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

arXiv:2408.01439v4 [quant-ph] 25 Mar 2026

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 provide a comprehensive characterization of achievable polynomial matrices and give recursive algorithms to construct the quantum circuits that realize desired polynomial transformations. As three example applications, we propose a framework to realize bi-variate polynomial functions, demonstrate N-interval decision achieving $\mathcal{O}(d)$ query complexity with a $\log_2 N$ improvement over iterative $U(2)$-QSP requiring $\mathcal{O}(d \log_2 N)$ queries, and present a quantum amplitude estimation algorithm achieving the Heisenberg limit without adaptive measurements.

Contents

1 Introduction 1

2 Theories 2
- 2.1 Review of Quantum Signal Processing and Quantum Singular Value Transformation 2
- 2.2 $U(N)$-Quantum Signal Processing . 4
- 2.3 $U(N)$-Quantum Singular Value Transformation 7

3 Applications 9
- 3.1 Bi-variate Quantum Signal Processing 9
- 3.2 Multi-interval Decision 11
- 3.3 Quantum Amplitude Estimation . 13

4 Conclusion and Outlook 16

Acknowledgement 16

Code Availability 16

References 16

1 Introduction

Quantum Signal Processing (QSP) is a powerful tool for building quantum algorithms, capable of unifying many other existing algorithms [1, 2, 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 Transformation (QSVT) [2], another framework derived from QSP, extends the application to polynomial transformations of singular value of even non-square matrices. QSP-based quantum algorithms have been developed for various tasks, such as Hamiltonian simulation [1, 4, 5], linear system solving [6], ground state preparation [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, 11, 12] and has direct applications in numerical integration [13], quantum tomography [14, 15, 16, 17, 18], overlap and expectation value estimation in quantum simulation [19, 20, 21, 22, 23], Gibbs sampling [24], variational quantum algorithms and

quantum machine learning [25, 26, 27, 28]. Recent research in QSP theories has focused on efficient realization of block encoding [29, 30], classical evaluation of phase angles [31, 32, 33], and generalization [34, 35, 36, 37, 38]. Experiments have also been conducted to realize QSP on a noisy quantum computer [39, 40].

Meanwhile, the original framework of QSP has some restrictions that limit its applicability. On the mathematical side, the original framework utilizes a series of parameterized $U(2)$ 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 multiple polynomials at once if we use a sequence of parameterized $U(N)$ elements instead of $U(2)$ elements. On the practical side, realizing multiple target functions simultaneously is essential for quantum algorithms like the quantum phase estimation (QPE) and quantum amplitude estimation (QAE) algorithms [41], where different measurement outcomes must correspond to different functions that collectively partition the domain of interest. In addition, by expanding the toolkit in manipulating matrices in quantum computers, QSP and QSVT on $U(N)$ can also help us in more complicated tasks like the multivariate 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, Laneve [34] studied the generalization of QSP over $SU(N)$, which realizes state preparation for N-dimensional outputs by preparing the state $\sum_m P_m(z)\,|m\rangle$ from $|0\rangle$, with applications to quantum phase estimation. Our framework on $U(N)$ is more general: Laneve's result corresponds to the special case of our Theorem 4 where $\boldsymbol{P}(z)$ is a $N\times 1$ polynomial block, whereas we provide a complete theory for arbitrary $N\times N$ polynomial matrix blocks, enabling full exploitation of the $U(N)$ structure in all three applications demonstrated in this work.

In this paper, we establish a complete theory of QSP and QSVT on $U(N)$ with multiple outputs block encoded in a single unitary. Given any mathematically permissible set of target polynomials, we provide a recursive procedure to determine the sequence of $U(N)$ circuit elements that realizes them. Compared to the $U(2)$ framework, our $U(N)$ theory requires new perspectives on quantum circuits and additional mathematical tools from matrix theory. We demonstrate three key applications: (i) bi-variate polynomial functions with an expanded range of achievable polynomials, (ii) multi-interval decision with an $O(\log_2 N)$ reduction in query complexity, and (iii) quantum amplitude estimation achieving the Heisenberg limit without adaptive measurements. A graphical summary is given in FIG. 1.

The paper is organized as follows. Sec. 2 reviews fundamental results on uni-variate QSP with single block encoding, then generalizes to $U(N)$ for both QSP-U and QSVT, establishing the main theorems on achievable polynomial sets. We then demonstrate three key applications where $U(N)$-QSP provides concrete advantages. Sec. 3.1 presents bi-variate quantum signal processing that leverages product structures to realize bi-variate polynomial functions with practical advantages over naive decomposition approaches. Sec. 3.2 demonstrates multi-interval decision with $\mathcal{O}(d)$ query complexity, providing a factor of $\log_2 N$ improvement over the $\mathcal{O}(d\log_2 N)$ complexity required by iterative $U(2)$-QSP methods. Sec. 3.3 shows that QAE measurement outputs correspond to polynomial transformations on $U(N)$, achieving Heisenberg-limited precision in a single non-adaptive measurement round. Sec. 4 provides conclusions and future research directions.

2 Theories

In this section, we first briefly review the fundamental results about QSP in Sec. 2.1. Then, in Sec. 2.2 and Sec. 2.3, we first define the generalization on $U(N)$, then construct a quantum circuit with parameterized parts that help achieving different target functions, and finally state and prove the achievable polynomial sets by the circuit.

2.1 Review of Quantum Signal Processing and Quantum Singular Value Transformation

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

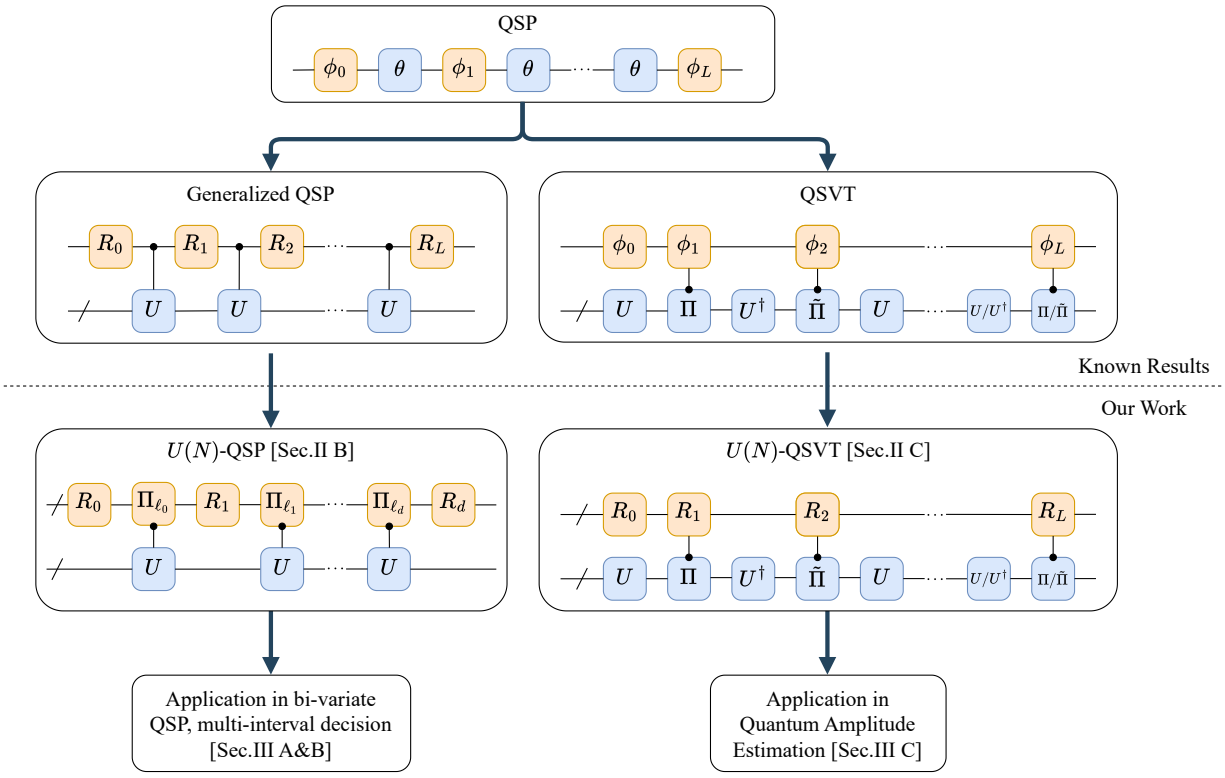


Figure 1: A summary of our contributions in the paper. The orange quantum gates are for parameterized unitaries or projectors, while the blue gates are for fixed input variables.

unitary U such that,

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

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 unitary 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, 42]. A fundamental result in QSP-U is as follows.

Theorem 1 (Generalized QSP [42]) *Given any polynomial $P(z)$ of degree d s.t. $|P(z)| \leq 1, \forall |z| = 1$. Then one can block-encode $P(U)$ using d calls to controlled-U for any unitary matrix input U.*

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,

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

where d is the number of calls to U and $U^\dagger$ in total, and $A = \sum_j \lambda_j |\psi_j\rangle\langle\tilde{\psi}_j|$ for two orthogonal sets $\{|\psi_j\rangle\}, \{|\tilde{\psi}_j\rangle\}$ and $\lambda_j \in \mathbb{R}$, and P naturally subjects to the parity condition that $P(-x) = (-1)^d P(x)$. 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 (QSVT [2]) *Given any polynomial $P(z)$ satisfying,*

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

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

Compared to QSP-U, it has inherent 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 is well-defined 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 these two problems, we can utilize the linear combination of unitaries (LCU) [43], given additional access to controlled U and U^{-1}.

2.2 $U(N)$-Quantum Signal Processing

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

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

For this task, we construct a quantum circuit in FIG. 2, parameterized by arbitrary unitary operators $R_0, R_1, \ldots, R_d \in U(N)$ acting on the ancilla register. The circuit alternates between these unitaries and controlled-U operations, where the control is based on computational basis projectors. This structure generalizes the standard $U(2)$-QSP, which uses single-qubit unitaries

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

with $|1\rangle\langle 1|$-controlled U gates interleaved between them.

In the $U(N)$ generalization, we use N-dimensional ancilla systems where $N = 2^n$ for n ancilla qubits. The controlled operations are defined with respect to computational basis projectors: specifically, the Π_ℓ-controlled U gate is

$$C_{\Pi_\ell}(U) := \Pi_\ell \otimes U + (I - \Pi_\ell) \otimes I, \tag{5}$$

where

$$\Pi_\ell := \sum_{j=0}^{\ell-1} |j\rangle\langle j|. \tag{6}$$

For example, $C_{\Pi_N}(U)$ is simply the uncontrolled U gate, and $C_{\Pi_{N/2}}(U)$ is a single qubit controlled U gate.

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

Lemma 3 ($U(N)$-QSP, forward) *Using d calls to a unitary U, the quantum circuit in FIG. 2 implements the unitary operation,*

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

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

Proof of Lemma 3. The proof proceeds by induction on d. For $d = 0$, the circuit consists only of $R_0 \otimes I$, so P_{jk} is the constant function equal to the (j,k)-th entry of R_0.

For the inductive step, assume the lemma holds for $d-1$, meaning the circuit up to the $(d-1)$-th controlled-U implements $\boldsymbol{P}(U) = \sum_{l=0}^{d-1} \tilde{P}_l \otimes U^l$ for some constant matrices $\{\tilde{P}_l\}$. Applying R_d on the ancilla register followed by $C_{\Pi_d}(U)$ gives

$$\begin{aligned} &(R_d \otimes I) C_{\Pi_d}(U) \boldsymbol{P}(U) \\ =&R_d \Pi_{\ell_d} \otimes U\boldsymbol{P}(U) + R_d(I - \Pi_{\ell_d}) \otimes \boldsymbol{P}(U), \end{aligned} \tag{8}$$

which expands to polynomials of degree no more than d in U. □

Theorem 4 ($U(N)$-QSP, backward) *Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z)$ of degrees no more than d, such that $\boldsymbol{P}(z)$ has all singular values in $[0,1]$ whenever $|z| \le 1$. Then one can construct a quantum circuit with d calls to controlled-U to implement a block encoding of $\boldsymbol{P}(U)$, as defined in Eq. (3).*

Before the proof of Theorem 4, we first prove a special case where $\boldsymbol{P}(z)$ is not a partial block of a bigger unitary, but the entire unitary matrix.

Lemma 5 ($U(N)$-QSP for full unitary) *Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z)$ that is unitary for all $|z| \le 1$. Then one can determine the parameters $R_0, R_1, \ldots, R_d \in U(N)$ in FIG. 2 to implement the unitary transformation $\boldsymbol{P}(U)$.*

Proof of Lemma 5. We use induction on d to prove the lemma.

For $d = 0$, each entry of Eq. (7) is constant, so we simply set R_0 to be the target unitary. For the inductive step, assume the lemma

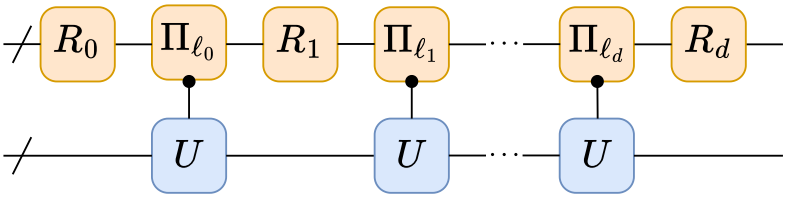


Figure 2: The quantum circuit for $U(N)$-QSP, parameterized by arbitrary unitaries $R_0, R_1, \ldots, R_d \in U(N)$ acting on an N-dimensional ancilla register. The circuit uses d applications of controlled-U operations, where $C_{\Pi_\ell}(U) := \sum_{j=0}^{\ell-1} |j\rangle\langle j| \otimes U + \sum_{j=\ell}^{N-1} |j\rangle\langle j| \otimes I$ applies U when the ancilla is in computational basis states $|0\rangle$ through $|\ell-1\rangle$.

holds for degree $d-1$. We show that for degree d, we can always find R_d and a computational basis projector $\Pi_d = \sum_{j=0}^{\ell-1} |j\rangle\langle j|$ such that $C_{\Pi_d}(U^{-1})(R_d \otimes I)\boldsymbol{P}(U)$ is of the form Eq. (7) with degree no more than $d-1$.

Write $\boldsymbol{P}(U) = \sum_{l=0}^{d} \tilde{P}_l \otimes U^l$. From the unitarity condition $\boldsymbol{P}(U)^\dagger \boldsymbol{P}(U) = I$, examining the coefficient of U^d gives $\tilde{P}_0^\dagger \tilde{P}_d = 0$, showing that the column spaces of $\tilde{P}_0$ and $\tilde{P}_d$ are orthogonal. Let $r_{\tilde{P}_d}$ and $r_{\tilde{P}_0}$ be the ranks of $\tilde{P}_d$ and $\tilde{P}_0$ respectively. Then we have

$$r_{\tilde{P}_d} + r_{\tilde{P}_0} \leq N. \tag{9}$$

Therefore, we can pick a basis $\{|\psi_j\rangle\}$ of $\mathbb{C}^N$ such that the first $r_{\tilde{P}_d}$ basis vectors span the column space of $\tilde{P}_d$, and the last $r_{\tilde{P}_0}$ basis vectors span the column space of $\tilde{P}_0$. Picking any

$$r_{\tilde{P}_d} \leq \ell_d \leq N - r_{\tilde{P}_0}, \tag{10}$$

and let

$$R_d = \sum_{j=0}^{N-1} |\psi_j\rangle\langle j| \,. \tag{11}$$

Then,

$$\begin{aligned} &C_{\Pi_d}(U^{-1})({R_d}^{-1} \otimes I)\boldsymbol{P}(U) \\ &= \sum_{l=0}^{d} \left[\Pi_d {R_d}^{-1} \tilde{P}_l \otimes U^{l-1} + (I - \Pi_d){R_d}^{-1}\tilde{P}_l \otimes U^l\right] \\ &= \sum_{l=0}^{d-1} \left[\Pi_d {R_d}^{-1} \tilde{P}_{l+1} + (I - \Pi_d){R_d}^{-1}\tilde{P}_l\right] \otimes U^l, \end{aligned} \tag{12}$$

where in the last equation the degree-d term vanishes since $(I - \Pi_d){R_d}^{-1}\tilde{P}_d = 0$, and the degree-$(-1)$ term vanishes since $\Pi_d {R_d}^{-1}\tilde{P}_0 = 0$.

By induction, this provides a constructive algorithm to determine $R_0, R_1, \ldots, R_d$. □

Proof of Theorem 4. Since $I - \boldsymbol{P}(z)^\dagger \boldsymbol{P}(z)$ is positive semidefinite on $|z| = 1$, by the *Polynomial Matrix Spectral Factorization Theorem* [44, 45], there is a polynomial matrix $\boldsymbol{Q}(z)$ of degree no more than d such that,

$$I - \boldsymbol{P}(z)^\dagger \boldsymbol{P}(z) \;=\; \boldsymbol{Q}(z)^\dagger \boldsymbol{Q}(z). \tag{13}$$

Next, we construct a polynomial matrix block $\boldsymbol{R}(z)$ such that,

$$\begin{bmatrix} \boldsymbol{P}(z) & \boldsymbol{R}(z) \\ \boldsymbol{Q}(z) & \end{bmatrix} \tag{14}$$

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

$$\begin{aligned} &\begin{bmatrix} \boldsymbol{P}(z) & \boldsymbol{R}(z) \\ \boldsymbol{Q}(z) & \end{bmatrix} \begin{bmatrix} \boldsymbol{P}(z)^\dagger & \boldsymbol{Q}(z)^\dagger \\ \boldsymbol{R}(z)^\dagger & \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{P}(z) \\ \boldsymbol{Q}(z) \end{bmatrix} \begin{bmatrix} \boldsymbol{P}(z)^\dagger & \boldsymbol{Q}(z)^\dagger \end{bmatrix} + \boldsymbol{R}(z)\boldsymbol{R}(z)^\dagger = I, \end{aligned} \tag{15}$$

Again, this is always possible since

$$I - \begin{bmatrix} \boldsymbol{P}(z) \\ \boldsymbol{Q}(z) \end{bmatrix} \begin{bmatrix} \boldsymbol{P}(z)^\dagger & \boldsymbol{Q}(z)^\dagger \end{bmatrix} \tag{16}$$

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

$$\begin{bmatrix} \boldsymbol{P}(z)^\dagger & \boldsymbol{Q}(z)^\dagger \end{bmatrix} \begin{bmatrix} \boldsymbol{P}(z) \\ \boldsymbol{Q}(z) \end{bmatrix} = I \tag{17}$$

from Eq. (13) implies that

$$\begin{bmatrix} \boldsymbol{P}(z) \\ \boldsymbol{Q}(z) \end{bmatrix} \begin{bmatrix} \boldsymbol{P}(z)^\dagger & \boldsymbol{Q}(z)^\dagger \end{bmatrix} \tag{18}$$

is identity in some subspace. Finally,

$$\begin{bmatrix} \boldsymbol{P}(U) & \boldsymbol{R}(U) \\ \boldsymbol{Q}(U) & \end{bmatrix} \tag{19}$$

is a block encoding of $\boldsymbol{P}(U)$ and by Lemma 5, it can be implemented as desired. □

Theorem 4 is a generalization of the results in [42], in which only one ancilla qubit is used, and the corresponding $\boldsymbol{P}(z)$ contains a single entry $p(z)$, with prerequisites $|p(z)| \leq 1$ for all $|z| = 1$.

To find the circuit parameters in Theorem 4 given only the $\boldsymbol{P}(z)$ block, it is sufficient to find

only $\boldsymbol{Q}(z)$ in Eq. (13) using the algorithm described by the constructive proof in [45] and ignore the $\boldsymbol{R}(z)$ block. To see this, we merge $\boldsymbol{Q}(z)$ into $\boldsymbol{P}(z)$ and write

$$\boldsymbol{P}(z) = \sum_{l=0}^{d} \begin{bmatrix} \tilde{P}_l & * \end{bmatrix} z^l, \tag{20}$$

where $*$ corresponds to the $\boldsymbol{R}(z)$ block in Eq. (14) that we no longer need here.

Similar to the proof of Lemma 5, the constraint $\boldsymbol{P}(U)^\dagger \boldsymbol{P}(U) = I$ gives

$$\begin{bmatrix} \tilde{P}_0^\dagger \\ * \end{bmatrix} \begin{bmatrix} \tilde{P}_d & * \end{bmatrix} = 0, \tag{21}$$

which implies that $\tilde{P}_0^\dagger \tilde{P}_d = 0$. Let M be the number of columns of $\boldsymbol{P}(z)$, then there is a $M \times M$ projector $\tilde{\Pi}_d$ such that $\tilde{\Pi}_d \tilde{P}_0 = (I - \tilde{\Pi}_d)\tilde{P}_d = 0$. One can choose,

$$\Pi_d = \begin{bmatrix} \tilde{\Pi}_d & 0 \\ 0 & 0 \end{bmatrix}, \tag{22}$$

Then Eq. (12) becomes,

$$\begin{aligned} &\sum_{l=0}^{d-1} \left(\Pi_d \begin{bmatrix} \tilde{P}_{l+1} & * \end{bmatrix} + (I - \Pi_d) \begin{bmatrix} \tilde{P}_l & * \end{bmatrix} \right) \otimes U^l \\ =&\sum_{l=0}^{d-1} \begin{bmatrix} \tilde{\Pi}_d \tilde{P}_{l+1} + (I - \tilde{\Pi}_d)\tilde{P}_l & * \end{bmatrix} \otimes U^l. \end{aligned} \tag{23}$$

So it is sufficient to determine Π_d recursively only using information from the selected columns (or equivalently, rows) instead of the whole matrix.

When the target block encoded matrix $\boldsymbol{P}(z)$ has rank no more than $N/2$, we have $r_{\tilde{P}_0}, r_{\tilde{P}_d} \leq N/2$ in Eq. (10), so we can always choose $\ell_d = N/2$, and simplify the circuit in FIG. 2 to use only single-qubit controlled-U gates.

In some cases, we may need to realize Laurent polynomials [46], where each entry is of the form $P_{jk}(z) = \sum_{l=-d}^{d} P_{jk,l} z^l$.

Corollary 6 ($U(N)$-QSP for Laurent polynomials) *Given any unitary U and Laurent polynomial matrix $\boldsymbol{P}(z)$ of degrees no more than d, such that $\boldsymbol{P}(z)$ has all singular values in $[0,1]$ whenever $|z| \leq 1$. Then one can construct a quantum circuit with $(2d)$ calls to the double-headed gate $C_\Pi(U^{1/2}, U^{-1/2}) := \Pi \otimes U^{1/2} + (I - \Pi) \otimes U^{-1/2}$ to implement a block encoding of $\boldsymbol{P}(U)$.*

Proof of Corollary 6. We construct the circuit to realize the degree-$(2d)$ polynomial matrix $\sum_{l=-d}^{d} P_{jk,l} z^{l+d}$ using Theorem 4. By replacing each controlled-U gate with the double-headed gate $C_\Pi(U^{1/2}, U^{-1/2})$, we realize the Laurent polynomial matrix $\boldsymbol{P}(z)$ as desired. □

Corollary 7 (Approximate $U(N)$-QSP) *Given any unitary U and complex polynomial matrix $\boldsymbol{P}(z)$ of degrees no more than d, such that $\boldsymbol{P}(z)$ has all singular values in $[0,1]$ whenever $|z| \leq 1$. Let $\mathcal{G}$ be a finite set of unitary gates with determinant one and their inverses, generating a dense subset of $SU(N)$, where N is the ancilla dimension. Then for any $\epsilon > 0$, one can construct a quantum circuit using gates from $\mathcal{G}$ with d calls to controlled-U that implements a unitary $\tilde{\boldsymbol{U}}$ such that the realized block-encoded matrix satisfies*

$$\left\| \Pi^\dagger \tilde{\boldsymbol{U}} \Pi - \boldsymbol{P}(U) \right\| \leq \epsilon, \tag{24}$$

where $\Pi = |0\ldots0\rangle\langle 0\ldots0|$ projects onto the ancilla subspace. The total number of gates from $\mathcal{G}$ required is

$$O\left(d \cdot \log^c\left(\frac{d}{\epsilon} \right) \right), \tag{25}$$

where $c \geq 1$ is a constant depending on the gate set $\mathcal{G}$, and the constant hidden in the $O(\cdot)$ notation depends polynomially on the ancilla dimension N.

Proof of Corollary 7. By Theorem 4, we construct the circuit with unitaries $R_0, R_1, \ldots, R_d$ as in FIG. 2.

Let $\boldsymbol{U}_{\text{exact}} = R_0 \cdot C_{\Pi_1}(U) \cdot R_1 \cdots R_d \cdot C_{\Pi_d}(U)$ be the exact circuit by Theorem 4. Each R_k is a unitary operator on the ancilla system of dimension N. The Solovay-Kitaev theorem [47, 48, 49] of dimension N ensures that for any $V \in SU(N)$, there exists a finite sequence S of gates from $\mathcal{G}$ of length $O(\log^c(1/\delta))$ such that $\|V - S\| < \delta$, where c is a constant depending on $\mathcal{G}$ and the constant in the $O(\cdot)$ notation depends polynomially on the ancilla dimension N. We apply this to approximate each R_k by $\tilde{R}_k$ with error tolerance δ_k, obtaining

$$\|R_k - \tilde{R}_k\| \leq \delta_k. \tag{26}$$

We choose $\delta_k = \frac{\epsilon}{2d+2}$ for all $k \in \{0, 1, \ldots, d\}$. The compiled circuit is then

$$\tilde{\boldsymbol{U}} = \tilde{R}_0 \cdot C_{\Pi_1}(U) \cdot \tilde{R}_1 \cdots \tilde{R}_d \cdot C_{\Pi_d}(U). \tag{27}$$

We have,

$$\begin{aligned} &\left\| \Pi^\dagger \tilde{\boldsymbol{U}} \Pi - \boldsymbol{P}(U) \right\| \\ =&\left\| \tilde{\boldsymbol{U}} - \boldsymbol{U}_{\text{exact}} \right\| \\ =&\big\| \tilde{R}_0 \cdot C_{\Pi_1}(U) \cdot \tilde{R}_1 \cdots \tilde{R}_d \cdot C_{\Pi_d}(U) \\ &\quad - R_0 \cdot C_{\Pi_1}(U) \cdot R_1 \cdots R_d \cdot C_{\Pi_d}(U) \big\| \\ \leq&\sum_{k=0}^{d} \|\tilde{R}_k - R_k\| \\ \leq&\epsilon, \end{aligned} \tag{28}$$

where we used

$$\|A_1A_2\cdots A_n - B_1B_2\cdots B_n\| \le \sum_{j=1}^{n}\|A_j - B_j\|, \quad (29)$$

for any unitary operators $\{A_j, B_j\}$.

Each approximation $\tilde{R}_k$ requires $O(\log^c(1/\delta_k))$ gates from $\mathcal{G}$. Since there are $d+1$ unitaries R_k to approximate (for $k = 0, 1, \ldots, d$) with $\delta_k = \frac{\epsilon}{2d+2}$, the total gate count is

$$(d+1)\cdot O\left(\log^c\left(\frac{2d+2}{\epsilon}\right)\right) = O\left(d\cdot\log^c\left(\frac{d}{\epsilon}\right)\right), \quad (30)$$

where the constant hidden in the $O(\cdot)$ notation depends polynomially on the ancilla dimension N. □

2.3 $U(N)$-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 $|\Psi_k\rangle = |\mathbf{0}\rangle|\psi_k\rangle$, $\left|\tilde{\Psi}_k\right\rangle = |\tilde{\mathbf{0}}\rangle\left|\tilde{\psi}_k\right\rangle$, and define $\left|\Psi_k^{\perp}\right\rangle, \left|\tilde{\Psi}_k^{\perp}\right\rangle$ by

$$U|\Psi_k\rangle = \lambda_k\left|\tilde{\Psi}_k\right\rangle + \bar{\lambda}_k\left|\tilde{\Psi}_k^{\perp}\right\rangle, \quad (31)$$

$$U^{\dagger}\left|\tilde{\Psi}_k\right\rangle = \lambda_k|\Psi_k\rangle - \bar{\lambda}_k\left|\Psi_k^{\perp}\right\rangle, \quad (32)$$

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

$$U = \begin{bmatrix}\lambda_k & -\bar{\lambda}_k\\ \bar{\lambda}_k & \lambda_k\end{bmatrix}. \quad (33)$$

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

$$\sum_j |j\rangle|\mathbf{0}\rangle|\phi_j\rangle \mapsto \sum_k\left[|k\rangle|\mathbf{0}\rangle\sum_j P_{kj}(A)|\phi_j\rangle + \left|\mathbf{0}^{\perp}\right\rangle|\cdots\rangle\right]. \quad (34)$$

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

Lemma 8 ($U(N)$-QSVT for one singular value) *If d is odd, then the quantum circuit in FIG. 3 implements the unitary transformation,*

$$|j\rangle|\Psi_k\rangle \mapsto \sum_k|k\rangle\left[P_{kj}(\lambda_k)\left|\tilde{\Psi}_k\right\rangle + \bar{\lambda}_k Q_{kj}(\lambda_k)\left|\tilde{\Psi}_k^{\perp}\right\rangle\right], \quad (35)$$

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

$$\sum_k\left[|P_{kj}(x)|^2 + (1-x^2)|Q_{kj}(x)|^2\right] \equiv 1. \quad (36)$$

Otherwise, if d is even, then in Eq. (35) the $\left|\tilde{\Psi}_k\right\rangle, \left|\tilde{\Psi}_k^{\perp}\right\rangle$ should be replaced by $|\Psi_k\rangle, \left|\Psi_k^{\perp}\right\rangle$.

Proof of Lemma 8. We prove by induction on d. For $d = 0$, the output state is simply $\sum_k u_{kj}|k\rangle|\Psi_k\rangle$, with u_{kj} being the (k,j)-th entry of R_0, and these constant functions are 0-polynomials.

Suppose the lemma holds for some even number $(d-1)$, i.e., the state before the final U and $C_{\Pi}(R_d)$ gates in FIG. 3 is Eq. (35). Then after applying the two gates, the state is,

$$\sum_k|k\rangle\Big\{\sum_l u_{kl}\left[\lambda_k P_{lj}(\lambda_k) - (1-\lambda_k^2)Q_{lj}(\lambda_k)\right]\left|\tilde{\Psi}_k\right\rangle + \bar{\lambda}_k\left[P_{lk}(\lambda_k) + \lambda_k Q_{kj}(\lambda_k)\right]\left|\tilde{\Psi}_k^{\perp}\right\rangle\Big\}, \quad (37)$$

which is of the desired form in Eq. (35) with polynomials satisfying both the degree and parity constraints.

The case when d is even is analogous. □

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

Lemma 9 ($U(N)$-QSVT, forward) *The quantum circuit in FIG. 3 implements the unitary transformation Eq. (34) 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 10 ($U(N)$-QSVT, backward) *Given a matrix A block-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 d calls to U and U^{-1} in total, one can implement a*

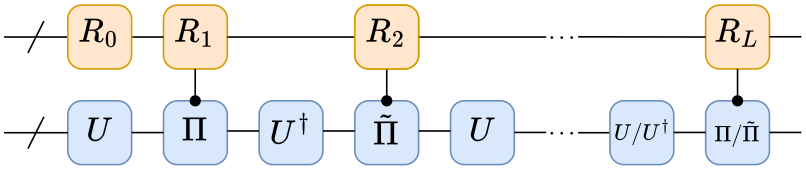


Figure 3: The $U(N)$-QSVT unit, in which $\Pi = |\mathbf{0}\rangle\langle\mathbf{0}|$ and $\tilde{\Pi} = |\tilde{\mathbf{0}}\rangle\langle\tilde{\mathbf{0}}|$. The U and $U^\dagger$ gates applied to the second register alternate, and it depends on the parity of d whether the last two gates in the second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

block encoding of $\boldsymbol{P}(A)$ by the following unitary transformation,

$$\begin{aligned} &|0\rangle \sum_j |j\rangle |\mathbf{0}\rangle |\phi_j\rangle \\ \mapsto &|0\rangle \sum_k |k\rangle |\mathbf{0}\rangle \sum_j P_{kj}(A) |\phi_j\rangle + |1\rangle |\cdots\rangle . \end{aligned} \tag{38}$$

Lemma 11 ($U(N)$-QSVT from 2 polynomials) *Given a matrix A and its block encoding U, a matrix of d-polynomials $\boldsymbol{P}(x)$ and a matrix of $(d-1)$-polynomials $\boldsymbol{Q}(x)$ of the same size such that,*

$$\boldsymbol{P}(x)^\dagger \boldsymbol{P}(x) + (1-x^2)\boldsymbol{Q}(x)^\dagger \boldsymbol{Q}(x) \equiv I, \tag{39}$$

for all $x \in [-1,1]$, one can find $R_0, \cdots, R_d$ in FIG. 3 to make it implement the transformation Eq. (35) for each j.

Proof of Lemma 11. We prove by induction on d. The case $d = 0$ is trivial, as $\boldsymbol{Q}(x) = 0$ and $\boldsymbol{P}(x)$ is a constant unitary matrix, and one can simply let $R_0 = \boldsymbol{P}(x)$.

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

$$\boldsymbol{P}(x) = \sum_{l=0}^{(d-1)/2} \tilde{P}_{2l+1} x^{2l+1}, \tag{40}$$

$$\boldsymbol{Q}(x) = \sum_{l=0}^{(d-1)/2} \tilde{Q}_{2l} x^{2l}. \tag{41}$$

Picking the x^{2d} terms out of the constraint Eq. (39),

$$\tilde{P}_d^\dagger \tilde{P}_d - \tilde{Q}_{d-1}^\dagger \tilde{Q}_{d-1} = 0, \tag{42}$$

so there is a unitary R_d such that $R_d^\dagger \tilde{P}_d = \tilde{Q}_{d-1}$.

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

$$\begin{aligned} &(I \otimes U)^{-1} C_\Pi (R_d)^{-1} \cdot \\ &\sum_k |k\rangle \left[P_{kj}(\lambda_k) |\tilde{\Psi}_k\rangle + \bar{\lambda}_k Q_{kj}(\lambda_k) |\tilde{\Psi}_k^\perp\rangle\right] \\ =&\sum_k |k\rangle \left\{ \left[\sum_l u_{kl}\lambda_k P_{lj}(\lambda_k) + (1-\lambda_k^2) Q_{kj}(\lambda_k)\right] |\Psi_k\rangle \right. \\ &\left. + \bar{\lambda}_k \left[-\sum_l u_{kl} P_{lj}(\lambda_k) + \lambda_k Q_{kj}(\lambda_k)\right] \left|\Psi_k^\perp\right\rangle \right\}, \end{aligned} \tag{43}$$

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

The case when d is even is analogous. □

Proof of Theorem 10. All we need to show is that one can find a matrix of d-polynomials $\boldsymbol{P}_1(x)$ and a matrix of $(d-1)$-polynomials $\boldsymbol{Q}_1(x)$ such that,

$$\begin{bmatrix}\boldsymbol{P}(x)^\dagger & \boldsymbol{P}_1(x)^\dagger\end{bmatrix} \begin{bmatrix}\boldsymbol{P}(x) \\ \boldsymbol{P}_1(x)\end{bmatrix} + (1-x^2)\boldsymbol{Q}_1(x)^\dagger \boldsymbol{Q}_1(x) = I, \tag{44}$$

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 d is even, and the other case is analogous. Write $\boldsymbol{P}$ as Eq. (40). Make substitution $x \to \cos\frac{\theta}{2}$, then $\boldsymbol{P}(x) = e^{-i\frac{d\theta}{2}} \tilde{\boldsymbol{P}}(e^{i\theta})$, for some polynomial matrix $\tilde{\boldsymbol{P}}(z)$ of degree no more than d. 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* [44, 45], there is a polynomial matrix $\tilde{\boldsymbol{Q}}(e^{i\theta})$ of degree no more than d such that

$$I - \tilde{\boldsymbol{P}}(e^{i\theta})^\dagger \tilde{\boldsymbol{P}}(e^{i\theta}) = \tilde{\boldsymbol{Q}}(e^{i\theta})^\dagger \tilde{\boldsymbol{Q}}(e^{i\theta}). \tag{45}$$

Write

$$e^{-i\frac{d\theta}{2}} \tilde{\boldsymbol{Q}}(e^{i\theta}) = \boldsymbol{P}_1\left(\cos\frac{\theta}{2}\right) + \sin\frac{\theta}{2} \boldsymbol{Q}_1\left(\cos\frac{\theta}{2}\right), \tag{46}$$

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

$$\begin{aligned}&\boldsymbol{Q}(e^{i\theta})^\dagger \boldsymbol{Q}(e^{i\theta}) - \boldsymbol{P}_1(x)^\dagger \boldsymbol{P}_1(x) - (1-x^2)\boldsymbol{Q}_1(x)^\dagger \boldsymbol{Q}_1(x)\\ &= \sin\frac{\theta}{2}\left[\boldsymbol{P}_1(x)^\dagger \boldsymbol{Q}_1(x) + \boldsymbol{Q}_1(x)^\dagger \boldsymbol{P}_1(x)\right],\end{aligned} \tag{47}$$

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. (44) holds. Finally, the proof is completed by Lemma 11. □

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 guarantee 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 d, then the circuit requires d calls to U, $U^\dagger$ and their controlled gates in total.

3 Applications

3.1 Bi-variate Quantum Signal Processing

Multi-variate quantum signal processing (M-QSP) generalizes uni-variate QSP to realize multi-variate polynomials $f(U_1, \cdots, U_n)$ using controlled operations on multiple signal operators. While uni-variate QSP achieves polynomial transformations through alternating signal processing unitaries and signal operators, M-QSP must handle signal vectors $\boldsymbol{z} = (z_1, \ldots, z_m)$ where each component z_k is encoded in a different signal operator, and the algorithm selects which operator to invoke at each step [37]. The characterization of achievable polynomials in M-QSP has attracted considerable attention. Németh et al. established complete necessary and sufficient conditions for homogeneous and low-degree cases, but the general case remains open [38]. Laneve and Wolf provided the first general sufficient condition by extending to three-dimensional Hilbert space, requiring non-zero endpoint coefficients, though this condition is restrictive [50]. Compared to the mature theory of uni-variate QSP, M-QSP lacks universal achievability criteria, with existing methods limited to specific assumptions such as variable commutativity, homogeneity, or low degree.

We propose an alternative approach based on the block encoding product rule. Our method differs fundamentally from existing M-QSP frameworks: while previous approaches attempt to directly construct alternating product decompositions of multi-variate polynomials—requiring solutions to algebraic geometry problems such as multi-variate polynomial factorization and positive extension—our method transforms the problem into block encoding construction and linear combination of uni-variate polynomials, circumventing the difficulties of multi-variate decomposition. Specifically, we express the bi-variate polynomial as $f(w,v) = \sum_j p_j(w)q_j(v)$, where $p_j(w)$ and $q_j(v)$ are uni-variate polynomials. Using uni-variate $U(N)$-QSP, we construct block encodings U_{p_j} and V_{q_j} for $p_j(w)$ and $q_j(v)$ respectively, then obtain the block encoding of $p_j(w)q_j(v)$ through the block encoding product rule (Lemma 12), and finally combine all terms through linear combination of unitaries [43] to obtain the block encoding of $f(w,v)$.

We focus on bi-variate Laurent polynomials of the form

$$f(\hat{w},\hat{v}) = \sum_{j,k=-d}^{d} f_{jk}\hat{w}^j\hat{v}^k, \tag{48}$$

where $\hat{w}$ and $\hat{v}$ are signal operators. Throughout this section, we use $w, v \in \mathbb{C}$ with $|w| = |v| = 1$ to denote complex scalars on the unit circle, and $\hat{w}, \hat{v}$ to denote signal operators that may be either scalars or commuting unitary matrices. When $\hat{w}, \hat{v}$ are commuting unitaries, the polynomial $f(\hat{w},\hat{v})$ acts on their simultaneous eigenspaces, and our constructions apply with $\hat{w}, \hat{v}$ representing the corresponding eigenvalues. This is useful in scenarios like $\hat{w} = e^{i\kappa\hat{q}_1}$ and $\hat{v} = e^{i\kappa\hat{q}_2}$, where $\hat{q}_1$ and $\hat{q}_2$ are the position operators on two bosonic modes, to encode potential energy terms in Hamiltonian simulation. We require all $\hat{w}$ to appear to the left of $\hat{v}$ and aim to realize the block encoding

$$\begin{bmatrix} f(\hat{w},\hat{v}) & * \\ * & * \end{bmatrix}. \tag{49}$$

Our protocol for constructing a block encoding of $f(\hat{w},\hat{v})$ is illustrated in FIG. 4. Two unitaries for variables $\hat{w}$ and $\hat{v}$ are constructed separately, and the block encoding of the target bi-variate polynomial is obtained via the following product rule.

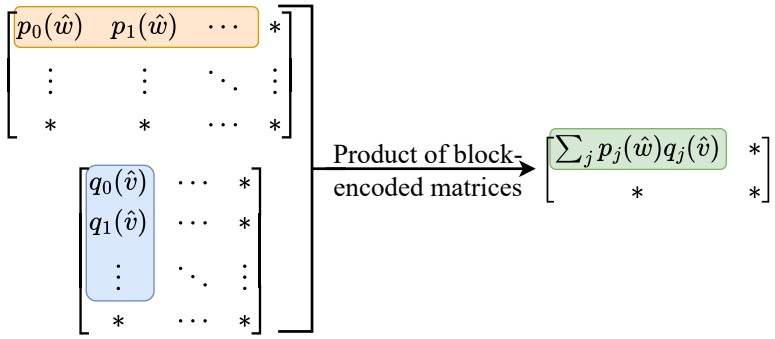


Figure 4: Block encoding of bi-variate polynomials via uni-variate $U(N)$-QSP. The product of block-encoded matrices is obtained by treating either the blue or orange box as a single block.

Lemma 12 (Product of block-encoded matrices [2]) *If U and V are block encodings of matrices A and B respectively, with ancilla qubits on different spaces a and b, then $(I_b \otimes U)(I_a \otimes V)$ is a block encoding of the product AB.*

To apply this lemma, we first express the polynomial as a linear combination of products of uni-variate polynomials:

$$f(\hat{w}, \hat{v}) = \sum_j p_j(\hat{w}) q_j(\hat{v}), \tag{50}$$

where $p_j(\hat{w})$ and $q_j(\hat{v})$ are uni-variate polynomials. The $U(N)$-QSP framework requires that the column vector $\{p_j(w)\}$ and row vector $\{q_j(v)\}$ have bounded norms: $\sum_j |p_j(w)|^2 \leq 1$ and $\sum_j |q_j(v)|^2 \leq 1$ for all unit complex numbers $|w| = |v| = 1$. We call such bi-variate polynomials *achievable* by the product of $U(N)$-QSP.

Corollary 13 (Achievable polynomials) *A bi-variate polynomial is achievable by product of $U(N)$-QSP if and only if it can be written as $f(\hat{w}, \hat{v}) = \sum_j p_j(\hat{w}) q_j(\hat{v})$ such that $\sum_j |p_j(w)|^2 \leq 1$ and $\sum_j |q_j(v)|^2 \leq 1$ for all $|w| = |v| = 1$.*

While this condition provides a clear achievability criterion, finding a decomposition $f(\hat{w}, \hat{v}) = \sum_j p_j(\hat{w}) q_j(\hat{v})$ satisfying the norm constraints requires numerical optimization. A natural approach is to use low-rank decomposition of the coefficient matrix $\boldsymbol{F} = (f_{jk})_{j,k=-d}^{d}$. However, direct decomposition may yield too many terms: for a $(2d+1) \times (2d+1)$ matrix, a full rank decomposition requires $O(d)$ terms, leading to correspondingly many $U(N)$-QSP sequences and excessive circuit complexity.

We employ principal component analysis (PCA) to find low-rank approximations. Decomposing the coefficient matrix as

$$\boldsymbol{F} = \sum_{i=1}^{N} \lambda_i \boldsymbol{v}_i \boldsymbol{u}_i^\top, \tag{51}$$

where $N = (2d+1)^2$, and retaining only the r largest eigenvalues yields the rank-r approximation

$$\boldsymbol{F}_r = \sum_{i=1}^{r} \lambda_i \boldsymbol{v}_i \boldsymbol{u}_i^\top, \tag{52}$$

corresponding to the polynomial approximation

$$f_r(\hat{w}, \hat{v}) = \sum_{i=1}^{r} \lambda_i p_i(\hat{w}) q_i(\hat{v}), \tag{53}$$

where $p_i(\hat{w}) = \sum_{j=-d}^{d} (\boldsymbol{v}_i)_j \hat{w}^j$ and $q_i(\hat{v}) = \sum_{k=-d}^{d} (\boldsymbol{u}_i)_k \hat{v}^k$. The reconstruction error is measured by

$$\varepsilon = \sum_{j,k} |f_{jk} - (f_r)_{jk}|. \tag{54}$$

The effectiveness of PCA depends on the structure of the coefficient matrix. In practical applications, target functions often possess smoothness, reflected in the decay of their Fourier coefficients. Consider coefficient matrices with spatial decay

$$f_{jk} = r_{jk} \cdot w(j,k), \tag{55}$$

where r_{jk} is a random value and $w(j,k) = [(|j|+1)(|k|+1)]^{-s}$ with decay exponent $s > 0$.

FIG. 5 compares the reconstruction error for different decay patterns at fixed matrix size $N = 32$: no decay versus polynomial decay $w(j,k) = [(|j|+1)(|k|+1)]^{-s}$ with $s \in \{1,2,3,4\}$. For completely random coefficient matrices (no decay), the reconstruction error scales as approximately $\sqrt{1 - r/N}$ with the retained principal component ratio r/N, requiring about 99% of

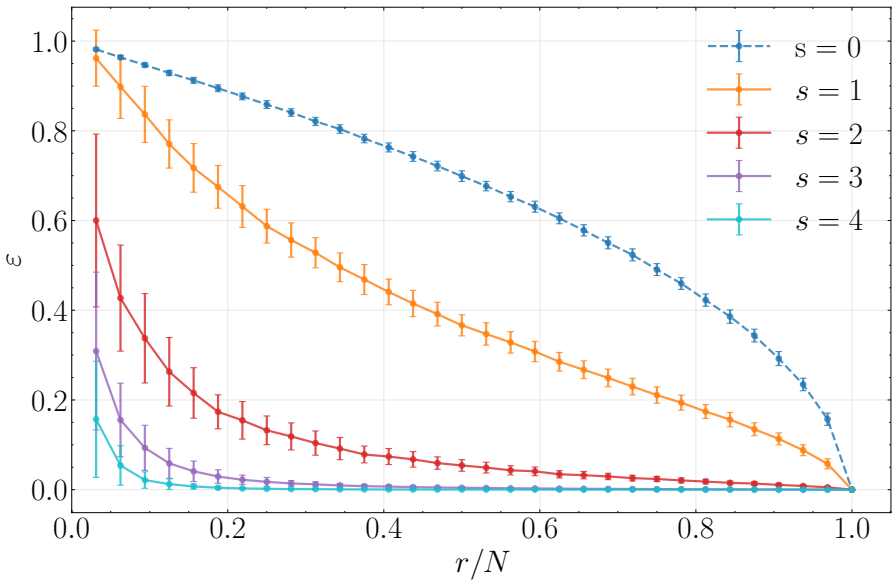


Figure 5: Comparison of PCA reconstruction error for different coefficient decay patterns. Polynomial decay significantly reduces the number of principal components needed to achieve the same error. Larger decay exponent s yields better low-rank approximation. When $s = 4$, only $r/N \approx 5\%$ is needed to achieve $\varepsilon < 0.1$, while random matrices require retaining over 90% of principal components.

principal components for small error ($\varepsilon < 0.1$). In contrast, for polynomial decay with increasing exponent s, the required number of principal components decreases substantially: when $s = 4$, only $r/N \approx 5\%$ is needed to achieve $\varepsilon < 0.1$. This demonstrates that for functions with good smoothness properties, very few principal components suffice for high-accuracy reconstruction.

This result has significant implications for quantum algorithms. In quantum simulation and optimization, target functions typically have physical meaning and thus possess smoothness and regularity, with Fourier coefficients exhibiting decay. For such functions, even as the coefficient matrix dimension d grows rapidly, PCA can keep the required rank r small, significantly reducing the number of ancilla qubits and gate complexity in $U(N)$-QSP.

Compared to existing M-QSP methods, our approach offers several advantages. First, the criterion is based on the complete theory of univariate QSP, avoiding the algebraic geometry difficulties of multi-variate positive extension without requiring verification of stability conditions or Fejér-Riesz decomposition. Second, the high-dimensional parameter space of the $U(N)$ framework makes numerical optimization more likely to find effective decompositions. Third, for functions with regular structure, PCA provides a systematic approximation method whose effectiveness is guaranteed by the smoothness of the target function.

The method also has limitations. While the condition is explicit, finding a satisfying decomposition still requires numerical optimization. The method naturally handles commuting signal operators; for non-commuting unitary matrix inputs, the fixed variable ordering required by the product rule ($\hat{w}$ always before $\hat{v}$) restricts applicability to cases where this ordering is physically meaningful. Additionally, the method requires $O(\log_2 r)$ ancilla qubits for linear combination, resulting in higher space complexity compared to existing methods that require only 1 or 2 ancilla qubits [37, 50]. Finally, the effectiveness of PCA strongly depends on the smoothness of the target function; for random or highly oscillatory functions, the rank reduction brings limited resource savings.

3.2 Multi-interval Decision

The multi-interval decision problem asks to determine which of N disjoint intervals a physical quantity of a quantum system belongs to. This problem has broad applications in quantum computing, including determining the interval containing the ground state energy of a Hamiltonian, the amplitude of a quantum state, or the eigenvalue phase of a unitary operator. Tra-

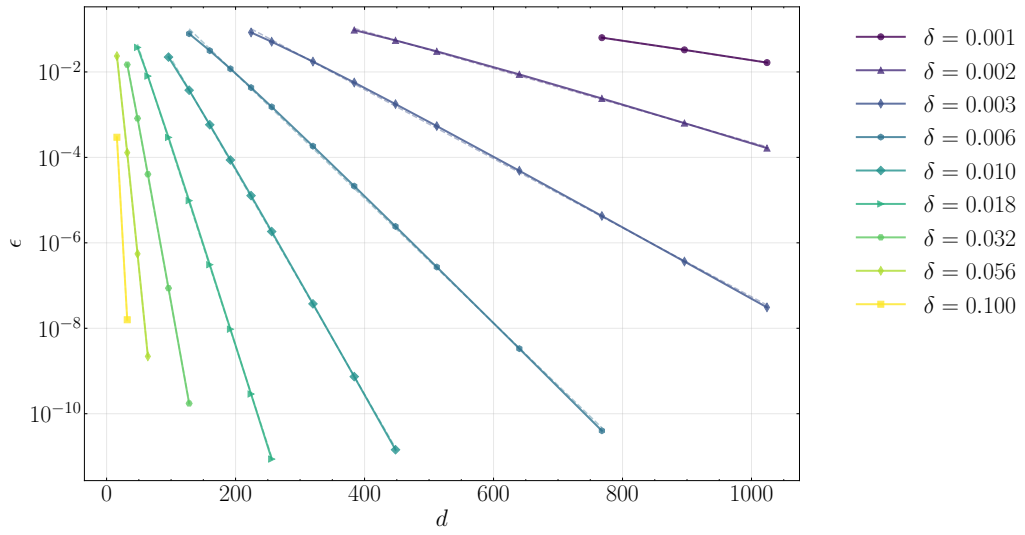


Figure 6: Empirical scaling of the degree d required to achieve error ϵ for different gap widths δ. The linear relationship between d and $\log(\epsilon^{-1})$ for each δ confirms the scaling $d \sim C(\delta)\cdot\log(\epsilon^{-1})$. The dashed lines fit $d = C(\delta)\cdot\log(\epsilon^{-1})$. Numerical regression shows that $C(\delta) \approx 0.170 \cdot \delta^{-1}$.

ditional $U(2)$-QSP uses a single ancilla qubit, which from an information-theoretic perspective extracts only one bit of information per measurement, requiring $\log_2 N$ measurement rounds to distinguish N intervals. In contrast, $U(N)$-QSP uses an N-dimensional ancilla system, extracting $\log_2 N$ bits of information in a single measurement and achieving a factor of $\log_2 N$ improvement in oracle complexity.

Let $\{I_0, \ldots, I_{N-1}\}$ be N disjoint intervals on $[-\frac{1}{2}, \frac{1}{2}]$ with pairwise distance at least 2δ. Consider determining which interval the parameter φ in the eigenvalue $e^{i2\pi\varphi}$ of a unitary operator U with respect to state $|\psi\rangle$ belongs to. Suppose one uses a quantum circuit that queries the signal d times and output a random variable $j \in \{0, 1, \ldots, N-1\}$ with probability $Pr(j|\varphi)$ when the true parameter is φ, to decide which interval φ belongs to, with target error ϵ such that,

$$Pr(j|\varphi) \geq 1 - \epsilon, \quad \forall \varphi \in I_j. \tag{56}$$

By the Fejér-Riesz theorem [51, 52], for any function $f(\varphi) = \sum_{j=-d}^{d} f_j e^{i2\pi j\varphi}$ satisfying $f(\varphi) \geq 1$ for all $\varphi \in [-\pi, \pi]$, one can by its square root $g(\varphi) = \sum_{j=0}^{d} g_j e^{i2\pi j\varphi}$ such that $|g(\varphi)|^2 = f(\varphi)$ for all $\varphi \in [-\pi, \pi]$.

For $N = 2$, one can find a pair of $Pr(0|\varphi)$ and $Pr(1|\varphi)$ that approximate the indicator functions of the two intervals respectively, and the Fejér-Riesz theorem guarantees the existence of their square roots $P_0(\varphi)$ and $P_1(\varphi)$. Using generalized QSP (Theorem 1), one can realize a circuit with output state,

$$|0\rangle P_0(U)|\psi\rangle + |1\rangle P_1(U)|\psi\rangle, \tag{57}$$

so measuring the first qubit gives probabilities $Pr(j|\varphi) = \| P_j(U)|\psi\rangle \|^2 = Pr(j|\varphi)$ for $j = 0, 1$.

In the problem of multi-interval decision, one can use binary search by repeating the two-interval decision process $\log_2 N$ times with different circuits [3, 46]. Alternatively, we can construct a set of decision polynomials $P_j(\varphi)$ ($j = 0, 1, \ldots, N-1$) such that the measurement probabilities $Pr(j|\varphi) = |P_j(\varphi)|^2$ approximate the indicator functions of the N intervals respectively. To realize these polynomials, we need to use $U(N)$-QSP (Theorem 4) to implement the transformation

$$\sum_{j=0}^{N-1} |j\rangle P_j(U)|\psi\rangle. \tag{58}$$

This allows us to decide which interval φ belongs to by measuring all the ancilla register in one go, saving a factor of $\log_2 N$ in oracle complexity compared to binary search.

In the rest of this section, we provide a numerical construction of decision polynomials $Pr(j|\varphi)$ that works for binary decision and general multi-interval decision, along with error bounds.

We define a family of Fourier polynomials optimized for decision problems. Let

$$p_{d,\delta}(\varphi) = \left| \sum_{j=0}^{d} c_j e^{i2\pi j\varphi} \right|^2, \tag{59}$$

and we minimize the window cost function,

$$\begin{aligned} W_\delta &= \int_{-1/2}^{1/2} w_\delta(\varphi) p_{d,\delta}(\varphi) d\varphi \\ &= \sum_{j,k=0}^{d} c_j c_k^* \int_{-1/2}^{1/2} w_\delta(\varphi) e^{i2\pi(j-k)\varphi} d\varphi \\ &= \sum_{j,k=0}^{d} c_j c_k^* M_{jk}, \end{aligned} \tag{60}$$

under constraints,

$$\int_{-1/2}^{1/2} p_{d,\delta}(\varphi) d\varphi = \sum_{j=0}^{d} |c_j|^2 = 1, \tag{61}$$

where $w_\delta(\varphi) = 0$ for $\varphi \in [-\delta, \delta]$ and 1 elsewhere on $[-1/2, 1/2]$, and

$$\begin{aligned} M_{jk} &= \int_{-1/2}^{1/2} w_\delta(\varphi) e^{i2\pi(j-k)\varphi} d\varphi \\ &= \begin{cases} 1 - 2\delta, & j = k, \\ -\frac{\sin(2\pi(j-k)\delta)}{\pi(j-k)}, & j \neq k. \end{cases} \end{aligned} \tag{62}$$

The minimal W_δ can be obtained by choosing $\{c_j\}$ as the eigenvector corresponding to the minimal eigenvalue of the $(N+1) \times (N+1)$ matrix $M = (M_{jk})$. To achieve window cost ϵ for fixed δ, one needs a large value of d such that a more narrow peak can be formed within $[-\delta, \delta]$. We numerically compute ϵ for various d and δ, and find the following empirical scaling relation (FIG. 6).

Claim 14 (Window cost scaling) *For the numerically optimized Fourier polynomial $p_{d,\delta}$ defined in Eq. (59), in the regime $\delta \in [10^{-3}, 10^{-1}]$, the polynomial degree required to achieve error ϵ for optimal window cost satisfies*

$$d \gtrsim 0.170 \cdot \delta^{-1} \cdot \log\left(\epsilon^{-1}\right). \tag{63}$$

The following theorem provides an explicit construction and error bound for general multi-interval decision.

Theorem 15 (Degree in multi-interval decision) *Let intervals $I_j = [a_j, b_j]$ $(j = 0, 1, \ldots, N-1)$ be disjoint with pairwise distance 2δ. For each interval I_j, define the decision polynomial*

$$Pr(j|\varphi) = \int_{\tilde{I}_j} p_{d,\delta}(\varphi - \varphi') d\varphi', \tag{64}$$

where $\tilde{I}_j := [a_j - \delta, b_j + \delta]$ is the extended interval and $p_{d,\delta}$ is defined in Eq. (59). Then, in the regime $\delta \in [10^{-3}, 10^{-1}]$, one can achieve

$$Pr(j|\varphi) \geq 1 - \epsilon, \quad \forall j \text{ and } \varphi \in I_j. \tag{65}$$

with

$$d \gtrsim 0.170 \cdot \delta^{-1} \cdot \log\left(\epsilon^{-1}\right) \tag{66}$$

number of queries to the signal.

Proof of Theorem 15. For any $\varphi \in I_j$ we have,

$$\begin{aligned} & 1 - Pr(j|\varphi) \\ =& \int_{[-\pi,\pi]-\tilde{I}_j} p_{d,\delta}(\varphi - \varphi') d\varphi' \\ \leq& \int_{[-\pi,\pi]-[-\delta,\delta]} p_{d,\delta}(\varphi - \varphi') d\varphi' \\ =& \epsilon, \end{aligned} \tag{67}$$

therefore, one can refer to Eq. (63) to determine the required degree d to achieve error ϵ. □

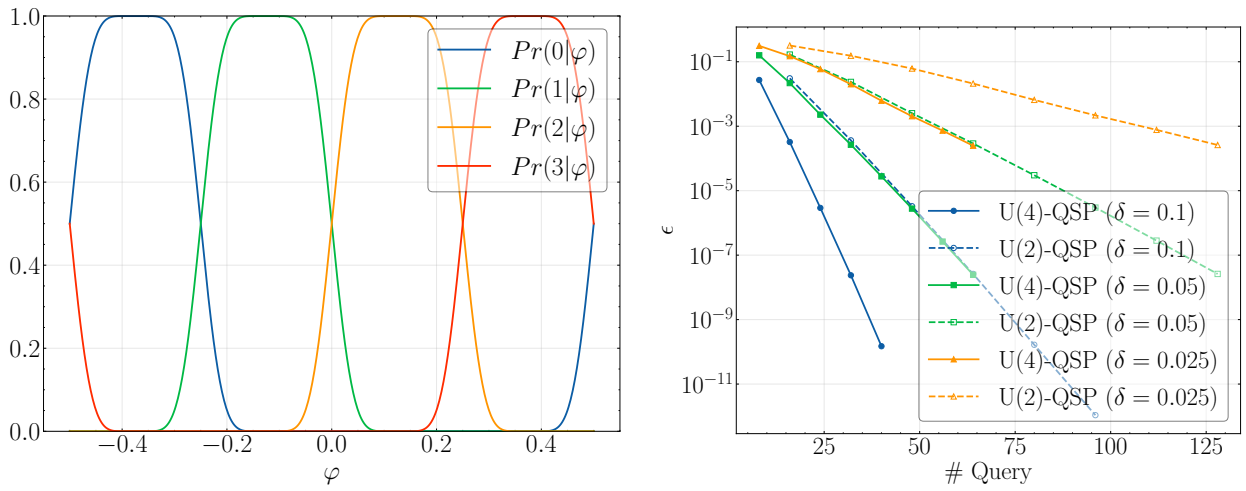
Example: 4-interval decision.— As a concrete example, we consider the 4-decision problem where we determine whether φ belongs to $I_0 = [-\pi+\delta, -\frac{\pi}{2}-\delta]$, $I_1 = [-\frac{\pi}{2}+\delta, -\delta]$, $I_2 = [\delta, \frac{\pi}{2}-\delta]$, or $I_3 = [\frac{\pi}{2}+\delta, \pi-\delta]$. FIG. 7a shows the 4 decision polynomials for $d = 16$ and $\delta = 0.1$ by Eq. (64), demonstrating that each polynomial approximates 1 in its corresponding interval and 0 elsewhere. One can implement these polynomials using $U(4)$-QSP with $d = 16$ queries to the signal in one go.

An alternative approach using traditional $U(2)$-QSP would require two-stage binary decision: the first stage performs binary decision at $\varphi = 0$ to distinguish left and right half-planes, and the second stage performs binary decisions at $\varphi = -\frac{\pi}{2}$ and $\varphi = \frac{\pi}{2}$ respectively. This $U(2)$-QSP based method extracts only one bit of information per stage, requiring $\log_2 N$ rounds. FIG. 7b compares the error performance of both approaches, clearly showing that $U(4)$-QSP achieves the same error with roughly half the number of signal calls.

3.3 Quantum Amplitude Estimation

Quantum amplitude estimation (QAE) addresses the following problem: given a state preparation operator U that prepares $|\psi\rangle = U|\psi_0\rangle$ from an initial state $|\psi_0\rangle$, and a projection operator Π, estimate $x = \langle\psi|\Pi|\psi\rangle$ using N queries to U and U^{-1}.

This is useful 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 $[-1, 1]$ and is block-encoded by U. The expectation value, $\langle\psi|A|\psi\rangle$, of a block-encoded observable A can be estimated via quantum amplitude estimation if we consider the state



(a) 4-decision polynomials for $U(N)$-QSP using numerically optimized Fourier polynomials ($d = 16$, $\delta = 0.1$). The four polynomials P_0, P_1, P_2, P_3 each approximate 1 in their corresponding intervals, demonstrating one-shot multi-interval decision capability of $U(N)$-QSP.

(b) Comparison of $U(4)$-QSP direct method versus $U(2)$-QSP two-stage method for 4-decision. Solid lines show $U(4)$-QSP, dashed lines show $U(2)$-QSP. The $U(4)$-QSP method achieves the same error with roughly half the number of queries.

Figure 7: 4-decision QSP polynomials and comparison.

$(|0\rangle|\mathbf{0}\rangle|\psi\rangle + |0\rangle U|\mathbf{0}\rangle|\psi\rangle)/\sqrt{2}$ and the projector $|+\rangle\langle+| \otimes I$, where the identity acts on the block-encoding ancilla and system qubits.

Let $Pr(k|x)$ denote the probability of obtaining the k-th measurement outcome when the amplitude is x. We assume the circuit has a fixed structure that does not adaptively change based on intermediate results, and each output probability $Pr(k|x)$ depends only on x. The total number of calls to U and U^{-1} is the *degree* of the QAE circuit, denoted d.

Lemma 16 (QAE probabilities are polynomials) *Each output probability of a degree-d QAE circuit is a polynomial in x of degree at most d.*

Proof. Consider a simple QAE setup with state preparation

$$W(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}, \tag{68}$$

initial state $|0\rangle$, and projector $|0\rangle\langle 0|$, where the target amplitude is $x = \cos^2(\theta/2)$. By induction on d, after d calls to $W(\theta)$ and its inverse, the quantum state becomes a polynomial vector in $\cos(\theta/2)$ and $\sin(\theta/2)$ of degree at most d with definite parity. Any projection measurement probability must have the form $P_1(x) + \sin\theta\, P_2(x)$, where P_1 and P_2 are polynomials of degrees at most d and $d-1$ respectively. However, since $W(\theta)$ and $W(-\theta)$ share the same amplitude x but opposite sign of $\sin\theta$, and must yield identical probabilities, we conclude $P_2 = 0$, establishing that the probability is indeed a polynomial in x. □

As a concrete example, if we apply the amplitude amplification operator [41]

$$U(I - 2\,|\psi_0\rangle\langle\psi_0|)U^{-1}(I - 2\Pi) \tag{69}$$

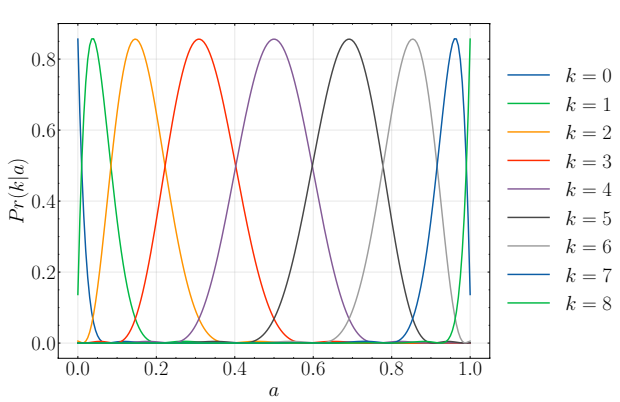
k times to $U\,|\psi_0\rangle$ and measure on $\{\Pi, I-\Pi\}$, the output probability for Π is

$$\sin^2\left(\frac{2k+1}{2}\theta\right) = \frac{1 - T_{2k+1}(2x-1)}{2}, \tag{70}$$

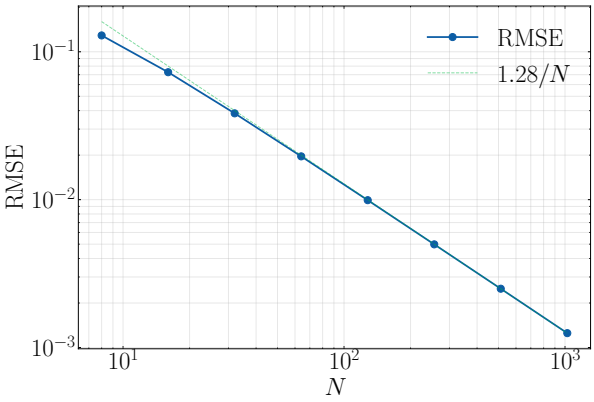
a polynomial of degree $2k+1$ in x, where T_k is the Chebyshev polynomial of the first kind. This matches the QAE circuit degree since each amplification adds degree 2, plus 1 for initial state preparation, giving total degree $d = 2k+1$.

QAE is structurally similar to multi-interval decision. Given target precision ϵ, partition $[0,1]$ into $k = \mathcal{O}(\epsilon^{-1})$ intervals $\{I_j = [j\epsilon, (j+1)\epsilon]\}$. The goal is to determine which interval contains the unknown amplitude x, thereby estimating x with precision $\mathcal{O}(\epsilon)$. This shares the same structure as multi-interval decision discussed in Sec. 3.2, but with each sampling point directly corresponding to a measurement outcome rather than being integrated over an interval.

Theorem 17 (QAE via $U(N)$-QSVT) *For any set of probability functions $\{Pr(k|x)\}$ that are*



(a) Measurement outcome probabilities $Pr(k|x)$ for QAE with $N = 16$.



(b) RMSE versus circuit degree N for QAE.

Figure 8: QAE measurement probabilities and RMSE scaling.

polynomials in x of degree at most d, non-negative on $[0, 1]$, and satisfy $\sum_k Pr(k|x) \equiv 1$, there exists a $U(N)$-QSVT circuit that produces measurement outcome k with probability $Pr(k|x)$.

Proof. Using Lemma 6 of [2], we decompose each probability polynomial as

$$\begin{aligned} &Pr(k|\cos^2(\theta/2)) \\ =&A_k(\cos(\theta/2))^2 + \sin^2(\theta/2)B_k(\cos(\theta/2))^2 \end{aligned} \tag{71}$$

for suitable polynomials A_k and B_k of degrees d and $d-1$ respectively. Write the state preparation as

$$U|\psi_0\rangle = \cos(\theta/2)\left|\tilde{\psi}_0\right\rangle + \sin(\theta/2)\left|\tilde{\psi}_1\right\rangle, \tag{72}$$

where $|\psi_0\rangle$ is on the projected subspace of Π, and $|\psi_1\rangle$ is orthogonal to $|\psi_0\rangle$. Define $|\psi_1\rangle = U^{-1}[-\sin(\theta/2)\left|\tilde{\psi}_0\right\rangle + \cos(\theta/2)\left|\tilde{\psi}_1\right\rangle]$ orthogonal to $|\psi_0\rangle$. In the basis $(|\psi_0\rangle, |\psi_1\rangle) \to (\left|\tilde{\psi}_0\right\rangle, \left|\tilde{\psi}_1\right\rangle)$, U has matrix representation

$$U = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}. \tag{73}$$

The target state for $U(N)$-QSVT is

$$\begin{aligned} \sum_{k=0}^{N-1} |k\rangle \Big[&A_k(\cos(\theta/2))\left|\tilde{\psi}_0\right\rangle \\ &+ \sin(\theta/2)B_k(\cos(\theta/2))\left|\tilde{\psi}_1\right\rangle \Big], \end{aligned} \tag{74}$$

if d is odd (or with $|\psi_0\rangle, |\psi_1\rangle$ replacing $\left|\tilde{\psi}_0\right\rangle, \left|\tilde{\psi}_1\right\rangle$ if d is even), which satisfies the conditions of Theorem 10. □

To minimize the standard deviation of the estimated amplitude, we use the decision polynomial,

$$Pr(k|x) = \begin{cases} |p_{\sin}(\theta_x - \theta_k)|^2 + |p_{\sin}(\theta_x + \theta_k)|^2, \\ \qquad k = 1, \ldots, \frac{N}{2} - 1, \\ |p_{\sin}(\theta_x - \theta_k)|^2, k = 0, \frac{N}{2}, \end{cases} \tag{75}$$

where $\theta_x = \arccos(1 - 2x)$, $\theta_k = k\pi/N$ for $k = 0, 1, \ldots, N/2$, and

$$p_{\sin}(\varphi) = \sqrt{\frac{2}{N(N+1)}} \sum_{k=0}^{N-1} \sin\left(\frac{(k+1)\pi}{N+1}\right) e^{ik\varphi}, \tag{76}$$

which is known to minimize the variance in phase estimation [53, 54, 55]. The range of k excludes values greater than $N/2$ because they correspond to amplitudes already covered by $k \leq N/2$ due to the symmetry $\theta_x \in [0, \pi]$. Using Bayesian estimation, the amplitude estimate for outcome k is

$$x_k = \frac{\int_0^1 xPr(k|x)dx}{\int_0^1 Pr(k|x)dx}. \tag{77}$$

FIG. 8a shows the probability curves $Pr(k|x)$ for $N = 8$. Different outcomes k have high probability in different amplitude regions, enabling inference of the amplitude from the measurement result.

To analyze performance, we compute the root mean square error (RMSE)

$$\text{RMSE} = \sqrt{\int_0^1 \sum_{k=0}^{N/2} (x_k - x)^2 Pr(k|x)dx}, \tag{78}$$

where x_k is given by Eq. (77). FIG. 8b shows RMSE versus circuit degree N. The numerical results indicate RMSE decreases as $\mathcal{O}(N^{-1})$,

matching the reference line $1.28N^{-1}$. This demonstrates that the $U(N)$-QSVT based QAE achieves the Heisenberg limit, where estimation precision is inversely proportional to the circuit degree. Similarly, $U(2)$-based QAE requires $\mathcal{O}(\log_2 N)$ rounds of binary search to achieve the same precision [46, 3].

4 Conclusion and Outlook

We have established a comprehensive theoretical framework for quantum signal processing and quantum singular value transformation on $U(N)$, generalizing the standard $U(2)$ framework by using N-dimensional ancilla systems with parameterized unitary operations. Our main theoretical contribution is a constructive characterization of achievable polynomial matrices: any polynomial matrix $\boldsymbol{P}(z)$ satisfying appropriate norm constraints on the unit circle can be block-encoded using controlled-U operations, with explicit recursive algorithms provided for circuit parameter determination.

Three applications demonstrate the practical advantages of this framework. First, we present a method for bi-variate quantum signal processing that leverages the product rule for block encodings and principal component analysis, avoiding the algebraic difficulties of existing multi-variate QSP approaches. Second, we show that $U(N)$-QSP achieves multi-interval decision with oracle complexity $\mathcal{O}(d)$ for N intervals, achieving a factor of $\log_2 N$ improvement over the $\mathcal{O}(d \log_2 N)$ complexity required by iterative $U(2)$-QSP methods. Third, we establish that quantum amplitude estimation via $U(N)$-QSVT achieves the Heisenberg limit scaling $\mathcal{O}(N^{-1})$ in a single non-adaptive measurement, eliminating the need for the $\mathcal{O}(\log_2 N)$ adaptive rounds required in conventional approaches.

Several directions for future research are promising. First, developing efficient classical algorithms for computing the unitary parameters $R_0, \ldots, R_d$ beyond the inductive construction, potentially using techniques from numerical optimization or tensor networks, would improve practical applicability. Second, investigating whether the expanded parameter space of $U(N)$-QSP can enhance the expressivity of variational quantum algorithms compared to $U(2)$-based approaches could reveal new applications in quantum machine learning. Third, extending PCA-based decomposition methods for bivariate QSP to higher-order multivariate polynomials and exploring connections to tensor decomposition would address the broader challenge of multi-variate quantum signal processing. Finally, practical implementation of $U(N)$-QSP on real quantum hardware, studying the effects of decoherence and gate errors on circuit fidelity, and extending these techniques to non-qubit architectures such as bosonic systems and hybrid quantum processors [46, 56] remain important open questions.

Acknowledgement

We thank Bojko Bakalov for fruitful discussions. X.L. and H.L. acknowledge support from the National Natural Science Foundation of China under Grant Nos. 62272406, 61932018.

Code Availability

The source code for numerical experiments and implementations presented in this paper is available at https://github.com/helloluxi/unqsp-code.

References

[1] Guang Hao Low and Isaac L Chuang. Optimal hamiltonian simulation by quantum signal processing. *Physical review letters*, 118(1):010501, 2017. doi:10.1103/PhysRevLett.118.010501.

[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. doi:10.1145/3313276.3316366.

[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. doi:10.1103/PRXQuantum.2.040203.

[4] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization.

Quantum, 3:163, 2019. doi:10.22331/q-2019-07-12-163.

[5] Zhiyan Ding, Xiantao Li, and Lin Lin. Simulating open quantum systems using hamiltonian simulations. *PRX Quantum*, 5:020332, May 2024. doi:10.1103/PRXQuantum.5.020332.

[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. doi:10.1137/16M1087072.

[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. doi:10.1103/PRXQuantum.3.040305.

[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. doi:10.1103/PhysRevLett.113.210501.

[9] Patrick Rall and Bryce Fuller. Amplitude estimation from quantum signal processing. *Quantum*, 7:937, 2023. doi:10.22331/q-2023-03-02-937.

[10] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004. doi:10.1126/science.1104149.

[11] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006. doi:10.1103/PhysRevLett.96.010401.

[12] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222–229, 2011. doi:10.1038/nphoton.2011.35.

[13] Ashley Montanaro. Quantum speedup of monte carlo methods. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 471(2181):20150301, 2015. doi:10.1098/rspa.2015.0301.

[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. doi:10.1145/2897518.2897585.

[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. doi:10.1145/2897518.2897544.

[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. doi:10.1145/3188745.3188802.

[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. doi:10.1137/1.9781611977554.ch47.

[19] Emanuel Knill, Gerardo Ortiz, and Rolando D Somma. Optimal quantum measurements of expectation values of observables. *Physical Review A*, 75(1):012328, 2007. doi:10.1103/PhysRevA.75.012328.

[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. doi:10.1073/pnas.0808245105.

[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. doi:10.1103/PhysRevResearch.4.033173.

[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. doi:10.1103/PhysRevLett.129.240501.

[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. doi:10.1038/ncomms5213.

[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. doi:10.26421/QIC15.3-4-7.

[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. doi:10.22331/q-2023-06-02-1031.

[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. doi:10.1137/22M1484298.

[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. doi:10.22331/q-2022-10-20-842.

[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. doi:10.1103/PhysRevA.103.042419.

[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. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1051–1062, 2024. doi:10.1109/FOCS61266.2024.00070.

[37] Zane M Rossi and Isaac L Chuang. Multivariable quantum signal processing (m-qsp): prophecies of the two-headed oracle. *Quantum*, 6:811, 2022. doi:10.22331/q-2022-09-20-811.

[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] Yuta Kikuchi, Conor Mc Keever, Luuk Coopmans, Michael Lubasch, and Marcello Benedetti. Realization of quantum signal processing on a noisy quantum computer. *npj Quantum Information*, 9(1):93, 2023. doi:10.1038/s41534-023-00762-0.

[40] J.-T. Bu, Lei Zhang, Zhan Yu, Jing-Bo Wang, W.-Q. Ding, W.-F. Yuan, B. Wang,

H.-J. Du, W.-J. Chen, L. Chen, J.-W. Zhang, J.-C. Li, F. Zhou, Xin Wang, and M. Feng. Exploring the experimental limit of deep quantum signal processing using a trapped-ion simulator. *Phys. Rev. Appl.*, 23:034073, Mar 2025. doi:10.1103/PhysRevApplied.23.034073.

[41] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv preprint quant-ph/0005055*, 2000.

[42] Danial Motlagh and Nathan Wiebe. Generalized quantum signal processing. *PRX Quantum*, 5(2):020368, 2024. doi:10.1103/PRXQuantum.5.020368.

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

[44] Norbert Wiener and Pesi Masani. The prediction theory of multivariate stochastic processes. *Acta mathematica*, 98(1):111–150, 1957. doi:10.1007/BF02404472.

[45] 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. doi:10.1017/S0308210512001552.

[46] Jasmine Sinanan-Singh, Gabriel L Mintzer, Isaac L Chuang, and Yuan Liu. Single-shot quantum signal processing interferometry. *Quantum*, 8:1427, 2024. doi:10.22331/q-2024-07-30-1427.

[47] Christopher M Dawson and Michael A Nielsen. The solovay-kitaev algorithm. *arXiv preprint quant-ph/0505030*, 2005.

[48] Tien Trung Pham, Rodney Van Meter, and Dominic Horsman. Optimization of the solovay-kitaev algorithm. *Physical Review A—Atomic, Molecular, and Optical Physics*, 87(5):052332, 2013. doi:10.1103/PhysRevA.87.052332.

[49] Greg Kuperberg. Breaking the cubic barrier in the solovay-kitaev algorithm. *arXiv preprint arXiv:2306.13158*, 2023.

[50] Lorenzo Laneve and Stefan Wolf. On multivariate polynomials achievable with quantum signal processing. *Quantum*, 9:1641, February 2025. doi:10.22331/q-2025-02-20-1641.

[51] Leopold Fejér. Über trigonometrische polynome. 1916.

[52] Frigyes Riesz. über ein problem des herrn carathéodory. *JOURNAL FUR DIE REINE UND ANGEWANDTE MATHEMATIK*, 146:83–87, 1916.

[53] 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. doi:10.1103/PhysRevLett.98.090501.

[54] Wim Van Dam, G Mauro D'Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Optimal phase estimation in quantum networks. *Journal of Physics A: Mathematical and Theoretical*, 40(28):7971, 2007. doi:10.1088/1751-8113/40/28/S07.

[55] Wojciech Górecki, Rafał Demkowicz-Dobrzański, Howard M Wiseman, and Dominic W Berry. π-corrected heisenberg limit. *Physical review letters*, 124(3):030501, 2020. doi:10.1103/PhysRevLett.124.030501.

[56] Yuan Liu, Shraddha Singh, Kevin C. Smith, Eleanor Crane, John M. Martyn, Alec Eickbusch, Alexander Schuckert, Richard D. Li, Jasmine Sinanan-Singh, Micheline B. Soley, Takahiro Tsunoda, Isaac L. Chuang, Nathan Wiebe, and Steven M. Girvin. Hybrid oscillator-qubit quantum processors: Instruction set architectures, abstract machine models, and applications. *PRX Quantum*, 7:010201, Jan 2026. doi:10.1103/4rf7-9tfx.