

# On efficient quantum block encoding of pseudo-differential operators

Haoya Li<sup>1</sup>, Hongkang Ni<sup>2</sup>, and Lexing Ying<sup>1,2</sup>

<sup>1</sup>Department of Mathematics, Stanford University, Stanford, CA 94305

<sup>2</sup>Institute for Computational and Mathematical Engineering, Stanford University, Stanford, CA 94305

Block encoding lies at the core of many existing quantum algorithms. Meanwhile, efficient and explicit block encodings of dense operators are commonly acknowledged as a challenging problem. This paper presents a comprehensive study of the block encoding of a rich family of dense operators: the pseudo-differential operators (PDOs). First, a block encoding scheme for generic PDOs is developed. Then we propose a more efficient scheme for PDOs with a separable structure. Finally, we demonstrate an explicit and efficient block encoding algorithm for PDOs with a dimension-wise fully separable structure. Complexity analysis is provided for all block encoding algorithms presented. The application of theoretical results is illustrated with worked examples, including the representation of variable coefficient elliptic operators and the computation of the inverse of elliptic operators without invoking quantum linear system algorithms (QLSAs).

## 1 Introduction

Block encoding [25] is a widely used technique in quantum computing and a crucial component of many quantum algorithms with a potentially exponential advantage over classical algorithms, such as quantum phase estimation (QPE) [23, 31], the HHL algorithm [21], quantum singular value transformation (QSVT) [18] and various quantum linear system solvers [1, 13, 24], to name a few. The idea of block encoding is to embed a linear operator  $A$  into a unitary operator  $U_A$  with larger dimensions after appropriate scaling. The unitary  $U_A$  is then converted into a quantum circuit, allowing a quantum computer to access  $U_A$  for actual computations.

The potential advantage of quantum algorithms depends critically on efficient and practical quantum circuits for block-encoding of the operators involved, and the construction of such circuits can be non-trivial in general. Researchers have constructed block encoding schemes leveraging different structures of the operators studied. For example, a block encoding scheme is provided in [5, 18] for sparse matrices, and a recipe is presented for hierarchical matrices in [30]. In this paper, we consider the problem of block encoding a large family of dense operators: the pseudo-differential operators (PDOs). PDO is a rich family of linear operators that include many commonly used examples in scientific

---

Haoya Li: [lihaoya@stanford.edu](mailto:lihaoya@stanford.edu)

Hongkang Ni: [hongkang@stanford.edu](mailto:hongkang@stanford.edu)

Lexing Ying: [lexing@stanford.edu](mailto:lexing@stanford.edu)

problems, which is typically given in the following form:

$$Af(\mathbf{x}) = \int_{\mathbb{R}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} a(\mathbf{x}, \boldsymbol{\xi}) \widehat{f}(\boldsymbol{\xi}) d\boldsymbol{\xi}, \quad (1)$$

where  $a(\mathbf{x}, \boldsymbol{\xi}) \in C^\infty(\mathbb{R}^d \times \mathbb{R}^d)$  is called the symbol of  $A$  and  $\widehat{f}$  is the Fourier transform of  $f$ . A major motivation for studying operators with the form (1) is that differential operators often enjoy a simple representation in the Fourier domain. For example, the elliptic operator:

$$A = I - \nabla \cdot (\omega(\mathbf{x}) \nabla) \quad (2)$$

with  $\omega(\mathbf{x}) > 0$  can be represented in the form of (1) with the symbol

$$a(\mathbf{x}, \boldsymbol{\xi}) = 1 - 2\pi i \nabla \omega(\mathbf{x}) \cdot \boldsymbol{\xi} + 4\pi^2 \omega(\mathbf{x}) |\boldsymbol{\xi}|^2. \quad (3)$$

More generally, an  $m$ -th order linear partial differential operator  $P(\mathbf{x}, D) = \sum_{|\alpha| \leq m} a_\alpha(\mathbf{x}) D^\alpha$  with  $D = -\frac{i}{2\pi} \nabla_{\mathbf{x}}$  can be represented by

$$Pf(\mathbf{x}) = \int_{\mathbb{R}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} \sum_{|\alpha| \leq m} a_\alpha(\mathbf{x}) \boldsymbol{\xi}^\alpha \widehat{f}(\boldsymbol{\xi}) d\boldsymbol{\xi} = \int_{\mathbb{R}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} P(\mathbf{x}, \boldsymbol{\xi}) \widehat{f}(\boldsymbol{\xi}) d\boldsymbol{\xi},$$

where  $\alpha = (\alpha_1, \dots, \alpha_d)$  is the  $d$ -dimensional multi-index and  $|\alpha| = \sum_{j=1}^d \alpha_j$ . Another popular example is the translation-invariant operator. Let  $\varphi_{\boldsymbol{\xi}}(\mathbf{x}) = e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}}$  be a function of  $\mathbf{x}$ . If an operator  $A$  is translation-invariant, i.e.,  $(A\varphi_{\boldsymbol{\xi}})(\mathbf{x}) = a(\boldsymbol{\xi})\varphi_{\boldsymbol{\xi}}(\mathbf{x})$ , then

$$Af(\mathbf{x}) = \int_{\mathbb{R}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} a(\boldsymbol{\xi}) \widehat{f}(\boldsymbol{\xi}) d\boldsymbol{\xi}, \quad (4)$$

in which case we say that the symbol  $a(\boldsymbol{\xi})$  is a multiplier. Apart from the examples mentioned above, the PDO family also contains other operators such as convolution operators, singular integral operators, etc. Moreover, a space of PDOs is often closed with respect to many elementary operations under certain conditions. For example, for the operator  $A$  in (4) with symbol  $a(\boldsymbol{\xi}) \neq 0$ , the inverse of  $A$  can be simply represented by

$$A^{-1}f(\mathbf{x}) = \int_{\mathbb{R}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} \frac{1}{a(\boldsymbol{\xi})} \widehat{f}(\boldsymbol{\xi}) d\boldsymbol{\xi}.$$

In general, the operator defined by  $C^\infty$  function  $a(\mathbf{x}, \boldsymbol{\xi})$  as in (1) is called a pseudo-differential operator only if  $a(\mathbf{x}, \boldsymbol{\xi})$  satisfies some additional requirements such as

$$|\partial_{\mathbf{x}}^\alpha \partial_{\boldsymbol{\xi}}^\beta a(\mathbf{x}, \boldsymbol{\xi})| \leq C_{\alpha\beta} \langle \boldsymbol{\xi} \rangle^{m-\alpha-\beta},$$

where  $\langle \boldsymbol{\xi} \rangle := \sqrt{1 + |\boldsymbol{\xi}|^2}$ , and the space of the corresponding PDOs is denoted by  $S^m$ . There are multiple monographs on PDOs that interested readers can refer to, such as [34, 37].

The PDOs considered in this paper are equipped with a periodic boundary condition on the space domain  $\Omega = [0, 1]^d$ . The frequency variable  $\boldsymbol{\xi}$  thus takes the value on the integer grid, and the operator  $A$  becomes

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \mathbb{Z}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} a(\mathbf{x}, \boldsymbol{\xi}) \widehat{f}(\boldsymbol{\xi}), \quad (5)$$

where  $\widehat{f}$  is the coefficient of the Fourier series of  $f$ . In this paper, we derive block encoding schemes for the PDO (5) based on different additional structures of the symbol  $a(\mathbf{x}, \boldsymbol{\xi})$ . First, we present a block encoding scheme for generic symbols  $a(\mathbf{x}, \boldsymbol{\xi})$  without additional

structures. We then point out that the success probability of the quantum circuit can be significantly improved if the symbol  $a(\mathbf{x}, \boldsymbol{\xi})$  can be expanded into series:

$$a(\mathbf{x}, \boldsymbol{\xi}) = \sum_j \alpha_j(\mathbf{x})\beta_j(\boldsymbol{\xi}), \quad (6)$$

with only  $\mathcal{O}(1)$  terms. Furthermore, the circuit can be constructed in a much more explicit way with the help of quantum signal processing (QSP) and quantum eigenvalue transformation (QET) if the symbol is a sum of *fully separable* terms, i.e., it can be expanded as

$$a(\mathbf{x}, \boldsymbol{\xi}) = \sum_j \alpha_{j1}(x_1) \cdots \alpha_{jd}(x_d) \beta_{j1}(\xi_1) \cdots \beta_{jd}(\xi_d), \quad (7)$$

with  $\mathcal{O}(1)$  terms, where  $\mathbf{x} = (x_1, \dots, x_d)$  and  $\boldsymbol{\xi} = (\xi_1, \dots, \xi_d)$ . See Definition 2 and Section 5 for details. Complexity analysis is included for all block encoding schemes, and their applications are showcased with specific examples. The contributions of this paper can be summarized as follows:

- We provide practical block encoding schemes for pseudo-differential operators, including algorithms applicable to generic PDOs (see Figure 3), efficient block encoding for separable PDOs (see Figure 6) and explicit circuits for fully separable PDOs (see Figure 7). Novel ideas of circuit design, such as the phase multiplication circuit (see Figure 4) and the prototype for diagonal multiplication (see Figure 8), are included in the block encoding schemes.
- We conduct comprehensive complexity analysis for the block encoding schemes proposed. The result for complexity analysis includes the success probability, the number of ancilla qubits needed, and the number of gates used. In addition to theorems applicable to general cases, we also demonstrate possibilities of improving the complexity results by leveraging particular structures of the problem (see Section 6.1 for example).
- We demonstrate the usage of our results with explicit examples. One can use our block-encoding scheme not only as an integrated part of established quantum algorithms but also as an option for conducting operations directly on certain operators. For the example shown in Section 6.2, we use the idea of symbol calculus to directly block-encode the inverse of an elliptic operator and the dependence of the complexity on  $P$  (the number of discretization points used for each dimension) is at least quadratically improved compared to previous results for block-encoding the inverse matrix (see Remark 3).

## 1.1 Contents

The paper is organized as follows. In Section 2, we specify the notation used in this paper and provide preliminary results needed in subsequent sections, such as quantum Fourier transform (QFT), the linear combination of unitaries (LCU), quantum signal processing (QSP) and quantum eigenvalue transformation (QET). In Section 3, an algorithm is given for block encoding of generic symbols. For a separable symbol  $a(\mathbf{x}, \boldsymbol{\xi}) = \alpha(\mathbf{x})\beta(\boldsymbol{\xi})$ , a more efficient block encoding scheme is provided in Section 4. Then a more explicit and practically feasible block encoding is developed in Section 5 for fully separable symbols of the form displayed in (7). Finally, Section 6 presents the application of the proposed block encoding method to two types of widely used PDOs, including a variable coefficient second-order elliptic operator and the inverse of a constant coefficient elliptic operator. The paper is ended with a conclusion and discussion for future directions in Section 7.

## 1.2 Related works

### 1.2.1 Block encoding

Most of the previous work [2, 9, 25] assumes that we have access to a matrix by querying two oracles that encode the locations and values of the non-zero elements of the objective matrix. Among them, [18]\*Lemma 48 provides a general framework to explicitly construct the block encoding of sparse matrices if we are given these two oracles. Following this routine, [5] constructs the block encoding of banded circulant matrices, extended binary tree matrices, and quantum walk operators.

For general non-sparse matrices, it is clearly impossible to block-encode them in logarithmic time, and [4] proposes a near-optimal scheme for block encoding general unstructured matrices. Many methods are also proposed to implement the block encoding for full-rank dense matrices with certain structures, such as Toeplitz and Hankel systems [26], and linear group convolutions [7] based on quantum Fourier transforms. The authors of [30] introduce a new method for kernel matrices with a hierarchical structure, which can be applied to non-uniform grids the Fourier transform cannot be used.

### 1.2.2 Quantum PDE solvers

Along with the development of quantum linear system solvers [9, 13, 18, 21, 24], many quantum PDE solvers are proposed to take advantage of exponential acceleration. Quantum counterparts of the finite element method (FEM) [28] and the finite difference method (FDM) [6, 12] emerged for solving Poisson's equation and wave equation. In [10], adaptive finite difference and spectral methods are proposed to improve the dependence of the complexity on the error  $\epsilon$  from  $\mathcal{O}(\text{poly}(1/\epsilon))$  to  $\mathcal{O}(\text{polylog}(1/\epsilon))$ . It is worth noting that the process of block encoding the discretized differential operator is often not provided in these works, and constructing the block encoding for generic partial differential operators is highly non-trivial.

### 1.2.3 Numerical algorithms for PDOs

There are also various classical numerical algorithms that compute PDOs efficiently. For example, [15] exploits the following expansion of symbols:

$$a(\mathbf{x}, \boldsymbol{\xi}) \approx \sum_j \alpha_j(\mathbf{x}) \beta_j(\boldsymbol{\xi}).$$

The paper presents efficient numerical approximations of  $\beta_j(\boldsymbol{\xi})$  with Chebyshev polynomials and hierarchical splines and further reduces the number of terms in the expansion by SVD or QR decomposition. However, a naive extension to high-dimensional PDOs leads to exponential overhead, as is the case for most classical methods. This is also one of the reasons why a quantum implementation of PDOs can be potentially useful.

## 2 Preliminaries and notations

### 2.1 Notations

We adopt the commonly used notation for binary numbers: for an integer power of two  $P = 2^p$  and any  $y \in \{0, \dots, P - 1\}$  if  $y = y_0 + 2y_1 + \dots + 2^{p-1}y_{p-1} = (y_{p-1}y_{p-2} \dots y_0)$  in the binary system, the corresponding quantum state is  $|y\rangle \equiv |y_{p-1} \dots y_0\rangle$ .

This extends to an  $m$ -tuple  $\mathbf{x} = (x_1, \dots, x_m)$  with  $x_j \in \{0, \dots, P-1\}$ . The corresponding quantum state is given by  $|x_m\rangle \cdots |x_1\rangle$ , where  $|x_j\rangle = |x_{j,p-1} \cdots x_{j,0}\rangle$  for each  $j$ . For a multivariate function  $g : \{0, \dots, P-1\}^m \rightarrow \mathbb{R}$ , we denote by  $D_g$  the diagonal multiplication operator on the Hilbert space  $\mathbb{C}^{mp}$ :

$$|x_m\rangle \cdots |x_1\rangle \rightarrow g(x_1, \dots, x_m) |x_m\rangle \cdots |x_1\rangle. \quad (8)$$

For a vector  $\mathbf{v} = (v_1, v_2, \dots, v_m)$ , we denote by  $\text{diag}(\mathbf{v})$  the diagonal matrix with diagonal elements  $(v_1, v_2, \dots, v_m)$ .

The notation  $|\mathbf{v}|$  for a  $d$ -dimensional vector  $\mathbf{v}$  stands for the Euclidean norm  $\sqrt{\sum_{j=1}^d |v_j|^2}$ , where  $v_j$  is the  $j$ -th coordinate of  $\mathbf{v}$ .

We also use the single qubit rotations  $R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$  and  $R_z(\theta) = e^{i\frac{\theta}{2}} e^{-i\frac{\theta}{2}Z} = \begin{bmatrix} 1 & \\ & e^{i\theta} \end{bmatrix}$ , where  $Y$  and  $Z$  are the Pauli matrices  $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$  and  $Z = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$ . The phase gate  $S = \sqrt{Z}$  denotes the matrix  $S = \begin{bmatrix} 1 & \\ & i \end{bmatrix}$ . To simplify the discussion, we assume access to all single qubit rotations, the Hadamard gate, the CNOT gate, the 2-qubit SWAP gate, and the Toffoli gate when counting the number of elementary gates used. If one wants to use certain commonly used universal gate sets such as Hadamard and Toffoli, there will be some overhead linear in the number of gates involved and polylogarithm in the precision  $\epsilon$ , as bounded by the famous Solovay–Kitaev theorem [22]. There are also many established results on decomposing commonly seen quantum gates with a certain universal gate set, such as [14, 32, 36], to name a few.

An  $(m+n)$ -qubit unitary operator  $U$  is called a  $(\gamma, m, \epsilon)$ -block-encoding of an  $n$ -qubit operator  $A$ , if

$$\|A - \gamma(\langle 0^m | \otimes I_n) U (|0^m\rangle \otimes I_n)\| \leq \epsilon,$$

where  $I_n$  denotes the  $n$ -qubit identity operator. In the matrix form, a  $(\gamma, m, \epsilon)$ -block-encoding is a  $2^{m+n}$  dimensional unitary matrix

$$U = \begin{pmatrix} \tilde{A}/\gamma & * \\ * & * \end{pmatrix}$$

where  $*$  can be any block matrices of the correct size and  $\|\tilde{A} - A\| \leq \epsilon$ . In addition, when  $A$  is a Hermitian matrix, it is possible to construct  $U_A$  such that it is also Hermitian, in which case it is called a  $(\gamma, m, \epsilon)$ -Hermitian-block-encoding of  $A$ . The error  $\epsilon$  is omitted in the notation of block encodings if  $\epsilon = 0$ .

For an  $n$ -qubit system, the quantum Fourier transform (QFT) is an implementation of

$$U_{\text{FT}} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{kj}{N}} |k\rangle, \quad (9)$$

where  $N = 2^n$ , using a circuit  $U_{\text{FT}}$  with  $\mathcal{O}(n^2)$  elementary gates and no ancilla qubit. The elementary gates involved include 2-qubit swap gates and 2-qubit controlled rotation gates. We refer the readers to [11, 31] for more details on QFT. If only an approximation of  $U_{\text{FT}}$  is needed, one can use approximated QFT [29], which has gate complexity  $\mathcal{O}(n \log(n/\epsilon))$ , where  $\epsilon$  is the spectral norm error of the approximation.

## 2.2 Linear combination of unitaries (LCU)

Given a few block-encoded matrices, a block encoding of a certain linear combination of them is often needed in practice. To this end, the linear combination of unitaries (LCU) technique has been developed ([2, 9, 18]). For example, for two matrices  $A$  and  $B$ , a block encoding of  $A + B$  can be given by the circuit in Figure 1, where  $U_A$  and  $U_B$  are block encodings of  $A$  and  $B$ , respectively.

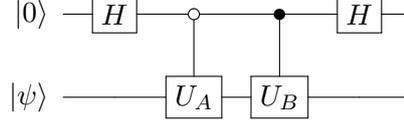


Figure 1: LCU for two unitaries

For general linear combinations, we recall the following result from [18] for general linear combinations.

**Lemma 1.** *For a vector  $y \in \mathbb{C}^m$  with  $\|y\|_1 \leq \beta$ , assume we have*

1. *a pair of unitaries  $(U_L, U_R)$  with shape  $2^b \times 2^b$  such that  $U_L |0^b\rangle = \sum_{j=0}^{2^b-1} c_j |j\rangle$ ,  $U_R |0^b\rangle = \sum_{j=0}^{2^b-1} d_j |j\rangle$ ,  $\sum_{j=0}^{m-1} |\beta c_j^* d_j - y_j| < \epsilon_1$  and  $\sum_{j=m}^{2^b-1} |c_j^* d_j| = 0$ , and*
2. *a unitary  $W = \sum_{j=0}^{m-1} |j\rangle \langle j| \otimes U_j + \sum_{j=m}^{2^b-1} |j\rangle \langle j| \otimes I_{a+s}$  where each  $U_j$  is an  $(\alpha, a, \epsilon_2)$ -block-encoding of  $A_j$  for  $j = 0, 1, \dots, m-1$ ,*

*then  $(U_L^\dagger \otimes I_{a+s})W(U_R \otimes I_{a+s})$  is an  $(\alpha\beta, a+b, \alpha\epsilon_1 + \beta\epsilon_2)$ -block-encoding of  $\sum_{j=0}^{m-1} y_j A_j$ , where  $I_{a+s}$  denotes the identity operator with size  $2^{a+s} \times 2^{a+s}$ .*

## 2.3 Quantum eigenvalue transformation and quantum signal processing

Given a Hermitian block encoding of Hermitian matrix  $A$ , one can construct a block encoding of  $f(A)$  for a certain function  $f$  using the qWeET) technique [18, 25]. Let  $f^e(\mathbf{x}) = \frac{1}{2}(f(\mathbf{x}) + f(-\mathbf{x}))$  and  $f^o(\mathbf{x}) = \frac{1}{2}(f(\mathbf{x}) - f(-\mathbf{x}))$  be the even and odd part of  $f(\mathbf{x})$ , respectively. The standard procedure consists of the following steps, where we assume that  $f(\mathbf{x})$  is properly scaled such that  $\|f^e\| < 1$ ,  $\|f^o\| < 1$ , and  $\|\cdot\|$  denotes the  $L^\infty$  norm on  $[-1, 1]$ .

1. Approximate  $f^e$  and  $f^o$  with degree  $\deg_{f^e}(\epsilon)$  even polynomial  $\tilde{f}^e$  and degree  $\deg_{f^o}(\epsilon)$  odd polynomial  $\tilde{f}^o$ , respectively, such that  $\|\tilde{f}^e - f^e\| + \|\tilde{f}^o - f^o\| < \epsilon$  and  $\|\tilde{f}^e\| \leq 1$ ,  $\|\tilde{f}^o\| \leq 1$ .
2. Find two sequences of phase factors  $(\phi_0^e, \dots, \phi_{\deg_{f^e}(\epsilon)}^e), (\phi_0^o, \dots, \phi_{\deg_{f^o}(\epsilon)}^o)$  with each element in  $[-\pi, \pi]$  using quantum signal processing (QSP) such that  $\tilde{f}^e(\mathbf{x}) = \text{Re}(p^e(\mathbf{x}))$ ,  $\tilde{f}^o(\mathbf{x}) = \text{Re}(p^o(\mathbf{x}))$ , where  $p^e$  and  $p^o$  are complex polynomials with degree  $\deg_{f^e}(\epsilon)$  and  $\deg_{f^o}(\epsilon)$ , respectively, given by

$$\begin{bmatrix} p(\mathbf{x}) & r(\mathbf{x}) \\ r^*(\mathbf{x}) & p^*(\mathbf{x}) \end{bmatrix} = e^{i\phi_0 Z} e^{i \arccos x X} e^{i\phi_1 Z} e^{i \arccos x X} \dots e^{i\phi_{\deg_{f^e}(\epsilon)-1} Z} e^{i \arccos x X} e^{i\phi_{\deg_{f^e}(\epsilon)} Z}. \quad (10)$$

Here, the superscripts  $e$  and  $o$  are omitted for simplicity. The phase factors are then used in the QET circuit shown in Figure 2(b) to construct block encodings  $U_{f^e(A)}$  and  $U_{f^o(A)}$ , where the controlled rotation gate  $\text{CR}_\phi$  is described in Figure 2(a)

3. Combine the block encodings  $U_{f^e(A)}$  and  $U_{f^o(A)}$  with the LCU circuit in Figure 1 to form the block encoding  $U_{f(A)}$

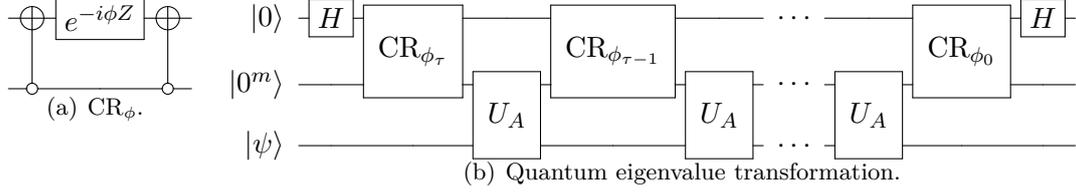


Figure 2: (a): Circuit for the controlled rotation gate  $\text{CR}_\phi$ . (b): Circuit for quantum eigenvalue transformation. The circuit in (b) gives a block encoding for  $U_{\text{Re}(p(A))}$  based on the block encoding  $U_A$  and phase factors  $(\phi_0, \dots, \phi_\tau)$ , where  $\tau = \deg_f(\epsilon)$  and the polynomial  $p(x)$  and the phase factors satisfy (10).

There are several methods to find the phase factors  $(\phi_0^e, \dots, \phi_{\deg_f(\epsilon)}^e)$  and  $(\phi_0^o, \dots, \phi_{\deg_f(\epsilon)}^o)$  in  $[-\pi, \pi]^{\deg_f(\epsilon)+1}$  in a stable and efficient way. For example, we refer to [8, 16, 17, 20, 38] for more details. We summarize the procedure given above in Lemma 2 below, where we assume that  $f$  is either even or odd for simplicity.

**Lemma 2.** *For an even (resp. odd) function  $f : \mathbb{R} \rightarrow \mathbb{R}$  and an  $(\alpha, m)$ -Hermitian-block-encoding of  $A$  denoted as  $U_A$ , there is an  $(\alpha C_f, m + 1, \epsilon)$ -block-encoding of  $f(A)$  with gate complexity  $\mathcal{O}(\deg_f(\epsilon)(G_A + m))$  using the circuit shown in Figure 2(b), where  $C_f \geq \max\{1, \|f\|\}$  is a scaling factor,  $G_A$  is the gate complexity of  $U_A$  and  $\deg_f(\epsilon)$  is the smallest integer such that there exists an even (resp. odd) polynomial  $\tilde{f}$  with a degree bounded by  $\deg_f(\epsilon)$  satisfying  $\|f - C_f \tilde{f}\| < \epsilon$  and  $\|\tilde{f}\| \leq 1$ . The phase factors  $(\phi_0, \dots, \phi_{\deg_f(\epsilon)})$  in Figure 2(b) are related with  $\tilde{f}$  through (10) and  $\tilde{f} = \text{Re}(p)$ .*

## 2.4 Discretization of pseudo-differential operators

As mentioned in Section 1, the PDO considered in this paper is defined for periodic functions on  $\Omega = [0, 1]^d$ :

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \mathbb{Z}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}} a(\mathbf{x}, \boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}).$$

In most numerical treatments, the function  $f$  is given on a discrete grid  $X = \{\frac{\mathbf{x}}{P} \equiv (\frac{x_1}{P}, \dots, \frac{x_d}{P}) : x_j \in \{0, 1, \dots, P-1\}\}$ , where  $P = 2^p$  is the number of discrete points used for each dimension. Notice that here we slightly abuse the notation by reusing  $\mathbf{x}$  for the integer index of the grid points. Since the space variable takes value on the Cartesian grid  $X$ , the frequency domain is discretized correspondingly on  $\{-\frac{P}{2}, \dots, \frac{P}{2} - 1\}^d$ , which leads to the discretized PDO:

$$Af(\mathbf{x}) \equiv \sum_{\boldsymbol{\xi} \in \{-\frac{P}{2}, \dots, \frac{P}{2} - 1\}^d} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} a(\frac{\mathbf{x}}{P}, \boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}), \quad \mathbf{x} \in \Xi, \quad (11)$$

where  $\Xi = \{0, 1, \dots, P-1\}^d$ . We adopt an abuse of notation and denote the discretized PDO by  $A$  too.

Though the frequency variable  $\boldsymbol{\xi}$  is discretized on  $\{-\frac{P}{2}, \dots, \frac{P}{2} - 1\}^d$  in (11), by the convention of discrete Fourier transform (DFT) and fast Fourier transform (FFT), the frequency  $(P/2, \dots, P-1)$  is often identified with  $(-P/2, \dots, -1)$ , respectively, since  $P$

is a period for the frequency variable after DFT. In other words, the discretized PDO can be written as

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \Xi} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \tilde{a}\left(\frac{\mathbf{x}}{P}, \boldsymbol{\xi}\right) \hat{f}(\boldsymbol{\xi}), \quad \mathbf{x} \in \Xi = \{0, 1, \dots, P-1\}^d,$$

where

$$\tilde{a}(\mathbf{x}, \boldsymbol{\xi}) \equiv a\left(\mathbf{x}, \boldsymbol{\xi} - P \sum_{\xi_j \geq P/2} \mathbf{e}_j\right),$$

and  $\mathbf{e}_j$  is the  $j$ -th standard basis vector in  $\mathbb{C}^d$ . As an example, when  $d = 1$ , we have

$$\tilde{a}(x, \xi) = \begin{cases} a(x, \xi), & 0 \leq \xi < P/2, \\ a(x, \xi - P), & P/2 \leq \xi < P. \end{cases}$$

To simplify the notation and avoid repetitive use of  $P$ , we further define

$$\check{a}(\mathbf{x}, \boldsymbol{\xi}) \equiv \tilde{a}\left(\frac{\mathbf{x}}{P}, \boldsymbol{\xi}\right), \quad (12)$$

and the discretized PDO becomes

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \Xi} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \check{a}(\mathbf{x}, \boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}), \quad \mathbf{x} \in \Xi. \quad (13)$$

It is clear that  $\sup |\check{a}| = \sup |a|$ . In what follows, we also refer to  $\check{a}$  as the symbol of the PDO to be computed.

### 3 Block encoding for generic symbols

This section is concerned with the block encoding of the PDO (11) (or rather (13)) with a generic symbol  $a(\mathbf{x}, \boldsymbol{\xi})$ , without assuming any additional structure. In order to compute the PDO in (13), a simple strategy is to first lift the state to the phase space  $\Xi \times \Xi$ . Then the multiplication of  $\check{a}(\mathbf{x}, \boldsymbol{\xi})$  in (13) can be performed by diagonal matrix block encodings. Combining the QFT circuit and the block encoding of diagonal matrices, one can construct the entire circuit as illustrated in Figure 3.

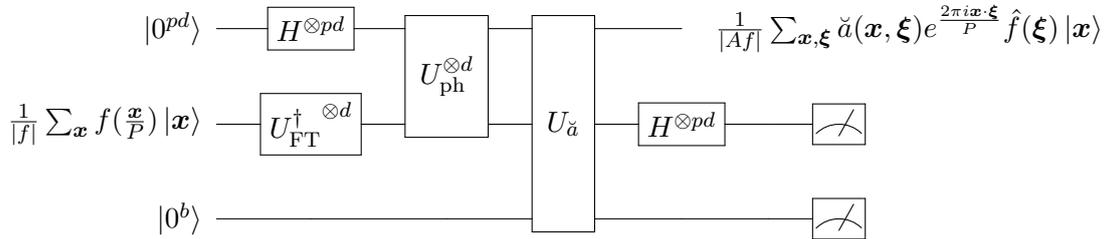


Figure 3: Circuit that implements the PDO in (13) with a generic symbol. Here  $b$  is the number of ancilla qubits needed for  $U_{\check{a}}$ ,  $H$  is the Hadamard gate,  $\frac{1}{|f|} \sum_{\mathbf{x}} f(\frac{\mathbf{x}}{P}) |\mathbf{x}\rangle$  is the normalized input data,  $U_{FT}$  is the QFT circuit,  $U_{ph}$  and  $U_{\check{a}}$  are the circuits that perform the multiplication of  $e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P}$  and  $\check{a}(\mathbf{x}, \boldsymbol{\xi})$  in (13), and the desired output is obtained with normalizing factor  $\frac{1}{|Af|}$  when getting  $|0^{pd+b}\rangle$  for the  $pd + b$  qubits on the bottom.

Now we explain the circuit displayed in Figure 3 in more detail. First, we assume that the information of the function  $f$  is prepared by a normalized vector  $\frac{1}{|f|} \sum_{\mathbf{x}} f(\frac{\mathbf{x}}{P}) |\mathbf{x}\rangle$ , where

$|f|$  is the normalization factor

$$|f| = \sqrt{\sum_{\mathbf{x} \in \Xi} \left| f\left(\frac{\mathbf{x}}{P}\right) \right|^2},$$

and  $\Xi = \{0, 1, \dots, P-1\}^d$ . For functions  $f$  with certain properties such as integrability, the state  $\frac{1}{|\mathcal{F}|} \sum_{\mathbf{x}} f\left(\frac{\mathbf{x}}{P}\right) |\mathbf{x}\rangle$  can be constructed efficiently (see [19] for more details). For the rest of the paper, we assume the accessibility of the state  $\frac{1}{|\mathcal{F}|} \sum_{\mathbf{x}} f\left(\frac{\mathbf{x}}{P}\right) |\mathbf{x}\rangle$  as an input.

**Step 1. Apply QFT and lift the input state to the phase space.** We first obtain the representation of  $f$  in the frequency domain by QFT. After applying the (inverse) QFT to the state  $\frac{1}{|\mathcal{F}|} \sum_{\mathbf{x}} f\left(\frac{\mathbf{x}}{P}\right) |\mathbf{x}\rangle$  for  $d$  times, we get

$$\frac{1}{|f|} \frac{1}{\sqrt{P^d}} \sum_{\xi} \sum_{\mathbf{x}} f\left(\frac{\mathbf{x}}{P}\right) e^{-2\pi i \xi \cdot \mathbf{x}/P} |\xi\rangle = \frac{\sqrt{P^d}}{|f|} \sum_{\xi} \hat{f}(\xi) |\xi\rangle. \quad (14)$$

Then the state  $\frac{1}{|\mathcal{F}|} \sum_{\mathbf{x}, \xi} \hat{f}(\xi) |\mathbf{x}\rangle |\xi\rangle$  is obtained by applying the Hadamard gates  $H^{\otimes pd}$  to the  $\mathbf{x}$ -register and putting both registers together.

**Step 2. Multiply the phase  $e^{2\pi i \mathbf{x} \cdot \xi/P}$  with  $U_{\text{ph}}$ .** A naive way of multiplying the phase  $e^{2\pi i \mathbf{x} \cdot \xi/P}$  is to use Proposition 19, which involves many ancilla qubits and reduces the success probability. Here, we develop an efficient implementation for multiplication without involving any extra error or ancilla qubits in the following lemma.

**Lemma 3.** *The  $2p$ -qubit circuit  $U_{\text{ph}}$  displayed in Figure 4 implements the unitary operator:*

$$|x\rangle |\xi\rangle \mapsto e^{2\pi i x \xi/P} |x\rangle |\xi\rangle, \quad 0 \leq x, \xi < P, \quad (15)$$

with  $\mathcal{O}(p^2)$  gate complexity precisely without ancilla qubits.

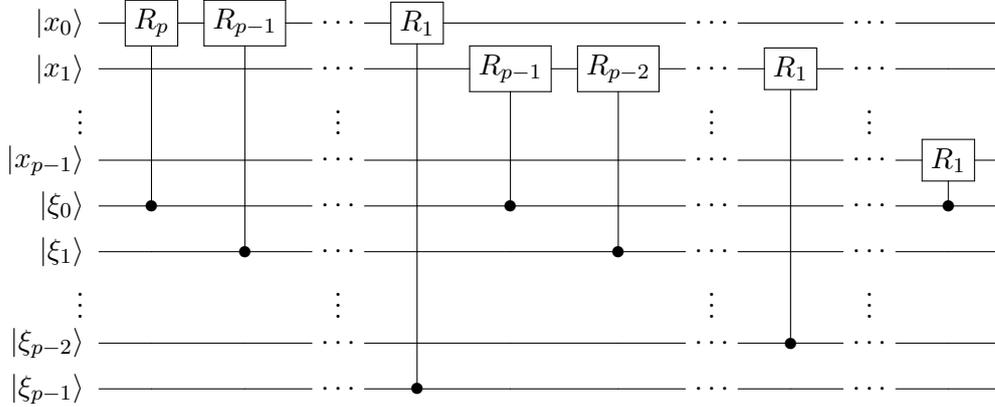


Figure 4: Circuit for  $U_{\text{ph}}$ , the phase multiplication  $|x\rangle |\xi\rangle \mapsto e^{2\pi i x \xi/P} |x\rangle |\xi\rangle$ . Here  $R_j = |0\rangle\langle 0| + e^{2\pi i \cdot 2^{-j}} |1\rangle\langle 1|$  is a rotation operator.

*Proof.* The idea of the construction is similar to the implementation of QFT, which is based on bit-wise controlled rotation. We first write the binary representation of integers

$$x = (x_{p-1} \cdots x_0.), \quad \xi = (\xi_{p-1} \cdots \xi_0.),$$

and do the following calculation:

$$\begin{aligned}
e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} |x\rangle |\boldsymbol{\xi}\rangle &= \left( \prod_{j=0}^{p-1} \prod_{k=0}^{p-1} e^{2\pi i x_j \xi_k \cdot 2^{j+k-p}} \right) |x_{p-1} \cdots x_0\rangle |\xi_{p-1} \cdots \xi_0\rangle \\
&= \left( \prod_{0 \leq j+k < p} e^{2\pi i x_j \xi_k \cdot 2^{j+k-p}} \right) |x_{p-1} \cdots x_0\rangle |\xi_{p-1} \cdots \xi_0\rangle \\
&= \left( \left( \prod_{k=0}^{p-1} e^{2\pi i x_0 \xi_k \cdot 2^{k-p}} \right) |x_0\rangle \right) \otimes \cdots \otimes \left( \left( \prod_{k=0}^0 e^{2\pi i x_{p-1} \xi_k \cdot 2^{k-1}} \right) |x_{p-1}\rangle \right) \otimes |\xi_{p-1} \cdots \xi_0\rangle,
\end{aligned} \tag{16}$$

where the second equality is true because  $e^{2\pi i x_j \xi_k \cdot 2^{j+k-p}} = 1$  when  $j+k \geq p$ . The circuit corresponding to the unitary in (16) can be implemented by a series of controlled rotations

$$\begin{array}{ccc}
|x_j\rangle & \text{---} \boxed{R_{p-j-k}} \text{---} & e^{2\pi i x_j \xi_k \cdot 2^{j+k-p}} |x_j\rangle \\
|\xi_k\rangle & \text{---} \bullet \text{---} & |\xi_k\rangle
\end{array}$$

where  $R_j = R_z(\pi/2^{j-1}) = |0\rangle\langle 0| + e^{2\pi i \cdot 2^{-j}} |1\rangle\langle 1|$ . Finally, the circuit shown in Figure 4 is obtained after arranging the controlled rotations in the corresponding places.  $\square$

Rewriting the state  $\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle$  as

$$\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i x_d \xi_d / P} \cdots e^{2\pi i x_1 \xi_1 / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle,$$

then the map from  $\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle$  to  $\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle$  can be performed by applying Lemma 3 for  $d$  times to the register pairs  $(x_d, \xi_d), \dots, (x_1, \xi_1)$ . The corresponding circuit is denoted as  $U_{\text{ph}}^{\otimes d}$  and involves  $\mathcal{O}(p^2 d)$  elementary gates with no ancilla qubits. After the multiplication of  $U_{\text{ph}}^{\otimes d}$ , one obtains the state  $\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle$ .

**Step 3. Multiply the symbol  $\check{a}(\mathbf{x}, \boldsymbol{\xi})$ .** The next component in Figure 3 is the diagonal multiplication  $U_{\check{a}}$ , which is designed to approximate the map

$$\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle |0^b\rangle \mapsto \frac{1}{C_a |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{a}(\mathbf{x}, \boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle |0^b\rangle + \perp, \tag{17}$$

where  $C_a > 0$  is a constant that depends on  $\check{a}(\mathbf{x}, \boldsymbol{\xi})$ ,  $b$  is the number of ancilla qubits used for  $U_{\check{a}}$  and  $\perp$  is an unnormalized state that is orthogonal to any state of the form  $|\mathbf{x}\rangle |\boldsymbol{\xi}\rangle |0^b\rangle$ . As mentioned earlier, the idea is to treat  $(\mathbf{x}, \boldsymbol{\xi})$  as a  $2d$ -dimensional variable and utilize the result from arithmetic circuit construction. Leveraging the reversible computational model and the uncomputation technique, any classical arithmetic operation can be implemented by a quantum circuit efficiently. More specifically, one can construct a corresponding quantum circuit using  $\mathcal{O}(\text{polylog}(\frac{1}{\epsilon}))$  ancilla qubits and  $\mathcal{O}(\text{polylog}(\frac{1}{\epsilon}))$  gates, where  $\epsilon$  is the precision one wants to achieve (Cf. [31, 32]). We state a general result for an efficient block encoding of diagonal matrices  $D_g$ , as defined in (8), which is summarized in Proposition 4. A similar idea has been used in [19] to create a given state, in [21] to construct the reciprocals of the eigenvalues and in [35] to implement the diagonal preconditioner.

**Proposition 4.** *Assume that  $g : \mathbb{R}^m \rightarrow \mathbb{R}$  is a smooth arithmetic function with  $\sup |g| < \infty$ . Then there is an  $(C, \mathcal{O}(\text{polylog}(\frac{1}{\epsilon}) + \text{poly}(mp)), \epsilon)$ -block-encoding of  $D_g$  with  $\mathcal{O}(\text{polylog}(\frac{1}{\epsilon}) + \text{poly}(mp))$  gates, where  $D_g$  is a diagonal operator on the Hilbert space  $\mathbb{C}^{mp}$  defined in (8), and  $C \geq \sup |g|$ .*

*Proof.* The circuit  $U_g$  is constructed as follows. Let  $t = \lceil \log_2(\frac{C\pi}{\epsilon}) \rceil$ , and let  $\theta(x_1, \dots, x_m)$  be a map that gives  $|\theta_{\text{sgn}}\theta_{t-1}\theta_{t-2}\dots\theta_0\rangle$ , where  $(.\theta_{t-1}\theta_{t-2}\dots\theta_0)$  is the closest  $t$ -bit fixed-point representation of  $\frac{1}{\pi} \arcsin(|g(x_1, \dots, x_m)|/C)$ , and  $\theta_{\text{sgn}}$  is assigned the value 0 if  $g \geq 0$  and the value 1 otherwise. For an arbitrary basis state  $|x_m\rangle \dots |x_1\rangle$ , we consider the system with  $t+2$  ancilla qubits  $|0\rangle |x_m\rangle \dots |x_1\rangle |0^{t+1}\rangle$ . Here  $|x_j\rangle = |x_{j,p-1} \dots x_{j,0}\rangle$  for each  $j$ . Using the reversible computational model and uncomputation ([31, 32]), the classical circuit:

$$|0\rangle |x_m\rangle \dots |x_1\rangle |0^{t+1}\rangle \rightarrow |0\rangle |x_m\rangle \dots |x_1\rangle |\theta_{\text{sgn}}\theta_{t-1}\theta_{t-2}\dots\theta_0\rangle$$

can be constructed with  $\mathcal{O}(\text{poly}(t) + \text{poly}(mp))$  gates and  $\mathcal{O}(\text{poly}(mp))$  ancilla qubits. Then we apply the circuit in Figure 5 on the  $t+2$  ancilla qubits. The state obtained is:

$$(-1)^{\theta_{\text{sgn}}} (\cos(\pi(. \theta_{t-1} \dots \theta_0)) |1\rangle + \sin(\pi(. \theta_{t-1} \dots \theta_0)) |0\rangle) |x_m\rangle \dots |x_1\rangle |\theta_{\text{sgn}}\theta_{t-1}\theta_{t-2}\dots\theta_0\rangle,$$

which can then be mapped to

$$(-1)^{\theta_{\text{sgn}}} (\cos(\pi(. \theta_{t-1} \dots \theta_0)) |1\rangle + \sin(\pi(. \theta_{t-1} \dots \theta_0)) |0\rangle) |x_m\rangle \dots |x_1\rangle |0^{t+1}\rangle,$$

via uncomputation.

Since  $|(. \theta_{t-1} \dots \theta_0) - \frac{1}{\pi} \arcsin(|g(x_1, \dots, x_m)|/C)| < \frac{\epsilon}{C\pi}$ , we have  $|(-1)^{\theta_{\text{sgn}}} \sin(\pi(. \theta_{t-1} \dots \theta_0)) - \frac{1}{C}g(x_1, \dots, x_m)| < \frac{\epsilon}{C}$ , which means the desired state  $\frac{1}{C}g(x_1, \dots, x_m) |x_m\rangle \dots |x_1\rangle$  is obtained with error at most  $\frac{\epsilon}{C}$  upon measuring the ancilla qubits and getting  $|0^{t+2}\rangle$ .  $\square$

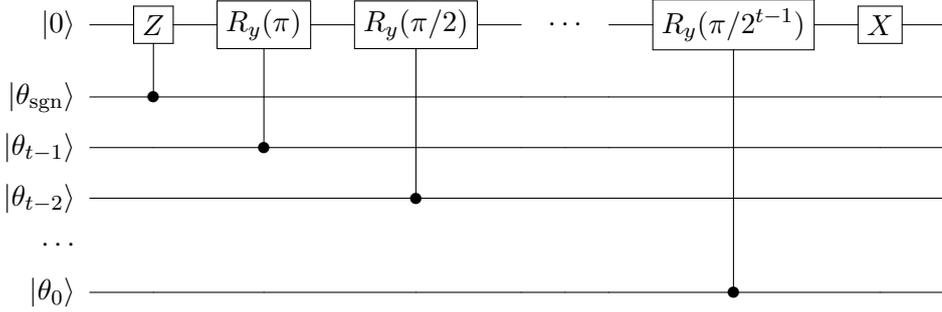


Figure 5: The controlled rotation part of  $U_g$ .

As a result of applying the block encoding given in Proposition 4 with  $m = 2d$ ,  $g = \check{a}$  and  $\epsilon$  replaced by  $\epsilon/\sqrt{P^d}$  to the state  $\frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}/P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle |0^b\rangle$ , one obtains the state

$$|\phi\rangle |0^b\rangle + \perp,$$

using  $\mathcal{O}(\text{polylog}(\frac{1}{\epsilon}) + \text{poly}(pd))$  ancilla qubits and  $\mathcal{O}(\text{polylog}(\frac{1}{\epsilon}) + \text{poly}(pd))$  gates where

$$\left\| |\phi\rangle - \frac{1}{C_a |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{a}(\mathbf{x}, \boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}/P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |\boldsymbol{\xi}\rangle \right\| < \frac{\epsilon}{\sqrt{P^d} C_a}, \quad (18)$$

and  $C_a \geq \sup |a| = \sup |\check{a}|$  is a constant. Here  $|\phi\rangle$  denotes an unnormalized  $2pd$ -qubit state and  $\perp$  is an unnormalized state orthogonal to all state with the form  $|\mathbf{x}\rangle |\boldsymbol{\xi}\rangle |0^b\rangle$ .

**Step 4. Sum over the frequency variable.** Finally, after applying the Hadamard gate  $H^{\otimes pd}$  to the  $\boldsymbol{\xi}$  registers, we obtain the state

$$\left( (I_{pd} \otimes |0^{pd}\rangle) (I_{pd} \otimes \langle 0^{pd}|) (I_{pd} \otimes H^{\otimes pd}) |\phi\rangle \right) |0^b\rangle + \tilde{\perp}, \quad (19)$$

where  $\tilde{\perp}$  is an unnormalized state that is orthogonal to all states of the form  $|\mathbf{x}\rangle|0^{pd+b}\rangle$  and

$$\left\| \left( (I_{pd} \otimes |0^{pd}\rangle)(I_{pd} \otimes \langle 0^{pd}|)(I_{pd} \otimes H^{\otimes pd})|\phi\rangle \right) |0^b\rangle - \frac{1}{\sqrt{P^d}|f|C_a} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\alpha}(\mathbf{x}, \boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle |0^{pd}\rangle |0^b\rangle \right\| < \frac{\epsilon}{\sqrt{P^d}C_a}, \quad (20)$$

which can be seen from (18). Therefore, one obtains the desired state on the  $\mathbf{x}$  registers upon measuring  $|0^{pd}\rangle$  for the  $\boldsymbol{\xi}$  registers and  $|0^b\rangle$  for the ancilla qubits. Notice that there is an extra scaling factor  $\frac{1}{\sqrt{P^d}}$  due to the application of Hadamard gates, so the success probability is  $\mathcal{O}(2^{-pd})$ . The complete circuit we use is exactly the one shown in Figure 3.

The block encoding scheme of the PDO (13) constructed in this section can be summarized in the following theorem:

**Theorem 5.** *For a generic symbol  $a(\mathbf{x}, \boldsymbol{\xi})$ , a block encoding of the corresponding discretized PDO defined by (13) can be  $(2^{\frac{pd}{2}}C_a, \mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon)), \epsilon)$ -block-encoded using the circuit displayed in Figure 3 with gate complexity  $\mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$ , where  $C_a \geq \sup |a|$  is a constant.*

**Challenge.** Despite being applicable to generic symbols, one can observe from (20) that the success probability of the circuit in Figure 3 can be low when  $pd$  is large. In the following sections, we show that this challenge can be overcome when the symbol  $a(\mathbf{x}, \boldsymbol{\xi})$  has additional structures.

## 4 Efficient block encoding for separable symbols

As explained in Section 3, the circuit designed as in Figure 3 suffers from exponentially small success probability, despite being simple and applicable to generic PDOs. In this section, we are concerned with symbols with particular structures and an efficient block encoding of the corresponding PDOs with  $\mathcal{O}(1)$  success probability is constructed.

### 4.1 Separable symbols

We first give the following definition for separable symbols.

**Definition 1.** A symbol  $a(\mathbf{x}, \boldsymbol{\xi})$  is *separable* if  $a(\mathbf{x}, \boldsymbol{\xi}) = \alpha(\mathbf{x})\beta(\boldsymbol{\xi})$ .

As explained in Section 2.4, we identify the frequency  $(P/2, \dots, P-1)$  with  $(-P/2, \dots, -1)$ , respectively, since  $P$  is a period for the frequency variable after DFT. We also define

$$\check{\alpha}(\mathbf{x}) = \alpha\left(\frac{\mathbf{x}}{P}\right), \quad \check{\beta}(\boldsymbol{\xi}) = \beta\left(\boldsymbol{\xi} - P \sum_{\xi_j \geq P/2} \mathbf{e}_j\right), \quad (21)$$

where  $\mathbf{e}_j$  is the  $j$ -th standard basis vector in  $\mathbb{C}^d$ . With help of the notations (21), the PDO (11) becomes

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \Xi} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \check{\alpha}(\mathbf{x}) \check{\beta}(\boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}), \quad \mathbf{x} \in \Xi = \{0, 1, \dots, P-1\}^d, \quad (22)$$

It is clear from the definition that  $\check{\alpha}$  is  $P$ -periodic since  $\alpha$  is 1-periodic, and we also have  $\sup |\alpha| = \sup |\check{\alpha}|$ ,  $\sup |\beta| = \sup |\check{\beta}|$ .

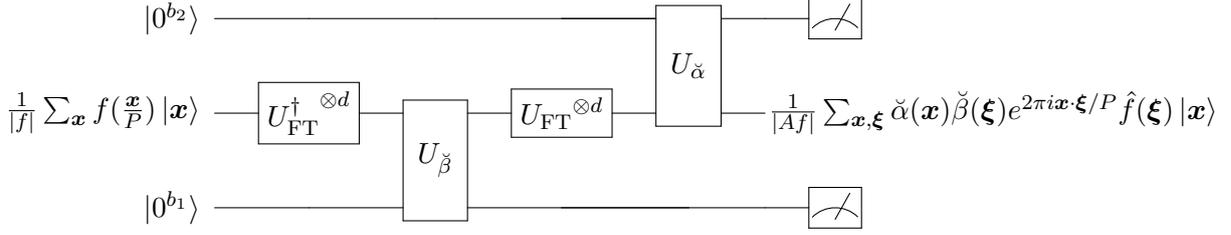


Figure 6: Circuit for an efficient block encoding for separable PDOs (22). Here  $b_1, b_2$  are the number of ancilla qubits needed for  $U_{\check{\beta}}$  and  $U_{\check{\alpha}}$ , respectively,  $\frac{1}{|f|} \sum_{\mathbf{x}} f(\frac{\mathbf{x}}{P}) |\mathbf{x}\rangle$  is the normalized input data,  $U_{\text{FT}}$  is the QFT circuit,  $U_{\check{\beta}}$ , and  $U_{\check{\alpha}}$  are the block encodings of  $D_{\check{\beta}}$  and  $D_{\check{\alpha}}$ , respectively, and the desired output is obtained with normalizing factor  $\frac{1}{|Af|}$  when getting  $|0^{b_1+b_2}\rangle$  for the  $b_1 + b_2$  ancilla qubits.  $D_{\check{\beta}}$  and  $D_{\check{\alpha}}$  are diagonal matrices defined in (8).

For the PDO (22), we propose an efficient block encoding illustrated by the following circuit.

For the rest of this section, we explain the circuit in Figure 6 with more details and show that it significantly improves the success probability compared with Figure 3. The circuit begins with a QFT step similar to that in Figure 3.

**Step 1. Apply QFT and multiply the factor  $\check{\beta}(\boldsymbol{\xi})$ .** With the same argument as (14), one obtains the state:

$$\frac{\sqrt{P^d}}{|f|} \sum_{\boldsymbol{\xi}} \hat{f}(\boldsymbol{\xi}) |\boldsymbol{\xi}\rangle |0^{b_1+b_2}\rangle,$$

after applying the QFT gates  $U_{\text{FT}}^{\dagger \otimes d}$ . Now that the input is represented on the frequency domain, one can naturally implement the multiplication of the factor  $\check{\beta}(\boldsymbol{\xi})$  since it only depends on the frequency variable  $\boldsymbol{\xi}$ . The corresponding block  $U_{\check{\beta}}$  can be constructed using Proposition 4 with  $m = d$ ,  $g = \check{\beta}$  and  $\epsilon$  replaced by  $\frac{\epsilon}{2C_\alpha}$ , where the constant  $C_\alpha \geq \sup |\alpha|$ . Then one obtains the state

$$(|\phi_1\rangle |0^{b_1}\rangle + \perp_1) |0^{b_2}\rangle, \quad (23)$$

where  $\perp_1$  is an unnormalized state orthogonal to all states of the form  $|\boldsymbol{\xi}\rangle |0^{b_1}\rangle$  and  $|\phi_1\rangle$  satisfies

$$\left\| |\phi_1\rangle - \frac{\sqrt{P^d}}{C_\beta |f|} \sum_{\boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}) |\boldsymbol{\xi}\rangle \right\| < \frac{\epsilon}{2C_\alpha C_\beta}, \quad (24)$$

using  $\mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$  gates and  $b_1 = \mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$  ancilla qubits. Here  $C_\beta \geq \sup |\beta|$  is a constant.

**Step 2. Apply QFT and multiply the factor  $\check{\alpha}(\mathbf{x})$ .** In order to multiply the factor  $\check{\alpha}(\mathbf{x})$  in the symbol, we apply QFT and convert the state to the space domain. Since  $\sqrt{P^d} U_{\text{FT}}^{\otimes d} \sum_{\boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}) |\boldsymbol{\xi}\rangle = \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle$ , we have

$$\begin{aligned} & \left\| U_{\text{FT}}^{\otimes d} |\phi_1\rangle - \frac{1}{C_\beta |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle \right\| \\ &= \left\| U_{\text{FT}}^{\otimes d} |\phi_1\rangle - U_{\text{FT}}^{\otimes d} \frac{\sqrt{P^d}}{C_\beta |f|} \sum_{\boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}) |\boldsymbol{\xi}\rangle \right\| \\ &= \left\| |\phi_1\rangle - \frac{\sqrt{P^d}}{C_\beta |f|} \sum_{\boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) \hat{f}(\boldsymbol{\xi}) |\boldsymbol{\xi}\rangle \right\| < \frac{\epsilon}{2C_\alpha C_\beta}, \end{aligned} \quad (25)$$

where we have used (24) in the last line. By using Proposition 4 again with  $m = d$ ,  $g = \check{\alpha}$  and  $\epsilon$  replaced by  $\frac{\epsilon}{2C_\beta}$ , the state  $|\phi_1\rangle|0^{b_2}\rangle$  is mapped to  $|\phi_2\rangle|0^{b_2}\rangle + \perp_2$ , where  $\perp_2$  is an unnormalized state orthogonal to all state of the form  $|\mathbf{x}\rangle|0^{b_2}\rangle$  and  $|\phi_2\rangle$  satisfies  $\| |\phi_2\rangle - \frac{1}{C_\alpha} D_{\check{\alpha}} U_{\text{FT}}^{\otimes d} |\phi_1\rangle \| < \frac{\epsilon}{2C_\alpha C_\beta}$ . In this step,  $\mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$  gates and  $b_2 = \mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$  ancilla qubits are used. The image of  $\perp_1$  is still orthogonal to all states of the form  $|\boldsymbol{\xi}\rangle|0^{b_1}\rangle$  since the  $b_1$  ancilla qubits used in the previous step are unchanged. Therefore, the final state is

$$|\phi_2\rangle|0^{b_1+b_2}\rangle + \perp, \quad (26)$$

where  $\perp$  is an unnormalized state orthogonal to all states of the form  $|\mathbf{x}\rangle|0^{b_1+b_2}\rangle$  and  $|\phi_2\rangle$  satisfies

$$\begin{aligned} & \left\| C_\alpha C_\beta |\phi_2\rangle - \frac{1}{|f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\alpha}(\mathbf{x}) \check{\beta}(\boldsymbol{\xi}) e^{\frac{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}}{P}} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle \right\| \\ & \leq C_\alpha C_\beta \left\| |\phi_2\rangle - \frac{1}{C_\alpha} D_{\check{\alpha}} U_{\text{FT}}^{\otimes d} |\phi_1\rangle \right\| + C_\beta \left\| D_{\check{\alpha}} U_{\text{FT}}^{\otimes d} |\phi_1\rangle - \frac{1}{C_\beta |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\alpha}(\mathbf{x}) \check{\beta}(\boldsymbol{\xi}) e^{\frac{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}}{P}} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle \right\| \\ & < \frac{\epsilon}{2} + C_\beta \left\| D_{\check{\alpha}} U_{\text{FT}}^{\otimes d} |\phi_1\rangle - D_{\check{\alpha}} \frac{1}{C_\beta |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle \right\| \\ & \leq \frac{\epsilon}{2} + C_\beta \sup |\check{\alpha}| \left\| U_{\text{FT}}^{\otimes d} |\phi_1\rangle - \frac{1}{C_\beta |f|} \sum_{\mathbf{x}, \boldsymbol{\xi}} \check{\beta}(\boldsymbol{\xi}) e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi} / P} \hat{f}(\boldsymbol{\xi}) |\mathbf{x}\rangle \right\| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \end{aligned} \quad (27)$$

where we have used the inequality (25) and the fact that  $C_\alpha \geq \sup |\alpha| = \sup |\check{\alpha}|$  in the last line. By checking the definition of block encoding and adding up the gates and ancilla qubits used, we obtain the following theorem.

**Theorem 6.** *If  $a(\mathbf{x}, \boldsymbol{\xi}) = \alpha(\mathbf{x})\beta(\boldsymbol{\xi})$  is a separable symbol as defined in Definition 1, then the discretized PDO (22) can be  $(C_\alpha C_\beta, \mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon)), \epsilon)$ -block-encoded using the circuit displayed in Figure 6 with gate complexity  $\mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$ , where  $C_\alpha, C_\beta > 0$  are constants such that  $C_\alpha \geq \sup |\alpha|$  and  $C_\beta \geq \sup |\beta|$ .*

*Remark 1.* In contrast to the result in Theorem 5, one can observe that the exponential factor  $2^{\frac{pd}{2}}$  is removed, and thus the success probability for the circuit in Figure 6 is improved exponentially compared to the one in Figure 3.

## 4.2 Linear combination of separable terms

With the block encoding for PDOs with separable symbols ready, the PDO for a linear combination of separable terms, i.e.,

$$a(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j a_j(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j \alpha_j(\mathbf{x}) \beta_j(\boldsymbol{\xi}),$$

can also be block-encoded, thanks to LCU (see Section 2.2). More precisely, we have the following corollary.

**Corollary 7.** *For a linear combination of separable symbols  $a(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j a_j(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j \alpha_j(\mathbf{x}) \beta_j(\boldsymbol{\xi})$ , where  $\sup |\alpha_j| \leq 1$ ,  $\sup |\beta_j| \leq 1$  and  $y \in \mathbb{C}^m$  with  $\|y\|_1 \leq \delta$ , assume that  $(U_L, U_R)$  is a pair of unitaries described in Lemma 1 with  $\epsilon_1 = \epsilon$ , and  $W =$*

$\sum_{j=0}^{m-1} |j\rangle \langle j| \otimes U_j + \sum_{j=m}^{2^b-1} |j\rangle \langle j| \otimes I_{a+s}$ , where each  $U_j$  is a  $(1, a, \epsilon)$ -block-encoding of the discretized PDO  $A_j$  associated with symbol  $a_j(\mathbf{x}, \boldsymbol{\xi})$  (see (22)) constructed in Theorem 6 with  $a = \mathcal{O}(\text{poly}(pd) + \text{polylog}(1/\epsilon))$ . Then  $(U_L^\dagger \otimes I_{a+s})W(U_R \otimes I_{a+s})$  is a  $(\delta, a+b, (1+\delta)\epsilon)$ -block-encoding of  $\sum_{j=0}^{m-1} y_j A_j$ , where  $I_{a+s}$  denotes the identity operator with size  $2^{a+s} \times 2^{a+s}$ . The gate complexity of the corresponding circuit is  $\mathcal{O}(m(\text{poly}(pd) + \text{polylog}(1/\epsilon)))$ .

## 5 Efficient block encoding for fully separable symbols with explicit circuits

For separable symbols, the circuit presented in Figure 6 significantly increases the success probability compared to the one in Figure 3. However, this relies on circuits for arithmetic functions (see Proposition 4), which can still be challenging to construct in practice. In this section, we develop a more explicit circuit with the help of QSP and QET (see Section 2.3).

### 5.1 Dimension-wise fully separable symbols

To begin with, we consider the fully separable symbols defined as follows.

**Definition 2.** A symbol  $a(\mathbf{x}, \boldsymbol{\xi})$  is called *fully separable* if  $a(\mathbf{x}, \boldsymbol{\xi}) = \alpha(\mathbf{x})\beta(\boldsymbol{\xi})$  with  $\alpha(\mathbf{x}) = \alpha_1(x_1) \cdots \alpha_d(x_d)$  and  $\beta(\boldsymbol{\xi}) = \beta_1(\xi_1) \cdots \beta_d(\xi_d)$  where each function in the set  $\{\alpha_k\}_{k=1}^d \cup \{\beta_k\}_{k=1}^d$  is a real even function, a real odd function or an exponential function of the form  $f(y) = \exp(i\theta y)$  for some real parameter  $\theta$ .

Similar with (21), we introduce the following notations:

$$\check{\alpha}_k(x_k) = \alpha_k\left(\frac{x_k}{P}\right), \quad \check{\beta}_k(\xi_k) = \begin{cases} \beta_k(\xi_k), & 0 \leq \xi_k < P/2 \\ \beta_k(\xi_k - P), & P/2 \leq \xi_k < P \end{cases}, \quad k = 1, 2, \dots, d. \quad (28)$$

Then the discretized PDO (11) becomes

$$Af(\mathbf{x}) = \sum_{\boldsymbol{\xi} \in \Xi} e^{2\pi i \mathbf{x} \cdot \boldsymbol{\xi}/P} \left( \prod_{k=1}^d \check{\alpha}_k(x_k) \right) \left( \prod_{k=1}^d \check{\beta}_k(\xi_k) \right) \hat{f}(\boldsymbol{\xi}), \quad \mathbf{x} \in \Xi = \{0, 1, \dots, P-1\}^d. \quad (29)$$

In order to block-encode the PDO (29), we adopt the following circuit, as shown in Figure 7, which is similar with the one in Figure 6:

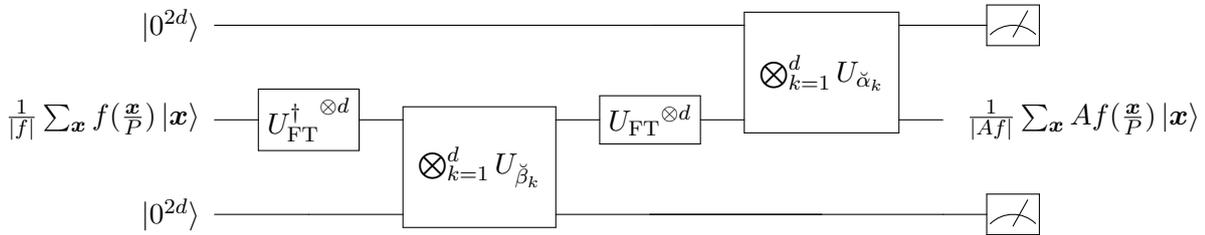


Figure 7: Circuit for an explicit and efficient block encoding for fully separable PDOs (29). Here  $\frac{1}{|f|} \sum_{\mathbf{x}} f(\frac{\mathbf{x}}{P}) |\mathbf{x}\rangle$  is the normalized input data,  $U_{FT}$  is the QFT circuit,  $U_{\check{\beta}_k}$  and  $U_{\check{\alpha}_k}$  are the block encodings of  $D_{\check{\beta}_k}$  and  $D_{\check{\alpha}_k}$ , respectively, and the desired output is obtained with normalizing factor  $\frac{1}{|Af|}$  when getting  $|0^{b_1+b_2}\rangle$  for the  $b_1 + b_2$  ancilla qubits. Here  $D_{\check{\beta}_k}$  and  $D_{\check{\alpha}_k}$  are diagonal matrices defined in (8).

Exploiting the fully separable structure of the symbol, one can construct explicit circuits for the diagonal multiplications shown in Figure 7 by leveraging QSP and QET (see Section 2.3). To this end, we first introduce a lemma that gives Hermitian block encodings for two diagonal multiplication prototypes that allow us to build the QET circuit afterward. More specifically, by combining a series of single-qubit rotations, one can construct a diagonal matrix with diagonal elements  $\{\exp(ij\theta)\}_{j=0}^{P-1}$ . Then one can build a diagonal matrix with diagonal elements  $\{\sin(ij\theta)\}_{j=0}^{P-1}$  using a simple LCU circuit, from which a diagonal matrix with diagonal elements  $\{g(ij\theta)\}_{j=0}^{P-1}$  can be built with QET for some smooth function  $g$ . Since the grid points of the frequency variables are taken as  $\{-\frac{P}{2}, -\frac{P}{2} + 1, \dots, \frac{P}{2} - 1\}$ , one also needs the corresponding diagonal matrices where the index  $j$  takes values in  $\{-\frac{P}{2}, -\frac{P}{2} + 1, \dots, \frac{P}{2} - 1\}$  rather than from 0 to  $P$ . We denote the corresponding matrices by subscript  $-$  as opposed to  $+$  if the index  $j$  goes from 0 to  $P$ . During the preparation of this paper, we notice that a similar result is built in [27] independently.

**Lemma 8.** For a fixed  $P = 2^p$ , let  $\mathbf{v}_-, \mathbf{v}_+$  be the vectors:

$$\mathbf{v}_- = \left(0, 1, \dots, \frac{P}{2} - 1, -\frac{P}{2}, -\frac{P}{2} + 1, \dots, -1\right),$$

and

$$\mathbf{v}_+ = \left(0, 1, \dots, \frac{P}{2} - 1, \frac{P}{2}, \frac{P}{2} + 1, \dots, P - 1\right),$$

respectively, and  $D_-, D_+$  be the diagonal matrices  $\text{diag}(\mathbf{v}_-)$ ,  $\text{diag}(\mathbf{v}_+)$ , respectively. Then there is an  $(1, 1)$ -Hermitian-block-encoding of  $\sin(\theta D_\sigma)$  with gate complexity  $2p + 5$ , where  $\sigma \in \{-, +\}$  and  $\theta > 0$  is a parameter.

*Proof.* For an arbitrary parameter  $\theta > 0$ , we first construct matrices  $R_- = \exp(i\theta D_-)$  and  $R_+ = \exp(i\theta D_+)$  with quantum circuits. Using the binary representation of  $\xi$ , we get

$$R_- |\xi_{p-1} \cdots \xi_0\rangle = e^{i((-\xi_{p-1})\xi_{p-2} \cdots \xi_0)\theta} |\xi_{p-1} \cdots \xi_0\rangle,$$

and

$$R_+ |\xi_{p-1} \cdots \xi_0\rangle = e^{i(\xi_{p-1} \cdots \xi_0)\theta} |\xi_{p-1} \cdots \xi_0\rangle.$$

Then

$$\begin{aligned} R_+ |\xi_{p-1} \cdots \xi_0\rangle &= e^{i(\xi_{p-1} \cdots \xi_0)\theta} |\xi_{p-1} \cdots \xi_0\rangle = e^{i \sum_j \xi_j 2^j \theta} |\xi_{p-1} \cdots \xi_0\rangle \\ &= \prod_j e^{i \xi_j 2^j \theta} \bigotimes_j |\xi_j\rangle = \bigotimes_j e^{i \xi_j 2^j \theta} |\xi_j\rangle = \bigotimes_j R_z(2^j \theta) |\xi_j\rangle, \end{aligned}$$

and

$$R_- |\xi_{p-1} \cdots \xi_0\rangle = e^{-i \xi_{p-1} 2^{p-1} \theta} R_+ |\xi_{p-1} \cdots \xi_0\rangle = \bigotimes_j R_z((-1)^{\delta_{j,p-1}} 2^j \theta) |\xi_j\rangle,$$

so  $R_+ = \bigotimes_j R_z(2^j \theta)$  and  $R_- = \bigotimes_j R_z((-1)^{\delta_{j,p-1}} 2^j \theta)$ , where  $R_z$  is the single qubit rotation defined in Section 2.1. Let  $U_\sigma$  be the circuit displayed in Figure 8, where  $\sigma \in \{-, +\}$ , then  $U_\sigma$  is a  $(1, 1)$ -Hermitian-block-encoding of  $\sin(\theta D_\sigma)$ . In fact, the matrix corresponding to  $U_\sigma$  is

$$\begin{aligned} U_\sigma &= \begin{bmatrix} I & \\ & iI \end{bmatrix} \begin{bmatrix} I & \\ & I \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} \begin{bmatrix} R_\sigma & \\ & R_\sigma^\dagger \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} \begin{bmatrix} I & \\ & iI \end{bmatrix} \\ &= \begin{bmatrix} I & \\ & iI \end{bmatrix} \begin{bmatrix} I & \\ & I \end{bmatrix} \frac{1}{2} \begin{bmatrix} R_\sigma + R_\sigma^\dagger & R_\sigma - R_\sigma^\dagger \\ R_\sigma - R_\sigma^\dagger & R_\sigma + R_\sigma^\dagger \end{bmatrix} \begin{bmatrix} I & \\ & iI \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} R_\sigma - R_\sigma^\dagger & i(R_\sigma + R_\sigma^\dagger) \\ i(R_\sigma + R_\sigma^\dagger) & -(R_\sigma - R_\sigma^\dagger) \end{bmatrix} = i \begin{bmatrix} \sin(\theta D_\sigma) & \cos(\theta D_\sigma) \\ \cos(\theta D_\sigma) & -\sin(\theta D_\sigma) \end{bmatrix}, \end{aligned}$$

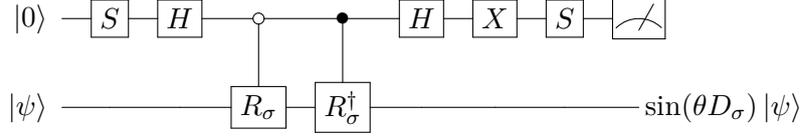


Figure 8: Hermitian block encoding of  $\sin(\theta D_\sigma)$ .

and this is a Hermitian matrix with the first diagonal block being  $\sin(\theta D_\sigma)$  after ignoring the global phase factor  $i$ , since  $\begin{bmatrix} \sin(\theta D_\sigma) & \cos(\theta D_\sigma) \\ \cos(\theta D_\sigma) & -\sin(\theta D_\sigma) \end{bmatrix}$  is Hermitian. It can be seen from Figure 8 that the number of elementary gates used is  $2p + 5$ .  $\square$

Now, we aim to construct the block encoding of diagonal matrices  $D_{\check{\alpha}_j} = \check{\alpha}_j(D_+)$  and  $D_{\check{\beta}_j} = \check{\beta}_j(D_+) = \beta_j(D_-)$ , namely  $U_{\check{\alpha}_k}$  and  $U_{\check{\beta}_k}$  in Figure 7. For the case where  $\alpha_j(x_j) = \exp(i\theta x_j)$  or  $\beta_j(\xi_j) = \exp(i\theta \xi_j)$ , the matrices  $R_- = \exp(i\theta D_-)$  and  $R_+ = \exp(i\theta D_+)$  constructed in Lemma 8 are exactly the diagonal matrices  $D_{\check{\beta}_j} = \beta_j(D_-)$  and  $D_{\check{\alpha}_j} = \check{\alpha}_j(D_+)$ , respectively. Therefore, we devote the rest of this section to the case where  $\beta_j$  and  $\alpha_j$  are even or odd real functions. Thanks to the block encodings  $U_+$  and  $U_-$  introduced in Lemma 8, what remains to do is to find polynomial approximations of  $\check{\alpha}$  and  $\beta$  so as to complete the QET procedure described in Section 2.3. Specifically, we restrict the parameter  $\theta$  to be  $0 < \theta < \frac{\pi}{2P}$  in order to recover  $\theta D_\sigma$  from  $\sin(\theta D_\sigma)$  with the arcsin function. Going through the QET procedure, one obtains the following result.

**Proposition 9.** *Let  $U_-$  and  $U_+$  be the  $(1, 1)$ -Hermitian-block-encodings of  $\sin(\theta D_-)$  and  $\sin(\theta D_+)$  constructed in Lemma 8 for  $0 < \theta < \frac{\pi}{2P}$  with  $P = 2^p$ . Assume that  $g$  is an even (resp. odd) continuous real function on  $[-P, P]$  and that  $\deg_g(\epsilon)$  is the smallest positive integer such that there exists an even (resp. odd) polynomial  $\tilde{g}$  with the degree bounded by  $\deg_g(\epsilon)$  satisfying*

$$\sup_{-\sin(P\theta) \leq x \leq \sin(P\theta)} \left| C_g \tilde{g}(x) - g\left(\frac{1}{\theta} \arcsin x\right) \right| < \epsilon, \quad \|\tilde{g}\| \leq 1, \quad (30)$$

where  $\|\cdot\|$  is the  $L^\infty$  norm on  $[-1, 1]$  and  $C_g$  is a constant such that  $C_g \geq \sup |g|$ . Then there is a  $(C_g, 2, \epsilon)$ -block-encoding for both  $g(D_-)$  and  $g(D_+)$  with  $\mathcal{O}(p \deg_g(\epsilon))$  gates, where  $D_-$  and  $D_+$  are defined in Lemma 8.

*Proof.* The circuit in Figure 2(b) with  $U_A$  replaced by  $U_\sigma$  gives a  $(C_g, 2)$ -block-encoding for  $\tilde{g}(\sin(\theta D_\sigma))$ , and since

$$\sup_{-\sin(P\theta) \leq x \leq \sin(P\theta)} \left| C_g \tilde{g}(x) - g\left(\frac{1}{\theta} \arcsin x\right) \right| < \epsilon,$$

we have

$$\left\| C_g \tilde{g}(\sin(\theta D_\sigma)) - g\left(\frac{1}{\theta} \arcsin(\sin(\theta D_\sigma))\right) \right\| < \epsilon,$$

where the operator 2-norm is used. Thus the circuit in Figure 2(b) with  $U_A$  replaced by  $U_\sigma$  gives a  $(C_g, 2, \epsilon)$ -block-encoding for

$$g\left(\frac{1}{\theta} \arcsin(\sin(\theta D_\sigma))\right) = g\left(\frac{1}{\theta} \cdot \theta D_\sigma\right) = g(D_\sigma),$$

where  $\sigma \in \{-, +\}$  and we have used the fact that  $0 < \theta < \frac{\pi}{2P}$  in the first equality. Since  $\mathcal{O}(p)$  gates are used in  $U_\sigma$ , the gate complexity of the circuit described above is  $\mathcal{O}(p \deg_g(\epsilon))$ , which closes the proof.  $\square$

The gate complexity of the circuit built with QET in Proposition 9 depends on the smoothness of  $g$ . For instance, we have the following corollary.

**Corollary 10.** *Assume that  $g$  is an even (resp. odd) differentiable real function on  $[-\frac{\pi}{2\theta}, \frac{\pi}{2\theta}]$ . Let  $\eta_g(\epsilon, \theta)$  be the smallest integer such that there exists a polynomial  $u$  with degree  $\eta_g(\epsilon, \theta)$  satisfying  $\sup_{|y| < \frac{\pi}{2\theta}} |u(y) - g(y)| < \frac{\epsilon}{3}$ , then the gate complexity of the circuit used in Proposition 9 is*

$$\mathcal{O}\left(p \log\left(\frac{C'_g}{\theta\epsilon}\right) \eta_g(\epsilon, \theta)\right),$$

where  $C'_g = \sup_{|y| < \frac{\pi}{2\theta}} |g'(y)|$ . In particular, if  $g$  is a polynomial, the gate complexity reduces to  $\mathcal{O}\left(p \log\left(\frac{C'_g}{\theta\epsilon}\right) \deg g\right)$ .

*Proof.* Without loss of generality, assume  $1 > \frac{\epsilon}{2C'_g}$ , otherwise we can just let  $\tilde{g} = 0$  (30). Since  $\frac{1}{\theta} \arcsin(x)$  is an analytic function whose power series centered at  $x = 0$  has convergence radius  $1 > \sin(P\theta)$ , there is a truncation  $v$  of the Taylor series of  $\frac{1}{\theta} \arcsin(x)$  with degree  $\mathcal{O}(\log(\frac{C'_g}{\theta\epsilon}))$  such that  $\sup_{|x| < \sin(P\theta)} |v(x) - \frac{1}{\theta} \arcsin(x)| < \frac{\epsilon}{3C'_g}$ . Now since the coefficients of the Taylor series of  $\frac{1}{\theta} \arcsin(x)$  at  $x = 0$  are all non-negative, it holds that  $v([-1, 1]) \subset [-\frac{\pi}{2\theta}, \frac{\pi}{2\theta}]$ . Let  $\bar{g}(x) = \frac{1}{C'_g} u(v(x))$  and  $\tilde{g} = (1 - \frac{\epsilon}{3C'_g})\bar{g}$ , then  $\tilde{g}$  has degree  $\mathcal{O}(\log(\frac{C'_g}{\theta\epsilon})) \eta_g(\epsilon, \theta)$ , and

$$\begin{aligned} \left| C_g \bar{g}(x) - g\left(\frac{1}{\theta} \arcsin(x)\right) \right| &\leq |u(v(x)) - g(v(x))| + \left| g(v(x)) - g\left(\frac{1}{\theta} \arcsin(x)\right) \right| \\ &< \frac{\epsilon}{3} + \sup_{|y| < \frac{\pi}{2\theta}} |g'(y)| \left| v(x) - \frac{1}{\theta} \arcsin(x) \right| < \frac{\epsilon}{3} + C'_g \cdot \frac{\epsilon}{3C'_g} = \frac{2\epsilon}{3}, \end{aligned}$$

for  $x \in [-\sin(P\theta), \sin(P\theta)]$ . In addition, since  $v$  maps  $[-1, 1]$  into  $[-\frac{\pi}{2\theta}, \frac{\pi}{2\theta}]$ , we have

$$|\bar{g}(x)| \leq \sup_{|y| < \frac{\pi}{2\theta}} \left| \frac{1}{C_g} u(y) \right| \leq \sup_{|y| < \frac{\pi}{2\theta}} \left| \frac{1}{C_g} u(y) - \frac{1}{C_g} g(y) \right| + \sup_{|y| < \frac{\pi}{2\theta}} \left| \frac{1}{C_g} g(y) \right| \leq \frac{\epsilon}{3C_g} + 1,$$

and therefore  $|\tilde{g}(x)| = (1 - \frac{\epsilon}{3C'_g}) |\bar{g}(x)| < 1$  for  $x \in [-1, 1]$ . In addition, we have

$$\begin{aligned} \left| C_g \tilde{g}(x) - g\left(\frac{1}{\theta} \arcsin(x)\right) \right| &= \left| \left(1 - \frac{\epsilon}{3C'_g}\right) \left( C_g \bar{g}(x) - g\left(\frac{1}{\theta} \arcsin(x)\right) \right) + \frac{\epsilon}{3C'_g} g\left(\frac{1}{\theta} \arcsin(x)\right) \right| \\ &\leq \left(1 - \frac{\epsilon}{3C'_g}\right) \frac{2\epsilon}{3} + \frac{\epsilon}{3C'_g} C_g < \frac{2\epsilon}{3} + \frac{\epsilon}{3} = \epsilon, \end{aligned}$$

for  $x \in [-\sin(P\theta), \sin(P\theta)]$ . According to Proposition 9, we have  $\deg_g(\epsilon) = \mathcal{O}(\log(\frac{C'_g}{\theta\epsilon})) \eta_g(\epsilon, \theta)$  and the gate complexity of the circuit used in Proposition 9 is  $\mathcal{O}\left(p \log\left(\frac{C'_g}{\theta\epsilon}\right) \eta_g(\epsilon, \theta)\right)$ , where the factor  $p$  comes from preparing  $\sin(\theta D_\sigma)$  as mentioned in Lemma 8. In the case that  $g$  is a polynomial, we can simply let  $u = g$  and thus  $\eta_g(\epsilon, \theta) \leq \deg g$ .  $\square$

For the final step, we first introduce the notation

$$\deg_a(\epsilon) \equiv \sum_{k=1}^d \left[ \deg_{\alpha_k}(\epsilon) + \deg_{\beta_k}(\epsilon) \right], \quad (31)$$

where  $\text{deg}_{\check{\alpha}_k}(\epsilon)$  and  $\text{deg}_{\check{\beta}_k}(\epsilon)$  are defined in Proposition 9. Denote by  $U_{\check{\alpha}_k}$  and  $U_{\check{\beta}_k}$  the block encodings of  $\check{\alpha}_k(D_+)$  and  $\check{\beta}_k(D_+) = \beta_k(D_-)$  obtained in Proposition 9 with  $\epsilon$  replaced by  $\epsilon/2dC$ , respectively, where

$$C = \tilde{C}_\alpha \tilde{C}_\beta, \quad \tilde{C}_\alpha = \prod_{k=1}^d C_{\check{\alpha}_k}, \quad \tilde{C}_\beta = \prod_{k=1}^d C_{\check{\beta}_k}, \quad (32)$$

and  $C \geq \prod_{k=1}^d (\sup |\check{\alpha}_k| \sup |\check{\beta}_k|)$  since  $C_{\check{\alpha}_k} \geq \sup |\check{\alpha}_k|$  and  $C_{\check{\beta}_k} \geq \sup |\check{\beta}_k|$ . Now we are ready to prove the following theorem that relies on the block encodings  $\bigotimes_{k=1}^d U_{\check{\alpha}_k}$  and  $\bigotimes_{k=1}^d U_{\check{\beta}_k}$  in Figure 7.

**Theorem 11.** *If  $a(\mathbf{x}, \boldsymbol{\xi}) = \alpha(\mathbf{x})\beta(\boldsymbol{\xi}) = \alpha_1(x_1) \cdots \alpha_d(x_d)\beta_1(\xi_1) \cdots \beta_d(\xi_d)$  is a fully separable symbol as defined in Definition 2, then the corresponding PDO defined by (29) can be  $(C, \mathcal{O}(d), \epsilon)$ -block-encoded with gate complexity  $\mathcal{O}(dp \text{deg}_a(\frac{\epsilon}{2dC}) + dp^2)$  using the circuit displayed in Figure 7, where  $C > 0$  is a constant defined in (32), and  $\text{deg}_a(\frac{\epsilon}{2dC})$  is defined in (31).*

*Proof.* Since each  $U_{\check{\alpha}_k}$  is a  $(C_{\check{\alpha}_k}, 2, \epsilon/2dC)$ -block-encoding for  $\check{\alpha}_k(D_+)$  according to Proposition 9,  $\bigotimes_{k=1}^d U_{\check{\alpha}_k}$  is a  $(\prod_{k=1}^d C_{\check{\alpha}_k}, 2d, \epsilon/2\tilde{C}_\alpha)$ -block-encoding for

$$\bigotimes_{k=1}^d \check{\alpha}_k(D_+) = \bigotimes_{k=1}^d D_{\check{\alpha}_k} = D_{\check{\alpha}}.$$

Similarly,  $\bigotimes_{k=1}^d U_{\check{\beta}_k}$  is a  $(\prod_{k=1}^d C_{\check{\beta}_k}, 2d, \epsilon/2\tilde{C}_\beta)$ -block-encoding for

$$\bigotimes_{k=1}^d \check{\beta}_k(D_+) = \bigotimes_{k=1}^d D_{\check{\beta}_k} = D_{\check{\beta}}.$$

Hence by the same argument as the proof of Theorem 6 (especially (23), (24), (25), (26) and (27)), the circuit in Figure 7 gives a  $(C, 4d, \epsilon)$  block encoding of the PDO (29) with gate complexity  $\mathcal{O}(p \text{deg}_a(\frac{\epsilon}{2dC}) + p^2d)$ , where the  $\mathcal{O}(p^2d)$  term comes from the QFT part of the circuit.  $\square$

*Remark 2.* The approximate QFT (see [29] for example) can be used to replace the QFT blocks in Figure 7. With similar arguments as in the proof of Theorem 11, one can show that the gate complexity can be reduced to  $\mathcal{O}(dp \text{deg}_a(\frac{\epsilon}{2dC}))$ .

## 5.2 Linear combination of fully separable terms

Similar to Corollary 7, we can block-encode the PDO for a linear combination of fully separable terms, i.e.,

$$a(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j a_j(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j \alpha_{j1}(x_1) \cdots \alpha_{jd}(x_d) \beta_{j1}(\xi_1) \cdots \beta_{jd}(\xi_d),$$

with LCU (see Section 2.2) and Theorem 11, which is stated in the following corollary.

**Corollary 12.** *For a linear combination of fully separable symbols  $a(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j a_j(\mathbf{x}, \boldsymbol{\xi}) = \sum_{j=0}^{m-1} y_j \alpha_{j1}(x_1) \cdots \alpha_{jd}(x_d) \beta_{j1}(\xi_1) \cdots \beta_{jd}(\xi_d)$ , where  $\sup_{[0,1]} |\alpha_{jk}| \leq 1$ ,  $\sup_{[-P/2, P/2]} |\beta_{jk}| \leq 1$  and  $y \in \mathbb{C}^m$  with  $\|y\|_1 \leq \delta$ , assume that  $(U_L, U_R)$  is a pair of unitaries described in Lemma 1*

with  $\epsilon_1 = \epsilon$ , and  $W = \sum_{j=0}^{m-1} |j\rangle \langle j| \otimes U_j + \sum_{j=m}^{2^b-1} |j\rangle \langle j| \otimes I_{a+s}$ , where each  $U_j$  is a  $(1, a, \epsilon)$ -block-encoding of the discretized PDO  $A_j$  associated with symbol  $a_j(\mathbf{x}, \boldsymbol{\xi})$  (see (29)) constructed in Theorem 11 with  $a = \mathcal{O}(d)$ . Then  $(U_L^\dagger \otimes I_{a+s})W(U_R \otimes I_{a+s})$  is an  $(\delta, a+b, (1+\delta)\epsilon)$ -block-encoding of  $\sum_{j=0}^{m-1} y_j A_j$ , where  $I_{a+s}$  denotes the identity operator with size  $2^{a+s} \times 2^{a+s}$ . The gate complexity of the corresponding circuit is  $\mathcal{O}(dp \sum_{j=0}^{m-1} \deg_a(\frac{\epsilon}{2d}) + dp^2 m)$ .

## 6 Applications

In this section, we provide worked examples for particular symbols using the circuit shown in Figure 7 and provide complexity analysis, beginning with a variable coefficient second-order elliptic operator.

### 6.1 Second-order elliptic operator with variable coefficients

Recall that the elliptic operator introduced in (2) is of the following form:

$$(Au)(\mathbf{x}) = u(\mathbf{x}) - \nabla \cdot (\omega(\mathbf{x}) \nabla u(\mathbf{x})). \quad (33)$$

In this section, we assume that  $\omega(\mathbf{x}) > 0$  has a low-rank Fourier expansion

$$\omega(\mathbf{x}) = \sum_{j=1}^r c_j \exp(2\pi i \mathbf{q}_j \cdot \mathbf{x}), \quad \mathbf{q}_j \in \mathbb{Z}^d. \quad (34)$$

Many commonly seen functions have low-rank expansions or approximations. For instance,  $\omega(\mathbf{x}) = 2 + \sin(2\pi \sum_{l=1}^d x_l) > 0$  can be written in the rank-3 form

$$\omega(\mathbf{x}) = 2 + \frac{i}{2} (\exp(-2\pi i(x_1 + \dots + x_d)) - \exp(2\pi i(x_1 + \dots + x_d))).$$

Plugging the form (34) of  $\omega$  into (3), one obtains the symbol associated with the PDO above

$$a(\mathbf{x}, \boldsymbol{\xi}) = 1 + \sum_{j=1}^r \sum_{l=1}^d (4\pi^2 P q_{jl} c_j) e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l}{P} + \sum_{j=1}^r \sum_{l=1}^d (4\pi^2 P^2 c_j) e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l^2}{P^2},$$

where  $P = 2^p$  is the number of discrete points used for each dimension (see Section 2.4). Notice that the terms  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l}{P}$  and  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l^2}{P^2}$  above are fully separable by Definition 2, thus by Corollary 12, we know that the corresponding PDO can be block-encoded. As explained in Section 5, the multiplication of  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} = \prod_{l=1}^d e^{2\pi i q_{jl} x_l}$  can be implemented directly using  $R_-$  and  $R_+$  constructed in Lemma 8. Consequently, the number of gates needed for multiplying each  $e^{2\pi i q_{jl} x_l}$  factor without error is  $\mathcal{O}(p)$ , and no ancilla qubits are used. Since  $\frac{\xi_l}{P}$  and  $\frac{\xi_l^2}{P^2}$  are polynomials, by Corollary 10, the multiplication of each  $\frac{\xi_l}{P}$  and  $\frac{\xi_l^2}{P^2}$  factor can be implemented with  $\mathcal{O}(p \log(\frac{1}{\epsilon}))$  gates to  $\mathcal{O}(\epsilon)$  precision, and  $\mathcal{O}(d)$  ancilla qubits are used. Going through the proof of Theorem 11, one can see that the PDO associated with  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l}{P}$  and  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}} \frac{\xi_l^2}{P^2}$  can be  $(1, \mathcal{O}(d), \epsilon)$ -block-encoded with gate complexity  $\mathcal{O}(p \log(\frac{1}{\epsilon}) + p^2 + dp)$ , where the three terms account for implementing the polynomials of  $\xi_l$ , the QFT of the  $l$ -th component, and the multiplication of  $e^{2\pi i \mathbf{q}_j \cdot \mathbf{x}}$ , respectively. Finally, going through the LCU step as in Corollary 12 with  $\mathcal{O}(dr)$  terms, one obtains a  $(\gamma, \mathcal{O}(d + \log(dr)), (1 + \gamma)\epsilon)$ -block-encoding of the PDO (2) with total gate complexity  $\mathcal{O}(dr(p \log(\frac{1}{\epsilon}) + p^2 + dp)) = \mathcal{O}(dpr(\log \frac{1}{\epsilon} + d + p))$ , where  $\gamma = 1 + 4\pi^2(P \sum_{j=1}^r |c_j| \|\mathbf{q}_j\|_1 + P^2 d \sum_{j=1}^r |c_j|)$ . This result is summarized in the following theorem, where we have used  $\mathcal{O}(d + \log(dr)) = \mathcal{O}(d + \log(r))$ .

**Theorem 13.** For the elliptic operator (2) with variable coefficient, where  $\omega(\mathbf{x})$  has a low-rank expansion (34), there exists a  $(\gamma, \mathcal{O}(d + \log(r)), (1 + \gamma)\epsilon)$ -block-encoding for the corresponding discretized PDO defined in (29) with gate complexity

$$\mathcal{O}\left(dr \log P \left(\log \frac{P}{\epsilon} + d\right)\right),$$

where  $\gamma = 1 + 4\pi^2(P \sum_{j=1}^r |c_j| \|q_j\|_1 + P^2 d \sum_{j=1}^r |c_j|)$ .

Similar to previous sections and by a slight abuse of notation, we denote the discretization of the operator defined in (33) also by  $A$ . Now we can use the QLSA in [13] to get the following corollary:

**Corollary 14.** Let  $(A, b)$  be the discretization of the operator and the right-hand side of (33), respectively, there is a quantum algorithm finding the normalized state  $|A^{-1}b\rangle = \frac{A^{-1}b}{\|A^{-1}b\|}$  within error  $\epsilon$  with gate complexity

$$\mathcal{O}\left(\gamma dr \log \frac{1}{\epsilon} \log P \left(\log \frac{\gamma P}{\epsilon} + d\right)\right).$$

*Proof.* It is clear that  $\|A\| \leq \gamma$  and  $\|A^{-1}\| \leq 1$ . According to Theorem 13, one can construct  $U_A$ , the  $(\gamma, \mathcal{O}(d + \log(r)), \epsilon/\gamma)$ -block-encoding of  $A$ , with complexity

$$\mathcal{O}\left(dr \log P \left(\log \frac{\gamma P}{\epsilon} + d\right)\right).$$

In other words,  $U_A$  is a  $(1, \mathcal{O}(d + \log(r)), 0)$ -block-encoding of some matrix  $\tilde{A}/\gamma$  such that  $\|A - \tilde{A}\| < \epsilon/\gamma$ . Therefore, we have  $\|\tilde{A}\| = \mathcal{O}(\gamma)$ ,  $\|\tilde{A}^{-1}\| = \mathcal{O}(1)$ , and thus  $\kappa(\tilde{A}) = \mathcal{O}(\gamma)$ . The main theorem of [13] gives a quantum algorithm that can output a state  $|y\rangle$  that is  $\mathcal{O}(\epsilon)$  close to  $|(\tilde{A}/\gamma)^{-1}b\rangle = |\tilde{A}^{-1}b\rangle = \frac{\tilde{A}^{-1}b}{\|\tilde{A}^{-1}b\|}$ , using

$$\mathcal{O}\left(\kappa(\tilde{A}) \log \frac{1}{\epsilon}\right) = \mathcal{O}\left(\gamma \log \frac{1}{\epsilon}\right)$$

queries of  $U_A$ . Finally, we have the estimation

$$\begin{aligned} \||A^{-1}b\rangle - |\tilde{A}^{-1}b\rangle\| &= \left\| \frac{A^{-1}b}{\|A^{-1}b\|} - \frac{\tilde{A}^{-1}b}{\|\tilde{A}^{-1}b\|} \right\| \\ &\leq \frac{\|(A^{-1} - \tilde{A}^{-1})b\|}{\|A^{-1}b\|} + \|\tilde{A}^{-1}b\| \left| \frac{1}{\|A^{-1}b\|} - \frac{1}{\|\tilde{A}^{-1}b\|} \right| \\ &\leq \frac{\|A^{-1}\| \|\tilde{A}^{-1}\| \|A - \tilde{A}\| \|b\|}{\|A\|^{-1} \|b\|} + \frac{\|A^{-1}\| \|\tilde{A}^{-1}\| \|A - \tilde{A}\| \|b\|}{\|A\|^{-1} \|b\|} \\ &= \mathcal{O}\left(\gamma \cdot \frac{\epsilon}{\gamma}\right) = \mathcal{O}(\epsilon). \end{aligned}$$

So  $|y\rangle$  is also an  $\mathcal{O}(\epsilon)$  approximation of  $|A^{-1}b\rangle$  and the overall gate complexity is

$$\mathcal{O}\left(\gamma dr \log \frac{1}{\epsilon} \log P \left(\log \frac{\gamma P}{\epsilon} + d\right)\right).$$

□

## 6.2 Application for constant coefficient elliptic operator

In this part, we investigate the multiplier operators (see (4)), i.e., the PDOs with symbols of the form  $a(\mathbf{x}, \boldsymbol{\xi}) = \beta(\boldsymbol{\xi})$ . In particular, we showcase how to directly block-encode the inverse of multiplier operators based on the results obtained in the previous sections so that one can solve a discretized system of a PDE without invoking QLSAs (quantum linear system algorithms).

In practice, it is quite often the case that  $\beta(\boldsymbol{\xi})$  is radially symmetric. For example, many operators related to Laplacian have radial symmetric symbols since the symbol of  $\Delta$  is  $-4\pi^2|\boldsymbol{\xi}|^2$ . For the rest of this section, we focus on the radially symmetric symbol  $\beta(\boldsymbol{\xi}) = \varphi(|\boldsymbol{\xi}|)$ . The main idea of dealing with radially symmetric  $\beta$  is to consider an approximation in the following form

$$\beta(\boldsymbol{\xi}) = \varphi(|\boldsymbol{\xi}|) \approx \sum_{m=1}^M w_m e^{-a_m |\boldsymbol{\xi}|^2} = \sum_{m=1}^M w_m \prod_{i=1}^d e^{-a_m \xi_i^2}. \quad (35)$$

Notice that the right-hand side is in the fully separable form by Definition 2. Thus the results from Section 5 can be used. In fact, the authors of [3] developed an efficient algorithm to find a low-rank approximation of a single-variable function  $f(y)$  by exponential sums

$$f(y) \approx \sum_{m=1}^M w_m e^{-a_m y^2}, \quad (36)$$

for a large range of even functions  $f(y)$ , especially those whose amplitude decrease as  $y \rightarrow \infty$ .

Before diving into concrete examples, we first introduce a near-optimal polynomial approximation to the exponential functions in the following lemma, which is a direct corollary of [33]\*Theorem 4.1.

**Lemma 15.** *For every  $a, b > 0$ , and  $0 < \delta \leq 1$ , there exists an even polynomial  $r(y)$  satisfying*

$$\sup_{y \in [0, b]} \left| e^{-ay^2} - r(y) \right| \leq \delta, \quad \sup_{y \in [0, b]} |r(y)| \leq 1,$$

and has degree  $\mathcal{O}\left(\sqrt{\max\{ab^2, \log 1/\delta\}} \cdot \log 1/\delta\right)$ .

With Lemma 15 and established results in Section 5, we are ready to give the following block encoding result for the diagonal multiplication  $D_\beta$  associated with  $\beta(\boldsymbol{\xi})$  (see (8)).

**Theorem 16.** *If  $\beta(\boldsymbol{\xi})$  can be approximated in the following sense*

$$\left| \beta(\boldsymbol{\xi}) - \sum_{m=1}^M w_m e^{-a_m |\boldsymbol{\xi}|^2} \right| \leq \epsilon, \quad \text{for all } \boldsymbol{\xi} \in \left[-\frac{P}{2}, \frac{P}{2}\right]^d,$$

with  $w_m, a_m \geq 0$  and  $R := \max_m a_m$ ,  $W := \sum_{m=1}^M |w_m|$ , then we can implement a  $(\gamma, q, \epsilon)$ -block-encoding for the PDO associated with  $\beta$  (defined in (11)) with

$$\gamma = \mathcal{O}(W), \quad q = \mathcal{O}(d + \log M),$$

and gate complexity

$$\mathcal{O}\left(dM \log P \log\left(\frac{dWRP}{\epsilon}\right) \sqrt{\max\left\{RP^2, \log \frac{Wd}{\epsilon}\right\} \log \frac{Wd}{\epsilon}}\right).$$

*Proof.* For each exponential term  $g_m(z) = e^{-a_m z^2}$ , we know

$$\eta_{g'_m}(\epsilon, \theta) = \mathcal{O}\left(\sqrt{\max\left\{\frac{R}{\theta^2}, \log\frac{1}{\epsilon}\right\} \log\frac{1}{\epsilon}}\right)$$

according to Lemma 15, where  $\eta_{g'_m}(\epsilon, \theta)$  is defined in Corollary 10. Moreover, a simple calculation shows that

$$C_{g'_m} \leq \sup |g'_m(z)| = \sup |2a_m z e^{-a_m z^2}| < \sqrt{a_m} \leq \sqrt{R}. \quad (37)$$

Therefore, if we let  $\theta = \frac{\pi}{3P}$ , then the complexity of implementing a  $(1, 1, \frac{\epsilon}{2Wd})$ -block-encoding of matrix  $\exp(-a_m(D_-)^2)$  is

$$\mathcal{O}\left(\log P \log\left(\frac{dWRP}{\epsilon}\right) \sqrt{\max\left\{RP^2, \log\frac{Wd}{\epsilon}\right\} \log\frac{Wd}{\epsilon}}\right),$$

according to Corollary 10.

After implementing  $\exp(-a_m(D_-)^2)$  for each  $\xi_k$  register ( $k = 1, \dots, d$ ), we get a  $(1, d, \frac{\epsilon}{2W})$ -block-encoding of  $e^{-a_m|\xi|^2}$ . Since there are  $M$  such terms, the total gate complexity after conducting LCU becomes

$$\mathcal{O}\left(dM \log P \log\left(\frac{dWRP}{\epsilon}\right) \sqrt{\max\left\{RP^2, \log\frac{Wd}{\epsilon}\right\} \log\frac{Wd}{\epsilon}}\right). \quad (38)$$

Since only one QFT and one iQFT are needed with complexity  $\mathcal{O}(d \log^2 P)$ , the dominating term in the above complexity formula remains unchanged. The total error of this block encoding is  $\sum_{m=1}^M |w_m| \frac{\epsilon}{2W} < \epsilon$  as desired. Since  $\mathcal{O}(d)$  ancillae are used when encoding  $e^{-a_m|\xi|^2}$  and  $\mathcal{O}(\log M)$  ancillae are used for LCU, the total number of ancilla is  $\mathcal{O}(d + \log M)$ .  $\square$

With Theorem 16, we are ready to work on a concrete example. Consider the following  $d$ -dimensional elliptic equation with periodic boundary conditions:

$$-\frac{1}{4\pi^2} \Delta u(\mathbf{x}) + u(\mathbf{x}) = b(\mathbf{x}), \quad \mathbf{x} \in [0, 1]^d. \quad (39)$$

As explained by (35) and (36), the idea is to expand  $\varphi(y) = \frac{1}{1+y^2}$  as the sum of a series of exponential functions. To this end, we introduce a result for exponential approximations in the form of (35) and (36).

**Lemma 17.** *For any  $0 < \delta \leq 1$  and  $0 < \epsilon \leq \frac{1}{2}$ , there exist positive numbers  $p_m$  and  $v_m$  such that*

$$\left| r^{-1} - \sum_{m=1}^M v_m e^{-p_m r} \right| \leq r^{-1} \epsilon, \quad \text{for all } \delta \leq r \leq 1, \quad (40)$$

with

$$M = \mathcal{O}\left(\log \epsilon^{-1} \left(\log \epsilon^{-1} + \log \delta^{-1}\right)\right), \quad (41)$$

and

$$\max_m p_m = \mathcal{O}\left(\delta^{-1} \log \epsilon^{-1} \left(\log \epsilon^{-1} + \log \delta^{-1}\right)\right). \quad (42)$$

The proof of (41) can be found in Theorem A.1 of [3], and (42) is also implied in the proof there. We summarize the construction given in [3] in passing. Denote  $f_r(t) = e^{-re^t+t}$ , then  $r^{-1} = \int_{-\infty}^{\infty} f_r(t)dt$  and  $f_r(t)$  decays rapidly when  $|t| \rightarrow \infty$ . Therefore one can approximate this integral using the trapezoidal rule on a finite interval  $[a, b]$  with step size  $h$ , which is

$$h \left( \sum_{k=1}^{K-1} f_r(a + kh) + \frac{f_r(a) + f_r(b)}{2} \right), \quad (43)$$

where  $K = (b - a)/h$ . Since each term of (43) is of the form  $ve^{-pr}$ , the approximate integral formula above actually provides an approximation of the form (40). Finally, by choosing  $a = -\log \frac{4}{\epsilon}$ ,  $b = \log \left( 4 \log \frac{4}{\epsilon} \delta^{-1} \log \left( 2 \log \frac{4}{\epsilon} (\delta\epsilon)^{-1} \right) \right)$  and  $h \leq \pi / (2 \log \frac{4}{\epsilon} + 1)$ , one can show that the condition (40) is satisfied, and from  $M = K + 1 = (b - a)/h + 1$  one can check that (41) and (42) hold.

Now, with the substitutions  $\delta = (\frac{dP^2}{4} + 1)^{-1}$  and  $r = (1 + y^2) / (\frac{dP^2}{4} + 1)$  in Lemma 17 we get the following approximation:

$$\left| \frac{1}{1 + y^2} - \sum_{m=1}^M w_m e^{-a_m y^2} \right| \leq \epsilon, \quad \text{for all } -\frac{\sqrt{d}P}{2} \leq y \leq \frac{\sqrt{d}P}{2}, \quad (44)$$

where  $a_m = p_m / (\frac{dP^2}{4} + 1)$ ,  $w_m = e^{-a_m} v_m / (\frac{dP^2}{4} + 1)$ , and

$$\begin{aligned} M &= \mathcal{O} \left( \log \epsilon^{-1} \left( \log \epsilon^{-1} + \log(dP) \right) \right), \\ R &= \max_m a_m = \mathcal{O} \left( \log \epsilon^{-1} \left( \log \epsilon^{-1} + \log(dP) \right) \right), \\ W &= \sum_{m=1}^M |w_m| = \mathcal{O}(1). \end{aligned} \quad (45)$$

Here the estimation of  $W$  is deduced from plugging  $y = 0$  into (44) and the positivity of  $w_m$ . Finally, after plugging the estimations of  $M$ ,  $R$  and  $W$  into Theorem 16, we obtain the following result:

**Corollary 18.** *For the pseudo-differential operator associated with the symbol  $\beta(\xi) = 1 + |\xi|^2$  (see (39)), there is a  $(\gamma, q, \epsilon)$ -block-encoding for its inverse with  $\gamma = \mathcal{O}(1)$ ,  $q = \mathcal{O} \left( d + \log \log \frac{dP}{\epsilon} \right)$ , and gate complexity  $\mathcal{O} \left( dP \left( \log \frac{dP}{\epsilon} \right)^{2.5} \left( \log \frac{1}{\epsilon} \right)^{1.5} \left( \log \frac{d}{\epsilon} \right)^{0.5} \log P \right)$ .*

*Remark 3.* If one uses the uniform grid to discretize the operator  $(-\frac{1}{4\pi^2}\Delta + 1)$  in equation (39), then the condition number of the matrix obtained is at least  $\kappa = \mathcal{O}(dP^2)$ . This indicates that the complexity is at least  $\mathcal{O}(dP^2)$  when block-encoding its inverse matrix using the previous method, such as LCU or QSVT. However, here we achieved  $\tilde{\mathcal{O}}_\epsilon(dP) = \tilde{\mathcal{O}}_\epsilon(\sqrt{d}\kappa)$  complexity for encoding the discretization of  $(-\frac{1}{4\pi^2}\Delta + 1)^{-1}$ , where we omit the logarithm terms in  $\tilde{\mathcal{O}}$  and denote the dependence on  $\epsilon$  by the subscript. This improvement demonstrates the potential of directly working on the symbol level, as we did in this section. When solving the corresponding problem (38) with a particular right-hand side  $b$ , the worst case gate complexity becomes  $\tilde{\mathcal{O}}_\epsilon(\kappa\sqrt{d}\kappa)$  since the worst case success probability is  $\mathcal{O}(1/\kappa)$ , which is inferior comparing with the dependence on  $\kappa$  obtained in [13]. However, the block encoding scheme in this paper is independent of the right-hand side  $b$  and thus can be used repeatedly for different  $b$  without constructing the circuit again. Also, the circuit is simpler than the one in [13], making it more applicable in practice.

## 7 Conclusion and Discussion

This paper systematically investigates block encodings for pseudo-differential operators (PDOs) under different structural assumptions. A block encoding scheme for PDOs with generic symbols is developed in Section 3, and the quantum circuit is illustrated in Figure 3. For PDOs with linear combinations of separable symbols, we improve the success probability exponentially and present an efficient block encoding algorithm in Section 4. Then a more explicit and practical block encoding scheme is derived in Section 5 with the help of QSP and QET, along with which the complexity analysis is provided. Plenty of worked examples are given in Section 6, including the block encoding of elliptic operators with a variable coefficient that is difficult to deal with for quantum solvers that use finite difference schemes and the block encoding of the inverse of constant-coefficient elliptic operators without using quantum linear system algorithms. The block encoding schemes presented in this paper enrich the study of the block encoding of dense operators and shed new light on designing practical quantum circuits for scientific computing.

For future directions, one can apply the established results in this paper to other PDOs besides the ones presented in Section 6. One can also use the idea of symbol calculus to implement different operations on the PDO, such as taking square root or exponential, which can help solve certain PDEs in practice.

## References

- [1] D. An and L. Lin. Quantum linear system solver based on time-optimal adiabatic quantum computing and quantum approximate optimization algorithm. *ACM Transactions on Quantum Computing*, 3:1–28, 2022. DOI: [10.1145/3498331](https://doi.org/10.1145/3498331).
- [2] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma. Simulating hamiltonian dynamics with a truncated taylor series. *Physical review letters*, 114:090502, 2015. DOI: [10.1103/PhysRevLett.114.090502](https://doi.org/10.1103/PhysRevLett.114.090502).
- [3] G. Beylkin and L. Monzón. On approximation of functions by exponential sums. *Applied and Computational Harmonic Analysis*, 19:17–48, 2005. DOI: [10.1016/j.acha.2005.01.003](https://doi.org/10.1016/j.acha.2005.01.003).
- [4] D. Camps and R. Van Beeumen. Fable: Fast approximate quantum circuits for block-encodings. In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 104–113. IEEE, 2022. DOI: [10.1109/QCE53715.2022.00029](https://doi.org/10.1109/QCE53715.2022.00029).
- [5] D. Camps, L. Lin, R. Van Beeumen, and C. Yang. Explicit quantum circuits for block encodings of certain sparse matrices. *arXiv preprint arXiv:2203.10236*, 2022. DOI: [10.48550/arXiv.2203.10236](https://doi.org/10.48550/arXiv.2203.10236).
- [6] Y. Cao, A. Papageorgiou, I. Petras, J. Traub, and S. Kais. Quantum algorithm and circuit design solving the poisson equation. *New Journal of Physics*, 15(1):013021, 2013. DOI: [10.1088/1367-2630/15/1/013021](https://doi.org/10.1088/1367-2630/15/1/013021).
- [7] G. Castelazo, Q. T. Nguyen, G. De Palma, D. Englund, S. Lloyd, and B. T. Kiani. Quantum algorithms for group convolution, cross-correlation, and equivariant transformations. *Physical Review A*, 106:032402, 2022. DOI: [10.1103/PhysRevA.106.032402](https://doi.org/10.1103/PhysRevA.106.032402).
- [8] R. Chao, D. Ding, A. Gilyen, C. Huang, and M. Szegedy. Finding angles for quantum signal processing with machine precision. *arXiv preprint arXiv:2003.02831*, 2020. DOI: [10.48550/arXiv.2003.02831](https://doi.org/10.48550/arXiv.2003.02831).
- [9] A. M. Childs, R. Kothari, and R. D. Somma. Quantum algorithm for systems of linear

- equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46:1920–1950, 2017. DOI: [10.1137/16M1087072](https://doi.org/10.1137/16M1087072).
- [10] A. M. Childs, J.-P. Liu, and A. Ostrander. High-precision quantum algorithms for partial differential equations. *Quantum*, 5:574, 2021. DOI: [10.22331/q-2021-11-10-574](https://doi.org/10.22331/q-2021-11-10-574).
- [11] D. Coppersmith. An approximate fourier transform useful in quantum factoring. *arXiv preprint quant-ph/0201067*, 2002. DOI: [10.48550/arXiv.quant-ph/0201067](https://doi.org/10.48550/arXiv.quant-ph/0201067).
- [12] P. C. Costa, S. Jordan, and A. Ostrander. Quantum algorithm for simulating the wave equation. *Physical Review A*, 99:012323, 2019. DOI: [10.1103/PhysRevA.99.012323](https://doi.org/10.1103/PhysRevA.99.012323).
- [13] P. C. Costa, D. An, Y. R. Sanders, Y. Su, R. Babbush, and D. W. Berry. Optimal scaling quantum linear-systems solver via discrete adiabatic theorem. *PRX Quantum*, 3:040303, 2022. DOI: [10.1103/PRXQuantum.3.040303](https://doi.org/10.1103/PRXQuantum.3.040303).
- [14] A. J. da Silva and D. K. Park. Linear-depth quantum circuits for multiqubit controlled gates. *Physical Review A*, 106:042602, 2022. DOI: [10.1103/PhysRevA.106.042602](https://doi.org/10.1103/PhysRevA.106.042602).
- [15] L. Demanet and L. Ying. Discrete symbol calculus. *SIAM review*, 53:71–104, 2011. DOI: [10.1137/080731311](https://doi.org/10.1137/080731311).
- [16] Y. Dong, X. Meng, K. B. Whaley, and L. Lin. Efficient phase-factor evaluation in quantum signal processing. *Physical Review A*, 103:042419, 2021. DOI: [10.1103/PhysRevA.103.042419](https://doi.org/10.1103/PhysRevA.103.042419).
- [17] Y. Dong, L. Lin, H. Ni, and J. Wang. Infinite quantum signal processing. *arXiv preprint arXiv:2209.10162*, 2022. DOI: [10.48550/arXiv.2209.10162](https://doi.org/10.48550/arXiv.2209.10162).
- [18] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019. DOI: [10.1145/3313276.3316366](https://doi.org/10.1145/3313276.3316366).
- [19] L. Grover and T. Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv preprint quant-ph/0208112*, 2002. DOI: [10.48550/arXiv.quant-ph/0208112](https://doi.org/10.48550/arXiv.quant-ph/0208112).
- [20] J. Haah. Product decomposition of periodic functions in quantum signal processing. *Quantum*, 3:190, 2019. DOI: [10.22331/q-2019-10-07-190](https://doi.org/10.22331/q-2019-10-07-190).
- [21] A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103:150502, 2009. DOI: [10.1103/PhysRevLett.103.150502](https://doi.org/10.1103/PhysRevLett.103.150502).
- [22] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52:1191, 1997. DOI: [10.1070/RM1997v052n06ABEH002155](https://doi.org/10.1070/RM1997v052n06ABEH002155).
- [23] A. Y. Kitaev, A. Shen, M. N. Vyalyi, and M. N. Vyalyi. *Classical and quantum computation*. American Mathematical Soc., 2002. DOI: [10.1090/gsm/047](https://doi.org/10.1090/gsm/047).
- [24] L. Lin and Y. Tong. Optimal polynomial based quantum eigenstate filtering with application to solving quantum linear systems. *Quantum*, 4:361, 2020. DOI: [10.22331/q-2020-11-11-361](https://doi.org/10.22331/q-2020-11-11-361).
- [25] G. H. Low and I. L. Chuang. Optimal hamiltonian simulation by quantum signal processing. *Physical review letters*, 118:010501, 2017. DOI: [10.1103/PhysRevLett.118.010501](https://doi.org/10.1103/PhysRevLett.118.010501).
- [26] A. Mahasinghe and J. Wang. Efficient quantum circuits for toeplitz and hankel matrices. *Journal of Physics A: Mathematical and Theoretical*, 49:275301, 2016. DOI: [10.1088/1751-8113/49/27/275301](https://doi.org/10.1088/1751-8113/49/27/275301).
- [27] S. McArdle, A. Gilyén, and M. Berta. Quantum state preparation without coherent arithmetic. *arXiv preprint arXiv:2210.14892*, 2022. DOI: [10.48550/arXiv.2210.14892](https://doi.org/10.48550/arXiv.2210.14892).
- [28] A. Montanaro and S. Pallister. Quantum algorithms and the finite element method. *Physical Review A*, 93:032324, 2016. DOI: [10.1103/PhysRevA.93.032324](https://doi.org/10.1103/PhysRevA.93.032324).

- [29] Y. Nam, Y. Su, and D. Maslov. Approximate quantum fourier transform with  $\mathcal{O}(n \log(n))$  gates. *NPJ Quantum Information*, 6:26, 2020. DOI: [10.1038/s41534-020-0257-5](https://doi.org/10.1038/s41534-020-0257-5).
- [30] Q. T. Nguyen, B. T. Kiani, and S. Lloyd. Quantum algorithm for dense and full-rank kernels using hierarchical matrices. *Quantum*, 6:876, 2022. DOI: [10.22331/q-2022-12-13-876](https://doi.org/10.22331/q-2022-12-13-876).
- [31] M. A. Nielsen and I. Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002. DOI: [10.1119/1.1463744](https://doi.org/10.1119/1.1463744).
- [32] E. G. Rieffel and W. H. Polak. *Quantum computing: A gentle introduction*. MIT Press, 2011. DOI: [10.1063/PT.3.1442](https://doi.org/10.1063/PT.3.1442).
- [33] S. Sachdeva, N. K. Vishnoi, et al. Faster algorithms via approximation theory. *Foundations and Trends in Theoretical Computer Science*, 9:125–210, 2014. DOI: [10.1561/04000000065](https://doi.org/10.1561/04000000065).
- [34] E. M. Stein and T. S. Murphy. *Harmonic analysis: real-variable methods, orthogonality, and oscillatory integrals*, volume 3. Princeton University Press, 1993. ISBN 9780691032160. URL <https://press.princeton.edu/books/hardcover/9780691032160/harmonic-analysis-pms-43-volume-43>.
- [35] Y. Tong, D. An, N. Wiebe, and L. Lin. Fast inversion, preconditioned quantum linear system solvers, fast green’s-function computation, and fast evaluation of matrix functions. *Physical Review A*, 104, 2021. DOI: [10.1103/PhysRevA.104.032422](https://doi.org/10.1103/PhysRevA.104.032422).
- [36] R. Vale, T. M. D. Azevedo, I. Araújo, I. F. Araujo, and A. J. da Silva. Decomposition of multi-controlled special unitary single-qubit gates. *arXiv preprint arXiv:2302.06377*, 2023. DOI: [10.48550/arXiv.2302.06377](https://doi.org/10.48550/arXiv.2302.06377).
- [37] M. W. Wong. *An Introduction to Pseudo-Differential Operators*. World Scientific, 1999. DOI: [10.1142/4047](https://doi.org/10.1142/4047).
- [38] L. Ying. Stable factorization for phase factors of quantum signal processing. *Quantum*, 6:842, 2022. DOI: [10.22331/q-2022-10-20-842](https://doi.org/10.22331/q-2022-10-20-842).

## A Multiplication of two states

**Proposition 19.** Let  $U_a$  and  $U_b$  be unitary matrices of size  $N \times N$  with the first column being  $[a_0, a_1, \dots, a_{N-1}]^\top$  and  $[b_0, b_1, \dots, b_{N-1}]^\top$ , respectively. Then the following circuit gives the state  $\frac{1}{c} \sum_{j=0}^{N-1} a_j b_j |j\rangle$  with probability  $c^2$ , where  $c = \sqrt{\sum_{j=0}^{N-1} |a_j b_j|^2}$ .

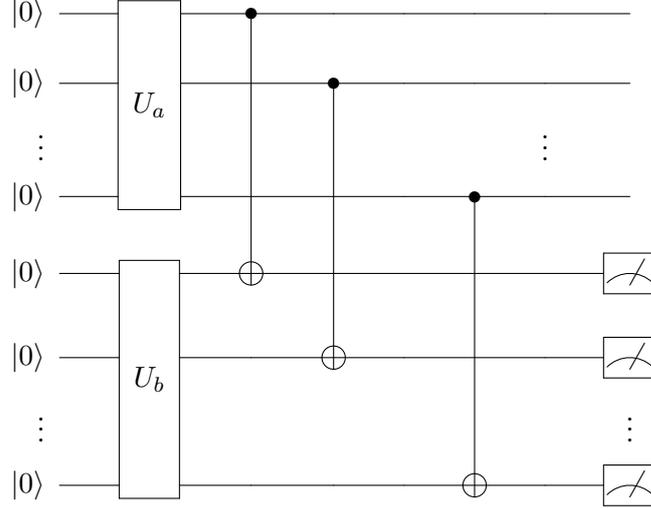


Figure 9: Circuit for element-wise multiplication

*Proof.* After applying  $U_a$  and  $U_b$ , the state becomes

$$\sum_{j,k=0}^{N-1} a_j b_k |j\rangle |k\rangle = \sum_{\substack{j_0, j_1, \dots, j_{n-1} \\ k_0, k_1, \dots, k_{n-1}}} a_j b_k |j_0 \cdots j_{n-1}\rangle |k_0 \cdots k_{n-1}\rangle,$$

and after applying the CNOT gates, the  $k$  register is only  $|0\rangle$  when  $j_l = k_l$  for all  $l = 0, \dots, n-1$ . which means the state becomes

$$\sum_{j_0, j_1, \dots, j_{n-1}} a_j b_j |j_0 \cdots j_{n-1}\rangle |0\rangle + |\perp\rangle = \sum_{j=0}^{N-1} a_j b_j |j\rangle |0\rangle + |\perp\rangle,$$

where  $|\perp\rangle$  is a term that is orthogonal to  $|j\rangle |0\rangle$  for any  $j$ . Thus the probability of obtaining  $|0\rangle$  after the measurement is  $\sum_{j=0}^{N-1} |a_j b_j|^2 = c^2$ , and the outcome of the system register is  $\frac{1}{c} \sum_{j=0}^{N-1} a_j b_j |j\rangle$  when the measurement gives  $|0\rangle$ .  $\square$