U^l, \tag{8}$$

which is of the form Eq. (7) with degree no more than L. □

Theorem 3 ($U(N)$-QSP, backward) *Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z)$ of degrees no more than L, such that $\boldsymbol{P}(z)$ has all singular values in $[0, 1]$ whenever $|z| \le 1$. Then one can construct a quantum circuit with L calls to controlled-U to implement a block encoding of $\boldsymbol{P}(U)$, as defined in Eq. (3).*

Before the proof of Theorem 3, we first prove its weaker version as follows.

Theorem 4 *Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z)$ that is unitary for all $|z| \le 1$. Then one can tune the parameters $V_0, \Pi_1, \cdots, \Pi_L$ in FIG. 2(d) to implement the unitary transformation $\boldsymbol{P}(U)$.*

Proof of Theorem 4. We use induction on L to prove the theorem.

For $L = 0$, each entry of Eq. (7) is constant, so we can simply choose V_0 to be the target unitary. If the theorem holds for $L - 1$, we show that when the degree is L, we can always find a Π_L such that $C_{\Pi_L}(U^{-1})\boldsymbol{P}(U)$ is also of the form Eq. (7), with each entry a polynomial of degree no more than $(L - 1)$.

Write, $\boldsymbol{P}(U) = \sum_{l=0}^{L} \tilde{P}_l \otimes U^l$. Picking the U^L term out of the identity $\boldsymbol{P}(U)^\dagger \boldsymbol{P}(U) = I$, we have, $\tilde{P}_0^\dagger \tilde{P}_L = 0$. This shows that the column spaces of $\tilde{P}_0$ and $\tilde{P}_L$ are orthogonal. Let Π_L be the projector onto the column space of $\tilde{P}_0$. Then $\Pi_L \tilde{P}_L = (I - \Pi_L)\tilde{P}_0 = 0$. As a result,

$$\begin{aligned} & C_{\Pi_L}(U^{-1})\boldsymbol{P}(U) \\ &= \sum_{l=0}^{L} \Pi_L \tilde{P}_l \otimes U^{l-1} + (I - \Pi_L)\tilde{P}_l \otimes U^l \\ &= \sum_{l=0}^{L-1} \left[\Pi_L \tilde{P}_{l+1} + (I - \Pi_L)\tilde{P}_l\right] \otimes U^l, \end{aligned} \tag{9}$$

which is of the form Eq. (7) with degree no more than $(L - 1)$. By induction, we show a constructive way to find $V_L, V_{L-1}, \cdots, V_0$. This proof also gives a classical algorithm to find the parameters. □

Proof of Theorem 3. Since $I - \boldsymbol{P}(z)^\dagger \boldsymbol{P}(z)$ is positive semidefinite on $|z| = 1$, by the *Polynomial Matrix Spectral Factorization Theorem* [43, 44], there is a polynomial matrix $\boldsymbol{Q}(z)$ of degree no more than L such that,

$$I - \boldsymbol{P}(z)^\dagger \boldsymbol{P}(z) \; = \; \boldsymbol{Q}(z)^\dagger \boldsymbol{Q}(z). \tag{10}$$

Next, we hope to find a block $\boldsymbol{R}(z)$ such that,

$$\left(\begin{array}{cc} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \\ \hdashline \multicolumn{2}{c}{\boldsymbol{R}(z)} \end{array}\right), \tag{11}$$

is unitary on $|z| = 1$, i.e., $\boldsymbol{R}(z)$ has proper size to make it a square matrix and,

$$\begin{aligned} & \left(\begin{array}{c:c} \boldsymbol{P}(z)^\dagger & \multirow{2}{*}{$\boldsymbol{R}(z)^\dagger$} \\ \boldsymbol{Q}(z)^\dagger & \end{array}\right) \left(\begin{array}{cc} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \\ \hdashline \multicolumn{2}{c}{\boldsymbol{R}(z)} \end{array}\right) \\ &= \begin{pmatrix} \boldsymbol{P}(z)^\dagger \\ \boldsymbol{Q}(z)^\dagger \end{pmatrix} \begin{pmatrix} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \end{pmatrix} + \boldsymbol{R}(z)^\dagger \boldsymbol{R}(z) = I, \end{aligned} \tag{12}$$

Again, this is always possible since

$$I - \begin{pmatrix} \boldsymbol{P}(z)^\dagger \\ \boldsymbol{Q}(z)^\dagger \end{pmatrix} \begin{pmatrix} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \end{pmatrix}, \tag{13}$$

is positive semidefinite for all $|z| = 1$, as

$$\begin{pmatrix} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \end{pmatrix} \begin{pmatrix} \boldsymbol{P}(z)^\dagger \\ \boldsymbol{Q}(z)^\dagger \end{pmatrix} = I \tag{14}$$

from Eq. (10) implies that

$$\begin{pmatrix} \boldsymbol{P}(z)^\dagger \\ \boldsymbol{Q}(z)^\dagger \end{pmatrix} \begin{pmatrix} \boldsymbol{P}(z) & \boldsymbol{Q}(z) \end{pmatrix} \tag{15}$$

is identity in some subspace. Finally,

$$\left(\begin{array}{cc} \boldsymbol{P}(U) & \boldsymbol{Q}(U) \\ \hdashline \multicolumn{2}{c}{\boldsymbol{R}(U)} \end{array}\right), \tag{16}$$

is a block encoding of $\boldsymbol{P}(U)$ and by Theorem 4, it can be implemented as desired. □

The Theorem 3 is a generalization of the results in [40], in which only one aniclla qubit is used, and the corresponding $\boldsymbol{P}(z)$ contains a single entry $p(z)$, with prerequisites $|p(z)| \le 1$ for all $|z| = 1$.

C. $U(N)$-Quantum Singular Value Transformation

In this subsection we assume all polynomial transformations of matrices are the singular value polynomial transformations in Eq. (2), and without ambiguity we omit the superscript (SV). Assume $|\psi\rangle$ is exactly some right singular vector $|\psi_k\rangle$ of A. Define $|\Psi_m\rangle = |\mathbf{0}\rangle |\psi_k\rangle$, $\left|\tilde{\Psi}_m\right\rangle = |\tilde{\mathbf{0}}\rangle \left|\tilde{\psi}_k\right\rangle$, and define $\left|\Psi_m^\perp\right\rangle, \left|\tilde{\Psi}_m^\perp\right\rangle$ by

$$U |\Psi_k\rangle \; = \; \lambda_m \left|\tilde{\Psi}_k\right\rangle + \bar{\lambda}_m \left|\tilde{\Psi}_k^\perp\right\rangle, \tag{17}$$

$$U^\dagger \left|\tilde{\Psi}_k\right\rangle \; = \; \lambda_m |\Psi_k\rangle - \bar{\lambda}_m \left|\Psi_k^\perp\right\rangle, \tag{18}$$

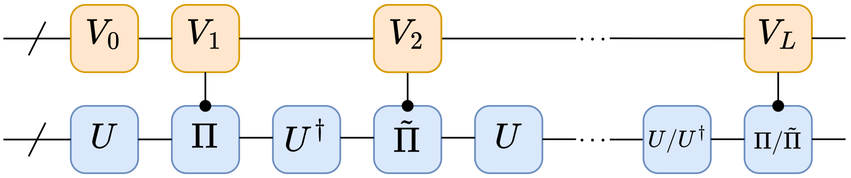

FIG. 3: The $U(N)$-QSVT unit, in which $\Pi = |\mathbf{0}\rangle\langle\mathbf{0}|$ and $\tilde{\Pi} = \left|\tilde{\mathbf{0}}\right\rangle\left\langle\tilde{\mathbf{0}}\right|$. The U and $U^\dagger$ gates applied to the second register alternate, and it depends on the parity of L whether the last two gates in the second register are U and Π, or $U^\dagger$ and $\tilde{\Pi}$.

where $\bar{\lambda}_m := \sqrt{1-\lambda_m^2}$. Thus in the basis $(|\Psi_m\rangle, |\Psi_m^\perp\rangle) \to (\left|\tilde{\Psi}_m\right\rangle, \left|\tilde{\Psi}_m^\perp\right\rangle)$,

$$U = \begin{pmatrix} \lambda_m & \bar{\lambda}_m \\ -\bar{\lambda}_m & \lambda_m \end{pmatrix}. \tag{19}$$

Given a general matrix A and a matrix of polynomials $\boldsymbol{P}$, the $U(N)$-QSVT is defined as the unitary transformation,

$$\begin{aligned} &\sum_j |j\rangle |\mathbf{0}\rangle |\phi_j\rangle \\ \mapsto &\sum_k \left[|k\rangle |\mathbf{0}\rangle \sum_j P_{kj}(A) |\phi_j\rangle + \left|\mathbf{0}^\perp\right\rangle |\cdots\rangle \right]. \end{aligned} \tag{20}$$

Similar to the idea of qubitization [2], we first give the following two lemmas that works with one singular value λ_m.

Lemma 2 *If L is odd, then the quantum circuit in FIG. 3 implements the unitary transformation,*

$$\begin{aligned} &|j\rangle |\Psi_m\rangle \\ \mapsto &\sum_k |k\rangle \left[P_{kj}(\lambda_m) \left|\tilde{\Psi}_m\right\rangle + \bar{\lambda}_m Q_{kj}(\lambda_m) \left|\tilde{\Psi}_m^\perp\right\rangle \right], \end{aligned} \tag{21}$$

for some L-polynomials $\{P_{kj}\}$ and $(L-1)$-polynomials $\{Q_{kj}\}$ such that,

$$\sum_k \left[|P_{kj}(x)|^2 + (1-x^2)|Q_{kj}(x)|^2 \right] \equiv 1. \tag{22}$$

Otherwise, if L is even, then in Eq. (21) the $\left|\tilde{\Psi}_m\right\rangle, \left|\tilde{\Psi}_m^\perp\right\rangle$ should be replaced by $|\Psi_m\rangle, |\Psi_m^\perp\rangle$.

Proof of Lemma 2. We prove by induction on L. For $L = 0$, the output state is simply $\sum_k u_{kj} |k\rangle |\Psi_m\rangle$, with u_{kj} being the (k,j)-th entry of V_0, and these constant functions are 0-polynomials.

Suppose the lemma holds for some even number $(L-1)$, i.e., the state before the final U and $C_\Pi(V_L)$ gates in FIG. 3 is Eq. (21). Then after applying the two gates, the state is,

$$\begin{aligned} \sum_k |k\rangle \Bigg\{ &\sum_l u_{kl} \left[\lambda_m P_{lj}(\lambda_m) - (1-\lambda_m^2) Q_{lj}(\lambda_m) \right] \left|\tilde{\Psi}_m\right\rangle \\ &\bar{\lambda}_m \left[P_{lk}(\lambda_m) + \lambda_m Q_{kj}(\lambda_m) \right] \left|\tilde{\Psi}_m^\perp\right\rangle \Bigg\}, \end{aligned} \tag{23}$$

which is of the desired form in Eq. (21) with polynomials satisfying both the degree and parity constraints.

The case when L is even is analogous. □

By the linearity of quantum circuits, the single singular value case can be immediately generalized as follows.

Lemma 3 **($U(N)$-QSVT, forward)** *The quantum circuit in FIG. 3 implements the unitary transformation Eq. (20) for some matrix of polynomials $\boldsymbol{P}$.*

The main theorem showing the usefulness of the quantum circuit in FIG. 3, as a generalization of Theorem 2, is as follows.

Theorem 5 **($U(N)$-QSVT, backward)** *Given a matrix A blocked-encoded by U as in Eq. (1), and a polynomial matrix $\boldsymbol{P}(x)$ such that $I - \boldsymbol{P}(x)^\dagger \boldsymbol{P}(x)$ is positive semidefinite for all $x \in [-1,1]$, with L calls to U and U^{-1} in total, one can implement a block encoding of $\boldsymbol{P}(A)$ by the following unitary transformation,*

$$\begin{aligned} &|0\rangle \sum_j |j\rangle |\mathbf{0}\rangle |\phi_j\rangle \\ \mapsto &|0\rangle \sum_k |k\rangle |\mathbf{0}\rangle \sum_j P_{kj}(A) |\phi_j\rangle + |1\rangle |\cdots\rangle . \end{aligned} \tag{24}$$

Lemma 4 *Given a matrix A and its blocking encoding U as in Eq. (1), a matrix of L-polynomials $\boldsymbol{P}(x)$ and a matrix of $(L-1)$-polynomials $\boldsymbol{Q}(x)$ of the same size such that,*

$$\boldsymbol{P}(x)^\dagger \boldsymbol{P}(x) + (1-x^2) \boldsymbol{Q}(x)^\dagger \boldsymbol{Q}(x) \equiv I, \tag{25}$$

for all $x \in [-1,1]$, one can find $V_0, \cdots, V_L$ in FIG. 3 to make it implement the transformation Eq. (21) for each j.

Proof of Lemma 4. We prove by induction on L. The case $L = 0$ is trivial, as $\boldsymbol{Q}(x) = 0$ and $\boldsymbol{P}(x)$ is a constant unitary matrix, and one can simply let $V_0 = \boldsymbol{P}(x)$.

Suppose the lemma holds for some even $(L-1)$, and now we consider the case for L. Write,

$$\boldsymbol{P}(x) = \sum_{l=0}^{(L-1)/2} \tilde{P}_{2l+1} x^{2l+1}, \tag{26}$$

$$\boldsymbol{Q}(x) = \sum_{l=0}^{(L-1)/2} \hat{Q}_{2l} x^{2l}. \tag{27}$$

Picking the x^{2L} terms out of the constraint Eq. (25),

$$\tilde{P}_L^\dagger \tilde{P}_L - \hat{Q}_{L-1}^\dagger \hat{Q}_{L-1} = 0, \tag{28}$$

so there is a unitary V_L such that $V_L^\dagger \tilde{P}_L = \hat{Q}_{L-1}$.

Write $V_L^\dagger = \{u_{kl}\}$. Then,

$$\begin{aligned}&(I \otimes U)^{-1} C_\Pi (V_L)^{-1} \cdot \\ &\sum_k |k\rangle \left[P_{kj}(\lambda_m)\left|\tilde{\Psi}_m\right\rangle + \bar{\lambda}_m Q_{kj}(\lambda_m)\left|\tilde{\Psi}_m^\perp\right\rangle\right] \\ =&\sum_k |k\rangle \left\{\left[\sum_l u_{kl}\lambda_m P_{lj}(\lambda_m) + (1-\lambda_m^2)Q_{kj}(\lambda_m)\right]|\Psi_m\rangle\right. \\ &\left.\bar{\lambda}_m\left[-\sum_l u_{kl}P_{lj}(\lambda_m) + \lambda_m Q_{kj}(\lambda_m)\right]\left|\Psi_m^\perp\right\rangle\right\},\end{aligned} \tag{29}$$

in which the coefficient polynomial of $|\Psi_m\rangle$ is actually a $(L-1)$-polynomial, since its λ_m^{L+1} term coefficient $\sum_l u_{kl}(\tilde{P}_L)_{lj} - (\hat{Q}_{L-1})_{kj} = 0$, and similarly the coefficient polynomial of $\left|\Psi_m^\perp\right\rangle$ is actually a $(L-2)$-polynomial. So we reduce the degree of the problem by 1.

The case when L is even is analogous. □

Proof of Theorem 5. All we need to show is that one can find a matrix of L-polynomials $\boldsymbol{P}_1(x)$ and a matrix of $(L-1)$-polynomials $\boldsymbol{Q}_1(x)$ such that,

$$\begin{pmatrix}\boldsymbol{P}(x)^\dagger & \boldsymbol{P}_1(x)^\dagger\end{pmatrix}\begin{pmatrix}\boldsymbol{P}(x) \\ \boldsymbol{P}_1(x)\end{pmatrix} + (1-x^2)\boldsymbol{Q}_1(x)^\dagger \boldsymbol{Q}_1(x) = I, \tag{30}$$

such that by rearranging order, one can label the flag qubit corresponding to the $\boldsymbol{P}(x)$ block to zero while $\boldsymbol{P}_1(x)$ and $\boldsymbol{Q}_1(x)$ to one, to obtain the desired block encoding of $\boldsymbol{P}(A)$.

Again, we prove the case when L is even, and the other case is analogous. Write $\boldsymbol{P}$ as Eq. (26). Make substitution $x \to \cos\frac{\theta}{2}$, then $\boldsymbol{P}(x) = e^{-i\frac{L\theta}{2}}\tilde{\boldsymbol{P}}(e^{i\theta})$, for some polynomial matrix $\tilde{\boldsymbol{P}}(z)$ of degree no more than L. Moreover, $I - \tilde{\boldsymbol{P}}(e^{i\theta})^\dagger \tilde{\boldsymbol{P}}(e^{i\theta})$ is positive semidefinite for all $|z| = 1$. By the *Polynomial Matrix Spectral Factorization Theorem* [43, 44], there is a polynomial matrix $\tilde{\boldsymbol{Q}}(e^{i\theta})$ of degree no more than L such that

$$I - \tilde{\boldsymbol{P}}(e^{i\theta})^\dagger \tilde{\boldsymbol{P}}(e^{i\theta}) = \tilde{\boldsymbol{Q}}(e^{i\theta})^\dagger \tilde{\boldsymbol{Q}}(e^{i\theta}). \tag{31}$$

Write

$$e^{-i\frac{L\theta}{2}}\tilde{\boldsymbol{Q}}(e^{i\theta}) = \boldsymbol{P}_1\left(\cos\frac{\theta}{2}\right) + \sin\frac{\theta}{2}\boldsymbol{Q}_1\left(\cos\frac{\theta}{2}\right), \tag{32}$$

then $\boldsymbol{P}_1(x)$ is a matrix of L-polynomials and $\boldsymbol{Q}_1(x)$ is a matrix of $(L-1)$-polynomials. Since,

$$\begin{aligned}&\boldsymbol{Q}(e^{i\theta})^\dagger \boldsymbol{Q}(e^{i\theta}) - \boldsymbol{P}_1(x)^\dagger \boldsymbol{P}_1(x) - (1-x^2)\boldsymbol{Q}_1(x)^\dagger \boldsymbol{Q}_1(x) \\ =&\sin\frac{\theta}{2}\left[\boldsymbol{P}_1(x)^\dagger \boldsymbol{Q}_1(x) + \boldsymbol{Q}_1(x)^\dagger \boldsymbol{P}_1(x)\right],\end{aligned} \tag{33}$$

in which the left hand side is even about θ and the right hand side is odd, thus both are zero. As a result, Eq. (30) holds. Finally, the proof is completed by Lemma 4. □

Like the original QSVT algorithm, for Hermitian matrix input A, one can block-encode polynomial matrix $\boldsymbol{P}(A)$ without definite parity constraints, by splitting the polynomial into even and odd parts, namely $\boldsymbol{P}_e(A)$ and $\boldsymbol{P}_o(A)$ such that $\boldsymbol{P}(A) = \frac{1}{2}(\boldsymbol{P}_e(A) + \boldsymbol{P}_o(A))$, and using *Linear Combination of Unitaries* (LCU) [6] to obtain a block encoding of $\boldsymbol{P}(A)$. To guarentee the nonnegativity of $I - \boldsymbol{P}_e(A)^\dagger \boldsymbol{P}_e(A)$ and $I - \boldsymbol{P}_o(A)^\dagger \boldsymbol{P}_o(A)$, a sufficient condition is that the maximum eigenvalue norm of $\boldsymbol{P}(A)$ is less than $\frac{1}{2}$. If $\boldsymbol{P}(A)$ is of degree no more than L, then the circuit requires L calls to U, $U^\dagger$ and their controlled gates in total.

III. APPLICATION IN QUANTUM AMPLITUDE ESTIMATION

The general problem of quantum amplitude estimation is, given a state preparation operator U that prepares a state $|\psi\rangle = U|\psi_0\rangle$ from an easy-to-obtain state $|\psi_0\rangle$, and a projection operator Π, estimate $x = \langle\psi|\Pi|\psi\rangle$ with the best possible accuracy using N number of queries to U and U^{-1} in total. In the literature there could be different definitions of the amplitude, some like ours [39, 45, 46] and some $\sqrt{\langle\psi|\Pi|\psi\rangle}$ [9]. We use the former definition for convience of establishing theories, and many applications are directly transferable to the latter definition. For example, in the task of estimating the expectation value of an observable A with respect to a state $|\psi\rangle$, where we assume A has all eigenvalues in $[-1, 1]$, then $\langle\mathbf{0}|\langle\psi| U |\mathbf{0}\rangle|\psi\rangle = \langle\psi|A|\psi\rangle$, where U is a block encoding of A in the format Eq. (1), and one can estimate it by applying QAE on the state $(|\mathbf{0}\rangle|\psi\rangle + U|\mathbf{0}\rangle|\psi\rangle)/\sqrt{2}$ and the projector $|+\rangle\langle+| \otimes I$.

In this section, we first show that every QAE circuit that works for any general input has polynomial output probabilities of x, and any valid probability distribution can be achieved by a $U(N)$-QSVT circuit. Then by numerical optimization on achievable polynomials, we calculate the asymptotic bound in several measures of accuracy, closing the gap between the optimal accuracy and existing algorithms in the literature.

A. Achievable Probabilities

Let $P_m(x) = P(m|x)$ denote the probability of obtaining the m-th measurement result when the amplitude is x. To study QAE that works in the most general setting, we call a QAE circuit *valid* if it has a fixed structure with calls to black boxes U and U^{-1} such that each output probability $P_m(x)$ is a function of x only. We call the total number of oracle calls to U and U^{-1} the *degree* of the QAE circuit.

Lemma 5 *Each output probability of a valid QAE circuit of degree N is a polynomial of x of degree no more than N.*

Proof of Lemma 5. Define the single-qubit unitary,

$$W(\theta) := \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}. \tag{34}$$

Consider the QAE problem with state preparation operator $W(\theta)$, initial state $|\psi_0\rangle = |0\rangle$ and projection operator $|0\rangle\langle 0|$, and the target amplitude is $x = \cos^2\frac{\theta}{2}$.

By induction on N, it is easy to see that the quantum state after N calls to $W(\theta)$ and its inverse in total, the quantum state becomes a polynomial vector of $\cos\frac{\theta}{2}$ and $\sin\frac{\theta}{2}$ of degree no more than N, and has parity (N mod 2). Then any projective measurement probability should be of the form $P_1(x)+\sin\theta P_2(x)$, where P_1, P_2 are polynomials of x of degree no more than N,$(N-1)$, respectively.

Substituting θ with $-\theta$, the output probability becomes $P_1(x) - \sin\theta P_2(x)$ as a direct result of variable substitution. Since $W(\theta)$ and $W(-\theta)$ share the same amplitude parameter x and thus have the same outcome probability, we deduct that $P_2 = 0$. Hence, the probability is a polynomial of x. □

As an example, if we apply *amplitude amplification* operator [39],

$$U(I - 2|\psi_0\rangle\langle\psi_0|)U^{-1}(I - 2\Pi), \tag{35}$$

on $U|\psi_0\rangle$ for k times and measure it on $\{\Pi, I - \Pi\}$, the output probability of getting Π is,

$$\sin^2\left(\frac{2k+1}{2}\theta\right) = \frac{1 - T_{2k+1}(2x-1)}{2}, \tag{36}$$

an odd polynomial of x of degree $2k+1$, where T_k is the m-th Chebyshev polynomial of the first kind. This matches the degree of the QAE circuit since each of the N amplitude amplification operators adds the degree by two and an extra one is used for the initial state preparation.

Theorem 6 (Equivalence to $U(N)$-QSVT) *For any polynomials $\{P_m(x)\}$ of degree no more than N and non-negative on $[0,1]$ such that $\sum_m P_m(x) \equiv 1$, there is a choice of $\{V_0, V_1, \cdots\}$ in the $U(N)$-QSVT circuit in FIG. 3 with input $|\mathbf{0}\rangle|\psi_0\rangle$, such that by measuring all qubits in the first register, the probability of the m-th outcome is exactly $P_m(x)$.*

Proof of Theorem 6. Replacing x with $\cos\frac{\theta}{2}$ in the Lemma 6 of [2], there is a pair of N-polynomial A_m and $(N-1)$-polynomial B_m such that,

$$P_m\left(\cos^2\frac{\theta}{2}\right) = A_m\left(\cos\frac{\theta}{2}\right)^2 + \sin^2\frac{\theta}{2}B_m\left(\cos\frac{\theta}{2}\right)^2. \tag{37}$$

Write

$$U|\psi_0\rangle = \cos\frac{\theta}{2}\left|\tilde{\psi}_0\right\rangle + \sin\frac{\theta}{2}\left|\tilde{\psi}_1\right\rangle, \tag{38}$$

where $\left|\tilde{\psi}_0\right\rangle \in \tilde{\mathcal{H}}_0$ and $\left|\tilde{\psi}_1\right\rangle \in \tilde{\mathcal{H}}_1$. Define,

$$|\psi_1\rangle = U^{-1}\left[-\sin\frac{\theta}{2}\left|\tilde{\psi}_0\right\rangle + \cos\frac{\theta}{2}\left|\tilde{\psi}_1\right\rangle\right], \tag{39}$$

then $|\psi_1\rangle$ is orthogonal to $|\psi_0\rangle$. Let $\mathcal{H}_0$ be the subspace spanned only by $|\psi_0\rangle$, and $\mathcal{H}_1$ its orthogonal complement. Let $\Pi', \Pi_1, \Pi, \tilde{\Pi}_1$ be the projection operators onto $\mathcal{H}_0, \mathcal{H}_1, \tilde{\mathcal{H}}_0, \tilde{\mathcal{H}}_1$, respectively. Under the basis $(|\psi_0\rangle, |\psi_1\rangle) \to (\left|\tilde{\psi}_0\right\rangle, \left|\tilde{\psi}_1\right\rangle)$, the matrix representation of U is

$$U = \begin{array}{c} \\ \\ \end{array}\begin{array}{cc} |\psi_0\rangle & |\psi_1\rangle \\ \end{array}$$
$$U = \left(\begin{array}{cc} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{array}\right)\begin{array}{l} \left|\tilde{\psi}_0\right\rangle \\ \left|\tilde{\psi}_1\right\rangle \end{array}. \tag{40}$$

In this way, a possible destination quantum state satisfying the outcome probability requirement can be,

$$\sum_{m=0}^{N-1}|m\rangle\left[A_m\left(\cos\frac{\theta}{2}\right)\left|\tilde{\psi}_0\right\rangle + \sin\frac{\theta}{2}B_m\left(\cos\frac{\theta}{2}\right)\left|\tilde{\psi}_1\right\rangle\right], \tag{41}$$

if N is odd, or with $\left|\tilde{\psi}_0\right\rangle, \left|\tilde{\psi}_1\right\rangle$ replaced with $|\psi_0\rangle, |\psi_1\rangle$ if N is even, which can be achieved by the $U(N)$-QSVT using Theorem 5. □

B. Asymptotic Bound

Though it is long known that QAE can achieve the Heisenberg scaling $\Delta x = O(N^{-1})$, the optimal accuracy of QAE is not well understood. In this section, we make use of the 1-1 corespondance between QAE and achievable polynomial probabilities, to calculate the asymptotic accuracy bound of QAE by numerical optimization. Throughout the section we assume x is uniformly distributed on $[0,1]$. We use two measures of accuracy, the standard deviation error Δx defined as,

$$(\Delta x)^2 = \sum_m \int_0^1 P_m(x)(x - \tilde{x}_m)^2 \mathrm{d}x, \tag{42}$$

which sums over all possible measurement results m, where $\tilde{x}_m$ is the Bayesian estimation output if the m-th outcome is obtained, and the error bound ϵ_δ at given confidence level $1-\delta$ defined as,

$$\sum_m \int_0^1 P_m(x)\mathbb{I}_{|x-\tilde{x}_m|>\epsilon_\delta}\mathrm{d}x = \delta, \tag{43}$$

where $\mathbb{I}$ is the indicator function. In particular, we show that the lower bound with standard deviation error is tight by giving an explicit construction of probabilities with the optimal asymptotic accuracy.

Empirical Claim 1 *For valid QAE circuits of degree N and standard deviation error Δx, as $N \to \infty$, we have the asymptotic lower bound,*

$$\Delta x \gtrsim \frac{\pi}{\sqrt{6}N}. \tag{44}$$

Empirical Claim 2 *For valid QAE circuits of degree N and window error δ, we have the asymptotic lower bound,*

$$\epsilon_{0.1} \gtrsim 1.63N^{-1}, \epsilon_{0.05} \gtrsim 2.09N^{-1}, \text{ and } \epsilon_{0.01} \gtrsim 3.03N^{-1}. \tag{45}$$

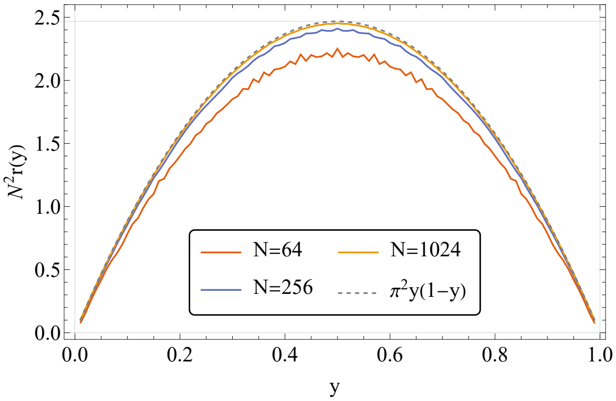

FIG. 4: Numerical calculation of $r(y)$ for different N. As N goes large, $N^2 \cdot r(y)$ approximates $\pi^2 y(1-y)$, shown as the outermost dashed curve.

Proof of Claim 1. We first show that for any polynomial $P(x)$ of degree no more than N and non-negative on $[0,1]$,

$$\int_0^1 P(x)(x-y)^2 \mathrm{d}x \gtrsim \frac{\pi^2}{N^2} y(1-y) \int_0^1 P(x)\mathrm{d}x. \tag{46}$$

There is a series of $\{A_m\}_{k=0}^N$ such that [47],

$$P\left(\cos^2\frac{\theta}{2}\right) = \left|\sum_{k=0}^N A_m e^{ik\theta}\right|^2, \tag{47}$$

or,

$$P(x) = b_0 + 2\sum_{k=1}^N a_k T_k(2x-1), \tag{48}$$

where T_k is m-th the Chebyshev polynomial of the first kind, and $a_k = \sum_{l=0}^{N-k} a_l a_{l+k}$.

Define,

$$\begin{aligned} r(y) &= \min_P \frac{\int_0^1 P(x)(x-y)^2 \mathrm{d}x}{\int_0^1 P(x)\mathrm{d}x} \\ &= \min_{\boldsymbol{a}} \frac{\sum_{j,k} a_j a_k \int_0^1 (x-y)^2 T_{|j-k|}(2x-1)\mathrm{d}x}{\sum_{j,k} a_j a_k \int_0^1 T_{|j-k|}(2x-1)\mathrm{d}x}. \end{aligned} \tag{49}$$

where the minimization is over all nonzero polynomials P of degree no more than N and non-negative on $[0,1]$, or nonzero vectors $\boldsymbol{a} = (a_1, a_2, \cdots)$. Both the numerator and the denominator are quadratic forms of $\boldsymbol{a}$, and the minimum is achieved by the smallest generalized eigenvalue of the pair of coefficient matrices [48].

We calculate the minimum generalized eigenvalue numerically [49] for different N and y, as shown in FIG. 4. The result shows that $r(y) \sim \frac{\pi^2}{N^2} y(1-y)$ holds asymptotically.

The output probabilities $\{P_m(x)\}$ are polynomials of x of degree no more than N by Lemma 5, such that $\sum_k P_m(x) \equiv 1$. Fixing $\{P_m(x)\}$, we assume to use the Bayesian estimation output,

$$\tilde{x}_m = \frac{\int_0^1 P_m(x) x \mathrm{d}x}{\int_0^1 P_m(x)\mathrm{d}x}, \tag{50}$$

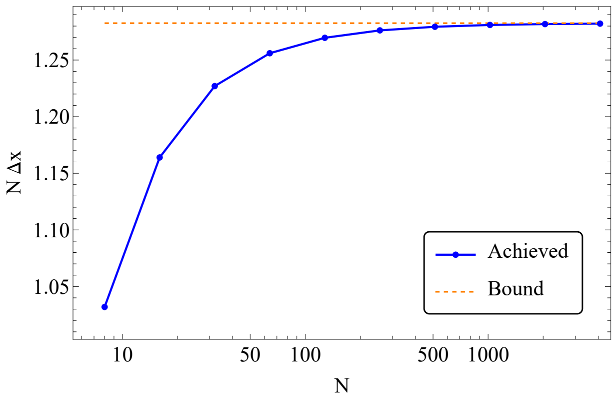

FIG. 5: The standard deviation error of QAE by QPE with sine initial state. As N goes large, the ratio of Δx to $\frac{\pi}{\sqrt{6N}}$ approaches 1. Note that $\Delta x < \frac{\pi}{\sqrt{6N}}$ for finite N does not violate our asymptotic lower bound.

as estimation of x if the m-th outcome is obtained, to minimize the square cost.

On one hand,

$$\begin{aligned} (\Delta x)^2 =& \sum_m \int_0^1 P_m(x)(x^2 - 2x\tilde{x}_m + \tilde{x}_m^2)\mathrm{d}x \\ =& \int_0^1 \left[\sum_m P_m(x)\right] x^2 \mathrm{d}x - \sum_m \tilde{P}_m \tilde{x}_m^2 \\ =& \frac{1}{3} + \left[\sum_m \tilde{P}_m \tilde{x}_m (1-\tilde{x}_m) - \sum_m \tilde{P}_m \tilde{x}_m\right] \\ =& -\frac{1}{6} + \sum_m \tilde{P}_m \tilde{x}_m (1-\tilde{x}_m), \end{aligned} \tag{51}$$

in which $\sum_m \tilde{P}_m \tilde{x}_m = \int_0^1 [\sum_m P_m(x)] x \mathrm{d}x = \frac{1}{2}$.

On the other hand,

$$\begin{aligned} (\Delta x)^2 \geq& \sum_m r(\tilde{x}_m) \int_0^1 P_m(x)\mathrm{d}x \\ \gtrsim& \frac{\pi^2}{N^2} \sum_m \tilde{P}_m \tilde{x}_m (1-\tilde{x}_m). \end{aligned} \tag{52}$$

Finally,

$$(\Delta x)^2 \gtrsim \frac{\pi^2}{N^2}\left((\Delta x)^2 + \frac{1}{6}\right) \gtrsim \frac{\pi^2}{6N^2}. \tag{53}$$

□

A common approach to QAE is to construct a rotation unitary $\mathcal{Q} = U^{-1}(2\Pi - I)U(2\Pi' - I)$, where $\Pi' := |\psi_0\rangle\langle\psi_0|$, with rotation angle θ satisfying $x = \cos^2\frac{\theta}{2}$. Then we use the quantum phase estimation (QPE) algorithm to estimate θ. Suppose we use n ancilla qubits for QPE and let $N = 2^n$. One may use the sine initial state,

$$\sqrt{\frac{2}{N+1}} \sum_{j=0}^{N-1} \sin\left(\frac{j+1}{N+1}\pi\right) |j\rangle, \tag{54}$$

to minimize the standard deviation error of the phase estimation [50]. The probability of the m-th outcome

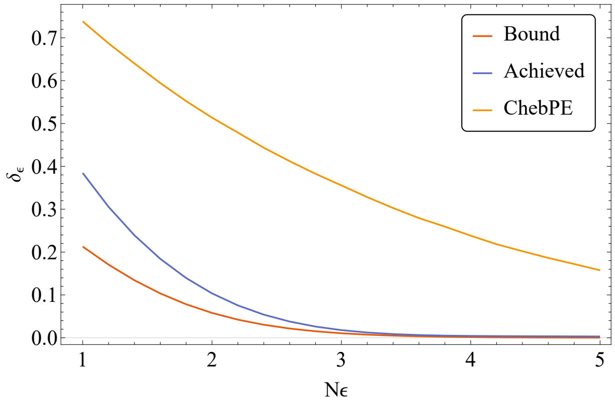

FIG. 6: A comparison among the lower bound $\tilde{\delta}_\epsilon$, the δ given by the ChebPE algorithm and our selected polynomials Eq. (47) in which $A_m = \frac{2}{N+1}\sin\left(\frac{k+1}{N+1}\pi\right)e^{i\frac{2\pi mk}{N}}$ for $m = 0, \cdots, N-1$, labelled as Achieved. The vertical axis gives one minus the confidence level for theoretical results or the frequency of error points for experimental results, and the horizontal axis gives the error bound times N.

is Eq. (47) in which $A_m = \frac{2}{N+1}\sin\left(\frac{k+1}{N+1}\pi\right)e^{i\frac{2\pi mk}{N}}$ for $m = 0, \cdots, N-1$. With the explicit expression of $P_m(x)$, we can calculate the Δx directly [49] by Eq. (42), in which $\tilde{x}_k$ is the Bayesian estimation Eq. (50). The results in FIG. 5 shows that $\Delta x \sim \frac{\pi}{\sqrt{6}N}$. However, it requires $(N-1)$ calls to $\mathcal{Q}$, i.e., $2(N-1)$ calls to U and U^{-1} in total to achieve. As a result, there is an extra double factor away from the lower bound in the QPE approach compared to our $U(N)$-QSVT one, since the probabilities have degrees only half the number of calls. But if one achieves this probability distribution by $U(N)$-QSVT, the asymptotically optimal accuracy can be achieved, thus the bound in Claim 1 is tight.

Similar analysis can be done for the window error to give Claim 2 on the window cost, with proof in Appx. A. We compare the confidence level δ given by the lower bound, our selected polynomials that achieve the lower bound in standard deviation error, and the ChebPE algorithm which is an adaption for the ChebAE algorithm for estimating the amplitude in our definition that achieves the best-known window cost error scaling to our knowledge [9], in which we set parameters $\epsilon = \alpha = 0.05$, in FIG. 6. This time the selected polynomials do not achieve the lower bound, but still gives a better error scaling than the best-known algorithm. More precisely, our selected polynomials give

$$\epsilon_{0.1} \approx 2.02N^{-1}, \epsilon_{0.05} \approx 2.44N^{-1}, \text{ and } \epsilon_{0.01} \approx 3.31N^{-1}. \tag{55}$$

As it does not saturate the lower bound, one may be able to find other polynomials that behave better than ours, and realize them by $U(N)$-QSVT.

IV. DISCUSSION ON MULTI-VARIATE QUANTUM SIGNAL PROCESSING

As another application, in this section we discuss a special case of multi-variate quantum signal processing (M-QSP) in which the variables commute. In this task, we are given access to multiple unitary inputs $U_1, U_2, \cdots, U_n$ and a target polynomial function $f(U_1, U_2, \cdots, U_n)$, and we hope to construct a unitary operator in quantum circuits to realize

$$\begin{pmatrix} f(U_1, U_2, \cdots, U_n) & * \\ * & * \end{pmatrix}. \tag{56}$$

It suffices to study scalar input $\boldsymbol{z} = \{z_1, \cdots, z_n\}$ with each component being a complex number of unit length. Before everything, we introduce some basic arithmetic operations on block encoding.

Lemma 6 (Linear Combination) *Given a set of unitaries $\{U_j\}$ and positive numbers $\{\alpha_j\}$ such that $\sum_j \alpha_j = 1$. Let V be a unitary mapping $|\mathbf{0}\rangle$ to $\sum_j \sqrt{\alpha_j}\,|j\rangle$. Then,*

$$V^\dagger \left(\sum_j |j\rangle\langle j| \otimes U_j\right) V, \tag{57}$$

is a block encoding of $\sum_i \alpha_i U_i$.

This technique is known as the *linear combination of unitaries* (LCU) [42]. In some references $\{\alpha_j\}$ is allowed to be complex, but here we absorb the global phase into $\{U_j\}$ for simplicity. Naturally, if each U_j block-encodes a smaller matrix A_j, then we obtain a block encoding of $\sum_i \alpha_i A_i$.

Lemma 7 (Dot Product) *Given block encoding of two matrices A and B with compatible dimensions to define the dot product AB, says*

$$U\,|\mathbf{0}\rangle\,|\psi\rangle = |\mathbf{0}\rangle\,A\,|\psi\rangle + \left|\mathbf{0}^\perp\right\rangle|\cdots\rangle, \tag{58}$$

$$V\,|\mathbf{0}\rangle\,|\psi\rangle = |\mathbf{0}\rangle\,B\,|\psi\rangle + \left|\mathbf{0}^\perp\right\rangle|\cdots\rangle. \tag{59}$$

Then a block encoding of BA is obtained by,

$$\begin{aligned} & |\mathbf{0}\rangle\,|\mathbf{0}\rangle\,|\psi\rangle \\ \xrightarrow{U[1,3]}\; & |\mathbf{0}\rangle\,|\mathbf{0}\rangle\,A\,|\psi\rangle + \left|\mathbf{0}^\perp\right\rangle|\mathbf{0}\rangle\,|\cdots\rangle \\ \xrightarrow{V[2,3]}\; & |\mathbf{0}\rangle\,|\mathbf{0}\rangle\,BA\,|\psi\rangle \\ & + \left|\mathbf{0}^\perp\right\rangle|\mathbf{0}\rangle\,|\cdots\rangle + |\mathbf{0}\rangle\left|\mathbf{0}^\perp\right\rangle|\cdots\rangle, \end{aligned} \tag{60}$$

where the indices in the square brackets indicate which two registers the unitary is acting on.

We show two approaches to block-encode multi-variate polynomials $p(\boldsymbol{z})$, one by $U(2)$-QSP and the other by $U(N)$-QSP. First, suppose we can write

$$f(\boldsymbol{z}) = \sum_{j=0}^{r-1} \alpha_j \prod_{k=1}^{n} p_{j,k}(z_k), \tag{61}$$

for polynomials $\{p_{j,k}\}$ such that $|p_{j,k}(z)| \leq 1$ for all $|z| = 1$, and positive numbers $\{\alpha_j\}$ such that $\sum_j \alpha_j = 1$. Any polynomial can be written in this form up to some scaling factor. Let $U_{j,k}$ be a block encoding of $p_{j,k}(z)$, then we can first block-encode each product $\prod_k p_{j,k}(z_k)$ by Lemma 7, and then combine them by LCU in Lemma 6. Every multivariate polynomial can be writen in the form of Eq. (61) up to some scaling factor, since we can always express the polynomial as sum of products of monomial terms, though one may find more efficient expressions.

With the tool of $U(N)$-QSP, we have more flexibility in constructing block encoding with the two lemmas. As an example of bivariate polynomials, consider the following function

$$f(z_1, z_2) = \sum_{j=0}^{r-1} p_j(z_1) q_j(z_2), \tag{62}$$

for polynomials $\{p_j, q_j\}$ such that $\sum_j |p_j(z)| \leq 1$ and $\sum_j |q_j(z)| \leq 1$ for all $|z| = 1$. Actually, if we write the target function as a quadratic form $f(z_1, z_2) = Z_1^\top A Z_2$, where $Z_1 = (1, z_1, z_1^2, \cdots)^\top$, $Z_2 = (1, z_2, z_2^2, \cdots)^\top$ and A is a constant matrix, then for any decomposition $A = B^\top C$, $f(z_1, z_2) = (BZ_1)^\top (CZ_2)$, which is equivalent to Eq. (62) when we let $p_j(z_1), q_j(z_2)$ be the j-th component of the vectors BZ_1, CZ_2, respectively. By Theorem 3, we can construct $U(N)$-QSP of the $r \times 1$ matrix $\boldsymbol{P}(z_1)$ and the $1 \times r$ matrix $\boldsymbol{Q}(z_2)$, whose entries are $p_j(z_1)$ and $q_j(z_2)$, respectively. The target function is then equal to the dot product $\boldsymbol{Q}(z_2)\boldsymbol{P}(z_1)$, and can be block-encoded accordingly. Note that the M-QSP by QSP on $U(2)$ is a special case of the M-QSP by QSP on $U(N)$ when writing $f(z_1, z_2) = \sum_j [\sqrt{\alpha_j} p_j(z_1)][\sqrt{\alpha_j} q_j(z_2)]$.

In both schemes, there are constraints on the magnitude of the polynomials. A necessary constraint on block encoding requires that $|f(z_1, z_2)| \leq 1$ for any $|z| = 1$ and $|z_2| = 1$. We can give deterministic answers to the following questions. However, it is not easy to fully characterize achievable functions of M-QSP by QSP on $U(N)$ or $U(2)$, like what has been done in univariate settings.

- Given any bivariate polynomial $f(z_1, z_2)$ that $|f(z_1, z_2)| \leq 1$ for all $|z_1| = 1$ and $|z_2| = 1$, is it achievable with M-QSP by QSP on $U(2)/U(N)$?

- Given any bivariate polynomial $f(z_1, z_2)$ achievable by QSP on $U(N)$, is it also achievable with M-QSP by QSP on $U(2)$?

In Appx. B, we give negative answers to both questions with two counter-examples.

Compared to previous M-QSP frameworks in [37, 38], in which alternative signal inputs of different variables are used to achieve the same goal, our approach guarantees that any function is achievable up to some scaling factor, and the quantum circuit to achieve it can be determined in a linear time. However, our framwork works only for commutable variables, and also non-commutable variables if they appear in a fixed order in the target function. If the variables are non-commutable and appear in any order, for example $f(A, B) = AB - BA$, one may treat it as a tri-variate function $f(A, B, C) = AB - BC$ with $C = A$ and then apply our M-QSP framework, but the efficiency is not guaranteed in more complex target functions. It remains an open question how to give an MQSP framework that works in the most general case where variables are non-commutable and appears in any order in the target function. Our framework may be further integrated with other toolkits, for example the *gadgets* in [37, 51], to inspire more possibilities in quantum algorithms.

V. CONCLUSION AND OUTLOOK

We generalize the framework of quantum signal processing and quantum singular value transformation to $U(N)$ by introducing multiple ancilla qubits, and the phase angles are changed into arbitrary controlled unitary gates correspondingly. As a first application, we show that any output probability in quantum amplitude estimation is a polynomial of the amplitude, and any set of polynomial probabilities summed to one can be achieves with the help of the $U(N)$-QSVT framework. Moreover, by numerical optimization on achievable probabilities, we give empirical lower bounds on the resource cost of quantum amplitude estimation. In particular, the asymptotic bound of standard deviation error is tight as we explicitly show a set of probabilities achieving the bound. The results can be a complement on the grand unification of quantum algorithms [3], in which we generalize the QSP for binary decision problem into multiple one. Finally, we show that the framework can be used to block-encode multi-variate polynomial functions, which can also be achieved by the original quantum signal processing framework on $U(2)$, but our framework extends the set of achievable polynomials.

Future work on QSP and QSVT on $U(N)$ may focus on efficient classical evaluation and the circuit realization of the tunable elements. Just like the evaluation of phase angles in QSP on $U(2)$ [31–33], though the computation is recursive and explicit when all the polynomial entries are given, as shown in the proof of Theorem 4, it remains a computational challenge when not all of them are given, as in the case of Theorem 3.

ACKNOWLEDGEMENT

X.L. and H.L. acknowledges support from the National Natural Science Foundation of China under Grant Nos.62272406, 61932018.

[1] Guang Hao Low and Isaac L Chuang. Optimal hamiltonian simulation by quantum signal processing. *Physical review letters*, 118(1):010501, 2017.

[2] 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.

[3] John M Martyn, Zane M Rossi, Andrew K Tan, and Isaac L Chuang. Grand unification of quantum algorithms. *PRX quantum*, 2(4):040203, 2021.

[4] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019.

[5] Zhiyan Ding, Xiantao Li, and Lin Lin. Simulating open quantum systems using hamiltonian simulations. *arXiv preprint arXiv:2311.15533*, 2023.

[6] Andrew M Childs, Robin Kothari, and Rolando D Somma. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46(6):1920–1950, 2017.

[7] Yulong Dong, Lin Lin, and Yu Tong. Ground-state preparation and energy estimation on early fault-tolerant quantum computers via quantum eigenvalue transformation of unitary matrices. *PRX Quantum*, 3(4):040305, 2022.

[8] Theodore J Yoder, Guang Hao Low, and Isaac L Chuang. Fixed-point quantum search with an optimal number of queries. *Physical review letters*, 113(21):210501, 2014.

[9] Patrick Rall and Bryce Fuller. Amplitude estimation from quantum signal processing. *Quantum*, 7:937, 2023.

[10] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[11] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006.

[12] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011.

[13] Ashley Montanaro. Quantum speedup of monte carlo methods. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 471(2181):20150301, 2015.

[14] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 913–925, 2016.

[15] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 899–912, 2016.

[16] Scott Aaronson. Shadow tomography of quantum states. In *Proceedings of the 50th annual ACM SIGACT symposium on theory of computing*, pages 325–338, 2018.

[17] Hong-Ye Hu, Ryan LaRose, Yi-Zhuang You, Eleanor Rieffel, and Zhihui Wang. Logical shadow tomography: Efficient estimation of error-mitigated observables. *arXiv preprint arXiv:2203.07263*, 2022.

[18] Joran van Apeldoorn, Arjan Cornelissen, András Gilyén, and Giacomo Nannicini. Quantum tomography using state-preparation unitaries. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1265–1318. SIAM, 2023.

[19] Emanuel Knill, Gerardo Ortiz, and Rolando D Somma. Optimal quantum measurements of expectation values of observables. *Physical Review A*, 75(1):012328, 2007.

[20] Ivan Kassal, Stephen P Jordan, Peter J Love, Masoud Mohseni, and Alán Aspuru-Guzik. Polynomial-time quantum algorithm for the simulation of chemical dynamics. *Proceedings of the National Academy of Sciences*, 105(48):18681–18686, 2008.

[21] Masaya Kohda, Ryosuke Imai, Keita Kanno, Kosuke Mitarai, Wataru Mizukami, and Yuya O Nakagawa. Quantum expectation-value estimation by computational basis sampling. *Physical Review Research*, 4(3):033173, 2022.

[22] William J Huggins, Kianna Wan, Jarrod McClean, Thomas E O'Brien, Nathan Wiebe, and Ryan Babbush. Nearly optimal quantum algorithm for estimating multiple expectation values. *Physical Review Letters*, 129(24):240501, 2022.

[23] Sophia Simon, Matthias Degroote, Nikolaj Moll, Raffaele Santagati, Michael Streif, and Nathan Wiebe. Amplified amplitude estimation: Exploiting prior knowledge to improve estimates of expectation values. *arXiv preprint arXiv:2402.14791*, 2024.

[24] Joran van Apeldoorn and András Gilyén. Quantum algorithms for zero-sum games. *arXiv preprint arXiv:1904.03180*, 2019.

[25] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik, and Jeremy L O'brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1):4213, 2014.

[26] Nathan Wiebe, Ashish Kapoor, and Krysta M Svore. Quantum deep learning. *arXiv preprint arXiv:1412.3489*, 2014.

[27] Nathan Wiebe, Ashish Kapoor, and Krysta M Svore. Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning. *Quantum Information & Computation*, 15(3-4):316–356, 2015.

[28] Iordanis Kerenidis, Jonas Landman, Alessandro Luongo, and Anupam Prakash. q-means: A quantum algorithm for unsupervised machine learning. *Advances in neural information processing systems*, 32, 2019.

[29] Haoya Li, Hongkang Ni, and Lexing Ying. On efficient quantum block encoding of pseudo-differential operators. *Quantum*, 7:1031, 2023.

[30] Daan Camps, Lin Lin, Roel Van Beeumen, and Chao Yang. Explicit quantum circuits for block encodings of certain sparse matrices. *SIAM Journal on Matrix Analysis and Applications*, 45(1):801–827, 2024.

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

[32] Lexing Ying. Stable factorization for phase factors of quantum signal processing. *Quantum*, 6:842, 2022.

[33] Yulong Dong, Xiang Meng, K Birgitta Whaley, and Lin Lin. Efficient phase-factor evaluation in quantum signal

processing. *Physical Review A*, 103(4):042419, 2021.

[34] Lorenzo Laneve. Quantum signal processing over su (n): exponential speed-up for polynomial transformations under shor-like assumptions. *arXiv preprint arXiv:2311.03949*, 2023.

[35] Yulong Dong and Lin Lin. Multi-level quantum signal processing with applications to ground state preparation using fast-forwarded hamiltonian evolution. *arXiv preprint arXiv:2406.02086*, 2024.

[36] Guang Hao Low and Yuan Su. Quantum eigenvalue processing. *arXiv preprint arXiv:2401.06240*, 2024.

[37] Zane M Rossi and Isaac L Chuang. Multivariable quantum signal processing (m-qsp): prophecies of the two-headed oracle. *Quantum*, 6:811, 2022.

[38] Balázs Németh, Blanka Kövér, Boglárka Kulcsár, Roland Botond Miklósi, and András Gilyén. On variants of multivariate quantum signal processing and their characterizations. *arXiv preprint arXiv:2312.09072*, 2023.

[39] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

[40] Danial Motlagh and Nathan Wiebe. Generalized quantum signal processing. *arXiv preprint arXiv:2308.01501*, 2023.

[41] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. *arXiv preprint arXiv:1806.01838*, 2018.

[42] Andrew M Childs and Nathan Wiebe. Hamiltonian simulation using linear combinations of unitary operations. *arXiv preprint arXiv:1202.5822*, 2012.

[43] Norbert Wiener and Pesi Masani. The prediction theory of multivariate stochastic processes. *Acta mathematica*, 98(1):111–150, 1957.

[44] Lasha Ephremidze. An elementary proof of the polynomial matrix spectral factorization theorem. *Proceedings of the Royal Society of Edinburgh Section A: Mathematics*, 144(4):747–751, 2014.

[45] Yohichi Suzuki, Shumpei Uno, Rudy Raymond, Tomoki Tanaka, Tamiya Onodera, and Naoki Yamamoto. Amplitude estimation without phase estimation. *Quantum Inf. Process.*, 19(2):1–17, 2020.

[46] Dmitry Grinko, Julien Gacon, Christa Zoufal, and Stefan Woerner. Iterative quantum amplitude estimation. *NPJ Quantum Inf.*, 7:1–6, 3 2021.

[47] Antoni Zygmund. *Trigonometric series*, volume 1. Cambridge university press, 2002.

[48] Benyamin Ghojogh, Fakhri Karray, and Mark Crowley. Eigenvalue and generalized eigenvalue problems: Tutorial. *arXiv preprint arXiv:1903.11240*, 2019.

[49] The source code can be found at https://github.com/helloluxi/oqae.

[50] Wim van Dam, G Mauro D'Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Optimal quantum circuits for general phase estimation. *Physical review letters*, 98(9):090501, 2007.

[51] Zane M Rossi, Jack L Ceroni, and Isaac L Chuang. Modular quantum signal processing in many variables. *arXiv preprint arXiv:2309.16665*, 2023.

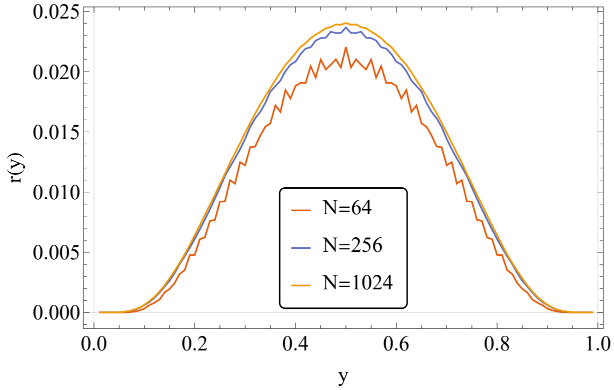

FIG. 7: Numerical caluclation of $r_\epsilon(y)$ for different N with $\epsilon = 3/N$. The results show that when choosing ϵ to have the Heisenberg scaling in N, $r_\epsilon(y)$ converges at each y.

Appendix A: Proof of the empirical claims on asymptotic bound in quantum amplitude estimation

Proof of Claim 2. Define,

$$r_\epsilon(y) = \min_P \frac{\int P(x)\mathbb{I}_{|x-y|>\epsilon}\mathrm{d}x}{\int P(x)\mathrm{d}x}. \tag{A1}$$

Then the window cost is given by,

$$\delta = \sum_k \int P_k(x)\mathbb{I}_{|x-\tilde{x}_m|>\epsilon}\mathrm{d}x \geq \sum_k r_\epsilon(\tilde{x}_m)\tilde{P}_m. \tag{A2}$$

By similar numerical calculation on generalized eigenvalues, we observe that when ϵ scales as N^{-1}, the window cost tends to a constant, as shown in FIG. 7. This illustrates a different aspect of the Heisenberg scaling in QAE. Based on the empirical observation that $r_\epsilon(y)$ is continuous in y and upper bounded by $r_\epsilon\left(\frac{1}{2}\right)$,

$$\begin{aligned}
&\left|\int_0^1 r_\epsilon(y)\mathrm{d}y - \sum_k r_\epsilon(\tilde{x}_m)\tilde{P}_m\right| \\
=&\left|\sum_k \int_0^1 [r_\epsilon(y) - r_\epsilon(\tilde{x}_m)]P_k(x)\mathrm{d}x\right| \\
\leq&\left|\sum_k \int_0^1 [r_\epsilon(y) - r_\epsilon(\tilde{x}_m)]P_k(x)\mathbb{I}_{|x-\tilde{x}_m|\leq\epsilon}\mathrm{d}x\right| \\
+&\left|\sum_k \int_0^1 [r_\epsilon(y) - r_\epsilon(\tilde{x}_m)]P_k(x)\mathbb{I}_{|x-\tilde{x}_m|>\epsilon}\mathrm{d}x\right| \\
\leq& \max_{k,|y-\tilde{x}_m|\leq\epsilon} |r_\epsilon(y) - r_\epsilon(\tilde{x}_m)| \\
+&r_\epsilon\left(\frac{1}{2}\right)\sum_k \int_0^1 P_k(x)\mathbb{I}_{|x-\tilde{x}_m|>\epsilon}\mathrm{d}x \\
\to& r_\epsilon\left(\frac{1}{2}\right)\delta,
\end{aligned} \tag{A3}$$

So asymptotically,

$$\delta \gtrsim \frac{\int_0^1 r_\epsilon(y)\mathrm{d}y}{1 + r_\epsilon\left(\frac{1}{2}\right)} =: \tilde{\delta}_\epsilon. \tag{A4}$$

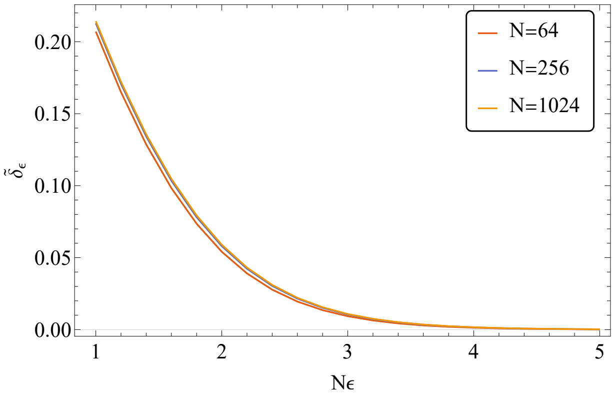

FIG. 8: Numerical caluclation of $\tilde{\delta}_\epsilon$ in Eq. (A4) for different N.

We perform numerical calculation on $\tilde{\delta}_\epsilon$ for different N, as shown in FIG. 8. By numerical root search with $N = 1024$, which is computationally feasible and close enough to the limit, we obtain Eq. (45). □

Appendix B: Two counter-examples regarding bivariate QSP

First, we show a counter-example of a bivariate function that has absolute values bounded by one but cannot be realized with M-QSP by QSP on $U(2)$. Consider,

$$F(z_1, z_2) = z_1 z_2 - \frac{(1-z_1)^2(1-z_2)^2}{16}. \tag{B1}$$

The magnitude constraint is satisfied since

$$|F(z_1, z_2)| = \left|1 - \frac{(1-\mathrm{Re}\, z_1)(1-\mathrm{Re}\, z_2)}{4}\right| \le 1, \tag{B2}$$

for all $|z_1| = 1$ and $|z_2| = 1$. In the set $S = \{(z_1, z_2) : z_1 = 1 \text{ or } z_2 = 1\}$, $|F(z_1, z_2)| = 1$. If $F(z_1, z_2) = \sum_j p_j(z_1) q_j(z_2)$, such that $\sum_j |p_j(z)|^2 \le 1$ and $\sum_j |q_j(z)|^2 \le 1$ for all $|z| = 1$, then on S, the Cauchy inequality

$$|F(z_1, z_2)|^2 \le \sum_j |p_j(z_1)|^2 \sum_j |q_j(z_2)|^2, \tag{B3}$$

is saturated, thus $p_j(z_1) = c q_j(z_2)^*$ for each j and a common unit complex constant c. Actually, for any $|z_1| = |z_2| = 1$, since $(z_1, 1), (z_2, 1) \in S$, $p_j(z_1) = c q_j(i)^* = p_j(z_2)$. Therefore, each $p_j(z_1)$ is constant on the unit complex circle, thus $F(z_1, z_2)$ is independent of z_1, which is a contradiction.

Next, we show a counter-example of bivariate polynomial that can be realized with M-QSP by QSP on $U(N)$ but not by QSP on $U(2)$, to show that M-QSP by QSP on $U(N)$ can enlarge the set of achievable functions. Consider,

$$F(z_1, z_2) = \sum_{j=0}^{n-1} B(z_1 w_j^*) B(z_2 w_{\mathcal{P}[j]}^*) \tag{B4}$$

where $\mathcal{P}$ is a permutation of $\{0, 1, \cdots, n-1\}$, and

$$B(z) = \frac{1}{n} \sum_{j=0}^{n-1} z^j. \tag{B5}$$

It is achievable with M-QSP by QSP on $U(N)$, in which $p_j(z_1) = B(z_1 w_j^*)$ and $q_j(z_2) = B(z_2 w_{\mathcal{P}[j]}^*)$. However, suppose it is also achievable with M-QSP by QSP on $U(2)$ for some polynomials $\{p_j, q_j\}$ such that $|p_j(z)| \le 1$ and $|q_j(z)| \le 1$ for all $|z| = 1$, and each $\alpha_j > 0$. Then, that $F(w_j, w_{\mathcal{P}[j]}) = 1$ for all j implies that $p_k(w_j) = q_k(w_{\mathcal{P}[j]})^*$ and $|p_k(w_j)| = |q_k(w_{\mathcal{P}[j]})| = 1$ for all j, k. Note that $z^n(|p_j(z)|^2 - 1)$ is a polynomial of degree at most $(2n-1)$ but have $(2n)$ algebraic zeros, i.e., double zero at each n-th root of unity, thus is a zero polynomial. So each $|p_j(z)|^2 \equiv 1$ on $|z| = 1$ and thus should be of the form $p_j(z) = \alpha z^\beta$ for some unit-length complex α_j and integer β_j, and so is each q_j. Picking out the k that $p_k(z_1) = z_1$ with coefficient absorbed into q_k, among all $n!$ possible permutations $\mathcal{P}$, there are at most n^2 permutations with $\alpha \in \{1, e^{i\frac{2\pi}{n}}, \cdots, e^{i\frac{2\pi(n-1)}{n}}\}$ and $\beta \in \{0, 1, \cdots, n-1\}$ that is necessary for $p_k(w_j) = q_k(w_{\mathcal{P}[j]})^*$ for all j, causing a contradiction.