Quantum Monte Carlo algorithm for solving Black-Scholes PDEs for high-dimensional option pricing in finance and its proof of overcoming the curse of dimensionality

Yongming Li[1], Ariel Neufeld[2]

[1] Department of Mathematics, Texas A&M University,
Texas, USA, e-mail: liyo0008@tamu.edu

[2] Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, Singapore, e-mail: ariel.neufeld@ntu.edu.sg

January 24, 2023

Abstract

In this paper we provide a quantum Monte Carlo algorithm to solve high-dimensional Black-Scholes PDEs with correlation for high-dimensional option pricing. The payoff function of the option is of general form and is only required to be continuous and piece-wise affine (CPWA), which covers most of the relevant payoff functions used in finance. We provide a rigorous error analysis and complexity analysis of our algorithm. In particular, we prove that the computational complexity of our algorithm is bounded polynomially in the space dimension d of the PDE and the reciprocal of the prescribed accuracy ε and so demonstrate that our quantum Monte Carlo algorithm does not suffer from the curse of dimensionality.

Contents

1 Introduction

An option in finance is a contract between a seller and a buyer, which provides a future payoff to the buyer of the option at the maturity date in dependence of the underlying financial securities involved in the contract, such as, for example, stocks or indexes. Since the underlying securities evolve randomly over time and hence their future values at maturity cannot be known at any previous time neither by the buyer nor the seller, the exact payoff the buyer of the option receives at maturity cannot be known either. Hence a key problem in financial theory is to evaluate the value of such options, i.e. to define and determine a fair price between buyer and seller of the option under consideration.

In 1973, Black, Scholes, and Merton introduced in [10] and [41] the so-called Black-Scholes-Merton model, also known simply as the Black-Scholes model, which is a pricing model allowing to evaluate the value of options which only depend on the underlying single security. They have shown in [10] and [41] that under the Black-Scholes model, the fair price of an option can be characterized as a solution of a particular partial differential equation (PDE). More precisely, at each time $t \leq T$ the value of an option with corresponding payoff function $h : \mathbb{R}_+ \to \mathbb{R}$, which provides a payoff $h(S_T)$ to the buyer in dependence of the value of the underlying single security S_T at maturity time T, coincides with the solution $u(t, x)$ of the so-called Black-Scholes PDE with terminal condition h, given that the value S_t of the underlying security at time t satisfies $S_t = x$.

Later, the Black-Scholes model has been extended to price options involving multiple securities and to incorporate their correlations into consideration. Analogously to the original model, the price of an option can be characterized by a PDE, whose space dimension d corresponds to the amount of securities involved in the financial contract. For example, an option depending on the index of the S&P 500 could be priced in the (multidimensional) Black-Scholes model by the solution of a 500-dimensional PDE.

Unfortunately, in the multidimensional setting of the Black-Scholes model, there are no explicit expressions for the solution of the corresponding PDE, and hence numerical methods are necessary to approximately solve these high-dimensional PDEs. It is crucial both from a theoretical, but especially also from a practical point of view to provide a rigorous error analysis and complexity analysis of these numerical methods. Indeed, while the precise error analysis allows, in the context of option pricing, to precisely determine the true absolute error of the output of the numerical algorithm to the theoretical price of the option under consideration, a rigorous complexity analysis allows to determine how well an algorithm scales in dependence of the space-dimension of the underlying PDE. Ideally, one would like to build a numerical algorithm whose precise error and complexity analysis can be determined and which does not suffer from the *curse of dimensionality* [8]. By the curse of dimensionality, one understands that for given pre-specified precision $\varepsilon \in (0, 1)$ determining the maximum absolute error of the output of the algorithm one is willing to accept compared to the correct theoretical value and dimension d of the input, here corresponding to the amount of financial securities involved in the option, an algorithm *suffers from the curse of dimensionality* if its complexity, i.e. number of computational operations, is of order ε^{-d}, i.e. grows *exponentially* in the dimension d. An algorithm is called *to overcome the curse of dimensionality* if its complexity only grows *polynomially* in the dimension d and the (reciprocal of the) precision ε. Due to the Feynman-Kac formula for the Black-Scholes PDE, allowing to write the solution of the Black-Scholes PDE in form of an expectation of the payoff function $h : \mathbb{R}_+^d \to \mathbb{R}$ with respect to the multivariate log-normal distribution, Monte Carlo based algorithms have demonstrated both theoretically and practically to be efficient for pricing high-dimensional options under the Black-Scholes model. In particular, Monte Carlo methods typically do not suffer from the curse of dimensionality, compared to, e.g., classical finite difference or finite element methods. We refer to, e.g., [2, 28] for numerical methods which involve finite difference or finite element, to, e.g., [11] for Monte Carlo based methods, as well as to, e.g., [7, 9, 25, 30, 33] for deep learning based methods to approximately solve the (multidimensional) Black-Scholes PDE.

In recent years, there has been a rapid development of numerical methods dealing with problems in quantitative finance using quantum computers. The motivation comes from the fact that qubits, compared to classical bits, are allowed quantum mechanically to be in a state of superposition, from which one anticipates that quantum computers should be able to achieve much higher computational power than classical (super-) computers. The applications of quantum algorithms in finance include portfolio optimization [53], the computation of risk measures such as *Value at Risk (VAR)* [62], and option pricing, particularly in the Black-Scholes model [15, 21, 26, 38, 50, 52, 53, 57]. We also refer to the monograph [36] and surveys [24, 46] for (further) applications of quantum computing in finance. Furthermore, [5, 6, 17, 39, 43] proposed quantum algorithms to approximately solve different PDEs than the Black-Scholes PDE used in finance for option pricing.

While [26] proposes a hybrid quantum-classical algorithm to approximately solve the one-dimensional Black-Scholes PDE exploiting its relation to the Schrödinger equation in imaginary time and [38] proposes a variational quantum approach, most literature uses quantum Monte Carlo methods to approximately solve the Black-Scholes PDE in order to price financial options. More precisely, these works rely on the *Quantum Amplitude Estimation algorithm (QAE)* [12] which estimates the expected value of a random parameter (see Section 2.3 for a detailed discussion) based on an extension of *Grover's search algorithm* [32]. Several variations of the Quantum Amplitude Estimation algorithm have been proposed recently, see e.g. [1, 27, 29, 48, 49, 58, 61, 63]. Quantum Monte Carlo methods can ideally achieve a quadratic speed-up [34],[42] compared to classical (i.e. non-quantum) Monte Carlo methods. However, the quadratic speedup can only be achieved if there is a so-called *oracle* quantum circuit which can correctly upload the corresponding distribution in rotated form, without any approximation errors (caused, e.g., from discretization and rotation), such that it is applicable to a quantum amplitude estimation algorithm. This assumption however in most cases cannot be justified in practice, as highlighted, e.g., in [15, 64].

In this paper, we propose a quantum Monte Carlo algorithm to solve high-dimensional Black-Scholes PDEs with correlation and general payoff function which is continuous and piece-wise affine (CPWA), enabling to price most relevant payoff functions used in finance (see also Section 2.1.2). Our algorithm follows the idea of the quantum Monte Carlo algorithm proposed in [57] which first uploads the multivariate log-normal distribution and the payoff function in rotated form and then applies a QAE algorithm to approximately solve the Black-Scholes PDE to price options. Our main contribution lies in a rigourous error analysis as well as complexity analysis of our algorithm. To that end, we first introduce quantum circuits that can perform arithmetic operations on two complement's numbers representing signed dyadic rational numbers, together with its complexity analysis. This allows us to provide a rigorous error and complexity analysis when uploading first a truncated and discretized approximation of the multivariate log-normal distribution and then uploading an approximation of the CPWA payoff function in rotated form, where the approximation consists of truncation as well as the rounding of the coefficients of the CPWA payoff function. This together with a rigorous error and complexity analysis when applying the modified iterative quantum amplitude estimation algorithm [27] allows us to control the output error of our algorithm to be bounded by the pre-specified accuracy level $\varepsilon \in (0,1)$, while bounding its computational complexity; we refer to Theorem 2.22 for the precise statement of our main result. In particular, we prove that the computational complexity of our algorithm only grows polynomially in the space dimension d of the Black-Scholes PDE and in the (reciprocal of the) accuracy level ε, demonstrating that our algorithm does not suffer from the curse of dimensionality. To the best of our knowledge this is the first work in the literature which mathematically proves that a quantum Monte Carlo algorithm can overcome the curse of dimensionality when approximately solving a high-dimensional PDE. We refer to Remark 2.23 for a detailed discussion of the complexity analysis.

The rest of this paper is organized as follows. In Section 2, we introduce the main setting of this paper, outline the steps of our algorithm, and state our main theorem, as well as provide a detailed discussion of our complexity analysis. In Section 3, we introduce and analyze all relevant quantum circuits we need in our quantum Monte Carlo algorithm. In Section 4, we provide a detailed error analysis of the steps of our algorithm outlined in Section 2.4.1. Finally, in Section 5, we provide the proof of Theorem 2.22.

Notation. We denote the set of real numbers and positive real numbers by $\mathbb{R}$ and $\mathbb{R}_+ := (0,\infty)$, respectively. The set of natural numbers is denoted by $\mathbb{N} := \{1,2,\dots\}$, and we use $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. The set of complex numbers is denoted by $\mathbb{C}$, and we define $\mathrm{i} := \sqrt{-1}$. Moreover, we denote by I_2 and $I_2^{\otimes n}$ the corresponding identity matrices in $\mathbb{C}^{2\times 2}$ and $\mathbb{C}^{2^n\times 2^n}$, respectively, for every $n \in \mathbb{N}$. Furthermore, for each $n \in \mathbb{N}$ we denote by $\mathcal{U}(2^n)$ the set of unitary matrices in $\mathbb{C}^{2^n\times 2^n}$, i.e. matrices $U \in \mathbb{C}^{2^n\times 2^n}$ satisfying $UU^\dagger = U^\dagger U = I_2^{\otimes n}$, where $U^\dagger$ denotes the *conjugate transpose* of U.

2 Setting and Main result

2.1 Black-Scholes PDE for option pricing

Let $r \in (0,\infty)$ be the risk-free interest rate, let $T \in (0,\infty)$ be a finite time horizon determining the maturity, and let $d \in \mathbb{N}$ be the number of assets. We consider the multiple-asset Black-Scholes PDE

$$\frac{\partial u}{\partial t} + \frac{1}{2}\sum_{i,j=1}^{d} C_{ij} x_i x_j \frac{\partial^2 u}{\partial x_i \partial x_j} + \sum_{i=1}^{d} r x_i \frac{\partial u}{\partial x_i} - ru = 0, \quad \text{in } [0,T]\times\mathbb{R}_+^d \tag{1}$$

subjected to a terminal condition $u(T,\cdot) = h(\cdot)$. Here, $h : \mathbb{R}_+^d \to \mathbb{R}$ represents the payoff function and $u(t,x)$ represents the option price at time t with spot price x. The covariance matrix $\boldsymbol{C} = (C_{i,j})_{i,j=1}^d \in \mathbb{R}^{d\times d}$ is assumed to be symmetric positive definite with a Cholesky factorization $\boldsymbol{C} = \boldsymbol{\sigma}\boldsymbol{\sigma}^\top$, where $\boldsymbol{\sigma} \in \mathbb{R}^{d\times d}$ is the log-volatility coefficient matrix, so that there is a unique risk-neutral measure (see, e.g., [14]). Note that the PDE (1) has a unique solution[1] whenever $h : \mathbb{R}_+^d \to \mathbb{R}$ is continuous and at most polynomially growing, see, e.g., [30, Proposition 2.22, Corollary 4.5].

[1]The solution $u(t,x)$ of the PDE (1) is meant in the viscosity sense, see, e.g., [18],[30].

2.1.1 Geometric Brownian motion process for the price evolution of multiple assets

In the multidimensional Black-Scholes model, the prices of the d stocks under consideration are modeled by a multidimensional geometric Brownian motion (GBM) having constant growth rate and volatility, see, e.g., [14]. We briefly describe the dynamics of the geometric Brownian motion process for multiple assets.

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and let $\boldsymbol{W} = (W^1, \ldots, W^d) : [0,T]\times\Omega \to \mathbb{R}^d$ be a standard d-dimensional Brownian motion. For a log-volatility coefficient matrix $\boldsymbol{\sigma} \in \mathbb{R}^{d\times d}$ assumed to be invertible, let $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_d \in \mathbb{R}^d$ denote the row vectors of matrix $\boldsymbol{\sigma}$, and let $\sigma_i := \|\boldsymbol{\sigma_i}\|_{\ell^2(\mathbb{R}^d)}$. Let $\boldsymbol{S} = (S^1, \ldots, S^d) : [0,T]\times\Omega \to \mathbb{R}^d_+$ be the stock price process governed by the following stochastic differential equation

$$dS^i_t = S^i_t(rdt + \sum_{j=1}^d \sigma_{ij} dW^j_t), \quad \text{for } i = 1, \ldots, d, \tag{2}$$

with some initial spot price $\boldsymbol{S}_0 \in \mathbb{R}^d_+$. Here $\boldsymbol{S}_t = (S^1_t, \ldots, S^d_t)$ represents the values of each stock $i = 1, \ldots, d$ at time $0 \le t \le T$. Let $\boldsymbol{R} = (R^1, \ldots, R^d) : [0,T]\times\Omega \to \mathbb{R}^d$ be the log-return process defined component-wise by $R^i_t = \ln\big(S^i_t/S^i_0\big)$ for $i = 1, \ldots, d$. It follows from Itô's formula for all $t \in [0,T]$ that

$$dR^i_t = (r - \frac{1}{2}\sigma_i^2)dt + \sum_{j=1}^d \sigma_{ij} dW^j_t, \quad \text{for } i = 1, \ldots, d, \tag{3}$$

with initial condition $R^i_0 = 0$ for $i = 1, \ldots, d$. Let $\hat{\boldsymbol{\mu}} = (\hat{\mu}_1, \ldots, \hat{\mu}_d) \in \mathbb{R}^d$ be a vector satisfying $\hat{\mu}_i = (r - \frac{1}{2}\sigma_i^2)$ for $i = 1, \ldots, d$. From equation (3), it holds that $\boldsymbol{R}_T$ is a multivariate normal distribution with mean $T\hat{\boldsymbol{\mu}}$ and covariance $T\boldsymbol{C}$. Hence, by taking the inverse of the log transform, we observe that the law of the stock price process $\boldsymbol{S}_T = \boldsymbol{S}_0 \exp(\boldsymbol{R}_T)$ is a multivariate log-normal distribution with log-mean $T\hat{\boldsymbol{\mu}}$ and log-covariance $T\boldsymbol{C}$. In general, for a given fixed initial condition $(t, x) \in [0,T]\times\mathbb{R}^d_+$, there is a well-known formula for the probability transition density function of $\boldsymbol{S}_T$, subjected to the condition that $\boldsymbol{S}_t = x$.

Lemma 2.1 (Density formula) *Let $d \in \mathbb{N}$, let $\boldsymbol{x} = (x_1, \ldots, x_d) \in \mathbb{R}^d_+$, and let $t \in [0,T)$. Let $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_d) \in \mathbb{R}^d$ be given by $\mu_i = \ln(x_i) + (r - \frac{1}{2}\sigma_i^2)(T - t)$ for $i = 1, \ldots, d$ and let $\boldsymbol{\Sigma} \in \mathbb{R}^{d\times d}$ be given by $\boldsymbol{\Sigma} = (T - t)\boldsymbol{C}$. Then, the stock price process $\boldsymbol{S}_T$ introduced by* (2) *conditional on $\boldsymbol{S}_t = x$ follows a multivariate log-normal distribution with log-mean $\boldsymbol{\mu}$ and log-covariance $\boldsymbol{\Sigma}$, and the joint transition probability density function is given by*

$$p(\boldsymbol{y}, T; \boldsymbol{x}, t) := \frac{\exp\big(-\frac{1}{2}(\log(\boldsymbol{y}) - \boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1}(\log(\boldsymbol{y}) - \boldsymbol{\mu})\big)}{(2\pi)^{d/2}(\det \boldsymbol{\Sigma})^{1/2} \prod_{i=1}^d y_i}, \tag{4}$$

where for $\boldsymbol{y} = (y_1, \ldots, y_d) \in \mathbb{R}^d_+$, $\log(\boldsymbol{y}) \in \mathbb{R}^d$ is given by

$$(\log(\boldsymbol{y}))_i = \ln(y_i), \quad i = 1, \ldots, d. \tag{5}$$

Proof. See, e.g., Campolieti and Makarov [14, page 485-486]. □

Throughout the paper we impose the following assumption on the covariance matrix $\boldsymbol{C} \equiv \boldsymbol{C}_d$ in dependence of the dimension d.

Assumption 2.2 (Covariance matrix) *There is a constant $C_1 \in [1, \infty)$ not depending on the dimension $d \in \mathbb{N}$ such that the covariance matrix $\boldsymbol{C} \equiv \boldsymbol{C}_d = ((\boldsymbol{C}_d)_{i,j})^d_{i,j=1} \in \mathbb{R}^{d\times d}$ defined as in* (1) *satisfies for every $i, j = 1, \ldots, d$ that*

$$|(\boldsymbol{C}_d)_{i,j}| \le C_1. \tag{6}$$

2.1.2 Continuous piece-wise affine (CPWA) payoff functions

For any $d \in \mathbb{N}$, we consider a payoff function $h : \mathbb{R}^d_+ \to \mathbb{R}$, which takes the stock prices $\boldsymbol{S}_T \in \mathbb{R}^d_+$ at terminal time T as input. The option price $u(t, x) \in \mathbb{R}$ at time $t \in [0,T)$ given that the spot price satisfies $\boldsymbol{S}_t = \boldsymbol{x} \in \mathbb{R}^d_+$ is characterized by the following Feynman-Kac formula (see, e.g., [14, Equation (13.33)])

$$u(t, x) = e^{-r(T-t)}\mathbb{E}[h(\boldsymbol{S}_T) \mid \boldsymbol{S}_t = \boldsymbol{x}] = e^{-r(T-t)} \int_{\mathbb{R}^d_+} h(\boldsymbol{y})p(\boldsymbol{y}, T; \boldsymbol{x}, t)dy, \tag{7}$$

where $p(\cdot, T; x, t)$ is the transition density formula given in Lemma 2.1. In this paper, we consider payoff functions restricted to the class of continuous piece-wise affine functions[2]. This type of function represents most of the payoff functions seen in financial mathematics literature [44]; see also the examples below.

[2] In particular, any CPWA function is linearly growing, see, e.g., Lemma 4.2. Hence the PDE (1) has a unique solution.

Definition 2.3 (CPWA payoff) *Let $d \in \mathbb{N}$. A function $h : \mathbb{R}^d_+ \to \mathbb{R}$ is a continuous piece-wise affine (CPWA) function if it can be represented as*

$$h(\boldsymbol{x}) = \sum_{k=1}^{K} \xi_k \max\{\boldsymbol{a}_{k,l} \cdot \boldsymbol{x} + b_{k,l} : l = 1, \dots, I_k\}, \tag{8}$$

where $K, I_k \in \mathbb{N}$ and $\xi_k \in \{-1, 1\}$ for $k = 1, \dots, K$, and where $\boldsymbol{a}_{k,l} \in \mathbb{R}^d$, $b_{k,l} \in \mathbb{R}$ for $k = 1, \dots, K$, $l = 1, \dots, I_k$.

Throughout the paper we impose the following assumptions on the CPWA payoff function $h : \mathbb{R}^d_+ \to \mathbb{R}$ in dependence of the dimension d.

Assumption 2.4 (CPWA) *There is a constant $C_2 \in [1, \infty)$ not depending on the dimension $d \in \mathbb{N}$ such that the CPWA function $h : \mathbb{R}^d_+ \to \mathbb{R}$ defined as in (8) satisfies both*

$$\max\{\|\boldsymbol{a}_{k,l}\|_\infty, |b_{k,l}| : k = 1, \dots, K, l = 1, \dots, I_k\} \leq C_2 \tag{9}$$

and

$$K \cdot \max\{I_1, \dots, I_K\} \leq C_2 d. \tag{10}$$

Example 2.5 *The list below contains examples showcasing that many popular payoff functions $h : \mathbb{R}^d_+ \to \mathbb{R}$ used in finance are CPWA, see also [44, Appendix EC.2]. In the following, we denote $\mathbf{e}_i$ the i-th unit vector in $\mathbb{R}^d$.*

1. *Call option on the i-th asset with strike κ: setting $K = 1$, $\xi_1 = 1$, $I_1 = 2$, $\boldsymbol{a}_{1,1} = \boldsymbol{e}_i$, $\boldsymbol{a}_{1,2} = \mathbf{0}$, $b_{1,1} = -\kappa$, $b_{1,2} = 0$, we have*
$$h(\boldsymbol{x}) = \max\{x_i - \kappa, 0\}. \tag{11}$$

2. *Basket call option with weights $\boldsymbol{w}$ and strike κ: setting $K = 1$, $\xi_1 = 1$, $I_1 = 2$, $\boldsymbol{a}_{1,1} = \boldsymbol{w}$, $\boldsymbol{a}_{1,2} = \mathbf{0}$, $b_{1,1} = -\kappa$, $b_{1,2} = 0$, we have*
$$h(\boldsymbol{x}) = \max\{\boldsymbol{w} \cdot \boldsymbol{x} - \kappa, 0\}. \tag{12}$$

3. *Spread call option: using setting 2., but by replacing $\boldsymbol{a}_{1,1}$ with $\boldsymbol{a}_{1,1} = \sum_{i \in \mathcal{I}} \boldsymbol{e}_i - \sum_{j \in \mathcal{I}'} \boldsymbol{e}_j$ for $\mathcal{I}, \mathcal{I}' \subset \{1, \dots, d\}$ and $\mathcal{I} \cap \mathcal{I}' = \emptyset$, we have*
$$h(\boldsymbol{x}) = \max\{\sum_{i \in \mathcal{I}} x - \sum_{j \in \mathcal{I}'} x_j - \kappa, 0\}. \tag{13}$$

4. *Call-on-max option with strike κ: setting $K = 1$, $\xi_1 = 1$, $I_1 = d + 1$, $\boldsymbol{a}_{1,j} = \boldsymbol{e}_j$, $b_{1,j} = -\kappa$ for all $j = 1, \dots, d$, $\boldsymbol{a}_{1,d+1} = \mathbf{0}$, $b_{1,d+1} = 0$, we have*
$$h(\boldsymbol{x}) = \max\{x_1 - \kappa, \dots, x_d - \kappa, 0\}. \tag{14}$$

5. *Call-on-min option with strike κ: setting $K = 2$, $\xi_1 = 1$, $\xi_2 = -1$, $I_1 = d$, $I_2 = d + 1$, $\boldsymbol{a}_{1,j} = \boldsymbol{a}_{2,j} = -\boldsymbol{e}_j$, $b_{1,j} = b_{2,j} = \kappa$ for all $j = 1, \dots, d$, $\boldsymbol{a}_{1,d+1} = \mathbf{0}$, $b_{1,d+1} = 0$, we have*
$$h(\boldsymbol{x}) = \max\{\kappa - x_1, \dots, \kappa - x_d, 0\} - \max\{\kappa - x_1, \dots, \kappa - x_d\}. \tag{15}$$

6. *Best-of-call option with strikes $\kappa_1, \dots, \kappa_d$: setting $K = 1$, $\xi_1 = 1$, $I_1 = d+1$, $\boldsymbol{a}_{1,j} = \boldsymbol{e}_j$, $b_{1,j} = -\kappa_j$ for all $j = 1, \dots, d$, $\boldsymbol{a}_{1,d+1} = \mathbf{0}$, $b_{1,d+1} = 0$, we have*
$$h(\boldsymbol{x}) = \max\{x_1 - \kappa_1, \dots, x_d - \kappa_d, 0\}. \tag{16}$$

We note that all of the above examples satisfy Assumption 2.4 provided that the coefficients $(\boldsymbol{a}_{k,l}, b_{k,l})$ are bounded by some constant $C_2 \in [1, \infty)$ uniformly in the dimension d, c.f. (9).

2.2 Brief Introduction to Quantum Computing

In this section, we briefly introduce the notions used in quantum computing. A classic reference for this subject is the textbook by Nielsen and Chuang [45].

2.2.1 Dirac Bra-Ket notation and tensor products

In this section, we introduce the Dirac *bra-ket* notation from quantum mechanics. Let $\mathcal{H}$ be a finite dimensional complex Hilbert space. A vector $v \in \mathcal{H}$, also referred as a *state*, is denoted by the *ket* notation $|v\rangle$. The inner product of two vectors $v, w \in \mathcal{H}$ is denoted by the *bra-ket* notation $\langle v|w\rangle := \langle v, w\rangle \in \mathbb{C}$. Elements $u \in \mathcal{H}^*$ of the dual space $\mathcal{H}^*$ are denoted by the *bra* notation $\langle u|$. The action of the dual vector $u \in \mathcal{H}^*$ on a vector $v \in \mathcal{H}$ is also denoted by the *bra-ket* notation $\langle u|v\rangle$. The action of a linear operator $A : \mathcal{H} \to \mathcal{H}$ on a vector $|v\rangle$ is denoted by $A|v\rangle$. The operator A acts on dual vectors $\langle u| \in \mathcal{H}^*$ by the rule $(\langle u| A)|v\rangle := \langle u|(A|v\rangle) := \langle u, Av\rangle$ for all $v \in \mathcal{H}$ which is also denoted by $\langle u|A|v\rangle$. A special case is the *expectation value* of an operator A on a normalized state, i.e. a state $|\psi\rangle$ satisfying $\langle\psi|\psi\rangle = 1$, which is denoted by $\langle A\rangle := \langle\psi|A|\psi\rangle$. The linear operator given by the *outer product* of two vectors $v, u \in \mathcal{H}$ is denoted by $|v\rangle\langle u| : \mathcal{H} \to \mathcal{H}$, whose action on a vector $|x\rangle \in \mathcal{H}$ is defined by $(|v\rangle\langle u|)|x\rangle := \langle u|x\rangle |v\rangle$.

For the Hilbert space $\mathcal{H} = \mathbb{C}^2$, we consider the n-fold tensor product Hilbert space $\mathcal{H}^{\otimes n} := \mathcal{H}\otimes\cdots\otimes\mathcal{H} \simeq \mathbb{C}^{2^n}$. We denote a state $\psi \in \mathcal{H}^{\otimes n}$ by $|\psi\rangle_n$, where the subscript n emphasizes the *($\log_2$)-dimension* of the tensor product Hilbert space $\mathcal{H}^{\otimes n}$. We use the orthonormal basis $\mathcal{B}_n = \{|i\rangle_n : i = (i_1, i_2, \ldots, i_n) \in \{0,1\}^n\} \subset \mathbb{C}^{2^n}$, where $|i\rangle_n := |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle := |i_1\rangle |i_2\rangle \cdots |i_n\rangle$, $i \in \{0,1\}^n$. The basis $\mathcal{B}_n$ is referred as the *computational basis* in the literature.

We illustrate some examples of tensor product of vectors and operators for $n = 2$ using the standard matrix-vector notation. The standard orthonormal basis $\{|0\rangle, |1\rangle\} \subset \mathcal{H} = \mathbb{C}^2$ is given by

$$|0\rangle := \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle := \begin{bmatrix}0\\1\end{bmatrix}. \tag{17}$$

The standard orthonormal basis for $\mathcal{H} \otimes \mathcal{H}$ is given by the tensor product basis,

$$\mathcal{B}_2 = \left\{ |i\rangle_2 = |i_1\rangle \otimes |i_2\rangle : i_1, i_2 \in \{0,1\} \right\} = \left\{ \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \right\}. \tag{18}$$

Let $|v\rangle = (v_1, v_2)^\top, |u\rangle = (u_1, u_2)^\top \in \mathcal{H}$. The tensor product of these two vectors is given by

$$|v\rangle \otimes |u\rangle = \begin{bmatrix}v_1\\v_2\end{bmatrix} \otimes \begin{bmatrix}u_1\\u_2\end{bmatrix} = \begin{bmatrix}v_1 u\\v_2 u\end{bmatrix} = \begin{bmatrix}v_1u_1\\v_1u_2\\v_2u_1\\v_2u_2\end{bmatrix}. \tag{19}$$

The Kronecker product of two square matrices $A, B \in \mathbb{C}^{2\times 2}$ is given by

$$A \otimes B = \begin{bmatrix}a_1 & a_2\\a_3 & a_4\end{bmatrix} \otimes \begin{bmatrix}b_1 & b_2\\b_3 & b_4\end{bmatrix} = \begin{bmatrix}a_1B & a_2B\\a_3B & a_4B\end{bmatrix} = \begin{bmatrix}a_1b_1 & a_1b_2 & a_2b_1 & a_2b_2\\a_1b_3 & a_1b_4 & a_2b_3 & a_2b_4\\a_3b_1 & a_3b_2 & a_4b_1 & a_4b_2\\a_3b_3 & a_3b_4 & a_4b_3 & a_4b_4\end{bmatrix}. \tag{20}$$

Furthermore, one can deduce from (20) and (19) that the following (multi)-linearity relation holds

$$(A \otimes B)(|v\rangle \otimes |u\rangle) = A|v\rangle \otimes B|u\rangle. \tag{21}$$

Similar rules for tensor and Kronecker products in $\mathcal{H}^{\otimes n}$, $n \geq 3$ can be deduced inductively. Note that the tensor product of vectors and operators *may not be commutative.*

2.2.2 Qubits, quantum gates, and quantum circuits

A classical computing bit, $x \in \{0,1\}$, represents a basic unit of computing information. The *qubit* (quantum bit) is the generalization of the classical bit, and it represents a unit of quantum information. Quantum mechanics allow the qubit to be in a state of *superposition.* For example, a single qubit may represent a normalized vector $|\psi\rangle$ in superposition of the state $|0\rangle$ and $|1\rangle$ simultaneously, and we may express $|\psi\rangle$ as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{with } |\alpha|^2 + |\beta|^2 = 1, \text{ and } \alpha, \beta \in \mathbb{C}. \tag{22}$$

For $n \geq 2$, an arbitrary n-qubit state $|\psi\rangle_n$ is represented by a normalized vector in $\mathbb{C}^{2^n}$ which can be described by a $\mathbb{C}$-linear combination in the computational basis $\mathcal{B}_n$, i.e.

$$|\psi\rangle_n = \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle_n, \quad \text{with} \sum_{i\in\{0,1\}^n} |\alpha_i|^2 = 1. \tag{23}$$

The coefficients $\alpha_i \in \mathbb{C}$ in (23) are referred as *probability amplitudes* (or simply *amplitudes*) due to the fact that for each $|i\rangle_n \in \mathcal{B}_n$ we have that the square amplitude $|\alpha_i|^2 = |\langle i|\psi\rangle|^2$ is the probability of observing that the state $|\psi\rangle_n$ collapses during a projective measurement to the state $|i\rangle_n$, according to *Born's rule*; see, e.g., [40, Chapter 2.5].

Both classical bits and qubits are manipulated using circuit *gates*. The classical bits on a computer are processed by a series of *logical/boolean gates*, e.g. NOT, OR, and AND gates. The input bits are connected by wires and gates to the output bits. A *circuit diagram* is often accompanied to show how these gates are placed. In contrast, the qubits on a quantum computer are manipulated by a sequence of elementary *quantum gates*; these quantum gates act on either one or two qubits at a time. The state evolution of the qubits, according to the axioms of quantum mechanics, is unitary. Thus, quantum gates are unitary operators, represented by *unitary matrices* in $\mathcal{U}(2^n) \subset \mathbb{C}^{2^n \times 2^n}$, where n is the number of qubits acted on by the quantum gate. A *quantum circuit* is a finite sequence of composition of quantum gates and wires (wires represent the identity operator). The fact that the product of unitary matrices is again a unitary matrix implies that the quantum circuit performs a unitary operation in the Hilbert space $\mathcal{H}^{\otimes n}$. Similar to classical computer boolean circuits, quantum circuits are presented by a circuit model diagram, which specifies where and how the quantum gates and wires are placed. For example, Figure 1 shows the quantum circuit for the Toffoli gate (see Example 2.18), which corresponds to the classical boolean gate NOT with two control bits.

Next, we provide some examples of quantum circuit gates commonly used in the literature which allows us to describe an *algebraic definition* for a quantum circuit; see Definition 2.14.

Example 2.6 (Pauli transformation gates) *The one-qubit gates corresponding to the Pauli transformations are*

$$I := \sigma_I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X := \sigma_x := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y := \sigma_y := \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad Z := \sigma_z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{24}$$

These gates satisfy the relations $I = -\mathrm{i}\sigma_x\sigma_y\sigma_z$, $I = \sigma_x^2 = \sigma_y^2 = \sigma_z^2$, *where* $\mathrm{i} := \sqrt{-1}$, *and they span the group of* 2×2*-unitary matrices.*

Example 2.7 (Hadamard gate) *The Hadamard gates is given by*

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{25}$$

It maps the computation basis states to a uniform superposition, i.e. $H|0\rangle := |+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ *and* $H|1\rangle := |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Example 2.8 (Phase shift gates) *For* $\phi \in [0, 2\pi]$, *we define the family of phase shift gates*

$$P(\phi) := \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\phi} \end{bmatrix}. \tag{26}$$

Special cases include the Pauli Z *gate,* S *gate, and* T *gate:*

$$Z := P(\pi) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad S := P(\pi/2) = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix}, \quad T := P(\pi/4) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\pi/4} \end{bmatrix}. \tag{27}$$

Example 2.9 (Rotation gates) *For* $\theta \in [0, 4\pi]$, *we introduce the three rotation gates:*

$$R_x(\theta) := \exp(-\mathrm{i}\theta X/2) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\mathrm{i}\sin\left(\frac{\theta}{2}\right) \\ -\mathrm{i}\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \tag{28}$$

$$R_y(\theta) := \exp(-\mathrm{i}\theta Y/2) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \tag{29}$$

$$R_z(\theta) := \exp(-\mathrm{i}\theta Z/2) = \begin{bmatrix} e^{-\mathrm{i}\theta/2} & 0 \\ 0 & e^{\mathrm{i}\theta/2} \end{bmatrix}. \tag{30}$$

Example 2.10 (Controlled-NOT gate) *The controlled-NOT gate has the following matrix representation*

$$CNOT := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{31}$$

The $CNOT$ *acts on two qubits: the first qubit is the control qubit and the second qubit is the target qubit, which is flipped if the control qubit is in state* $|1\rangle$.

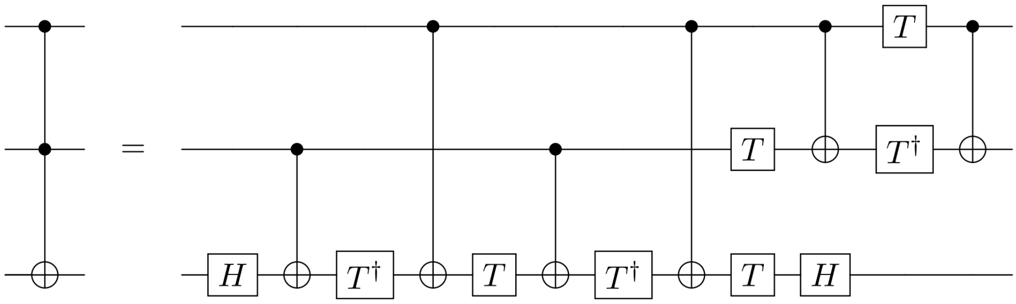

Figure 1: Implementation of the Toffoli gate as a quantum circuit using single-qubit gates and CNOT gates. [3]

Example 2.11 (Swap gate) *The swap gate has the following matrix representation*

$$SWAP := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{32}$$

Definition 2.12 (Elementary quantum gate set) *We call any element of the set of 1-qubit and 2-qubits quantum gates* $\mathbb{G} \subset \mathbb{C}^{2\times 2} \cup \mathbb{C}^{2^2 \times 2^2}$ *defined by*

$$\mathbb{G} := \big\{X, Y, Z, H, S, T, R_x(\theta), R_y(\theta), R_z(\theta), P(\phi) : \theta \in (0, 4\pi), \phi \in (0, 2\pi)\big\} \cup \big\{CNOT, SWAP\big\} \tag{33}$$

as elementary gates; (see Examples 2.6–2.11).

Remark 2.13 (Universality of $\mathbb{G}$) *We note that the set of quantum gates $\mathbb{G}$ in* (33) *is universal in the sense of the Solovay-Kitaev theorem [45, Appendix 3]. Moreover, the set $\mathbb{G}$ consists of quantum gates used in practical quantum computing softwares, such as IBM's Qiskit [59] and Google's Cirq [20].*

Definition 2.14 (Quantum circuit) *Let $n, M, L \in \mathbb{N}$. A quantum circuit $\mathcal{Q}$ acting on n qubits is a $2^n \times 2^n$ unitary matrix of the form*[4]

$$\mathcal{Q} = \prod_{l=1}^{L} (G_{l,1} \otimes G_{l,2} \otimes \cdots \otimes G_{l,n_l}) \in \mathcal{U}(2^n), \tag{34}$$

where $(G_{l,1}, G_{l,2}, \ldots, G_{l,n_l})_{l=1}^{L} \subset \mathbb{G} \cup \{I_2\}$, and $\prod_{m=1}^{n_l} \dim(G_{l,m}) = 2^n$ for all $l = 1, \ldots, L$. We define the following quantum circuit complexities[5]*:*

- *M = number of elementary quantum gates used to construct quantum circuit $\mathcal{Q}$, i.e.*

$$M := \sum_{l=1}^{L} \sum_{j=1}^{n_l} \mathbb{1}_{\mathbb{G}}(G_{l,j}), \tag{35}$$

- *n = number of qubits used in quantum circuit $\mathcal{Q}$, and*
- *L = depth of quantum circuit $\mathcal{Q}$.*

Remark 2.15 (Depth) *For any quantum circuit $\mathcal{Q}$, we may bound its depth complexity by the number of gates in the quantum circuit. In this paper, we focus only on the number of elementary gates and qubits used in constructing quantum circuits.*

Remark 2.16 (Inverse $\mathcal{Q}^\dagger$) *We note that the set of elementary quantum gates defined in* (33) *is closed under matrix inversion. Moreover, for any unitary matrix $\mathcal{Q}$, the matrix inverse $\mathcal{Q}^{-1}$ is also the conjugate transpose $\mathcal{Q}^\dagger$. Thus, for any quantum circuit $\mathcal{Q}$ satisfying Definition 2.14, we can construct the quantum circuit $\mathcal{Q}^\dagger$ representing its inverse by*

$$\mathcal{Q}^\dagger = \prod_{l=0}^{L-1} (G^\dagger_{L-l,1} \otimes G^\dagger_{L-l,2} \otimes \cdots \otimes G^\dagger_{L-l,n_{L-l}}). \tag{36}$$

[3] This figure can be found on `https://commons.wikimedia.org/wiki/File:Qcircuit_ToffolifromCNOT.svg`

[4] Note that for any $n \in \mathbb{N}$ and any $\mathcal{Q}_1 \ldots, \mathcal{Q}_L \in \mathcal{U}(2^n)$, their product is defined by $\prod_{l=1}^{L} \mathcal{Q}_l := \mathcal{Q}_L \mathcal{Q}_{L-1} \cdots \mathcal{Q}_2 \mathcal{Q}_1 \in \mathcal{U}(2^n)$.

[5] The indicator function $\mathbb{1}_S$ for a non-empty subset $S \subset H$ is the unique function satisfying $\mathbb{1}_S : H \to \{0, 1\}$ such that $\mathbb{1}_S(x) = 1$ if $x \in S$ and $\mathbb{1}_S(x) = 0$ if $x \notin S$.

Remark 2.17 (Ancilla qubits) *In most quantum circuits, auxiliary qubits are used as additional memory to perform necessary quantum computations but may not be used for the output. One calls these qubits ancilla qubits or simply ancillas and denotes them by* $|anc\rangle_\star$*, where the subscript* $\star$ *usually indicates in the literature that the amount of ancillas used are not specified precisely. The complexity of a quantum circuit is usually described by the number of elementary quantum gates used, and the number of qubits and ancilla qubits used. For simplicity, we count both qubits and ancilla qubits together as the number of qubits used in a circuit.*

Example 2.18 (Toffoli gate as a quantum circuit) *The classical AND gate, which takes a pair of bits* $x, y \in \{0,1\}$ *as input, returns the bit* $AND(x,y) := xy$ *as output. This classical gate is not a reversible operation. Hence the AND gate cannot be represented by a unitary matrix. However, we can implement the quantum version of this classical logic gate by using 3 qubits. The operation* $|a\rangle|b\rangle|c\rangle \mapsto |a\rangle|b\rangle|c+ab \mod 2\rangle$ *is reversible. This operation is implemented as a quantum gate called the Toffoli gate (also referred as the CCNOT gate). The Toffoli gate has the matrix representation*

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{37}$$

For $a, b, c \in \{0,1\}$*, we have*

$$CCNOT : |a\rangle|b\rangle|c\rangle \mapsto |a\rangle|b\rangle|c+ab \mod 2\rangle. \tag{38}$$

Here one refers $|a\rangle$ *as the control qubit,* $|b\rangle$ *the target qubit, and* $|c\rangle$ *the output qubit.*

The Toffoli gate is constructed as a quantum circuit on three qubits using the Hadamard gates, T gates, and CNOT gates; see also Figure 1 for the corresponding circuit diagram. The quantum circuit for the Toffoli gate uses 15 elementary gates in total.

2.2.3 Quantum measurements

We use the following definition to describe the quantum measurement of any arbitrary normalized state characterized by n-qubits. For further details, we refer to, e.g., [40, Chapter 2.5].

Definition 2.19 (Quantum measurement in the computational basis) *Let* $n \in \mathbb{N}$ *and let* $\mathcal{B}_n := \{|i\rangle_n := |i_1\rangle \otimes \cdots \otimes |i_n\rangle \mid i = (i_1, \ldots, i_n) \in \{0,1\}^n\}$ *be the computational basis of* $\mathbb{C}^{2^n}$*. For each* $|i\rangle_n \in \mathcal{B}_n$ *and for any normalized state* $|\psi\rangle_n$*, we define a projector* $M_i := |i\rangle_n \langle i|_n : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ *which is defined by* $(|i\rangle_n \langle i|_n)|\psi\rangle_n := \langle i|\psi\rangle_n |i\rangle_n$*. A measurement of a normalized state* $|\psi\rangle_n$ *in the computational basis induces a discrete probability space* $(\Omega, \mathcal{F}, \mathbb{P}_\psi)$*, where* $\Omega = \{0,1\}^n$ *is the sample space,* $\mathcal{F} = 2^\Omega$ *is the* σ*-algebra, and* $\mathbb{P}_\psi : \mathcal{F} \to [0,1]$ *is the discrete probability measure defined by*

$$\mathbb{P}_\psi(\{i\}) := \langle \psi | M_i^\dagger M_i | \psi \rangle_n = |\langle \psi | i \rangle_n|^2, \quad i \in \Omega. \tag{39}$$

2.3 Quantum amplitude estimation algorithms

In this section, we briefly review quantum algorithms for solving the quantum amplitude estimation (QAE) problem. Given an unitary operator $\mathcal{A}$ acting on $n+1$ qubits, defined by

$$\mathcal{A}|0\rangle_n|0\rangle = \sqrt{1-a}\,|\psi_0\rangle_n|0\rangle + \sqrt{a}\,|\psi_1\rangle_n|1\rangle, \tag{40}$$

where the so-called bad state is $|\psi_0\rangle_n|0\rangle$ and the good state is $|\psi_1\rangle_n|1\rangle$, Brassard et al. introduced in [12] the amplitude estimation problem where the goal is to estimate the unknown amplitude $a \in [0,1]$, which is the probability of measuring the good state $|\psi_1\rangle_n|1\rangle$ according to Born's rule. Let $a = \sin^2(\theta_a)$ for some $\theta_a \in [0, \frac{\pi}{2}]$ so that we can rewrite (40) as

$$\mathcal{A}|0\rangle_n|0\rangle = \cos(\theta_a)|\psi_0\rangle_n|0\rangle + \sin(\theta_a)|\psi_1\rangle_n|1\rangle. \tag{41}$$

To achieve a quantum speed-up, they introduced in [12] the amplitude amplification operator (also known as the Grover operator)

$$\mathcal{Q} := \mathcal{A}S_0\mathcal{A}^\dagger\mathcal{S}_{\psi_0}, \tag{42}$$

where $\mathcal{S}_0 := I_2^{\otimes n+1} - 2|0\rangle_{n+1}\langle 0|_{n+1}$, and $\mathcal{S}_{\psi_0} := I_2^{\otimes n} \otimes Z$. Note that for every $k \in \mathbb{N}$, it holds that

$$\mathcal{Q}^k\mathcal{A}|0\rangle_n|0\rangle = \cos((2k+1)\theta_a)|\psi_0\rangle_n|0\rangle + \sin((2k+1)\theta_a)|\psi_1\rangle_n|1\rangle, \tag{43}$$

(c.f. [12, Section 2]). We observe that measuring (43) boosts the probability of obtaining the good state to $\sin^2((2k+1)\theta_a)$ which is larger than $\sin^2(\theta_a)$ when measuring (41) directly, provided θ_a is sufficiently small so that $(2k+1)\theta_a \le \frac{\pi}{2}$. Using quantum Fourier transform and a number of multi-controlled operators for $\mathcal{Q}^k$, Brassard et al. designed the QAE algorithm [12, Algorithm(Est_Amp)] to estimate a with high probability using only $O(\varepsilon^{-1})$ queries of $\mathcal{A}$ (see [12, Theorem 12]). It is noted that Brassard et al.'s algorithm enables a quadratic speed-up for many approximation problems which are solved classically by Monte Carlo simulations under the assumption that the corresponding distribution can be uploaded in rotated form (41). However, due to difficulties in implementing large number of controlled unitary operators as well as the quantum Fourier transform (QFT) operator on quantum computers, several variants of the QAE algorithm without using QFT have been proposed recently; see [1, 29, 48, 49, 58, 61, 63]. In this paper, we use the modified iterative quantum amplitude estimation algorithm (Modified IQAE) [27, Algorithm 1] introduced recently by Fukuzawa et al. [27], which is a modification of the IQAE algorithm presented by Suzuki et al. [58]. In brief, the Modified IQAE algorithm consists of several rounds where for each round i, the algorithm maintains a confidence interval $[\theta_l^{(i)}, \theta_u^{(i)}]$ so that θ_a lies inside this interval with a certain probability. The confidence interval is narrowed in each subsequent round until the terminating condition $\theta_u - \theta_l < 2\varepsilon$ for prespecified $\varepsilon \in (0,1)$ is satisfied. The return output of the Modified IQAE algorithm is the confidence interval $[a_l, a_u]$ for a, where $a_l := \sin^2(\theta_l)$ and $a_u := \sin^2(\theta_u)$. The following result is a direct consequence of the main results in [27].

Proposition 2.20 *Let $\alpha, \varepsilon \in (0,1)$ and let $\mathcal{A}$ be an $(n+1)$-qubit quantum circuit satisfying*

$$\mathcal{A}\left|0\right\rangle_n\left|0\right\rangle = \sqrt{1-a}\left|\psi_0\right\rangle_n\left|0\right\rangle + \sqrt{a}\left|\psi_1\right\rangle_n\left|1\right\rangle \tag{44}$$

where $n \in \mathbb{N}$, $\left|\psi_0\right\rangle_n, \left|\psi_1\right\rangle_n$ are normalized states, $a \in [0,1]$, and where $\mathcal{A}$ can be constructed with $N_{\mathcal{A}} \in \mathbb{N}$ number of elementary gates. Then, the following holds.

1. *The Modified IQAE Algorithm [27, Algorithm 1] outputs a confidence interval $[a_l, a_u]$ that satisfies*

$$a \notin [a_l, a_u], \quad \text{with probability at most } \alpha, \tag{45}$$

where $0 \le a_u - a_l < 2\varepsilon$. In particular, the estimator $\widehat{a} := \frac{a_u - a_l}{2}$ of a satisfies

$$|a - \widehat{a}| < \varepsilon, \quad \text{with probability at least } 1-\alpha, \tag{46}$$

2. *the Modified IQAE Algorithm uses at most*

$$\frac{62}{\varepsilon}\ln\left(\frac{21}{\alpha}\right) \tag{47}$$

applications of $\mathcal{A}$, and

3. *the Modified IQAE Algorithm uses $n+1$ qubits and requires at most*

$$\frac{\pi}{4\varepsilon}(8n^2 + 23 + N_{\mathcal{A}}) \tag{48}$$

number of elementary gates.

Proof. Item 1. and Item 2. are proven in [27, Theorem 3.1] and [27, Lemma 3.7], respectively. For Item 3., we note that [27, Algorithm 1 Modified IQAE] uses quantum circuits $\mathcal{Q}^k\mathcal{A}$ which is defined by (43), where $k \in \mathbb{N}$. Let us construct the operator $\mathcal{Q}$ (c.f. (42)), as outlined in [51, Section 3]. We note that the operator $\mathcal{S}_{\psi_0}$ be constructed using one Z gate (c.f. Example 2.6). By direct computation (or see [51, Figure 5]), the operator $\mathcal{S}_0$ satisfy the identity

$$\mathcal{S}_0 = X^{\otimes(n+1)}(I_2^{\otimes n} \otimes H)C^n(X)(I_2^{\otimes n} \otimes H)X^{\otimes(n+1)}, \tag{49}$$

where $C^n(X)$ is the generalized version of Toffoli gate, which uses the first n-qubits for control. The multi-control gate $C^n(X)$ is constructed as a quantum circuit in [55, Theorem 2] using $2n^2 - 6n + 5$ controlled X-rotation gates $CR_x(\theta)$, where each $CR_x(\theta)$ gate can be constructed with 4 elementary gates by the following definition

$$CR_x(\theta) = (I_2 \otimes R_x(\tfrac{\theta}{2}))\mathrm{CNOT}(I_2 \otimes R_x(\tfrac{\theta}{2}))\mathrm{CNOT}, \tag{50}$$

see also the proof of Lemma 3.15. Thus, by (49), the operator $\mathcal{S}_0$ can be constructed using

$$(n+1) + 1 + 4(2n^2 - 6n + 5) + 1 + (n+1) \le 8n^2 + 22 \tag{51}$$

elementary gates. Finally, since the set of elementary gates is closed under inversion, the number of elementary gates used to construct $\mathcal{A}^\dagger$ is the same as the number of elementary gates used for $\mathcal{A}$. Hence, the number of elementary gates used to construct $\mathcal{Q}$ is at most

$$N_{\mathcal{A}} + 1 + N_{\mathcal{A}} + (8n^2 + 22) = 8n^2 + 23 + 2N_{\mathcal{A}}. \tag{52}$$

Next, by [27, Lemma 3.1], the integer k satisfies the bound $2k+1 \leq \frac{\pi}{4\varepsilon}$. Thus, the number of elementary gates used to construct the operator $\mathcal{Q}^k\mathcal{A}$ is at most

$$\begin{aligned} & k(8n^2+23+2N_{\mathcal{A}})+N_{\mathcal{A}} \\ & = k(8n^2+23)+(2k+1)N_{\mathcal{A}} \\ & \leq (2k+1)(8n^2+23+N_{\mathcal{A}}) \\ & \leq \frac{\pi}{4\varepsilon}(8n^2+23+N_{\mathcal{A}}). \end{aligned} \tag{53}$$

□

Remark 2.21 *Let us remark the following on the complexity of the Modified IQAE algorithm.*

1. *The total number of rounds $t \in \mathbb{N}$ in [27, Algorithm 1 Modified IQAE] is bounded by $\log_3(\frac{\pi}{4\varepsilon})$, see [27, Section 3.1]. For each round $i = 1,\ldots,t$, the quantum circuit $\mathcal{Q}^{k_i}\mathcal{A}$ is prepared on a quantum computer, where each $k_i \in \mathbb{N}$ are found recursively by using the subroutine [27, Algorithm 2, FindNextK]. Note that each of these quantum circuits require the same number of qubits as with the quantum circuit $\mathcal{A}$. Moreover, each k_i satisfy $2k_i+1 \leq \frac{\pi}{4\varepsilon}$, [27, Lemma 3.1].*
2. *Since the number k_t is the maximum among the k_i's, we infer that [27, Algorithm 1, Modified IQAE] requires the number of elementary gates used to construct the quantum circuit $\mathcal{Q}^{k_t}\mathcal{A}$ on a quantum computer in order to run the Modified IQAE algorithm, which can be bounded by* (48).
3. *The query complexity (i.e. number of applications) of $\mathcal{A}$ in Proposition 2.20 is defined to be the number of times the operator $\mathcal{Q}$ is applied in the algorithm, which is*

$$\sum_{i=1}^{t} k_i N_i, \tag{54}$$

where N_i is the number of measurements made on $\mathcal{Q}^{k_i}\mathcal{A}\,|0\rangle_n\,|0\rangle$ in round i. Hence, the query complexity of $\mathcal{A}$ can be interpreted as the computational running time for the Modified IQAE algorithm. It was shown in [27, Lemma 3.7] that this number is bounded by (47).

2.4 Outline of Algorithm 1 and main result

2.4.1 Outline of Algorithm 1

The steps of Algorithm 1 can be briefly described into four parts as follows:

1. upload the transition probability function $p(\cdot, T; x, t)$ given in (4),
2. upload the CPWA payoff function $h : \mathbb{R}_+^d \to \mathbb{R}$ given in (8),
3. apply the Modified IQAE algorithm [27, Algorithm 1] to obtain an estimated amplitude $\widehat{a} \in [0,1]$,
4. rescale the estimated amplitude $\widehat{a}$ to output $\widetilde{U}_{t,x}$ which approximates $u(t,x)$ defined in (7).

More precisely, in order to apply the Modified IQAE algorithm in step 3, we first need to upload both the probability distribution function and the payoff function as quantum circuits. For the first step, we need to truncate and discretize the distribution function on a grid. The corresponding parameters $n_1, m_1 \in \mathbb{N}$ encodes the grid $([-2^{n_1-1}, 2^{n_1-1} - 2^{-m_1}] \cap 2^{-m_1}\mathbb{Z})^d$, which is the support of the discretized distribution. Then, the truncated, discretized distribution can be uploaded approximately on the quantum computer using the quantum circuit $\mathcal{P}$, introduced in Section 3.3. The corresponding parameter γ is needed to renormalize the amplitude coefficients in $\mathcal{P}\,|0\rangle_{d(n_1+m_1)}$ to $[0,1]$. We note that step 1 accounts for the truncation error, quadrature error, and distribution loading error in Section 4, see Proposition 4.4, Proposition 4.5, and Proposition 4.10, respectively.

In step 2, we discretize the coefficients $(\boldsymbol{a}_{k,l}, b_{k,l})$ of the CPWA payoff function (8) onto a grid. The corresponding parameter $n_2 \in \mathbb{N}$ encodes the bounds on the coefficients while the parameter $m_2 \in \mathbb{N}$ encodes the rounding off accuracy level for the coefficients. We construct the quantum circuit $\mathcal{R}_h$ that encodes the approximated CPWA payoff in a phase amplitude using controlled Y-rotation gates. The corresponding parameter $\mathfrak{s} \equiv s$ indicates the scaling parameter for the rotation circuit $\mathcal{R}_h$, see Proposition 3.22. We account for the errors for approximating the payoff function $h : \mathbb{R}_+^d \to \mathbb{R}$ and the rotation errors in Proposition 4.8 and Proposition 4.11. The quantum circuit $\mathcal{A}$ is then defined as the combination (i.e. composition) of the two quantum circuits $\mathcal{P}$ and $\mathcal{R}_h$ which enables us to apply quantum amplitude estimation (QAE) algorithms.

In step 3, we apply the Modified IQAE algorithm [27] with $\mathcal{A}$ to get an output $\widehat{a} \in [0,1]$.[6] Then in the last step, since the estimated amplitude $\widehat{a}$ given by the Modified IQAE algorithm is between 0 and 1, we need to rescale this number to approximate the option price $u(t,x)$. We account for the QAE error in Proposition 4.12.

[6] We emphasize that the choice of QAE algorithms should not affect the estimated amplitude considerably.

2.4.2 Main Theorem

Theorem 2.22 *Let $\varepsilon \in (0,1)$, $\alpha \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, $(t,x) \in [0,T) \times \mathbb{R}_+^d$, and covariance matrix $\boldsymbol{C}_d \in \mathbb{R}^{d\times d}$ be the input of Algorithm 1. Let $u(t,x) \in \mathbb{R}$ be the option price given by* (7) *with CPWA payoff $h : \mathbb{R}_+^d \to \mathbb{R}$ given by* (8)*, let Assumption 2.2, Assumption 2.4, and Assumption 3.16 hold with respective constants $C_1, C_2, C_3 \in [1,\infty)$, and let $\mathfrak{c}, \mathfrak{C} \in [2,\infty)$ be defined by*

$$\mathfrak{c} := 2C_2^2 e^{4C_1^2T^2} e^{2rT} \max_{i=1,\dots,d}\{1, x_i^2\} \tag{55}$$

and

$$\mathfrak{C} := 2^{25}3^3 C_2^4 C_3 \mathfrak{c}^{\frac{3}{2}} (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}}. \tag{56}$$

Then, Algorithm 1 outputs $\widetilde{U}_{t,x} \in \mathbb{R}$ which satisfies

$$|u(t,x) - \widetilde{U}_{t,x}| \leq \varepsilon, \quad \text{with probability at least } 1-\alpha, \tag{57}$$

where the number of qubits used in Algorithm 1 is at most

$$\mathfrak{C}d^2(1 + \log_2(d\varepsilon^{-1})), \tag{58}$$

the number of elementary gates used in Algorithm 1 is at most

$$\mathfrak{C}d^{\max\{12,5+C_3\}}\varepsilon^{-3}(1 + \log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}}, \tag{59}$$

and the number of applications[7] *of quantum circuit $\mathcal{A}$ in Algorithm 1 is at most*

$$\mathfrak{C}d^5\varepsilon^{-3}\ln\left(\tfrac{21}{\alpha}\right). \tag{60}$$

Remark 2.23 *Let us remark the following on the complexity of Algorithm 1.*

1. *The bounds* (58) *and* (59) *on the number of qubits and the number of elementary gates in Algorithm 1 specify the requirements on the quantum computer needed to run Algorithm 1. The bound* (60) *on the number of applications of quantum circuit $\mathcal{A}$ can be interpreted as the computational running time for Algorithm 1.*

2. *The $O(\varepsilon^{-3})$ running time complexity in* (60) *can be attributed as follows.*

   (i) The truncation of the integral (7) *from $\mathbb{R}_+^d$ to the cube $[0,M]^d$ requires $M \sim 2^{n_1} \sim O(\varepsilon^{-1})$, see Proposition 4.4.*

   (ii) Since the payoff function h grows linearly, $\|h\|_{L^\infty((0,M)^d)}$ grows of order $O(\varepsilon^{-1})$. Hence we require the scaling parameter $\mathfrak{s}$ to satisfy $\mathfrak{s} \sim O((\frac{\varepsilon}{\|h\|^3_{L^\infty((0,M)^d)}})^{1/2}) \sim O(\varepsilon^2)$, see Proposition 4.11.

   (iii) We use the Modified IQAE to output $\widehat{a}$ with accuracy $\varepsilon\mathfrak{s} \sim O(\varepsilon^3)$ to obtain the estimate (57)*, see Proposition 4.12. This implies the query complexity bound* (60).

   In the case where the payoff function $h : \mathbb{R}_+^d \to \mathbb{R}$ is bounded uniformly in $x \in \mathbb{R}_+^d$, then the scaling parameter $\mathfrak{s}$ requires only $O(\varepsilon^{\frac{1}{2}})$, see (ii) above. This implies that the number of applications of $\mathcal{A}$ can be reduced to $O(\varepsilon^{-\frac{3}{2}})$, which is a speed-up compared to classical Monte Carlo methods and recovers the complexity observed in [57]. We highlight that the fact that an unbounded payoff function can lead to a higher complexity has been already outlined in [15, Equation (36)]. Moreover, we highlight that one cannot expect to obtain $O(\varepsilon^{-1})$, which would have meant to have a quadratic speed-up over classical Monte Carlo methods, since one cannot expect to have an oracle which can perfectly upload the distribution and payoff function in rotated form (see, e.g., (44) *or [15, Equation (16)]), as already pointed out, e.g., in [34].*

3. *We note from* (57)*-*(60) *that the number of qubits and elementary gates used in Algorithm 1 as well as the number of applications of the quantum circuit $\mathcal{A}$ grow only polynomially*[8] *in d and ε^{-1}. Hence, we have proven that Algorithm 1 does not suffer from the curse of dimensionality.*

4. *The explicit constant* (56) *is not likely to be sharp since we did not optimize every inequality when bounding the number of elementary gates used to construct the quantum circuits in Section 3.4.*

[7] c.f. Remark 2.21 Item 3. for the precise meaning of *number of applications*.

[8] under the additional assumption that $\max_{i=1,\dots,d}\{|x_i|\}$ is uniformly bounded in $d \in \mathbb{N}$. This assumption is naturally fulfilled in practice, as x_i^2 corresponds to the (squared) spot price of the i-th asset.

3 Quantum Circuits

In Section 3.1, we introduce the so-called *two's complement method* for representing signed dyadic rational numbers on a bounded interval using binary strings of finite length. These binary strings correspond to the grid points on the truncated interval. The binary strings are represented by the qubits on the quantum computer, in the form of linear combinations of the computational basis states $|i\rangle_n = |i_1\rangle |i_2\rangle \dots |i_n\rangle$, where $i = (i_1, \dots, i_n) \in \{0,1\}^n$. In Section 3.2, we describe how quantum circuits are constructed to perform arithmetic operations on two complement's numbers. In Section 3.3, we assume that the discretized multivariate log-normal distribution can be loaded on the quantum computer, justified by [15, 64]. In Section 3.4, the approximate option payoff function is loaded, by using quantum circuits that perform arithmetic operations on numbers represented by the two's complement method.

3.1 Representing signed dyadic rationals using the two's complement method

The two's complement method is a way of representing signed integers on a computer using binary strings, see e.g. Chapter 2.2 [13] for an introduction to the subject. We first describe the representation of signed integers using the two's complement method. For a given $n \in \mathbb{N}$ and for an integer $x \in [-2^{n-1}, 2^{n-1}-1] \cap \mathbb{Z}$, we encode x in the two's complement method by a n-bit string denoted by $(x_{n-1}, x_{n-2}, \cdots, x_0) \in \{0,1\}^n$. The value of the integer x is converted from the bit string $(x_{n-1}, \cdots, x_0)$ by the following formula

$$x = -x_{n-1}2^{n-1} + \sum_{k=0}^{n-2} x_k 2^k. \tag{61}$$

The most significant bit (MSB) is the bit $x_{n-1} \in \{0,1\}$ which determines the sign of x. There are classical computer algorithms for performing arithmetic operations (such as addition and multiplication) in the two's complement representation, such as the *carry adder algorithm* and *Booth's multiplication algorithm* [13]. Numbers with a fractional part can also be represented using the two's complement method. This can be done by introducing the *radix point* (commonly referred as the decimal point in decimal expansion) to separate the integer part and fractional part. The additional bits are mapped to the dyadics $2^{-m}, m \in \mathbb{N}$ to represent the fractional part of a number.

Definition 3.1 (Two's complement representation) *Let $n \in \mathbb{N}$, $m \in \mathbb{N}_0$. For $m \geq 1$, we define the following set of (n,m)-bit strings by*

$$\mathbb{F}_{n,m} := \{0,1\}^n \times \{0,1\}^m := \{((x_{n-1}, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m})) \in \{0,1\}^n \times \{0,1\}^m\}, \tag{62}$$

and the set of dyadic rational numbers on a closed interval by

$$\mathbb{K}_{n,m} := [-2^{n-1}, 2^{n-1} - 2^{-m}] \cap 2^{-m}\mathbb{Z} := \{-2^{n-1}, -2^{n-1} + 2^{-m}, -2^{n-1} + 2 \cdot 2^{-m}, \dots, 2^{n-1} - 2^{-m}\}. \tag{63}$$

Further, we denote

$$\mathbb{K}_{n,m,+} := \mathbb{K}_{n,m} \cap [0, \infty), \quad \textit{and} \quad \mathbb{K}_{n,m,-} := \mathbb{K}_{n,m} \cap (-\infty, 0), \tag{64}$$

and we denote

$$\begin{aligned} \mathbb{F}_{n,m,+} &:= \{((0, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m})) : x_{n-2}, \dots, x_{-m} \in \{0,1\}\}, \quad \textit{and} \\ \mathbb{F}_{n,m,-} &:= \{((1, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m})) : x_{n-2}, \dots, x_{-m} \in \{0,1\}\}. \end{aligned} \tag{65}$$

If $m = 0$, we then use the usual signed integers $\mathbb{K}_{n,0} := [-2^{n-1}, 2^{n-1}-1] \cap \mathbb{Z}$ and the set of n-bit strings $\mathbb{F}_{n,0} := \{(x_{n-1}, \cdots, x_0) \in \{0,1\}^n\}$, and define $\mathbb{K}_{n,0,\pm}$ and $\mathbb{F}_{n,0,\pm}$ analogously.

Definition 3.2 (Encoder and decoder maps) *Let $n \in \mathbb{N}$, $m \in \mathbb{N}_0$. We define the encoder function which maps the rational numbers to bit strings by*

$$\begin{aligned} \mathrm{E}_{n,m} : \mathbb{K}_{n,m} &\longrightarrow \mathbb{F}_{n,m} \\ y &\mapsto ((x_{n-1}, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m})) \end{aligned} \tag{66}$$

where we define $\mathrm{E}_{n,m}(y) = ((x_{n-1}, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m}))$ recursively by

$$\begin{aligned} x_{n-1} &= \begin{cases} 1, & \textit{if } y < 0, \\ 0, & \textit{if } y \geq 0, \end{cases} \\ x_{n-2} &= \begin{cases} 1, & \textit{if } -x_{n-1}2^{n-1} + 2^{n-2} \leq y, \\ 0, & \textit{if } -x_{n-1}2^{n-1} + 2^{n-2} > y, \end{cases} \end{aligned} \tag{67}$$

and for $k = n-3, n-4, \dots, -m$,

$$x_k = \begin{cases} 1, & \text{if } -x_{n-1}2^{n-1} + \sum_{j=k+1}^{n-2} x_j 2^j + 2^k \le y, \\ 0, & \text{if } -x_{n-1}2^{n-1} + \sum_{j=k+1}^{n-2} x_j 2^j + 2^k > y. \end{cases} \tag{68}$$

We define the decoder function which maps the bit strings to the rational numbers by

$$\begin{aligned} \mathrm{D}_{n,m} : \mathbb{F}_{n,m} &\longrightarrow \mathbb{K}_{n,m} \\ ((x_{n-1}, x_{n-2}, \dots, x_0), (x_{-1}, \dots, x_{-m})) &\mapsto -x_{n-1}2^{n-1} + \sum_{k=-m}^{n-2} x_k 2^k. \end{aligned} \tag{69}$$

The sets $\mathbb{F}_{n,m}$ and $\mathbb{K}_{n,m}$ are equivalent in the following sense.

Proposition 3.3 (Bijection between (n, m)-bit strings and dyadics) *Let $n \in \mathbb{N}$, $m \in \mathbb{N}_0$. The sets $\mathbb{F}_{n,m}$ and $\mathbb{K}_{n,m}$ (c.f. Definition 3.1) have the same finite cardinality, and the encoder and decoder functions $\mathrm{E}_{n,m} : \mathbb{K}_{n,m} \longrightarrow \mathbb{F}_{n,m}$ and $\mathrm{D}_{n,m} : \mathbb{F}_{n,m} \longrightarrow \mathbb{K}_{n,m}$ (c.f. Definition 3.2) are bijective and inverses of the other.*

Proof. For the first part of the statement, by observing that

$$\mathbb{K}_{n,m} = \{j \cdot 2^{-m} : j = 0, 1, \dots, 2^{n+m-1} - 1\} \cup \{-j \cdot 2^{-m} : j = 1, \dots, 2^{n+m-1}\}, \tag{70}$$

it follows that

$$\#\mathbb{K}_{n,m} = 2 \cdot 2^{n+m-1} = 2^n \cdot 2^m = \#(\{0,1\}^n \times \{0,1\}^m) = \#\mathbb{F}_{n,m},$$

where we denote by $\#A$ the cardinality of a set A. This shows that the two sets $\mathbb{F}_{n,m}$ and $\mathbb{K}_{n,m}$ have the same cardinality. Injectivity is clear from Definition 3.2, and bijectivity follows from injectivity since both sets have same finite cardinality. $\square$

Later, for any $k \in \mathbb{N}$, we will use the notation $\mathbb{F}^k_{n,m} := \underbrace{\mathbb{F}_{n,m} \times \cdots \times \mathbb{F}_{n,m}}_{k\text{-times}}$. The arithmetic algorithms in two's complement (TC) representation for signed rational numbers can be extended from the arithmetic algorithms on the two's complemment signed integers. The modifying process is done by shifting the fractional bits to the integer bits, applying the integer arithmetic algorithms, then shifting the integer bits back to fractional bits. The proofs in the two following lemmas provide the extension procedure.

Lemma 3.4 (Addition in two's complement) *Let $n_1, n_2 \in \mathbb{N}$, and let $n := \max\{n_1, n_2\}$. Let $\boxplus : \mathbb{F}_{n_1,0} \times \mathbb{F}_{n_2,0} \to \mathbb{F}_{n+1,0}$ be the addition algorithm for integers represented in the two's complement method. Then, for any $m_1, m_2 \in \mathbb{N}_0$ with $m := \max\{m_1, m_2\}$, there is a natural extension of the addition algorithm to the rational numbers represented in the two's complement method where $\boxplus : \mathbb{F}_{n_1,m_1} \times \mathbb{F}_{n_2,m_2} \to \mathbb{F}_{n+1,m}$, such that for any $x \in \mathbb{F}_{n_1,m_1}$, $y \in \mathbb{F}_{n_2,m_2}$, there is an unique element $x \boxplus y \in \mathbb{F}_{n+1,m}$ that satisfies*

$$x \boxplus y = \mathrm{E}_{n+1,m}(\mathrm{D}_{n_1,m_1}(x) + \mathrm{D}_{n_2,m_2}(y)). \tag{71}$$

Proof. First, consider the case where both m_1 and m_2 are positive. Let $x = ((x_{n_1-1}, \dots, x_0), (x_{-1}, \dots, x_{-m_1})) \in \mathbb{F}_{n_1,m_1}$ and $y = ((y_{n_2-1}, \dots, y_0), (y_{-1}, \dots, y_{-m_2})) \in \mathbb{F}_{n_2,m_2}$ be given. For every $p, q, r \in \mathbb{N}$ with $r \ge q$, define a left-shift operator $\tau_r : \mathbb{F}_{p,q} \to \mathbb{F}_{p+r,0}$ defined by

$$\tau_r : ((z_{p-1}, \dots, z_0), (z_{-1}, \dots, z_{-q})) \mapsto (z_{p-1}, \dots, z_0, z_{-1}, \dots, z_{-q}, \underbrace{0, \dots, 0}_{(r-q)\text{-times}}). \tag{72}$$

Then, it holds that

$$\tau_m(x) = (x_{n_1-1}, \dots, x_0, x_{-1}, \dots, x_{-m_1}, \dots, x_{-m}) \in \mathbb{F}_{n_1+m,0}, \tag{73}$$

$$\tau_m(y) = (y_{n_2-1}, \dots, y_0, y_{-1}, \dots, y_{-m_2}, \dots, y_{-m}) \in \mathbb{F}_{n_2+m,0}, \tag{74}$$

where $x_{-k} = 0$ for $k = m_1 + 1, \dots, m$ if $m_1 < m$ and $y_{-l} = 0$ for $l = m_2 + 1, \dots, m$ if $m_2 < m$. Hence, we may apply the integer addition algorithm and get an output $\tau_m(x) \boxplus \tau_m(y) \in \mathbb{F}_{n+1+m,0}$. Then, for every $p, r \in \mathbb{N}$ with $r \le p$, we define a right-shift operator $\tau_{-r} : \mathbb{F}_{p,0} \to \mathbb{F}_{p-r,r}$ defined by

$$\tau_{-r} : (z_{p-1}, \dots, z_0) \mapsto ((z_{p-1}, \dots, z_r), (z_{r-1}, \dots, z_0)). \tag{75}$$

Let $\tau_m(x) \boxplus \tau_m(y) = z = (z_{n+m}, z_{n+m-1}, \dots, z_0)$, for some bit string $z \in \mathbb{F}_{n+m+1,0}$. Then, we have

$$\tau_{-m}(\tau_m(x) \boxplus \tau_m(y)) = ((z_{n+m}, z_{n+m-1}, \dots, z_m), (z_{m-1}, \dots, z_0)) \in \mathbb{F}_{n+1,m}. \tag{76}$$

Furthermore, it holds that $\mathrm{D}_{n_1+m,0}(\tau_m(x)) = 2^m \mathrm{D}_{n_1,m_1}(x)$ and $\mathrm{D}_{n_2+m,0}(\tau_m(x)) = 2^m \mathrm{D}_{n_2,m_2}(y)$. This implies that

$$x \boxplus y := \tau_{-m}(\tau_m(x) \boxplus \tau_m(y)) = \tau_{-m}\mathrm{E}_{n+m+1,0}(2^m(\mathrm{D}_{n_1,m_1}(x) + \mathrm{D}_{n_2,m_2}(y))) = \mathrm{E}_{n+1,m}(\mathrm{D}_{n_1,m_1}(x) + \mathrm{D}_{n_2,m_2}(y)). \tag{77}$$

Hence we have shown (71). The cases where m_1 and/or m_2 equals to zero follow analogously.

□

Lemma 3.5 (Multiplication in two's complement) *Let $n_1, n_2 \in \mathbb{N}$, and let $n := n_1 + n_2$. Let $\boxdot : \mathbb{F}_{n_1,0} \times \mathbb{F}_{n_2,0} \to \mathbb{F}_{n,0}$ be the multiplication algorithm for integers represented in the two's complement method. Then, for any $m_1, m_2 \in \mathbb{N}_0$ with $m := m_1 + m_2$, there is a natural extension of the multiplication algorithm to the rational numbers represented in the two's complement method where $\boxdot : \mathbb{F}_{n_1,m_1} \times \mathbb{F}_{n_2,m_2} \to \mathbb{F}_{n,m}$ such that for any $x \in \mathbb{F}_{n_1,m_1}$, $y \in \mathbb{F}_{n_2,m_2}$, there is an unique element $x \boxdot y \in \mathbb{F}_{n,m}$, where*

$$x \boxdot y = \mathrm{E}_{n,m}(\mathrm{D}_{n_1,m_1}(x) \cdot \mathrm{D}_{n_2,m_2}(y)). \tag{78}$$

Proof. First, consider the case where both m_1 and m_2 are positive. Let $x = ((x_{n_1}, \dots, x_0), (x_{-1}, \dots, x_{-m_1})) \in \mathbb{F}_{n_1,m_1}$ and $y = ((y_{n_2}, \dots, y_0), (y_{-1}, \dots, y_{-m_2})) \in \mathbb{F}_{n_2,m_2}$ be given. Then, with the left-shift operator τ_m defined in (72) in the proof of the previous lemma, it holds that $\tau_m(x) \in \mathbb{F}_{n_1+m,0}$ and $\tau_m(y) \in \mathbb{F}_{n_2+m,0}$. Hence, applying the multiplication algorithm on integers we have $\tau_m(x) \boxdot \tau_m(y) \in \mathbb{F}_{n+m,0}$. This implies that $\tau_{-m}(\tau_m(x) \boxdot \tau_m(y)) \in \mathbb{F}_{n,m}$. We verify that

$$x \boxdot y := \tau_{-m}(\tau_m(x) \boxdot \tau_m(y)) = \tau_{-m}\left(\mathrm{E}_{n+m,0}(2^m \mathrm{D}_{n_1,m_1}(x) \cdot \mathrm{D}_{n_2,m_2}(y))\right) = \mathrm{E}_{n,m}(\mathrm{D}_{n_1,m_1}(x) \cdot \mathrm{D}_{n_2,m_2}(y)). \tag{79}$$

Hence we have shown (78). The cases where m_1 and/or m_2 equals to zero follow analogously. □

3.2 Quantum circuits for elementary arithmetic operations

We now describe quantum circuits for arithmetic and elementary operations (such as addition, multiplication, comparison, absolute value), on qubit registers representing numbers in two's complement method. Many quantum circuits for performing arithmetic operations with its quantum circuit complexities are available in the literature, see, e.g., [4, 19, 22, 54, 56, 60]. We first introduce in Lemma 3.8 a quantum circuit to perform permutations, which will be necessary for arithmetic computations in the later part.

Definition 3.6 (Cycle) *([23, Section 1.3, pg 29]) Let $n, m \in \mathbb{N}$ satisfy $2 \le m \le n$, and let $\{a_1, \dots, a_m\} \subset \{1, 2, \dots, n\}$ be distinct numbers. A cycle $C := (a_1 a_2 \cdots a_m)$ is a permutation $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ such that*

$$\sigma(j) = \begin{cases} a_{i+1}, & \text{if } j = a_i \text{ for } 1 \le i \le m-1, \\ a_1, & \text{if } j = a_m, \\ j, & \text{if } j \notin \{a_1, \dots, a_m\}. \end{cases} \tag{80}$$

Proposition 3.7 (Cycle decomposition theorem) *([23, Section 4.1, pg 115]) Let $n \in \mathbb{N}$ and $\pi : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ be a permutation. Then π can be written as a composition of disjoint cycles*[9]

$$\pi = C_1 C_2 \cdots C_k = (a_1 a_2 \cdots a_{m_1})(a_{m_1+1} a_{m_1+2} \cdots a_{m_2}) \cdots (a_{m_{k-1}+1} a_{m_{k-1}+2} \cdots a_{m_k}), \tag{81}$$

where k is the number of cycles, and $\{a_j : j = 1, \dots, m_k\} \subset \{1, \dots, n\}$ are distinct integers. Moreover, the cycle decomposition above is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers within each cycle.

Lemma 3.8 (Quantum circuit for permutation) *1. Let $n \in \mathbb{N}$, and let $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ be a permutation. Then, there is a quantum circuit $\mathcal{T}_\pi \in U(2^n)$ on n qubits such that for every $|i\rangle_n = |i_1\rangle \cdots |i_n\rangle \in \{0,1\}^n$, it holds that*

$$\mathcal{T}_\pi |i\rangle_n = \mathcal{T}_\pi |i_1\rangle \cdots |i_n\rangle = |i_{\pi(1)}\rangle \cdots |i_{\pi(n)}\rangle, \tag{82}$$

and that $\mathcal{T}_\pi$ uses at most $2n^2$ swap gates (c.f. Example 2.11).

[9] We adopt the convention that cycles of length 1 will not be written.

2. Let $\mathcal{Q} \in U(2^n)$ be a given quantum circuit such that for every $|i\rangle_n \in \{0,1\}^n$,

$$\mathcal{Q}\,|i\rangle_n = \sum_{j=(j_1,\ldots,j_n)\in\{0,1\}^n} \alpha_{i,j}\,|j_1\rangle\cdots|j_n\rangle\,, \tag{83}$$

where $\alpha_{i,j} \in \mathbb{C}$. Then, $\mathcal{T}_\pi \mathcal{Q}$ is also a quantum circuit such that for every $|i\rangle_n \in \{0,1\}^n$,

$$\mathcal{T}_\pi \mathcal{Q}\,|i\rangle_n = \sum_{j\in\{0,1\}^n} \alpha_{i,j}\,\left|j_{\pi(1)}\right\rangle\cdots\left|j_{\pi(n)}\right\rangle. \tag{84}$$

Proof. Firstly, we show that for any $j,k \in \{1,2,\ldots,n\}$, $j<k$, and for any n-qubit $|i\rangle_n = |i_1\rangle\cdots|i_n\rangle \in \{0,1\}^n$, that there exists a quantum circuit $\mathcal{T}_{j\leftrightarrow k}$ consisting of $2(k-j)-1$ swap gates (c.f. Example 2.11) where it holds that

$$\begin{aligned}\mathcal{T}_{j\leftrightarrow k} : |i\rangle_n &= |i_1\rangle\cdots|i_{j-1}\rangle\,|i_j\rangle\,|i_{j+1}\rangle\cdots|i_{k-1}\rangle\,|i_k\rangle\,|i_{k+1}\rangle\cdots|i_n\rangle \\ &\mapsto |i_1\rangle\cdots|i_{j-1}\rangle\,|i_k\rangle\,|i_{j+1}\rangle\cdots|i_{k-1}\rangle\,|i_j\rangle\,|i_{k+1}\rangle\cdots|i_n\rangle\,.\end{aligned} \tag{85}$$

Denote by $\mathcal{S} := SWAP \in U(2^2)$ the swap gate (c.f. Example 2.11) which satisfy for all $|i_1\rangle\,|i_2\rangle \in \{0,1\}^2$ that

$$\mathcal{S}\,|i_1\rangle\,|i_2\rangle = |i_2\rangle\,|i_1\rangle\,. \tag{86}$$

If $k-j=1$, (i.e. $k=j+1$) then we simply set

$$T_{j\leftrightarrow j+1} = I_2^{\otimes j-1} \otimes \mathcal{S} \otimes I_2^{\otimes n-j-1}. \tag{87}$$

If $k-j \geq 2$, then proceeding inductively set

$$\mathcal{T}_{j\leftrightarrow k} = \prod_{l=1}^{k-j-1} (I_2^{\otimes k-2-l} \otimes \mathcal{S} \otimes I_2^{\otimes n-k+l}) \prod_{l=0}^{k-j-1} (I_2^{\otimes j-1+l} \otimes \mathcal{S} \otimes I_2^{\otimes n-j-1-l}), \tag{88}$$

(c.f. Definition 2.14), where we use the usual convention that $I_2^{\otimes 0} = 1 \in \mathbb{C}$ and $A \otimes 1 = A = 1 \otimes A$ for any $A \in U(2^m)$, $m \in \mathbb{N}$. By direct verification, we note that $\mathcal{T}_{j\leftrightarrow k}$ satisfy (85) for all $|i\rangle_n \in \{0,1\}^n$ and that only $2(k-j)-1$ swap gates were required in its construction.

Secondly, by the cycle decomposition theorem (Proposition 3.7), the given permutation π can be written as a composition of disjoint cycles (c.f. Definition 3.6, Proposition 3.7) as

$$\pi = C_1C_2\cdots C_k = (a_1a_2\cdots a_{m_1})(a_{m_1+1}a_{m_1+2}\cdots a_{m_2})\cdots(a_{m_{k-1}+1}a_{m_{k-1}+2}\cdots a_{m_k}), \tag{89}$$

where k is the number of cycles, and $a_1,\ldots,a_{m_k} \in \{1,\ldots,n\}$ are distinct numbers. Note by convention that each of these cycles has length $m_l \geq 2$. For each of these cycles $C_l = (a_{m_{l-1}+1}\cdots a_{m_l})$, $l = 1\ldots,k$, with $m_0 := 0$ we construct the quantum circuits $\mathcal{T}_{C_l}$, $l=1,\ldots,k$, via

$$\mathcal{T}_{C_l} = \prod_{i=m_{l-1}}^{m_l-1} \mathcal{T}_{a_i\leftrightarrow a_{i+1}} = \mathcal{T}_{a_{m_l-1}\leftrightarrow a_{m_l}}\cdots\mathcal{T}_{a_{m_{l-1}+1}\leftrightarrow a_{m_{l-1}+2}}\mathcal{T}_{a_{m_{l-1}}\leftrightarrow a_{m_{l-1}+1}}, \tag{90}$$

where the quantum circuits $\mathcal{T}_{a_i\leftrightarrow a_{i+1}}$ are constructed based on the first step of the proof (c.f. (85), (87), (88)). Finally, we construct the quantum circuit $\mathcal{T}_\pi$ via

$$\mathcal{T}_\pi = \prod_{l=1}^{k} \mathcal{T}_{C_l} = \mathcal{T}_{C_k}\cdots\mathcal{T}_{C_2}\mathcal{T}_{C_1}. \tag{91}$$

Thus, (85), (89), (90), and (91) imply that the quantum circuit $\mathcal{T}_\pi$ satisfies (82). Moreover, we note that the total number of quantum circuits of the form $\mathcal{T}_{j\leftrightarrow k}$ (c.f. (85)) is $m_k \leq n$, where each of these quantum circuits requires $2|a_i - a_{i+1}| - 1 \leq (2n-1)$ swap gates. Hence, the total number of swap gates used to construct $\mathcal{T}_\pi$ is at most $n\cdot(2n-1) \leq 2n^2$. Thus, we have proved the first statement of the lemma. The second statement of the lemma follows directly from the fact that $\mathcal{T}_\pi$ is a linear operator. □

Lemma 3.9 (Quantum circuit for addition) *([56, Section 3.1, QNMAdd]) Let $n_1,n_2 \in \mathbb{N}$, with $n_1 \geq n_2$. Then, there is a quantum circuit $\mathcal{Q}_{(+)}$ on (n_1+n_2+1) qubits such that for any $a \in \mathbb{F}_{n_1,0}, b \in \mathbb{F}_{n_2,0}$,*

$$\mathcal{Q}_{(+)} : |0\rangle\,|a\rangle_{n_1}\,|b\rangle_{n_2} \mapsto |a \boxplus b\rangle_{n_1+1}\,|b\rangle_{n_2}\,. \tag{92}$$

The quantum circuit $\mathcal{Q}_{(+)}$ requires $n_1^2 + 3n_1 + 18 + \frac{1}{2}(n_2(2n_1 - n_2 + 3))$ elementary gates.

Corollary 3.10 (Quantum circuit for addition with fractional part) *Let $n_1, n_2, m_1, m_2 \in \mathbb{N}$, with $n_1 + m_1 \geq n_2 + m_2$. Let $n = n_1 + n_2$, and $m = m_1 + m_2$. Then, there is a quantum circuit $\widetilde{\mathcal{Q}}_{(+)}$ on $(n + m + 1)$ qubits such that for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$,*

$$\widetilde{\mathcal{Q}}_{(+)} : |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle \mapsto |b\rangle_{n_2+m_2} |a \boxplus b\rangle_{n_1+m_1+1} . \tag{93}$$

The quantum circuit $\widetilde{\mathcal{Q}}_{(+)}$ requires at most $29(n + m + 1)^2$ elementary gates.

Proof. By Lemma 3.8, there is a quantum circuit $\mathcal{T}_{\pi_1}$ with at most $2(n_1 + m_1 + n_2 + m_2 + 1)^2 = 2(n + m + 1)^2$ swap gates satisfying

$$\mathcal{T}_{\pi_1} : |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle \mapsto |0\rangle |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} . \tag{94}$$

Note that by Lemma 3.4, we can extend the addition operation $\boxplus : \mathbb{F}_{n_1+m_1,0} \times \mathbb{F}_{n_2+m_2,0} \to \mathbb{F}_{n+m+1,0}$ to $\boxplus : \mathbb{F}_{n_1,m_1} \times \mathbb{F}_{n_2,m_2} \to \mathbb{F}_{\tilde{n}+1,\tilde{m}}$ where $\tilde{n} = \max\{n_1, n_2\}$ and $\tilde{m} = \max\{m_1, m_2\}$. This, the hypothesis that $n_1 + m_1 \geq n_2 + m_2$, and Lemma 3.9 (with $n_1 \leftarrow n_1 + m_1$, $n_2 \leftarrow n_2 + m_2$ in the notation of Lemma 3.9)imply that there exists a quantum circuit $\mathcal{Q}_{(+)}$ such that for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$ that

$$\mathcal{Q}_{(+)} : |0\rangle |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} \mapsto |a \boxplus b\rangle_{n_1+m_1+1} |b\rangle_{n_2+m_2} , \tag{95}$$

and that the number of elementary gates required to construct $\mathcal{Q}_{(+)}$ is

$$(n_1 + m_1)^2 + 3(n_1 + m_1) + 18 + \tfrac{1}{2}(n_2 + m_2)(2(n_1 + m_1) - (n_2 + m_2) + 3). \tag{96}$$

Moreover, by Lemma 3.8, there is a quantum circuit $\mathcal{T}_{\pi_2}$ such that

$$|a \boxplus b\rangle_{n_1+m_1+1} |b\rangle_{n_2+m_2} \mapsto |b\rangle_{n_2+m_2} |a \boxplus b\rangle_{n_1+m_1+1} , \tag{97}$$

which uses at most $2(n + m + 1)^2$ swap gates.

Define the quantum circuit $\widetilde{\mathcal{Q}}_{(+)} := \mathcal{T}_{\pi_2} \mathcal{Q}_{(+)} \mathcal{T}_{\pi_1}$. Observe that (94), (95), and (97) shows that $\widetilde{\mathcal{Q}}_{(+)}$ satisfies (93), and that the total number of elementary gates required to construct $\widetilde{\mathcal{Q}}_{(+)}$ is at most

$$\begin{aligned}
&2(n + m + 1)^2 + (n_1 + m_1)^2 + 3(n_1 + m_1) + 18 + \tfrac{1}{2}(n_2 + m_2)(2(n_1 + m_1) - (n_2 + m_2) + 3) + 2(n + m + 1)^2 \\
&\leq 2(n + m + 1)^2 + (n_1 + m_1)^2 + 3(n_1 + m_1) + 18 + (n + m + 1)^2 + \frac{3}{2}(n + m + 1)^2 + 2(n + m + 1)^2 \\
&\leq (2 + 1 + 3 + 18 + 1 + 2 + 2)(n + m + 1)^2 \\
&= 29(n + m + 1)^2.
\end{aligned} \tag{98}$$

□

Lemma 3.11 (Quantum circuit for multiplication) *([56, Section 3.5, QNMMul]) Let $n_1, n_2 \in \mathbb{N}$, with $n_1 \geq n_2$. Then, there is a quantum circuit $\mathcal{Q}_{(\times)}$ on $(2n_1 + 3n_2 + 3)$ qubits such that for any $a \in \mathbb{F}_{n_1,0}, b \in \mathbb{F}_{n_2,0}$,*

$$\mathcal{Q}_{(\times)} : |0\rangle |0\rangle_{n_1+n_2} |a\rangle_{n_1} |b\rangle_{n_2} |0\rangle_{n_2} |0\rangle_2 \mapsto |anc\rangle |a \boxdot b\rangle_{n_1+n_2} |a\rangle_{n_1} |b\rangle_{n_2} |anc\rangle_{n_2+2} . \tag{99}$$

The quantum circuit $\mathcal{Q}_{(\times)}$ requires $(\frac{1}{2}(5n_1^2 + n_1) + 4n_2^2 + 4n_1 n_2 + 6n_2 + 7)$ elementary gates.

Corollary 3.12 (Quantum circuit for multiplication with fractional part) *Let $n_1, n_2, m_1, m_2 \in \mathbb{N}$, with $n_1 + m_1 \geq n_2 + m_2$. Let $n := n_1 + n_2$ and $m := m_1 + m_2$. Then, there is a quantum circuit $\widetilde{\mathcal{Q}}_{(\times)}$ on $(2n + 2m + n_2 + m_2 + 3)$ qubits such that for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$,*

$$\widetilde{\mathcal{Q}}_{(\times)} : |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3} \mapsto |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |a \boxdot b\rangle_{n+m} |anc\rangle_{n_2+m_2+3} . \tag{100}$$

The quantum circuit $\widetilde{\mathcal{Q}}_{(\times)}$ requires at most $61(n + m + 1)^2$ elementary gates.

Proof. By Lemma 3.8, there is a quantum circuit $\mathcal{T}_{\pi}$ with at most $2(2n + 2m + n_2 + m_2 + 3)^2$ swap gates satisfying for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$ that

$$\mathcal{T}_{\pi} : |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle_{n+2m+3} \mapsto |0\rangle |0\rangle_{n+m} |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle_m |0\rangle_2 . \tag{101}$$

Note that by Lemma 3.5, we can extend the multiplication operation $\boxdot : \mathbb{F}_{n_1+m_1,0} \times \mathbb{F}_{n_2+m_2,0} \to \mathbb{F}_{n+m,0}$ to $\boxdot : \mathbb{F}_{n_1,m_1} \times \mathbb{F}_{n_2,m_2} \to \mathbb{F}_{n,m}$. This, the condition that $n_1 + m_1 \geq n_2 + m_2$, and Lemma 3.11 (with

$n_1 \leftarrow n_1 + m_1, n_2 \leftarrow n_2 + m_2$ in the notation of Lemma 3.11) imply that there exists a quantum circuit $\mathcal{Q}_{(\times)}$ such that for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$

$$\mathcal{Q}_{(\times)} : |0\rangle\, |0\rangle_{n+m}\, |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |0\rangle_{n_2+m_2}\, |0\rangle_2 \mapsto |\mathrm{anc}\rangle\, |a \boxdot b\rangle_{n+m}\, |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |\mathrm{anc}\rangle_{n_2+m_2+2}\,, \tag{102}$$

and that the number of elementary gates required to construct $\mathcal{Q}_{(\times)}$ is at most

$$(\frac{1}{2}(5(n_1+m_1)^2 + (n_1+m_1)) + 4(n_2+m_2)^2 + 4(n_1+m_1)(n_2+m_2) + 6(n_2+m_2) + 7). \tag{103}$$

By another application of Lemma 3.8, there is a quantum circuit $\mathcal{T}_{\pi'}$ with at most $2(2n+2m+n_2+m_2+3)^2$ swap gates satisfying

$$\mathcal{T}_{\pi'} : |\mathrm{anc}\rangle\, |a \boxdot b\rangle_{n+m}\, |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |\mathrm{anc}\rangle_{n_2+m_2+2} \mapsto |a \boxdot b\rangle_{n+m}\, |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |\mathrm{anc}\rangle_{n_2+m_2+3}\,. \tag{104}$$

We define the quantum circuit $\widetilde{\mathcal{Q}}_{(\times)} = \mathcal{T}_{\pi'}\mathcal{Q}_{(\times)}\mathcal{T}_{\pi}$. Hence, (101), (102), and (104) imply that the quantum circuit $\widetilde{\mathcal{Q}}_{(\times)}$ satisfy (100) for all $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$. Moreover, the number of elementary gates required to construct $\widetilde{\mathcal{Q}}_{(\times)}$ is at most

$$\begin{aligned}
&2(2n+2m+n_2+m_2+3)^2 + \frac{1}{2}(5(n_1+m_1)^2 + (n_1+m_1)) + 4(n_2+m_2)^2 + 4(n_1+m_1)(n_2+m_2)\\
&\quad + 6(n_2+m_2) + 7 + 2(2n+2m+n_2+m_2+3)^2\\
&\leq 2\cdot 3^2(n+m+1)^2 + \frac{5}{2}(n+m+1)^2 + \frac{1}{2}(n+m+1) + 4(n+m+1)^2 + 4(n+m+1)^2\\
&\quad + 6(n+m+1) + 7(n+m+1) + 2\cdot 3^2(n+m+1)^2\\
&\leq (18+3+1+4+4+6+7+18)(n+m+1)^2\\
&= 61(n+m+1)^2.
\end{aligned} \tag{105}$$

□

Lemma 3.13 (Quantum circuit for integer comparison) *([56, Section 3.4, QComp]) Let $n_1, n_2 \in \mathbb{N}$, with $n_1 \geq n_2$. Let $n = n_1 + n_2$. Then, there is a quantum circuit $\mathcal{Q}_{(comp)}$ on (n_1+n_2+4) qubits such that for any $a \in \mathbb{F}_{n_1,0}, b \in \mathbb{F}_{n_2,0}$,*

$$\mathcal{Q}_{(comp)} : |0\rangle\, |a\rangle_{n_1}\, |b\rangle_{n_2}\, |0\rangle\, |0\rangle\, |0\rangle \mapsto |a\rangle_{n_1}\, |b\rangle_{n_2}\, |c_1\rangle\, |c_2\rangle\, |c_3\rangle\, |anc\rangle\,, \tag{106}$$

where

$$|c_1\rangle\,|c_2\rangle\,|c_3\rangle = \begin{cases} |1\rangle\,|0\rangle\,|0\rangle\,, & \text{if } \mathrm{D}_{n,0}(a) > \mathrm{D}_{n,0}(b),\\ |0\rangle\,|1\rangle\,|0\rangle\,, & \text{if } \mathrm{D}_{n,0}(a) < \mathrm{D}_{n,0}(b),\\ |0\rangle\,|0\rangle\,|1\rangle\,, & \text{if } \mathrm{D}_{n,0}(a) = \mathrm{D}_{n,0}(b). \end{cases} \tag{107}$$

The quantum circuit $\mathcal{Q}_{(comp)}$ uses $(n_1^2 + 3n_1 + 41 + n_2(2n_1 - n_2 + 3)/2)$ elementary gates.

Corollary 3.14 (Quantum circuit for fractional comparison) *Let $n_1, n_2, m_1, m_2 \in \mathbb{N}$, with $n_1 + m_1 \geq n_2 + m_2$. Let $n = n_1 + n_2$, and $m = m_1 + m_2$. Then, there is a quantum circuit $\widetilde{\mathcal{Q}}_{(comp)}$ on $(n+m+4)$ qubits such that for any $a \in \mathbb{F}_{n_1,m_1}$, $b \in \mathbb{F}_{n_2,m_2}$,*

$$\widetilde{\mathcal{Q}}_{(comp)} : |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |0\rangle_4 \mapsto |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |c_1\rangle\, |c_2\rangle\, |c_3\rangle\, |anc\rangle\,, \tag{108}$$

where

$$|c_1\rangle\,|c_2\rangle\,|c_3\rangle = \begin{cases} |1\rangle\,|0\rangle\,|0\rangle\,, & \text{if } \mathrm{D}_{n,m}(a) > \mathrm{D}_{n,m}(b),\\ |0\rangle\,|1\rangle\,|0\rangle\,, & \text{if } \mathrm{D}_{n,m}(a) < \mathrm{D}_{n,m}(b),\\ |0\rangle\,|0\rangle\,|1\rangle\,, & \text{if } \mathrm{D}_{n,m}(a) = \mathrm{D}_{n,m}(b). \end{cases} \tag{109}$$

The quantum circuit $\widetilde{\mathcal{Q}}_{(comp)}$ requires at most $80(n+m+1)^2$ elementary gates.

Proof. Let $a \in \mathbb{F}_{n_1,m_1}$ and $b \in \mathbb{F}_{n_2,m_2}$. By Lemma 3.8, there is a quantum circuit $\mathcal{T}_\pi$ with at most $2(n+m+4)^2$ elementary gates satisfying

$$\mathcal{T}_\pi : |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |0\rangle_4 \mapsto |0\rangle\, |a\rangle_{n_1+m_1}\, |b\rangle_{n_2+m_2}\, |0\rangle\, |0\rangle\, |0\rangle\,. \tag{110}$$

Next, for any $p, q \in \mathbb{N}$, we define the left-shift operator $\tau_q : \mathbb{F}_{p,q} \to \mathbb{F}_{p+q,0}$ by $\tau_q((z_{p-1},\ldots,z_0),(z_{-1},\ldots,z_{-q})) = (z_{p-1},\ldots,z_0,z_{-1},\ldots,z_{-q})$. Note that since $\mathbb{F}_{n_1,m_1}, \mathbb{F}_{n_2,m_2} \subset \mathbb{F}_{n,m}$, we have $a, b \in \mathbb{F}_{n,m}$. Hence, we have

$\tau_m(a), \tau_m(b) \in \mathbb{F}_{n+m,0}$. Furthermore, we have the relation $\mathrm{D}_{n+m,0}(\tau_m(a)) = 2^m \mathrm{D}_{n,m}(a)$ and $\mathrm{D}_{n+m,0}(\tau_m(b)) = 2^m \mathrm{D}_{n,m}(b)$. Thus, it holds that

$$\mathrm{D}_{n,m}(a)\ (<,=,>)\ \mathrm{D}_{n,m}(b) \iff \mathrm{D}_{n+m,0}(\tau_m(a))\ (<,=,> \text{ respectively})\ \mathrm{D}_{n+m,0}(\tau_m(b)). \tag{111}$$

By Lemma 3.13 (with $n_1 \leftarrow n_1 + m_1$, $n_2 \leftarrow n_2 + m_2$ in the notation of Lemma 3.13), there is a quantum circuit $\mathcal{Q}_{(\mathrm{comp})}$ constructed with $((n_1+m_1)^2 + 3(n_1+m_1) + 41 + (n_2+m_2)(2(n_1+m_1) - (n_2+m_2) + 3)/2)$ elementary gates that satisfy

$$\mathcal{Q}_{(\mathrm{comp})} : |0\rangle\, |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |0\rangle\, |0\rangle\, |0\rangle \mapsto |a\rangle_{n_1+m_1} |b\rangle_{n_2+m_2} |c_1\rangle\, |c_2\rangle\, |c_3\rangle\, |\mathrm{anc}\rangle\,, \tag{112}$$

where

$$|c_1\rangle\, |c_2\rangle\, |c_3\rangle = \begin{cases} |1\rangle\, |0\rangle\, |0\rangle\,, & \text{if } \mathrm{D}_{n+m,0}(\tau_m(a)) > \mathrm{D}_{n+m,0}(\tau_m(b)), \\ |0\rangle\, |1\rangle\, |0\rangle\,, & \text{if } \mathrm{D}_{n+m,0}(\tau_m(a)) < \mathrm{D}_{n+m,0}(\tau_m(b)), \\ |0\rangle\, |0\rangle\, |1\rangle\,, & \text{if } \mathrm{D}_{n+m,0}(\tau_m(a)) = \mathrm{D}_{n+m,0}(\tau_m(b)). \end{cases} \tag{113}$$

Using the relation (111), we observe that (113) is equivalent to (109). Finally, we define the quantum circuit $\widetilde{Q}_{(\mathrm{comp})} := \mathcal{Q}_{(\mathrm{comp})}\mathcal{T}_\pi$. Thus, the definition of $\widetilde{Q}_{(\mathrm{comp})}$, (110), and (112) imply (108) as required. We note that the number of elementary gates used to construct $\widetilde{Q}_{(\mathrm{comp})}$ is at most

$$\begin{aligned} &2(n+m+4)^2 + (n_1+m_1)^2 + 3(n_1+m_1) + 41 + (n_2+m_2)(2(n_1+m_1) - (n_2+m_2) + 3)/2 \\ &\leq 2 \cdot 4^2(n+m+1)^2 + (n_1+m_1)^2 + 3(n_1+m_1) + 41 + (n_2+m_2)(n_1+m_1) + \frac{3}{2}(n_2+m_2) \\ &\leq (32+1+3+41+1+2)(n+m+1)^2 \\ &= 80(n+m+1)^2. \end{aligned} \tag{114}$$

□

Lemma 3.15 (Controlled Y-rotations) *([45, Section 4.3]) For any $\theta \in (0, 4\pi)$, there is a controlled Y-rotation gate acting on two qubits that performs the following operation*

$$CR_y(\theta) : |c\rangle\, |0\rangle \mapsto |c\rangle\, (R_y(\theta))^c\, |0\rangle = \begin{cases} |c\rangle\, |0\rangle\,, & \textit{if } c = 0, \\ |c\rangle\, (\cos(\theta/2)\, |0\rangle + \sin(\theta/2)\, |1\rangle), & \textit{if } c = 1. \end{cases} \tag{115}$$

The quantum circuit to construct $CR_y(\theta)$ requires two $R_y(\theta/2)$ gates (see Example 2.9) and two CNOT gates (see Example 2.10).

Proof. The quantum circuit can be constructed by the following definition

$$CR_y(\theta) = (I_2 \otimes R_y(\theta/2))(\mathrm{CNOT})(I_2 \otimes R_y(\theta/2))(\mathrm{CNOT}). \tag{116}$$

□

3.3 Distribution loading

The task of loading an arbitrary n-qubit state on a quantum computer is known generally to be a hard problem, as highlighted, e.g., in [37]. However, in some cases, the problem of loading states representing certain probability distributions on a quantum computer have been shown to be polynomially tractable. Grover and Rudolph have shown an efficient method to load a discrete approximation of any log-concave probability distributions [31]. Recently, Zoufal et al. have employed the so-called *quantum Generative Adversarial Networks* (qGANs) for learning and loading of probability distributions such as the uniform, normal, or log-normal distributions, including their multivariate versions [64]. For these distributions, it has been shown empirically that the qGANs can well approximate the truncated and discretized distributions, and the gate complexity of the qGANs circuits scale only polynomially in the number of input qubits. In [15], the authors constructed a quantum circuit for uploading the discretized multivariate log-normal distributions, where they used the Variational Quantum Eigensolvers (VQE) approach [47] to upload quantum circuits for approximating the cumulative log-return process R_t^i, defined in (3). It was estimated that loading the discretized multivariate log-normal distribution requires $O(nd^2 \log_2(\varepsilon^{-1}) L\mathfrak{T})$ gates, where $L \in \mathbb{N}$ is the depth of each variational quantum circuit for approximating the Gaussian distribution, $\mathfrak{T}$ is the number of timesteps, and n is the number of qubits used in each quantum circuit for approximating the Gaussian distribution, see [15, Appendix E]. Justified by the above examples in the literature, we make the following assumption.

Assumption 3.16 (Loading of discretized multivariate log-normal distribution) *Let $n, m \in \mathbb{N}$, and let $T > 0$. For every $d \in \mathbb{N}$ and $(t, x) \in [0, T) \times \mathbb{R}_+^d$ let $p_d(\cdot, T; x, t) : \mathbb{R}_+^d \to \mathbb{R}_+$ be the log-normal transition density given by (4). Then, we assume that there exists a constant $C_3 \in [1, \infty)$ such that for every $d \in \mathbb{N}$ and $\varepsilon > 0$ there exists a quantum circuit $\mathcal{P}_{d,\varepsilon}$ on $d(n+m)$ qubits such that the number of elementary gates used to construct $\mathcal{P}_{d,\varepsilon}$ is at most*

$$C_3 d^{C_3} (n+m)^{C_3} (\log_2(\varepsilon^{-1}))^{C_3} \tag{117}$$

and that $\mathcal{P}_{d,\varepsilon}$ satisfies

$$\mathcal{P}_{d,\varepsilon} |0\rangle_{d(n+m)} = \sum_{\boldsymbol{i}=(i_1,\ldots,i_d)\in\mathbb{F}_{n,m,+}^d} \sqrt{\widetilde{p}_{\boldsymbol{i}}}\, |i_1\rangle_{n+m} \cdots |i_d\rangle_{n+m}, \tag{118}$$

with coefficients $\widetilde{p}_{\boldsymbol{i}} \in [0,1]$ satisfying

$$\sum_{\boldsymbol{i}\in\mathbb{F}_{n,m,+}^d} \widetilde{p}_{\boldsymbol{i}} = 1 \tag{119}$$

and

$$\sum_{\boldsymbol{i}\in\mathbb{F}_{n,m,+}^d} \left|\widetilde{p}_{\boldsymbol{i}} - \gamma^{-1} p_{\boldsymbol{i},m}\right| \le \varepsilon, \tag{120}$$

where

$$p_{\boldsymbol{i},m} := \int_{Q_{\boldsymbol{i},m}} p_d(y, T; x, t) dy, \quad Q_{\boldsymbol{i},m} := [\mathrm{D}_{n,m}(i_1), \mathrm{D}_{n,m}(i_1) + 2^{-m}) \times \cdots \times [\mathrm{D}_{n,m}(i_d), \mathrm{D}_{n,m}(i_d) + 2^{-m}), \tag{121}$$

and

$$\gamma := \sum_{\boldsymbol{i}\in\mathbb{F}_{n,m,+}^d} p_{\boldsymbol{i},m} \in (0,1) \tag{122}$$

is a normalization constant.

3.4 Loading CPWA payoff functions

The goal of this section is to upload (an approximation of) the payoff function $h : \mathbb{R}^d \to \mathbb{R}$ given in (8) to a quantum circuit. To that end, let $K \in \mathbb{N}$ be the number of component functions of the payoff function h given in (8), and for $k = 1, \ldots, K$, let $h_k : [0, M]^d \to \mathbb{R}$ be (up to the sign) the corresponding k-th component of h given by

$$h_k(x) = \max\{\boldsymbol{a}_{k,l} \cdot \boldsymbol{x} + b_{k,l} : l = 1, \ldots, I_k\}, \tag{123}$$

where $\boldsymbol{a}_{k,l} \in \mathbb{R}^d$, $b_{k,l} \in \mathbb{R}$ for $l = 1, \ldots, I_k$. The parameters $(\boldsymbol{a}_{k,l}, b_{k,l})$ are approximated by the two's complement method with binary strings of a suitable length. These binary strings are loaded on a qubit register using quantum circuits with X-gates, see Lemma 3.17. Using the arithmetic quantum circuits in the Section 3.2, we construct a quantum circuit which computes the two's complement-discretized version of the payoff function $h_k(x)$. The discrete payoff function is then loaded by a controlled Y-rotation circuit, see Lemma 3.21 and Proposition 3.22.

Lemma 3.17 (Quantum circuit for affine sums) *Let $d, n_1, n_2 \in \mathbb{N}$, $m_1, m_2 \in \mathbb{N}_0$. Let $n := n_1 + n_2$, and $m := m_1 + m_2$. Let $a_1, \ldots, a_d, b \in \mathbb{F}_{n_2,m_2}$. Then, there is a quantum circuit $\mathcal{Q}_+^{d,n,m}$ on N qubits, where*

$$N := d(n_1 + m_1) + (d+1)(n_2 + m_2) + d(n+m) + d(n_2 + m_2 + 3) + d \tag{124}$$

such that for any $i_1, \ldots, i_d \in \mathbb{F}_{n_1,m_1}$,

$$\begin{aligned} \mathcal{Q}_+^{d,n,m} : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |0\rangle_{(d+1)(n_2+m_2)} |0\rangle_{d(n+m)} |0\rangle_{d(n_2+m_2+3)} |0\rangle_d \\ &\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} \left|(\boxplus_{k=1}^{d} (a_k \boxdot i_k)) \boxplus b\right\rangle_{n+m+d} |anc\rangle_p, \end{aligned} \tag{125}$$

with $p := d(2n_2 + 2m_2 + 3) + (n_2 + m_2) + (d-1)(n+m)$, and where $(\boxplus_{k=1}^d (a_k \boxdot i_k)) \boxplus b \in \mathbb{F}_{d+n,m}$ is the two's complement binary string representing the affine sum

$$\left(\sum_{k=1}^{d} (\mathrm{D}_{n_2,m_2}(a_k) \cdot \mathrm{D}_{n_1,m_1}(i_k))\right) + \mathrm{D}_{n_2,m_2}(b) \in \mathbb{K}_{n+d,m}, \tag{126}$$

(c.f. Definition 3.2). The quantum circuit $\mathcal{Q}_+^{d,n,m}$ uses at most $563d^3(n+m+1)^2$ elementary gates.

Proof. The computation in this circuit involves the following steps:

1. We first load the given two's complement binary strings $a_1, \ldots, a_d, b \in \mathbb{F}_{n_2,m_2}$ on the qubit register $|0\rangle_{(d+1)(n_2+m_2)} = |0\rangle_{n_2+m_2} \cdots |0\rangle_{n_2+m_2}$. To that end, we use the Pauli X gate (see Example 2.6) to flip the bit 0 to 1 according the binary strings $a_1, \ldots, a_d, b$ if necessary, to obtain the state

$$\mathcal{X}_{\boldsymbol{a},b} : |0\rangle_{n_2+m_2} \cdots |0\rangle_{n_2+m_2} \mapsto |a_1\rangle_{n_2+m_2} \cdots |a_d\rangle_{n_2+m_2} |b\rangle_{n_2+m_2} , \tag{127}$$

where we define

$$\mathcal{X}_{\boldsymbol{a},b} := \left(\bigotimes_{k=1}^{d} \bigotimes_{l=-m_2}^{n_2-1} X^{a_k(l)} \right) \otimes \left(\bigotimes_{l=-m_2}^{n_2-1} X^{b(l)} \right), \tag{128}$$

given the binary strings $a_k = ((a_k(l))_{l=0}^{n_2-1}, (a_k(l))_{l=-m_2}^{-1}) = ((a_k(n_2-1), \ldots, a_k(0)), (a_k(-1), \ldots, a_k(-m_2))) \in \mathbb{F}_{n_2,m_2}$ and $b = ((b(n_2-1), \ldots, b(0)), (b(-1), \ldots, b(-m_2))) \in \mathbb{F}_{n_2,m_2}$. Note that we use the convention of $X^0 = I_2$ for any unitary matrix X. We define the quantum circuit

$$\widetilde{\mathcal{X}}_{\boldsymbol{a},b} := I_2^{\otimes d(n_1+m_1)} \otimes \mathcal{X}_{\boldsymbol{a},b} \otimes I_2^{\otimes (d(n+m)+d(n_2+m_2+3)+d)}. \tag{129}$$

Hence, for any $i_1, \ldots, i_d \in \mathbb{F}_{n_1,m_1}$, we have

$$\begin{aligned} \widetilde{\mathcal{X}}_{\boldsymbol{a},b} : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |0\rangle_{(d+1)(n_2+m_2)} |0\rangle_{d(n+m)} |0\rangle_{d(n_2+m_2+3)} |0\rangle_d \\ &\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_1\rangle_{n_2+m_2} \cdots |a_d\rangle_{n_2+m_2} |b\rangle_{n_2+m_2} |0\rangle_{d(n+m)} |0\rangle_{d(n_2+m_2+3)} |0\rangle_d , \end{aligned} \tag{130}$$

and the number of Pauli X gates used to construct the quantum circuit $\widetilde{\mathcal{X}}_{\boldsymbol{a},b}$ is at most

$$(d+1)(n_2+m_2). \tag{131}$$

2. Next, we apply the permutation quantum circuit $\mathcal{T}_\pi$ from Lemma 3.8 to prepare for the upcoming d multiplications so that

$$\begin{aligned} \mathcal{T}_\pi : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_1\rangle_{n_2+m_2} \cdots |a_d\rangle_{n_2+m_2} |b\rangle_{n_2+m_2} |0\rangle_{d(n+m)} |0\rangle_{d(n_2+m_2+3)} |0\rangle_d \\ &\mapsto \bigotimes_{k=1}^{d} \big(|i_k\rangle_{n_1+m_1} |a_k\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3} \big) \otimes |b\rangle_{n_2+m_2} |0\rangle_d \\ &= |i_1\rangle_{n_1+m_1} |a_1\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3} \cdots |i_d\rangle_{n_1+m_1} |a_d\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3} |b\rangle_{n_2+m_2} |0\rangle_d . \end{aligned} \tag{132}$$

The number of swap gates used to construct $\mathcal{T}_\pi$ in this step is at most $2N^2$.

3. Next, for each $k = 1, \ldots, d$, we apply the multiplication quantum circuit $\mathcal{Q}_{(\times)}^{(k)} := \widetilde{\mathcal{Q}}_{(\times)}$ from Corollary 3.12 (with $n_1 \leftarrow n_1, n_2 \leftarrow n_2, m_1 \leftarrow m_1, m_2 \leftarrow m_2, a \leftarrow i_k, b \leftarrow a_k$ in the notation of Corollary 3.12) on each component $(|i_k\rangle_{n_1+m_1} |a_k\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3})$ such that

$$\begin{aligned} \bigotimes_{k=1}^{d} \mathcal{Q}_{(\times)}^{(k)} : &\bigotimes_{k=1}^{d} \big(|i_k\rangle_{n_1+m_1} |a_k\rangle_{n_2+m_2} |0\rangle_{n+m} |0\rangle_{n_2+m_2+3} \big) \otimes |b\rangle_{n_2+m_2} |0\rangle_d \\ &\mapsto \bigotimes_{k=1}^{d} \big(|i_k\rangle_{n_1+m_1} |a_k\rangle_{n_2+m_2} |a_k \boxdot i_k\rangle_{n+m} |\mathrm{anc}\rangle_{n_2+m_2+3} \big) \otimes |b\rangle_{n_2+m_2} |0\rangle_d \\ &= |i_1\rangle_{n_1+m_1} |a_1\rangle_{n_2+m_2} |a_1 \boxdot i_1\rangle_{n+m} |\mathrm{anc}\rangle_{n_2+m_2+3} \cdots \\ &\quad \cdots |i_d\rangle_{n_1+m_1} |a_d\rangle_{n_2+m_2} |a_d \boxdot i_d\rangle_{n+m} |\mathrm{anc}\rangle_{n_2+m_2+3} |b\rangle_{n_2+m_2} |0\rangle_d . \end{aligned} \tag{133}$$

The number of elementary gates used in this step is at most

$$d \cdot 61(n+m+1)^2. \tag{134}$$

4. We apply the permutation quantum circuit $\mathcal{T}_\pi$ from Lemma 3.8 to prepare for the upcoming d additions so that

$$\begin{aligned} \mathcal{T}_\pi : &\bigotimes_{k=1}^{d} \big(|i_k\rangle_{n_1+m_1} |a_k\rangle_{n_2+m_2} |a_k \boxdot i_k\rangle_{n+m} |\mathrm{anc}\rangle_{n_2+m_2+3} \big) \otimes |b\rangle_{n_2+m_2} |0\rangle_d \\ &\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_1 \boxdot i_1\rangle_{n+m} |a_2 \boxdot i_2\rangle_{n+m} |0\rangle |a_3 \boxdot i_3\rangle_{n+m} |0\rangle \cdots \\ &\quad \cdots |a_d \boxdot i_d\rangle_{n+m} |0\rangle |b\rangle_{n_2+m_2} |0\rangle |\mathrm{anc}\rangle_{d(2n_2+2m_2+3)} . \end{aligned} \tag{135}$$

Here, we consolidate the qubits $|a_1\rangle_{n_2+m_2}, \dots, |a_d\rangle_{n_2+m_2}$ in the ancilla qubit placeholder $|\text{anc}\rangle_{d(2n_2+2m_2+3)}$ as we do not need them in the later computations. The number of elementary gates used for this step is at most $2N^2$.

5. We perform the following addition inductively on the sums for $k = 1, \dots, d-1$

$$\boxplus : \mathbb{F}_{n+k-1,m} \times \mathbb{F}_{n,m} \to \mathbb{F}_{n+k,m}, \quad \left(\boxplus_{l=1}^{k} (a_l \boxdot i_l), (a_{k+1} \boxdot i_{k+1}) \right) \mapsto \boxplus_{l=1}^{k+1} (a_l \boxdot i_l), \tag{136}$$

and the addition

$$\boxplus : \mathbb{F}_{n+d-1,m} \times \mathbb{F}_{n_2,m_2} \to \mathbb{F}_{n+d,m}, \quad \left(\boxplus_{l=1}^{d} (a_l \boxdot i_l), b \right) \mapsto (\boxplus_{l=1}^{d} (a_l \boxdot i_l)) \boxplus b, \tag{137}$$

(c.f. Lemma 3.4 for definition of $\boxplus$). That is, we apply the quantum circuit $\mathcal{Q}_{(+)}^{(k)} := \mathcal{Q}_{(+)}$ from Corollary 3.10 inductively for $k = 1, \dots, d-1$ (with $n_1 \leftarrow n+k-1$, $n_2 \leftarrow n$, $m_1 \leftarrow m$, $m_2 \leftarrow m$, $a \leftarrow \boxplus_{l=1}^{k} (a_l \boxdot i_l)$, $b \leftarrow a_{k+1} \boxdot i_{k+1}$ in the notation of Corollary 3.10), and we apply the quantum circuit $\mathcal{Q}_{(+)}^{(b)} := \mathcal{Q}_{(+)}$ (with $n_1 \leftarrow n+d-1$, $n_2 \leftarrow n_2$, $m_1 \leftarrow m$, $m_2 \leftarrow m_2$, $a \leftarrow \boxplus_{l=1}^{d} (a_l \boxdot i_l)$, $b \leftarrow b$ in the notation of Corollary 3.10) so that

$$\begin{aligned}
&|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_1 \boxdot i_1\rangle_{n+m} |a_2 \boxdot i_2\rangle_{n+m} |0\rangle |a_3 \boxdot i_3\rangle_{n+m} |0\rangle \cdots \\
&\quad \cdots |a_d \boxdot i_d\rangle_{n+m} |0\rangle |b\rangle_{n_2+m_2} |0\rangle |\text{anc}\rangle_{d(2n_2+2m_2+3)} \\
&\xmapsto{\mathcal{Q}_{(+)}^{(1)}} |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_2 \boxdot i_2\rangle_{n+m} \left| \boxplus_{l=1}^{2} a_l \boxdot i_l \right\rangle_{n+m+1} |a_3 \boxdot i_3\rangle_{n+m} |0\rangle \cdots \\
&\quad \cdots |a_d \boxdot i_d\rangle_{n+m} |0\rangle |b\rangle_{n_2+m_2} |0\rangle |\text{anc}\rangle_{d(2n_2+2m_2+3)} \\
&\xmapsto{\mathcal{Q}_{(+)}^{(2)}} |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_2 \boxdot i_2\rangle_{n+m} |a_3 \boxdot i_3\rangle_{n+m} \left| \boxplus_{l=1}^{3} a_l \boxdot i_l \right\rangle_{n+m+2} \cdots \\
&\quad \cdots |a_d \boxdot i_d\rangle_{n+m} |0\rangle |b\rangle_{n_2+m_2} |0\rangle |\text{anc}\rangle_{d(2n_2+2m_2+3)} \\
&\qquad\qquad \vdots \qquad\qquad\qquad \vdots \\
&\xmapsto{\mathcal{Q}_{(+)}^{(d-1)}} |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_2 \boxdot i_2\rangle_{n+m} |a_3 \boxdot i_3\rangle_{n+m} \cdots \\
&\quad \cdots |a_d \boxdot i_d\rangle_{n+m} \left| \boxplus_{l=1}^{d} a_l \boxdot i_l \right\rangle_{n+m+d-1} |b\rangle_{n_2+m_2} |0\rangle |\text{anc}\rangle_{d(2n_2+2m_2+3)} \\
&\xmapsto{\mathcal{Q}_{(+)}^{(b)}} |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_2 \boxdot i_2\rangle_{n+m} |a_3 \boxdot i_3\rangle_{n+m} \cdots \\
&\quad \cdots |a_d \boxdot i_d\rangle_{n+m} |b\rangle_{n_2+m_2} \left| (\boxplus_{l=1}^{d} a_l \boxdot i_l) \boxplus b \right\rangle_{n+m+d} |\text{anc}\rangle_{d(2n_2+2m_2+3)}.
\end{aligned} \tag{138}$$

The number of elementary gates used for this step is at most

$$\begin{aligned}
&\sum_{k=1}^{d-1} 29[(n+m+k-1) + (n+m) + 1]^2 + 29[(n+m+d-1) + (n_2+m_2) + 1]^2 \\
&\quad \leq 29d \cdot 4d^2(n+m+1)^2 \\
&\quad = 116d^3(n+m+1)^2,
\end{aligned} \tag{139}$$

where we use the fact that $[(n+m+k-1) + (n+m) + 1]^2 \leq (2n+2m+d)^2 \leq 4d^2(n+m+1)^2$ when $k \leq d$.

6. We consolidate the ancillary qubits by combining the qubits (labeled $|a_2 \boxdot i_2\rangle, \dots, |a_d \boxdot i_d\rangle, |b\rangle$) under ancilla qubits $|\text{anc}\rangle_\star$. The permutation circuit $\mathcal{T}_\pi$ from Lemma 3.8 performs the following operation

$$\begin{aligned}
\mathcal{T}_\pi : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |a_2 \boxdot i_2\rangle_{n+m} \cdots |a_d \boxdot i_d\rangle_{n+m} |b\rangle_{n_2+m_2} \left| (\boxplus_{l=1}^{d} a_l \boxdot i_l) \boxplus b \right\rangle_{n+m+d} |\text{anc}\rangle_{d(2n_2+2m_2+3)} \\
&\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} \left| (\boxplus_{l=1}^{d} a_l \boxdot i_l) \boxplus b \right\rangle_{n+m+d} |\text{anc}\rangle_{d(2n_2+2m_2+3)+(n_2+m_2)+(d-1)(n+m)}.
\end{aligned} \tag{140}$$

The number of elementary gates used for this step is at most $2N^2$.

The resulting quantum circuit $\mathcal{Q}_{+}^{d,n,m}$ is a composition of the quantum circuits from each of the above steps. To deduce its gate complexity, we sum up the number of elementary gates used in each step. We note from the definition of $n, m \in \mathbb{N}$ and the definition of N in (124) that

$$\begin{aligned} N &:= d(n_1+m_1)+(d+1)(n_2+m_2)+d(n+m)+d(n_2+m_2+3)+d \\ &\leq [d+2d+d+3d+d](n+m+1) \\ &= 8d(n+m+1). \end{aligned} \tag{141}$$

Summing the number of elementary gates used in each step, we find that the number of elementary gates used in total is at most

$$\begin{aligned} &(d+1)(n_2+m_2)+2N^2+61d(n+m+1)^2+2N^2+116d^3(n+m+1)^2+2N^2 \\ &\leq 2d(n+m+1)+3\cdot 2(8d(n+m+1))^2+61d(n+m+1)^2+116d^3(n+m+1)^2 \\ &\leq (2+3\cdot 2\cdot 8^2+61+116)d^3(n+m+1)^2 \\ &= 563d^3(n+m+1)^2. \end{aligned} \tag{142}$$

□

Lemma 3.18 (Quantum circuit for maximum of two numbers) *Let $n, m \in \mathbb{N}$, and let $\mathrm{M}_{n,m} : \mathbb{F}_{n,m} \times \mathbb{F}_{n,m} \to \mathbb{F}_{n,m}$ be a function defined by*

$$\mathrm{M}_{n,m}(a,b) := \mathrm{E}_{n,m}(\max\{\mathrm{D}_{n,m}(a), \mathrm{D}_{n,m}(b)\}), \quad \forall a, b \in \mathbb{F}_{n,m}. \tag{143}$$

(c.f. Definition 3.2) Then, there is a quantum circuit $\mathcal{Q}_{(\max)}^{n,m}$ on $3(n+m)+4$ qubits such that for any $a, b \in \mathbb{F}_{n,m}$,

$$\mathcal{Q}_{(\max)}^{n,m} : |a\rangle_{n+m}|b\rangle_{n+m}|0\rangle_4|0\rangle_{n+m} \mapsto |a\rangle_{n+m}|b\rangle_{n+m}|anc\rangle_4|\mathrm{M}_{n,m}(a,b)\rangle_{n+m}, \tag{144}$$

which uses at most $557(n+m+1)^3$ elementary gates.

Proof. The computation in this quantum circuit involves the following steps:

1. We use the comparison quantum circuit $\mathcal{Q}_{(\mathrm{comp})}$ in Corollary 3.14 (with $n_1 \leftarrow n, n_2 \leftarrow n$, $m_1 \leftarrow m, m_2 \leftarrow m$, $a \leftarrow a$ and $b \leftarrow b$ in the notation of Corollary 3.14) to obtain

$$\mathcal{Q}_{(\mathrm{comp})} \otimes I_2^{\otimes n+m} : |a\rangle_{n+m}|b\rangle_{n+m}|0\rangle_4|0\rangle_{n+m} \mapsto |a\rangle_{n+m}|b\rangle_{n+m}|c_1\rangle|c_2\rangle|c_3\rangle|\mathrm{anc}\rangle|0\rangle_{n+m}, \tag{145}$$

   where

$$|c_1\rangle|c_2\rangle|c_3\rangle = \begin{cases} |1\rangle|0\rangle|0\rangle, & \text{if } \mathrm{D}_{n,m}(a) > \mathrm{D}_{n,m}(b), \\ |0\rangle|1\rangle|0\rangle, & \text{if } \mathrm{D}_{n,m}(a) < \mathrm{D}_{n,m}(b), \\ |0\rangle|0\rangle|1\rangle, & \text{if } \mathrm{D}_{n,m}(a) = \mathrm{D}_{n,m}(b). \end{cases} \tag{146}$$

   The number of gates used in this step is at most $80(2n+2m+1)^2$ elementary gates.

2. We apply $(n+m)$ Toffoli gate (circuits) CCNOT defined in Example 2.18 on the control qubit $|c_1\rangle$, target qubits $|a\rangle_{n+m}$, and output qubits $|0\rangle_{n+m}$. More precisely, for $a = ((a_{n-1},\ldots,a_0),(a_{-1},\ldots,a_{-m})) \in \mathbb{F}_{n,m}$, we apply for each $j = -m,\ldots,n-1$ a Toffoli gate $\mathcal{C}_{c_1,a_j} = \mathrm{CCNOT}$ (with $a \leftarrow c_1$, $b \leftarrow a_j$, and $c \leftarrow 0$ in the notation of Example 2.18)

$$\mathcal{C}_{c_1,a_j} : |c_1\rangle|a_j\rangle|0\rangle \mapsto |c_1\rangle|a_j\rangle X^{c_1 a_j}|0\rangle = \begin{cases} |c_1\rangle|a_j\rangle|1\rangle, & \text{if } c_1 = 1 \text{ and } a_j = 1, \\ |c_1\rangle|a_j\rangle|0\rangle, & \text{otherwise.} \end{cases} \tag{147}$$

   For each $j = -m,\ldots,n-1$, we apply the permutation quantum circuit $\mathcal{T}_j$ before and after each Toffoli gate $\mathcal{C}_{c_1,a_j}$. We define the quantum circuit $\mathcal{X}_{c_1,j}$ by

$$\mathcal{X}_{c_1,j} := \mathcal{T}_j\left(I_2^{\otimes n+m-1} \otimes I_2^{\otimes n+m} \otimes I_2^{\otimes 3} \otimes I_2^{\otimes n-j-1} \otimes \mathcal{C}_{c_1,a_j} \otimes I_2^{\otimes m+j}\right)\mathcal{T}_j, \tag{148}$$

   which computes from (145) the following

$$\begin{aligned} &|a\rangle_{n+m}|b\rangle_{n+m}|c_1\rangle|c_2\rangle|c_3\rangle|\mathrm{anc}\rangle|0\rangle_{n+m} \\ &\xmapsto{\mathcal{T}_j} |\hat{a}^j\rangle_{n+m-1}|b\rangle_{n+m}|c_2\rangle|c_3\rangle|\mathrm{anc}\rangle|0\rangle_{n-j-1}|c_1\rangle|a_j\rangle|0\rangle|0\rangle_{m+j} \\ &\xmapsto{\mathcal{C}_{c_1,a_j}} |\hat{a}^j\rangle_{n+m-1}|b\rangle_{n+m}|c_2\rangle|c_3\rangle|\mathrm{anc}\rangle|0\rangle_{n-j-1}|c_1\rangle|a_j\rangle X^{c_1 a_j}|0\rangle|0\rangle_{m+j} \\ &\xmapsto{\mathcal{T}_j} |a\rangle_{n+m}|b\rangle_{n+m}|c_1\rangle|c_2\rangle|c_3\rangle|\mathrm{anc}\rangle|0\rangle_{n-j-1}X^{c_1 a_j}|0\rangle|0\rangle_{m+j}, \end{aligned} \tag{149}$$

where $\left|\hat{a}^j\right\rangle_{n+m-1} := |a_{n-1}\rangle \cdots |a_{j+1}\rangle |a_{j-1}\rangle \cdots |a_{-m}\rangle$. Finally, we define the quantum circuit $\mathcal{X}_{c_1,a}$ by

$$\mathcal{X}_{c_1,a} := \prod_{j=-m}^{n-1} \mathcal{X}_{c_1,j}, \tag{150}$$

and we compute that

$$\begin{aligned} &\mathcal{X}_{c_1,a} : |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle |0\rangle_{n+m} \\ &\mapsto |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_1 a_j} |0\rangle_{n+m} \right). \end{aligned} \tag{151}$$

Note that the number of elementary gates used in this step is at most $(n+m)[15 + 2 \cdot 2(3(n+m)+4)^2]$, since each Toffoli gate circuit requires 15 gates, and each permutation circuit uses $2(3(n+m)+4)^2$ gates.

3. We repeat step 2 but by instead using the control qubit $|c_2\rangle$ with target qubits $|b\rangle_{n+m}$. We define the quantum circuits $\mathcal{X}_{c_2,b}$ similarly, and we compute that

$$\begin{aligned} &\mathcal{X}_{c_2,b} : |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_1 a_j} |0\rangle_{n+m} \right) \\ &\mapsto |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_2 b_j} X^{c_1 a_j} |0\rangle_{n+m} \right). \end{aligned} \tag{152}$$

4. We repeat step 2 but by instead using the control qubit $|c_3\rangle$ with target qubits $|b\rangle_{n+m}$. We define the quantum circuits $\mathcal{X}_{c_3,b}$ similarly, and we compute that

$$\begin{aligned} &\mathcal{X}_{c_3,b} : |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_2 b_j} X^{c_1 a_j} |0\rangle_{n+m} \right) \\ &\mapsto |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_3 b_j} X^{c_2 b_j} X^{c_1 a_j} |0\rangle_{n+m} \right). \end{aligned} \tag{153}$$

Since the qubits $|c_1\rangle |c_2\rangle |c_3\rangle$ may only take one of the three possible values as in (146), it holds for each $j = -m, \ldots, n-1$ that

$$X^{c_3 b_j} X^{c_2 b_j} X^{c_1 a_j} = \begin{cases} X^{a_j}, & \text{if } \mathrm{D}_{n,m}(a) > \mathrm{D}_{n,m}(b), \\ X^{b_j}, & \text{if } \mathrm{D}_{n,m}(a) \leq \mathrm{D}_{n,m}(b). \end{cases} \tag{154}$$

Thus, we have

$$\begin{aligned} &|a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{c_3 b_j} X^{c_2 b_j} X^{c_1 a_j} |0\rangle_{n+m} \right) \\ &= \begin{cases} |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{a_j} |0\rangle_{n+m} \right), & \text{if } \mathrm{D}_{n,m}(a) > \mathrm{D}_{n,m}(b), \\ |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle \left(\bigotimes_{j=-m}^{n-1} X^{b_j} |0\rangle_{n+m} \right), & \text{if } \mathrm{D}_{n,m}(a) \leq \mathrm{D}_{n,m}(b), \end{cases} \\ &= \begin{cases} |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle |a\rangle_{n+m}, & \mathrm{D}_{n,m}(a) > \mathrm{D}_{n,m}(b), \\ |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle |b\rangle_{n+m}, & \mathrm{D}_{n,m}(a) \leq \mathrm{D}_{n,m}(b), \end{cases} \\ &= |a\rangle_{n+m} |b\rangle_{n+m} |c_1\rangle |c_2\rangle |c_3\rangle |\mathrm{anc}\rangle |\mathrm{M}_{n,m}(a,b)\rangle_{n+m}. \end{aligned} \tag{155}$$

This is the desired output of (144) that we are after. We find that the total number of elementary gates used is at most

$$\begin{aligned} &80(2n+2m+1)^2 + 3 \cdot (n+m)[15 + 2 \cdot 2(3(n+m)+4)^2] \\ &\leq 80 \cdot 2^2 (n+m+1)^2 + 3 \cdot 15(n+m) + 3(n+m) \cdot 4 \cdot 4^2 (n+m+1)^2 \\ &\leq (80 \cdot 2^2 + 3 \cdot 15 + 3 \cdot 4 \cdot 4^2)(n+m+1)^3 \\ &= 557(n+m+1)^3. \end{aligned} \tag{156}$$

□

Corollary 3.19 (Quantum circuit for maximum of I numbers) *Let $I, n, m \in \mathbb{N}$. Let $\mathrm{M}_{I,n,m} : \mathbb{F}_{n,m}^I \to \mathbb{F}_{n,m}$ be a function defined by*

$$\mathrm{M}_{I,n,m}(i_1, \dots, i_I) = \mathrm{E}_{n,m}(\max\{\mathrm{D}_{n,m}(i_1), \dots, \mathrm{D}_{n,m}(i_I)\}), \quad \forall (i_1, \dots, i_I) \in \mathbb{F}_{n,m}^I. \tag{157}$$

(c.f. Definition 3.2). Then, there is a quantum circuit $\mathcal{Q}_{(\max)}^{I,n,m}$ on N qubits, where

$$N := (I(n+m) + (I-1)(n+m+4)) \tag{158}$$

such that for any $i_1, \dots, i_I \in \mathbb{F}_{n,m}$,

$$\begin{aligned} \mathcal{Q}_{(\max)}^{I,n,m} : &|i_1\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_{(I-1)(n+m+4)} \\ &\mapsto |i_1\rangle_{n+m} \cdots |i_I\rangle_{n+m} |anc\rangle_{(I-2)(n+m)+4(I-1)} |\mathrm{M}_{I,n,m}(i_1, \dots, i_I)\rangle_{n+m}, \end{aligned} \tag{159}$$

which uses at most $657I^2(n+m+1)^3$ elementary gates.

Proof. For any $i_1, \dots, i_I \in \mathbb{F}_{n,m}$, observe that the function $\mathrm{M}_{I,n,m}$ can be written recursively by setting

$$\begin{aligned} \mathfrak{m}_1 &:= i_1, \\ \mathfrak{m}_2 &:= \mathrm{M}_{2,n,m}(i_1, i_2), \\ \mathfrak{m}_3 &:= \mathrm{M}_{2,n,m}(\mathfrak{m}_2, i_3) = \mathrm{M}_{3,n,m}(i_1, i_2, i_3), \\ &\vdots \\ \mathfrak{m}_I &:= \mathrm{M}_{2,n,m}(\mathfrak{m}_{I-1}, i_I) = \dots = \mathrm{M}_{I,n,m}(i_1, \dots, i_I). \end{aligned} \tag{160}$$

With this setup in mind, we construct the quantum circuit $\mathcal{Q}_{(\max)}^{I,n,m}$ as follows.

1. We first apply the permutation quantum circuit $\mathcal{T}_\pi$ from Lemma 3.8 to obtain

$$\begin{aligned} \mathcal{T}_\pi : &|i_1\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_{(I-1)(n+m+4)} \\ &\mapsto |i_1\rangle_{n+m} |i_2\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} |i_3\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} |i_4\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m}. \end{aligned} \tag{161}$$

   The number of elementary gates used is at most $2N^2$.

2. We apply inductively the maximum circuit for two TC numbers $\mathcal{Q}_{(\max)}^{(k)}$ from Lemma 3.18 for $k = 1, \dots, I-1$ (with $n \leftarrow n$, $m \leftarrow m$, $a \leftarrow \mathfrak{m}_k$, $b \leftarrow i_{k+1}$ in the notation of Lemma 3.18) so that

$$\begin{aligned} &|i_1\rangle_{n+m} |i_2\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} |i_3\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} |i_4\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\xmapsto{\mathcal{Q}_{(\max)}^{(1)}} |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathrm{M}_{2,n,m}(i_1, i_2)\rangle_{n+m} |i_3\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\quad =: |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\xmapsto{\mathcal{Q}_{(\max)}^{(2)}} |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathrm{M}_{2,n,m}(\mathfrak{m}_2, i_3)\rangle_{n+m} |i_4\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\qquad \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\quad =: |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_3\rangle_{n+m} |i_4\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\qquad \cdots |i_I\rangle_{n+m} |0\rangle_4 |0\rangle_{n+m} \\ &\qquad\qquad \vdots \qquad\qquad \vdots \\ &\xmapsto{\mathcal{Q}_{(\max)}^{(I)}} |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} \cdots |\mathfrak{m}_{I-1}\rangle_{n+m} |i_I\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathrm{M}_{2,n,m}(\mathfrak{m}_{I-1}, i_I)\rangle_{n+m} \\ &\quad =: |i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} \cdots |\mathfrak{m}_{I-1}\rangle_{n+m} |i_I\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_I\rangle_{n+m}. \end{aligned} \tag{162}$$

   The number of elementary gates used in this step is at most

$$I \cdot 557(n+m+1)^3. \tag{163}$$

3. We consolidate the ancillary qubits by combining the following qubits: $(I-1)$ times of $|\mathrm{anc}\rangle_4$, and $(I-1)$ times of $|\mathfrak{m}_2\rangle_{n+m}, \cdots, |\mathfrak{m}_{I-1}\rangle_{n+m}$ under the placeholder qubit $|\mathrm{anc}\rangle_{(I-2)(n+m)+4(I-1)}$. The permutation quantum circuit $\mathcal{T}_\pi$ from Lemma 3.8 performs the following operation

$$\begin{aligned}\mathcal{T}_\pi : &|i_1\rangle_{n+m} |i_2\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_2\rangle_{n+m} |i_3\rangle_{n+m} \cdots |\mathfrak{m}_{I-1}\rangle_{n+m} |i_I\rangle_{n+m} |\mathrm{anc}\rangle_4 |\mathfrak{m}_I\rangle \\ &\mapsto |i_1\rangle_{n+m} |i_2\rangle_{n+m} \cdots |i_I\rangle_{n+m} |\mathrm{anc}\rangle_{(I-2)(n+m)+4(I-1)} |\mathfrak{m}_I\rangle_{n+m}.\end{aligned} \tag{164}$$

The number of elementary gates used in this step is at most $2N^2$.

The resulting quantum circuit $\mathcal{Q}^{I,n,m}_{(\max)}$ is a composition of the quantum circuits from each of the above steps. The number of elementary gates used in total is the sum of the number of gates used in each step which is at most

$$\begin{aligned}&2N^2 + 557I(n+m+1)^3 + 2N^2 \\ &= 557I(n+m+1)^3 + 4[I(n+m) + (I-1)(n+m+4)]^2 \\ &\leq 557I(n+m+1)^3 + 4[I(n+m+1) + 4I(n+m+1)]^2 \\ &\leq 557I(n+m+1)^3 + 4\cdot(1+4)^2(I(n+m+1))^2 \\ &\leq 657I^2(n+m+1)^3.\end{aligned} \tag{165}$$

□

Proposition 3.20 (Quantum circuit for loading CPWA component functions) *Let $I, d, n_1, n_2, m_1, m_2 \in \mathbb{N}$. Define $n := n_1 + n_2$, $m := m_1 + m_2$, and $p := d(2n_2 + 2m_2 + 3) + (n_2 + m_2) + (d-1)(n+m)$. Let $\{a_{l,j}\}_{l=1,\dots,I; j=1,\dots,d}, \{b_l\}_{l=1,\dots,I} \subset \mathbb{F}_{n_2,m_2}$. Let $h_l : \mathbb{F}^d_{n_1,m_1} \to \mathbb{F}_{n+d,m}$, $l = 1,\dots,I$ be functions defined by*

$$h_l(i_1,\dots,i_d) = \underset{j=1}{\overset{d}{\boxplus}} (a_{l,j} \boxdot i_j) \boxplus b_l, \quad \forall (i_1,\dots,i_d) \in \mathbb{F}^d_{n_1,m_1}, \tag{166}$$

let $M_{I,n+d,m} : \mathbb{F}^I_{n+d,m} \to \mathbb{F}_{n+d,m}$ be a function defined by

$$M_{I,n+d,m}(i_1,\dots,i_I) = \mathrm{E}_{n+d,m}(\max\{\mathrm{D}_{n+d,m}(i_1),\dots,\mathrm{D}_{n+d,m}(i_I)\}), \quad \forall (i_1,\dots,i_I) \in \mathbb{F}^I_{n+d,m}. \tag{167}$$

Define $h : \mathbb{F}^d_{n_1,m_1} \to \mathbb{F}_{n+d,m}$ by

$$h(\boldsymbol{i}) := M_{I,n+d,m}\big(h_1(\boldsymbol{i}),\dots,h_I(\boldsymbol{i})\big), \quad \forall \boldsymbol{i} = (i_1,\dots,i_d) \in \mathbb{F}^d_{n_1,m_1}. \tag{168}$$

Then, there is a quantum circuit $\mathcal{Q}_h$ on N qubits, where

$$N := d(n_1+m_1) + I(n+m+d+p) + (I-1)(n+m+d+4), \tag{169}$$

such that for any $\boldsymbol{i} = (i_1,\dots,i_d) \in \mathbb{F}^d_{n_1,m_1}$,

$$\begin{aligned}\mathcal{Q}_h : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |0\rangle_{I(n+m+d+p)+(I-2)(n+m+d)+4(I-1)} |0\rangle_{n+d+m} \\ &\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |anc\rangle_{I(n+m+d+p)+(I-2)(n+m+d)+4(I-1)} |h(\boldsymbol{i})\rangle_{n+d+m},\end{aligned} \tag{170}$$

which uses at most $9915I^3d^4(n+m+1)^4$ elementary gates.

Proof. The construction of the quantum circuit $\mathcal{Q}_h$ involves the following steps:

1. We first prepare the I affine sums $h_l(i_1,\dots,i_d)$ from (166), using Lemma 3.17. For $l = 1,\dots,I$, we apply the quantum circuits $(\mathcal{Q}^{d,n,m}_{+,l})_{l=1,\dots,I}$ of Lemma 3.17 (with $(d,n_1,n_2,m_1,m_2,a_1,\dots,a_d,b) \leftarrow (d,n_1,n_2,m_1,m_2,a_{l,1},\dots,a_{l,d},b_l)$ in the notation of Lemma 3.17) followed by an application of the per-

mutation circuit $\mathcal{T}_\pi$ from Lemma 3.8, where we compute

$$\begin{aligned}
&\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|0\right\rangle_{I(n+m+d+p)}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\xmapsto{\mathcal{Q}^{d,n,m}_{+,1}}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_p\left|0\right\rangle_{(I-1)(n+m+d+p)}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\xmapsto{\mathcal{T}^1_\pi}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|0\right\rangle_{n+m+d+p}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_p\left|0\right\rangle_{(I-2)(n+m+d+p)}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\xmapsto{\mathcal{Q}^{d,n,m}_{+,2}}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_p\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_p\\
&\qquad\qquad\qquad\cdot\left|0\right\rangle_{(I-2)(n+m+d+p)}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\xmapsto{\mathcal{T}^2_\pi}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|0\right\rangle_{n+m+d+p}\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_{2p}\\
&\qquad\qquad\qquad\cdot\left|0\right\rangle_{(I-3)(n+m+d+p)}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\qquad\qquad\qquad\vdots\qquad\qquad\qquad\qquad\vdots\\
&\xmapsto{\mathcal{Q}^{d,n,m}_{+,I}}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_p\\
&\qquad\qquad\qquad\cdots\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_{(I-1)p}\left|0\right\rangle_{(I-1)(n+m+d+4)}\\
&\xmapsto{\mathcal{T}^I_\pi}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\cdots\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\\
&\qquad\qquad\qquad\cdot\left|0\right\rangle_{(I-1)(n+m+d+4)}\left|\text{anc}\right\rangle_{Ip}.
\end{aligned}\tag{171}$$

In this step, the number of elementary gates used is at most

$$I[2N^2+563d^3(n+m+1)^2].\tag{172}$$

2. Next, we compute the maximum value amongst the affine sums $h_1,\ldots,h_I$. We apply the quantum circuit $\mathcal{Q}^{I,n+d,m}_{(\max)}$ of Corollary 3.19 (with $I\leftarrow I$, $n\leftarrow d+n$, $m\leftarrow m$, $i_1,\ldots,i_I\leftarrow h_1(\boldsymbol{i}),\ldots,h_I(\boldsymbol{i})$ in the notation of Corollary 3.19) where we have

$$\begin{aligned}
&\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\cdots\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\\
&\qquad\qquad\cdot\left|0\right\rangle_{(I-1)(n+m+d+4)}\left|\text{anc}\right\rangle_{Ip}\\
&\xmapsto{\mathcal{Q}^{I,n+d,m}_{(\max)}}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\cdots\left|h_2(\boldsymbol{i})\right\rangle_{n+m+d}\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\\
&\qquad\qquad\left|\text{anc}\right\rangle_{(I-2)(n+m+d)+4(I-1)}\left|h(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_{Ip}
\end{aligned}\tag{173}$$

In this step, the number of elementary gates used is at most

$$657I^2(n+m+d+1)^3.\tag{174}$$

3. We use the permutation quantum circuit $\mathcal{T}_\pi$ from Lemma 3.8 and we put the qubits $\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\cdots\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}$ under $\left|\text{anc}\right\rangle$, so that we have

$$\begin{aligned}
&\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|h_I(\boldsymbol{i})\right\rangle_{n+m+d}\cdots\left|h_1(\boldsymbol{i})\right\rangle_{n+m+d}\\
&\qquad\qquad\cdot\left|\text{anc}\right\rangle_{(I-2)(n+m+d)+4(I-1)}\left|h(\boldsymbol{i})\right\rangle_{n+m+d}\left|\text{anc}\right\rangle_{Ip}\\
&\xmapsto{\mathcal{T}_\pi}\left|i_1\right\rangle_{n_1+m_1}\cdots\left|i_d\right\rangle_{n_1+m_1}\left|\text{anc}\right\rangle_{I(n+m+d+p)+(I-2)(n+m+d)+4(I-1)}\left|h(\boldsymbol{i})\right\rangle_{n+m+d}.
\end{aligned}\tag{175}$$

We hence reach the desired state (170). In this step, the number of elementary gates used is at most

$$2N^2.\tag{176}$$

We note that

$$p=d(2n_2+2m_2+3)+(n_2+m_2)+(d-1)(n+m)\leq 4d(n+m+1).\tag{177}$$

Hence, we obtain that

$$\begin{aligned}
N&=d(n_1+m_1)+I(n+m+d+p)+(I-1)(n+m+d+4)\\
&\leq(d+Id+Ip+Id+4I)(n+m+1)\\
&\leq 8Ipd(n+m+1)\\
&\leq 4\cdot 8Id^2(n+m+1)^2\\
&=32Id^2(n+m+1)^2.
\end{aligned}\tag{178}$$

Thus, the total number of elementary gates used is at most

$$\begin{aligned}
&I[2N^2 + 563d^3(n+m+1)^2] + 657I^2(n+m+d+1)^3 + 2N^2 \\
&= (I+1)2N^2 + 563Id^3(n+m+1)^2 + 657I^2(n+m+d+1)^3 \\
&\leq 4IN^2 + 563Id^3(n+m+1)^2 + 657I^2(2d)^3(n+m+1)^3 \\
&\leq 4I(32Id^2(n+m+1)^2)^2 + 563Id^3(n+m+1)^2 + 657I^2(2d)^3(n+m+1)^3 \\
&\leq (4\cdot 32^2 + 563 + 657\cdot 2^3)I^3d^4(n+m+1)^4 \\
&= 9915I^3d^4(n+m+1)^4.
\end{aligned} \tag{179}$$

□

Lemma 3.21 (Quantum circuit for Y-rotation) *Let $n \in \mathbb{N}$, $m \in \mathbb{N}_0$, $a_0, a_1 \in \mathbb{R}$, and let $f(x) = a_1x + a_0$ for $x \in \mathbb{R}$. Define*

$$\bar{f}(i) := f \circ \mathrm{D}_{n,m}(i), \quad \forall i \in \mathbb{F}_{n,m}. \tag{180}$$

Then, there is a quantum circuit $\mathcal{R}_f$ on $(n+m+1)$ qubits such that for any $i \in \mathbb{F}_{n,m}$,

$$\mathcal{R}_f : |i\rangle_{n+m} |0\rangle \mapsto |i\rangle_{n+m} [\cos(\bar{f}(i)/2) |0\rangle + \sin(\bar{f}(i)/2) |1\rangle], \tag{181}$$

which uses $13(n+m+1)^3$ elementary gates.

Proof. The quantum circuit $\mathcal{R}_f$ is inspired by [62, Fig. 2], and it involves the following computations:

1. We apply the Y-rotation gate $R_y(\theta)$ from Example 2.9 (with parameter $\theta \leftarrow a_0$ in the notation of Example 2.9) to obtain the state

$$I_2^{\otimes n+m} \otimes R_y(a_0) : |i\rangle_{n+m} |0\rangle \mapsto |i\rangle_{n+m} (\cos(a_0/2)|0\rangle + \sin(a_0/2)|1\rangle). \tag{182}$$

2. We apply the controlled Y-rotation gate $CR_y(\theta)$ of Lemma 3.15 on the qubit $|i_{n-1}\rangle$ (with parameter $\theta \leftarrow -a_1 \cdot 2^{n-1}$, control qubit $c \leftarrow i_{n-1}$ and target qubit $0 \leftarrow (\cos(a_0/2)|0\rangle + \sin(a_0/2)|1\rangle)$ in the notation of Lemma 3.15) to obtain

$$\begin{aligned}
&I_2^{\otimes n+m-1} \otimes CR_y(-a_1 \cdot 2^{n-1}) : |i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-1}\rangle (\cos(a_0/2)|0\rangle + \sin(a_0/2)|1\rangle) \\
&\mapsto |i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-1}\rangle (\cos((-a_1 2^{n-1} i_{n-1} + a_0)/2)|0\rangle + \sin((-a_1 2^{n-1} i_{n-1} + a_0)/2)|1\rangle) \\
&= \begin{cases} |i\rangle_{n+m} (\cos(a_0/2)|0\rangle + \sin(a_0/2)|1\rangle), & \text{if } i_{n-1} = 0, \\ |i\rangle_{n+m} (\cos((-a_1 2^{n-1} + a_0)/2)|0\rangle + \sin((-a_1 2^{n-1} + a_0)/2)|1\rangle), & \text{if } i_{n-1} = 1. \end{cases}
\end{aligned} \tag{183}$$

3. Similarly, we inductively apply for $k = n-2, \dots, 0, \dots, -m$ the permutation quantum circuit $\mathcal{T}_{k\leftrightarrow n-1}$ from Lemma 3.8, the controlled Y-rotation gate $CR_y(\theta)$ (with parameter $\theta \leftarrow a_1 2^k$ and control qubit $c \leftarrow i_k$ in the notation of Lemma 3.15), and another permutation circuit $\mathcal{T}_{k\leftrightarrow n-1}$ to obtain

$$\begin{aligned}
&|i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-1}\rangle (\cos((-a_1 2^{n-1} i_{n-1} + a_0)/2)|0\rangle + \sin((-a_1 2^{n-1} i_{n-1} + a_0)/2)|1\rangle) \\
&\xmapsto{\mathcal{T}_{n-2\leftrightarrow n-1}} |i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-1}\rangle |i_{n-2}\rangle (\cos((-a_1 2^{n-1} i_{n-1} + a_0)/2)|0\rangle + \sin((-a_1 2^{n-1} i_{n-1} + a_0)/2)|1\rangle) \\
&\xmapsto{CR_y(a_1 2^{n-2})} |i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-1}\rangle |i_{n-2}\rangle \Big(\cos((a_1(2^{n-2} i_{n-2} - 2^{n-1} i_{n-1}) + a_0)/2)|0\rangle \\
&\qquad + \sin((a_1(2^{n-2} i_{n-2} - 2^{n-1} i_{n-1}) + a_0)/2)|1\rangle \Big) \\
&\xmapsto{\mathcal{T}_{n-2\leftrightarrow n-1}} |i_{-m}\rangle \cdots |i_0\rangle \cdots |i_{n-2}\rangle |i_{n-1}\rangle \Big(\cos((a_1(2^{n-2} i_{n-2} - 2^{n-1} i_{n-1}) + a_0)/2)|0\rangle \\
&\qquad + \sin((a_1(2^{n-2} i_{n-2} - 2^{n-1} i_{n-1}) + a_0)/2)|1\rangle \Big) \\
&\qquad \vdots \qquad\qquad \vdots \\
&\mapsto |i\rangle_{n+m} \left(\cos\left((a_1(-2^{n-1} i_{n-1} + \sum_{k=-m}^{n-2} 2^k i_k) + a_0)/2 \right) |0\rangle + \sin\left((a_1(-2^{n-1} i_{n-1} + \sum_{k=-m}^{n-2} 2^k i_k) + a_0)/2 \right) |1\rangle\right) \\
&= |i\rangle_{n+m} [\cos(\bar{f}(i)/2)|0\rangle + \sin(\bar{f}(i)/2)|1\rangle]
\end{aligned} \tag{184}$$

The permutation circuits $\mathcal{T}_\pi$ from Lemma 3.8 requires $2(n+m+1)^2$ gates and the controlled Y-rotation gate $CR_y(\theta)$ requires 4 elementary gates (c.f. Lemma 3.15). Hence, the total number of gates required for circuit $\mathcal{R}_f$ is

$$1 + 4 + (n+m-1)[2 \cdot 2(n+m+1)^2 + 4] \leq 13(n+m+1)^3. \tag{185}$$

Thus, we conclude the proof of the lemma. □

Proposition 3.22 (Quantum circuit for CPWA payoff function with Y-rotation) *Let $d \in \mathbb{N}$, $n_1, n_2, m_1, m_2 \in \mathbb{N}$, $K \in \mathbb{N}$, $I_1, \cdots, I_K \in \mathbb{N}$, $\xi_1, \ldots, \xi_K \in \{-1, 1\}$, and $s \in (0,1)$. Define $n := n_1 + n_2$, $m = m_1 + m_2$, and $p := d(2n_2 + 2m_2 + 3) + (n_2 + m_2) + (d-1)(n+m)$. Let $\{a_{k,l,j}\}_{k=1,\ldots,K; l=1,\ldots,I_k; j=1,\ldots,d}$, $\{b_{k,l}\}_{k=1,\ldots,K; l=1,\ldots,I_k} \subset \mathbb{F}_{n_2,m_2}$. For $k = 1, \ldots, K$, $l = 1, \ldots, I_k$, let $h_{k,l} : \mathbb{F}^d_{n_1,m_1} \to \mathbb{F}_{n+d,m}$ be functions defined by*

$$h_{k,l}(\boldsymbol{i}) := \mathop{\boxplus}_{j=1}^{d} (a_{k,l,j} \boxdot i_j) \boxplus b_{k,l}, \quad \forall \boldsymbol{i} = (i_1, \ldots, i_d) \in \mathbb{F}^d_{n_1,m_1}. \tag{186}$$

For $k = 1, \ldots, K$, let $\bar{\xi}_k \in \mathbb{F}_{2,0}$ be defined by

$$\bar{\xi}_k := \mathrm{E}_{2,0}(\xi_k), \tag{187}$$

let $M_{I_k,n+d,m} : \mathbb{F}^{I_k}_{n+d,m} \to \mathbb{F}_{n+d,m}$ be defined by

$$M_{I_k,n+d,m}(i_1, \ldots, i_{I_k}) := \mathrm{E}_{n+d,m}(\max\{\mathrm{D}_{n+d,m}(i_1), \ldots, \mathrm{D}_{n+d,m}(i_{I_k})\}), \quad \forall (i_1, \ldots, i_{I_k}) \in \mathbb{F}^{I_k}_{n+d,m}, \tag{188}$$

and let $\boldsymbol{h}_k : \mathbb{F}^d_{n_1,m_1} \to \mathbb{F}_{n+d,m}$ be defined by

$$\boldsymbol{h}_k(\boldsymbol{i}) := M_{I_k,n+d,m}\big(h_{k,1}(\boldsymbol{i}), \ldots, h_{k,I_k}(\boldsymbol{i})\big), \quad \forall \boldsymbol{i} = (i_1, \ldots, i_d) \in \mathbb{F}^d_{n_1,m_1}. \tag{189}$$

Let $\boldsymbol{h} : \mathbb{F}^d_{n_1,m_1} \to \mathbb{F}_{n+d+K+1,m}$ be defined by

$$\boldsymbol{h}(\boldsymbol{i}) := \mathop{\boxplus}_{k=1}^{K} (\bar{\xi}_k \boxdot \boldsymbol{h}_k(\boldsymbol{i})), \quad \forall \boldsymbol{i} = (i_1, \ldots, i_d) \in \mathbb{F}^d_{n_1,m_1}. \tag{190}$$

Let $f : \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = sx + \frac{\pi}{2}$, and define $\bar{f} : \mathbb{F}_{n+d+K+1,m} \to \mathbb{R}$ by

$$\bar{f}(i) := f \circ \mathrm{D}_{n+d+K+1,m}(i), \quad \forall i \in \mathbb{F}_{n+d+K+1,m}. \tag{191}$$

Then, there is a quantum circuit $\mathcal{R}_{\boldsymbol{h}}$ on N qubits, where

$$\begin{aligned} N &:= d(n_1 + m_1) + \sum_{k=1}^{K} q_k + 2K(n+m+d+5), \\ q_k &:= I_k(n+m+d+p) + (I_k - 2)(n+m+d) + 4(I_k - 1), \quad k = 1, \ldots, K, \end{aligned} \tag{192}$$

such that for any $\boldsymbol{i} = (i_1, \ldots, i_d) \in \mathbb{F}^d_{n_1,m_1}$,

$$\begin{aligned} \mathcal{R}_{\boldsymbol{h}} : &|i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |0\rangle_{q_1+\cdots+q_K} |0\rangle_{2K(n+m+d+5)} \\ &\mapsto |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |anc\rangle_{q_1+\cdots+q_K+2K(n+m+d+5)-1} \left[\cos\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|0\rangle + \sin\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|1\rangle\right], \end{aligned} \tag{193}$$

which uses at most $15262K^3 \max_{k=1,\ldots,K}\{I_k\}^3 d^4 (n+m+1)^4$ elementary gates.

Proof. The construction of the quantum circuit $\mathcal{R}_{\boldsymbol{h}}$ involves the following steps:

1. We first prepare the K component functions $\boldsymbol{h}_k$ using Proposition 3.20. For $k = 1, \ldots, K$, we apply the quantum circuits $(\mathcal{Q}_{h_k})_{k=1,\ldots,K}$ of Proposition 3.20 (with $I, d, n_1, m_1, n_2, m_2 \leftarrow I_k, d, n_1, m_1, n_2, m_2$, $a_{l,j} \leftarrow a_{k,l,j}$, and $b_l \leftarrow b_{k,l}$ in the notation of Proposition 3.20) followed by an application of the permutation

circuit $\mathcal{T}_\pi$ from Lemma 3.8, where we compute

$$
\begin{aligned}
&|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|0\rangle_{q_1+\cdots+q_K}|0\rangle_{2K(n+m+d+5)}\\
&=|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|0\rangle_{q_1}|0\rangle_{n+m+d}|0\rangle_{q_2}|0\rangle_{n+m+d}\cdots|0\rangle_{q_K}|0\rangle_{n+m+d}|0\rangle_{K(n+m+d+10)}\\
&\xmapsto{\mathcal{Q}_{\boldsymbol{h}_1}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_{q_2}|0\rangle_{n+m+d}\cdots|0\rangle_{q_K}|0\rangle_{n+m+d}|0\rangle_{K(n+m+d+10)}\\
&\xmapsto{\mathcal{T}_1}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|0\rangle_{q_2}|0\rangle_{n+m+d}|\text{anc}\rangle_{q_1}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}\cdots|0\rangle_{q_K}|0\rangle_{n+m+d}|0\rangle_{K(n+m+d+10)}\\
&\xmapsto{\mathcal{Q}_{\boldsymbol{h}_2}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_2}|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|\text{anc}\rangle_{q_1}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}\cdots|0\rangle_{q_K}|0\rangle_{n+m+d}|0\rangle_{K(n+m+d+10)}\\
&\qquad\qquad\qquad\vdots\qquad\qquad\qquad\qquad\vdots\\
&\xmapsto{\mathcal{Q}_{\boldsymbol{h}_K}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_K}|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}\cdots|\text{anc}\rangle_{q_1}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_{K(n+m+d+10)}\\
&\xmapsto{\mathcal{T}_K}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\\
&\qquad\qquad\cdot|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5|0\rangle_K
\end{aligned}
\tag{194}
$$

In this step, the number of elementary gates used is at most

$$
K\cdot 2N^2+\sum_{k=1}^{K}9915 I_k^3 d^4(n+m+1)^4 \tag{195}
$$

2. Next, we load the strings $\overline{\xi}_k\in\mathbb{F}_{2,0}$ into the qubits $|0\rangle_2$ for $k=1,\dots,K$ using the Pauli X gates (c.f. Example 2.6)

$$
\begin{aligned}
&|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\\
&\qquad\qquad\cdot|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|0\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5|0\rangle_K\\
&\mapsto|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_1\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\\
&\qquad\qquad\cdot|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_2\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_K\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5|0\rangle_K.
\end{aligned}
\tag{196}
$$

The number of elementary gates used in this step is at most

$$
2K. \tag{197}
$$

3. We perform K multiplication using the quantum circuit $\widetilde{\mathcal{Q}}^{(k)}_{(\times)}=\widetilde{\mathcal{Q}}_{(\times)}$ from Corollary 3.12 (with $n_1\leftarrow n+d$, $m_1\leftarrow m$, $n_2\leftarrow 2$, $m_2\leftarrow 0$, $a\leftarrow\boldsymbol{h}_k(\boldsymbol{i})$, and $b\leftarrow\overline{\xi}_k$ in the notation of Corollary 3.12 for $k=1,\dots,K$)

$$
\begin{aligned}
&|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_1\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\\
&\qquad\qquad\cdot|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_2\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_K\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5|0\rangle_K\\
&\xmapsto{\widetilde{\mathcal{Q}}^{(1)}_{(\times)}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_1\rangle_2|\boldsymbol{h}_1(\boldsymbol{i})\boxdot\overline{\xi}_1\rangle_{n+m+d+2}|\text{anc}\rangle_5\\
&\qquad\qquad\cdot|\boldsymbol{h}_2(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_2\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_K\rangle_2|0\rangle_{n+m+d+2}|0\rangle_5|0\rangle_K\\
&\qquad\qquad\qquad\vdots\qquad\qquad\qquad\qquad\vdots\\
&\xmapsto{\widetilde{\mathcal{Q}}^{(K)}_{(\times)}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_1\rangle_2|\boldsymbol{h}_1(\boldsymbol{i})\boxdot\overline{\xi}_1\rangle_{n+m+d+2}|\text{anc}\rangle_5\\
&\qquad\qquad\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}|\overline{\xi}_K\rangle_2|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\rangle_{n+m+d+2}|\text{anc}\rangle_5|0\rangle_K.
\end{aligned}
\tag{198}
$$

The number of elementary gates used in this step is at most

$$
K\cdot 61(n+m+d+3)^2. \tag{199}
$$

4. We use the permutation circuit $\mathcal{T}_\pi$ to reorder the qubits for addition, where

$$\begin{aligned} &|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K}|\boldsymbol{h}_1(\boldsymbol{i})\rangle_{n+m+d}\left|\overline{\xi}_1\right\rangle_2\left|\boldsymbol{h}_1(\boldsymbol{i})\boxdot\overline{\xi}_1\right\rangle_{n+m+d+2}|\text{anc}\rangle_5 \\ &\qquad\cdots|\boldsymbol{h}_K(\boldsymbol{i})\rangle_{n+m+d}\left|\overline{\xi}_K\right\rangle_2\left|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\right\rangle_{n+m+d+2}|\text{anc}\rangle_5|0\rangle_K \\ &\xmapsto{\mathcal{T}_\pi}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K+K(n+m+d+7)}\left|\boldsymbol{h}_1(\boldsymbol{i})\boxdot\overline{\xi}_1\right\rangle_{n+m+d+2}\left|\boldsymbol{h}_2(\boldsymbol{i})\boxdot\overline{\xi}_2\right\rangle_{n+m+d+2}|0\rangle \\ &\qquad\left|\boldsymbol{h}_3(\boldsymbol{i})\boxdot\overline{\xi}_3\right\rangle_{n+m+d+2}|0\rangle\cdots\left|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\right\rangle_{n+m+d+2}|0\rangle|0\rangle. \end{aligned} \tag{200}$$

The number of elementary gates used in this step is at most

$$2N^2. \tag{201}$$

5. We perform the following addition inductively on the sums for $k=1,\dots,K-1$

$$\boxplus:\mathbb{F}_{n+d+2+k-1,m}\times\mathbb{F}_{n+d+2,m}\to\mathbb{F}_{n+d+2+k,m},\quad \Big(\boxplus_{l=1}^{k}(\boldsymbol{h}_l(\boldsymbol{i})\boxdot\overline{\xi}_l),\boldsymbol{h}_{k+1}(\boldsymbol{i})\boxdot\overline{\xi}_{k+1}\Big)\mapsto\boxplus_{l=1}^{k+1}(\boldsymbol{h}_l(\boldsymbol{i})\boxdot\overline{\xi}_l), \tag{202}$$

where we apply the quantum circuit $\mathcal{Q}_{(+)}$ from Corollary 3.10 inductively for $k=1,\dots,K-1$ (with $n_1\leftarrow n+d+2+k-1$, $m_1\leftarrow m$, $n_2\leftarrow n+d+2$, $m_2\leftarrow m$ in the notation of Corollary 3.10) so that

$$\begin{aligned} &|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K+K(n+m+d+7)}\left|\boldsymbol{h}_1(\boldsymbol{i})\boxdot\overline{\xi}_1\right\rangle_{n+m+d+2}\left|\boldsymbol{h}_2(\boldsymbol{i})\boxdot\overline{\xi}_2\right\rangle_{n+m+d+2}|0\rangle \\ &\qquad\left|\boldsymbol{h}_3(\boldsymbol{i})\boxdot\overline{\xi}_3\right\rangle_{n+m+d+2}|0\rangle\cdots\left|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\right\rangle_{n+m+d+2}|0\rangle|0\rangle \\ &\xmapsto{\mathcal{Q}_{(+)}^{(1)}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K+K(n+m+d+7)}\left|\boldsymbol{h}_2(\boldsymbol{i})\boxdot\overline{\xi}_2\right\rangle_{n+m+d+2}\left|\boxplus_{l=1}^{2}(\boldsymbol{h}_l(\boldsymbol{i})\boxdot\overline{\xi}_l)\right\rangle_{n+m+d+3} \\ &\qquad\left|\boldsymbol{h}_3(\boldsymbol{i})\boxdot\overline{\xi}_3\right\rangle_{n+m+d+2}|0\rangle\cdots\left|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\right\rangle_{n+m+d+2}|0\rangle|0\rangle \\ &\qquad\vdots\qquad\qquad\qquad\vdots \\ &\xmapsto{\mathcal{Q}_{(+)}^{(K)}}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K+K(n+m+d+7)}\left|\boldsymbol{h}_2(\boldsymbol{i})\boxdot\overline{\xi}_2\right\rangle_{n+m+d+2}\left|\boldsymbol{h}_3(\boldsymbol{i})\boxdot\overline{\xi}_3\right\rangle_{n+m+d+2} \\ &\qquad\cdots\left|\boldsymbol{h}_K(\boldsymbol{i})\boxdot\overline{\xi}_K\right\rangle_{n+m+d+2}\left|\boxplus_{l=1}^{K}(\boldsymbol{h}_l(\boldsymbol{i})\boxdot\overline{\xi}_l)\right\rangle_{n+m+d+K+1}|0\rangle \\ &=:|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_k+K(n+m+d+7)+(K-1)(n+m+d+2)}|\boldsymbol{h}(\boldsymbol{i})\rangle_{n+m+d+K+1}|0\rangle. \end{aligned} \tag{203}$$

The number of elementary gates used in this step is at most

$$\sum_{k=1}^{K-1}29[(n+m+d+2+k-1)+(n+m+d+2)+1]^2 \tag{204}$$

6. Lastly, we apply the quantum circuit $\mathcal{R}_f$ from Lemma 3.21 (with $a_1\leftarrow s$, $a_0\leftarrow\pi/2$, $n\leftarrow n+d+K+1$, $m\leftarrow m$ in the notation of Lemma 3.21)

$$\begin{aligned} &|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_k+K(n+m+d+7)+(K-1)(n+m+d+2)}|\boldsymbol{h}(\boldsymbol{i})\rangle_{n+m+d+K+1}|0\rangle \\ &\xmapsto{\mathcal{R}_f}|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_k+K(n+m+d+7)+(K-1)(n+m+d+2)}|\boldsymbol{h}(\boldsymbol{i})\rangle_{n+m+d+K+1} \\ &\qquad\left[\cos\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|0\rangle+\sin\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|1\rangle\right] \\ &=:|i_1\rangle_{n_1+m_1}\cdots|i_d\rangle_{n_1+m_1}|\text{anc}\rangle_{q_1+\cdots+q_K+2K(n+m+d+5)-1}\left[\cos\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|0\rangle+\sin\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big)|1\rangle\right]. \end{aligned} \tag{205}$$

This is the desired state (193). The number of elementary gates used in this step is at most

$$13(n+d+K+1+m+1)^3. \tag{206}$$

Note that $p\le 4d(n+m+1)$ (c.f. (177)), hence, for each $k=1,\dots,K$,

$$\begin{aligned} q_k&=I_k(n+m+d+p)+(I_k-2)(n+m+d)+4(I_k-1) \\ &\le I_k(n+m+d+4d(n+m+1))+(I_k-2)(n+m+d)+4(I_k-1) \\ &\le I_k(d(n+m+1)+4d(n+m+1))+5I_kd(n+m+1) \\ &=10I_kd(n+m+1). \end{aligned} \tag{207}$$

Hence,

$$\begin{aligned} N &= d(n_1+m_1) + \sum_{k=1}^{K} q_k + 2K(n+m+d+5) \\ &\le d(n+m+1) + K\cdot \max_{k=1,\dots,K}\{I_k\}\cdot 10d(n+m+1) + 12Kd(n+m+1) \\ &\le 23K\cdot \max_{k=1,\dots,K}\{I_k\}\cdot d(n+m+1). \end{aligned} \tag{208}$$

Thus, the total number of elementary gates used is at most

$$\begin{aligned} & K\cdot 2N^2 + \sum_{k=1}^{K} 9915 I_k^3 d^4 (n+m+1)^4 + 2K + K\cdot 61(n+m+d+3)^2 + 2N^2 \\ &\quad + \sum_{k=1}^{K-1} 29[(n+m+d+2+k-1) + (n+m+d+2) + 1]^2 + 13(n+d+K+1+m+1)^3 \\ &\le 2\cdot 23^2 K^3 \max_{k=1,\dots,K}\{I_k\}^2 d^2 (n+m+1)^2 + 9915K \max_{k=1,\dots,K}\{I_k\}^3 d^4 (n+m+1)^4 + 2K \\ &\quad + 61\cdot 4^2 K d^2 (n+m+1)^2 + 2\cdot 23^2 K^2 \max_{k=1,\dots,K}\{I_k\}^2 d^2 (n+m+1)^2 \\ &\quad + 29K[3Kd(n+m+1) + 3d(n+m+1) + 1]^2 + 13(4Kd(n+m+1))^3 \\ &\le 2\cdot 23^2 K^3 \max_{k=1,\dots,K}\{I_k\}^2 d^2 (n+m+1)^2 + 9915K \max_{k=1,\dots,K}\{I_k\}^3 d^4 (n+m+1)^4 + 2K \\ &\quad + 61\cdot 4^2 K d^2 (n+m+1)^2 + 2\cdot 23^2 K^2 \max_{k=1,\dots,K}\{I_k\}^2 d^2 (n+m+1)^2 \\ &\quad + 29K[7Kd(n+m+1)]^2 + 13\cdot 4^3 K^3 d^3 (n+m+1)^3 \\ &\le (2\cdot 23^2 + 9915 + 2 + 61\cdot 4^2 + 2\cdot 23^2 + 29\cdot 7^2 + 13\cdot 4^3) K^3 \max_{k=1,\dots,K}\{I_k\}^3 d^4 (n+m+1)^4 \\ &= 15262 K^3 \max_{k=1,\dots,K}\{I_k\}^3 d^4 (n+m+1)^4. \end{aligned} \tag{209}$$

□

4 Error analysis

In this section, we provide the detailed error analysis of the steps of Algorithm 1 outlined in Section 2.4.1. We begin the error analysis with a few basic lemmas.

Lemma 4.1 (Lipschitz constant of CPWA functions) *Let $h:\mathbb{R}_+^d\to\mathbb{R}$ be a CPWA function given by* (8). *Let Assumption 2.4 hold with corresponding constant $C_2\in[1,\infty)$. Then, $h:\mathbb{R}_+^d\to\mathbb{R}$ is Lipschitz continuous with Lipschitz constant*

$$L := \sum_{k=1}^{K} \max_{1\le l\le I_k}\{\|\boldsymbol{a}_{k,l}\|_\infty\}\sqrt{d} \le C_2^2 d^{\frac{3}{2}}, \tag{210}$$

i.e.

$$\forall \boldsymbol{x},\boldsymbol{y}\in\mathbb{R}_+^d:\quad |h(\boldsymbol{x})-h(\boldsymbol{y})| \le C_2^2 d^{\frac{3}{2}}\|\boldsymbol{x}-\boldsymbol{y}\|_2. \tag{211}$$

Proof. Following the proof of Lemma 3.3 in [44], the CPWA function $h:\mathbb{R}_+^d\to\mathbb{R}$ admits the following representation:

$$h(\boldsymbol{x}) = \begin{cases} \boldsymbol{a}_1'\cdot\boldsymbol{x} + b_1', & \text{if } \boldsymbol{x}\in\Omega_1, \\ \quad\vdots & \\ \boldsymbol{a}_J'\cdot\boldsymbol{x} + b_J', & \text{if } \boldsymbol{x}\in\Omega_J, \end{cases} \tag{212}$$

where $J := \prod_{k=1}^{K} I_k \in\mathbb{N}$ and the coefficients $\{\boldsymbol{a}_j', b_j' : j=1,\dots,J\}$ are of the form

$$\boldsymbol{a}_j' := \sum_{k=1}^{K} \xi_k \boldsymbol{a}_{k,l_k^*}, \quad b_j' := \sum_{k=1}^{K} \xi_k b_{k,l_k^*}, \tag{213}$$

for some $l_k^*\in\{1,2,\dots,I_k\}$ (*the specific choice of index l_k^* can be found in the proof of Lemma 3.3 in [44]*), and where $\Omega_1,\dots,\Omega_J$ are polyhedrons whose union is $\mathbb{R}_+^d$. Note that some of these sets Ω_j can be empty. We claim that

$$\forall \boldsymbol{x},\boldsymbol{y}\in\mathbb{R}_+^d:\quad |h(\boldsymbol{x})-h(\boldsymbol{y})| \le \max_{1\le j\le J}\{\|\boldsymbol{a}_j'\|_\infty\}\cdot\sqrt{d}\|\boldsymbol{x}-\boldsymbol{y}\|_2. \tag{214}$$

Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}_+^d$ be fixed. Consider the line segment from $\boldsymbol{x}$ to $\boldsymbol{y}$ given by the set $\Gamma := \{\gamma(t) := \boldsymbol{x} + t(\boldsymbol{y} - \boldsymbol{x}) : t \in [0,1]\}$. If the line segment Γ lies entirely in one of polyhedron Ω_{j_*}, then by linearity of h in Ω_{j_*} and the Hölder's inequality, it follows that

$$|h(\boldsymbol{x}) - h(\boldsymbol{y})| = |\boldsymbol{a}'_{j_*} \cdot (\boldsymbol{x} - \boldsymbol{y})| \leq \|\boldsymbol{a}'_{j_*}\|_\infty \|\boldsymbol{x} - \boldsymbol{y}\|_1 \leq \max_{1 \leq j \leq J} \{\|\boldsymbol{a}'_j\|_\infty\} \cdot \sqrt{d} \|\boldsymbol{x} - \boldsymbol{y}\|_2.$$

In the general case, the line segment Γ may be contained in some $n \geq 2$ polyhedrons $\Omega_{j_1}, \dots, \Omega_{j_n}$, such that there are $n+1$ points $\{\gamma(t_0), \gamma(t_1), \dots, \gamma(t_n)\} \subset \Gamma$ with a partition $\{0 =: t_0 < t_1 < \cdots < t_n := 1\}$, satisfying $\gamma(t_m) \in \Omega_{j_m} \cap \Omega_{j_{m+1}}$ for $m = 1, \dots, n-1$. Again by the same argument, it holds for all $m = 1, \dots, n-1$ that

$$|h(\gamma(t_m)) - h(\gamma(t_{m-1}))| = |\boldsymbol{a}'_{j_m} \cdot (\gamma(t_m) - \gamma(t_{m-1}))| \leq \|\boldsymbol{a}'_{j_m}\|_\infty (t_m - t_{m-1}) \sqrt{d} \|\boldsymbol{x} - \boldsymbol{y}\|_2.$$

Hence, summing over m, we have

$$\begin{aligned} |h(\boldsymbol{x}) - h(\boldsymbol{y})| &\leq \sum_{m=1}^{n} \|\boldsymbol{a}'_{j_m}\|_\infty (t_j - t_{j-1}) \sqrt{d} \|\boldsymbol{x} - \boldsymbol{y}\|_2 \\ &\leq \max_{1 \leq j \leq J} \{\|\boldsymbol{a}'_j\|_\infty\} \cdot \sqrt{d} \|\boldsymbol{x} - \boldsymbol{y}\|_2. \end{aligned}$$

Thus, the claim (214) is proven. Next, by (213), it follows that

$$\max_{1 \leq j \leq J} \{\|\boldsymbol{a}'_j\|_\infty\} \leq \sum_{k=1}^{K} \max_{1 \leq l \leq I_k} \{\|\boldsymbol{a}_{k,l}\|_\infty\}. \tag{215}$$

This, (214) and Assumption 2.4 concludes the lemma. □

Lemma 4.2 (Linear growth of CPWA) *Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be a CPWA function given by (8). Let Assumption 2.4 hold with corresponding constant $C_2 \in [1, \infty)$. Then, for all $x \in \mathbb{R}_+^d$, it holds that*

$$|h(x)| \leq C_2^2 d^{\frac{3}{2}} (1 + \|x\|_2). \tag{216}$$

Proof. Note that Lemma 4.1 and an application of the triangle equality shows that

$$|h(x)| \leq |h(x) - h(0)| + |h(0)| \leq C_2^2 d^{\frac{3}{2}} \|x\|_2 + |h(0)|. \tag{217}$$

Moreover, by (8) and Assumption 2.4, we have for all $k = 1, \dots, K$ that

$$|h(0)| \leq K \cdot \max\{|b_{k,l}| : l = 1, \dots, I_k\} \leq C_2^2 d. \tag{218}$$

This and (217) implies (216). □

4.1 Step 1: Truncation error bounds

Lemma 4.3 *Let Y be a log-normal random variable with parameters $\mu \in \mathbb{R}$ and $\sigma^2 \in (0, \infty)$. Let Z be a standard normal random variable. Then it holds that*

(i) for all $k \in \mathbb{N}$,

$$\mathbb{E}[Y^k] = e^{k\mu + \frac{k^2 \sigma^2}{2}}, \tag{219}$$

(ii) for all $y \in [0, \infty)$ that

$$\mathbb{P}(Z \geq y) \leq \frac{1}{2} e^{-\frac{y^2}{2}}. \tag{220}$$

Proof. Item (i) is proven in [3, Chapter 2.3], and Item (ii) is proved in [16, Eq. 6]. □

Proposition 4.4 (Truncation error) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0, \infty)$, and $(t, x) \in [0, T) \times \mathbb{R}_+^d$. Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be a CPWA function given by (8). Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1, \infty)$. Let $p(\cdot, T; x, t) : \mathbb{R}_+^d \to \mathbb{R}_+$ be the log-normal transition density function given by (4). Let $M_{d,\varepsilon} \in [1, \infty)$ satisfy*

$$M_{d,\varepsilon} = 2 C_2^2 d^{\frac{5}{2}} \varepsilon^{-1} e^{4 C_1^2 T^2} e^{2rT} \max_{i=1,\dots,d} \{1, x_i^2\}. \tag{221}$$

Let $u : [0,T] \times \mathbb{R}_+^d \to \mathbb{R}$ be the option price given by

$$u(t,x) := e^{-r(T-t)} \int_{\mathbb{R}_+^d} h(y)p(y,T;x,t)dy, \tag{222}$$

and for every $M \geq M_{d,\varepsilon}$, let $\bar{u}_{M,t,x} \in \mathbb{R}$ be the truncated solution given by

$$\bar{u}_{M,t,x} := e^{-r(T-t)} \int_{[0,M]^d} h(y)p(y,T;x,t)dy. \tag{223}$$

Then, the truncation solution satisfies the following estimate

$$|u(t,x) - \bar{u}_{M,t,x}| \leq \varepsilon. \tag{224}$$

Proof. Let $\boldsymbol{\Sigma} \equiv \boldsymbol{\Sigma_d} := (T-t)\boldsymbol{C}_d \in \mathbb{R}^{d\times d}$, and $\boldsymbol{\mu} \equiv \boldsymbol{\mu_d} \in \mathbb{R}^d$ denote the log-covariance and log-mean parameters for the multivariate log-normal random variable $\boldsymbol{Y}$ with the probability density function $p(\cdot,T;x,t)$ given by Lemma 2.1. Using Lemma 4.2, (222), (223), the fact that $e^{-r(T-t)} \leq 1$, and Cauchy-Schwarz inequality,

$$\begin{aligned} |u(t,x) - \bar{u}_{M,t,x}| &= e^{-r(T-t)} \Big| \int_{\mathbb{R}_+^d} h(y)p(y,T;x,t)dy - \int_{[0,M]^d} h(y)p(y,T;x,t)dy \Big| \\ &\leq C_2^2 d^{\frac{3}{2}} \mathbb{E}[(1+\|\boldsymbol{Y}\|_2)^2]^{1/2} \mathbb{P}(\boldsymbol{Y} \notin [0,M]^d)^{1/2}, \end{aligned} \tag{225}$$

where

$$\mathbb{P}(\boldsymbol{Y} \notin [0,M]^d) = \int_{\mathbb{R}_+^d \setminus [0,M]^d} p(y,T;x,t)dy.$$

Let $\boldsymbol{X} = (X_1,\ldots,X_d) \sim \mathcal{N}(\boldsymbol{\mu},\boldsymbol{\Sigma})$ be the multivariate Gaussian random variable and recall that $X_i = \ln(Y_i)$ for $i = 1,\ldots,d$. Using Lemma 4.3 (i), we have

$$\mathbb{E}[\|\boldsymbol{Y}\|_2^2] = \sum_{i=1}^d \mathbb{E}[Y_i^2] = \sum_{i=1}^d \mathbb{E}[e^{2X_i}] = \sum_{i=1}^d e^{2\mu_i + 2\sigma_{ii}^2}, \tag{226}$$

where $\mu_i = \ln(x_i) + (r - \frac{1}{2}\sigma_{ii}^2)(T-t)$ and $\sigma_{ii} = \boldsymbol{\Sigma}_{i,i}$. We use the bound $e^{2\mu_i} \leq \max_{i=1,\ldots,d}\{1, x_i^2\} e^{2rT}$ and $e^{2\sigma_{ii}^2} \leq e^{2C_1^2T^2}$ by Assumption 2.2 and conclude that

$$\mathbb{E}[\|\boldsymbol{Y}\|_2^2] \leq d e^{2C_1^2T^2} e^{2rT} \max_{i=1,\ldots,d}\{1, x_i^2\}. \tag{227}$$

By Cauchy-Schwarz inequality, we have $(1+\|\boldsymbol{Y}\|_2)^2 \leq 2(1+\|\boldsymbol{Y}\|_2^2)$. Also, note that $\max_i\{1,x_i^2\}^{1/2} = \max_i\{1,|x_i|\}$ and $1 \leq d e^{2C_1^2T^2} e^{2rT} \max_i\{1,x_i^2\}$. Combining the above bounds, we arrive at

$$\mathbb{E}[(1+\|\boldsymbol{Y}\|_2)^2]^{1/2} \leq 2d^{1/2} e^{C_1^2T^2} e^{rT} \max_{i=1,\ldots,d}\{1,|x_i|\}. \tag{228}$$

Hence, we have

$$|u(t,x) - \bar{u}_{M,t,x}| \leq 2C_2^2 d^2 e^{C_1^2T^2} e^{rT} \max_{i=1,\ldots,d}\{1,|x_i|\} \cdot \mathbb{P}(\boldsymbol{Y} \notin [0,M]^d)^{1/2}. \tag{229}$$

Moreover, for all $i = 1,\ldots,d$, we have the inclusions

$$\{Y_i \leq M\} = \{X_i \leq \ln(M)\} \supseteq \{|X_i - \mu_i| \leq \ln(M) - \mu_i\}. \tag{230}$$

Note that since $M \geq M_{d,\varepsilon} \geq e^{\mu_i}$, we have that $\ln(M) \geq \mu_i$. By Sidak's correlation inequality [35, Corollary 1], we have

$$\mathbb{P}\Big(\bigcap_{i=1}^d \{|X_i - \mu_i| \leq \ln(M) - \mu_i\}\Big) \geq \prod_{i=1}^d \mathbb{P}(\{|X_i - \mu_i| \leq \ln(M) - \mu_i\}), \tag{231}$$

and hence,

$$\mathbb{P}(\boldsymbol{Y} \notin [0,M]^d) = 1 - \mathbb{P}\Big(\bigcap_{i=1}^d \{Y_i \leq M\}\Big) \leq 1 - \prod_{i=1}^d \mathbb{P}(\{|X_i - \mu_i| \leq \ln(M) - \mu_i\}). \tag{232}$$

Denote by Z the standard normal random variable. Using Lemma 4.3 (ii) and Assumption 2.2, we have

$$\mathbb{P}(\{|X_i - \mu_i| \leq \ln(M) - \mu_i\}) = 1 - 2\mathbb{P}(Z \geq \frac{\ln(M) - \mu_i}{\sigma_{ii}}) \geq 1 - e^{-\frac{(\ln(M)-\mu_i)^2}{2\sigma_{ii}^2}} \geq 1 - e^{-\frac{(\ln(M)-\mu_i)^2}{2C_1^2T^2}}. \tag{233}$$

Moreover, using $\ln(M) > 0$ and $M \geq M_{d,\varepsilon} \geq \max_{i=1,\dots,d}\{1, x_i^2\} e^{2rT} e^{4C_1^2T^2} \geq e^{2\mu_i} e^{4C_1^2T^2}$, we have

$$\begin{aligned}
&\ln(M) \geq 2\mu_i + 4C_1^2T^2 \\
&\iff (\ln(M))^2 \geq (2\mu_i + 4C_1^2T^2)\ln(M) \\
&\iff (\ln(M))^2 - 2\mu_i \ln(M) + \mu_i^2 \geq 4C_1^2T^2\ln(M) + \mu_i^2 \\
&\implies (\ln(M) - \mu_i)^2 \geq 4C_1^2T^2 \ln(M) \\
&\iff -\frac{(\ln(M)-\mu_i)^2}{2C_1^2T^2} \leq -2\ln(M) \\
&\iff e^{-\frac{(\ln(M)-\mu_i)^2}{2C_1^2T^2}} \leq M^{-2}.
\end{aligned} \tag{234}$$

Using Bernoulli's inequality, that is $(1+z)^d \geq 1 + dz$ for any $z \in [-1, \infty)$, and the fact that $-M^{-2} \in [-1, 0)$, we have

$$\mathbb{P}(\boldsymbol{Y} \notin [0, M]^d) \leq 1 - (1 - M^{-2})^d \leq dM^{-2}. \tag{235}$$

Thus, by (229), (235), and (221), we conclude that

$$|u(t,x) - \bar{u}_{M,t,x}| \leq 2C_2^2 d^{\frac{5}{2}} e^{C_1^2T^2} e^{rT} \max_{i=1,\dots,d}\{1, |x_i|\} M^{-1} \leq 2C_2^2 d^{\frac{5}{2}} e^{C_1^2T^2} e^{rT} \max_{i=1,\dots,d}\{1, |x_i|\} M_{d,\varepsilon}^{-1} \leq \varepsilon. \tag{236}$$

□

4.2 Step 2: Quadrature error bounds

Proposition 4.5 (Quadrature error) *Let $d \in \mathbb{N}$, $r, T \in (0, \infty)$, $n \in \mathbb{N} \cap \{2, 3, \dots\}$, $m \in \mathbb{N}$, and $(t, x) \in [0, T) \times \mathbb{R}_+^d$. Let $M \in [1, \infty)$ be defined by $M := 2^{n-1}$. Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be the CPWA function given by (8). Let Assumption 2.4 hold with corresponding constant $C_2 \in [1, \infty)$. Let $p(\cdot, T; x, t) : \mathbb{R}_+^d \to \mathbb{R}_+$ be the log-normal transition density given by (4). Let $\widetilde{u}_{n,t,x} \in \mathbb{R}$ be the truncated solution given by*

$$\widetilde{u}_{n,t,x} := e^{-r(T-t)} \int_{[0,M]^d} h(y) p(y, T; x, t) dy, \tag{237}$$

and let $\widetilde{u}_{n,m,t,x} \in \mathbb{R}$ be the truncated quadrature solution given by

$$\widetilde{u}_{n,m,t,x} := e^{-r(T-t)} \sum_{\boldsymbol{j} \in \mathbb{K}_{n,m,+}^d} h(\boldsymbol{j}) p_{\boldsymbol{j},m}, \tag{238}$$

where for $\boldsymbol{j} = (j_1, \dots, j_d) \in \mathbb{K}_{n,m,+}^d$ (c.f Definition 3.1),

$$p_{\boldsymbol{j},m} := \int_{Q_{\boldsymbol{j},m}} p(y, T; x, t) dy, \quad \textit{and} \quad Q_{\boldsymbol{j},m} := [j_1, j_1 + 2^{-m}) \times \dots \times [j_d, j_d + 2^{-m}). \tag{239}$$

Then,

$$|\widetilde{u}_{n,t,x} - \widetilde{u}_{n,m,t,x}| \leq C_2^2 d^2 2^{-m}. \tag{240}$$

Proof. Let $[\cdot]_m : \mathbb{R}_+^d \to (2^{-m}\mathbb{Z})^d$ be a function defined by

$$[y]_m = \left(\frac{\lfloor 2^m y_1 \rfloor}{2^m}, \dots, \frac{\lfloor 2^m y_d \rfloor}{2^m} \right), \tag{241}$$

where $\lfloor \cdot \rfloor$ is the floor function. With this function, it holds for every $\boldsymbol{j} \in \mathbb{K}_{n,m,+}^d$ that

$$\forall y \in Q_{\boldsymbol{j},m}, \quad [y]_m = \boldsymbol{j}. \tag{242}$$

Moreover, since

$$[0, M)^d = \bigsqcup_{\boldsymbol{j} \in \mathbb{K}_{n,m,+}^d} Q_{\boldsymbol{j},m} \tag{243}$$

is a disjoint union of sets, it follows that

$$\widetilde{u}_{n,m,t,x} = e^{-r(T-t)} \sum_{\boldsymbol{j} \in \mathbb{K}_{n,m,+}^d} \int_{Q_{\boldsymbol{j},m}} h([y]_m) p(y, T; x, t) dy = e^{-r(T-t)} \int_{[0,M]^d} h([y]_m) p(y, T; x, t) dy. \tag{244}$$

Furthermore, observe that

$$\forall y \in \mathbb{R}^d_+, \quad \|y - [y]_m\|_1 \le d2^{-m}. \tag{245}$$

Hence, by definition of $\widetilde{u}_{n,t,x}$ in (237), (244), by the fact that $e^{-r(T-t)} \le 1$, by the Lipschitz continuity of $h(\cdot)$ in Lemma 4.2, by Assumption 2.4, (245), and by the fact that $p(y,T;x,t)$ is a probability density function supported on $\mathbb{R}^d_+$, we conclude that

$$\begin{aligned} |\widetilde{u}_{n,t,x} - \widetilde{u}_{n,m,t,x}| &\le e^{-r(T-t)} \int_{[0,M]^d} |h(y) - h([y]_m)| p(y,T;x,t) dy \\ &\le \int_{[0,M]^d} C_2^2 d \|y - [y]_m\|_1 p(y,T;x,t) dy \\ &\le C_2^2 d^2 2^{-m}. \end{aligned} \tag{246}$$

□

Corollary 4.6 (Truncation and quadrature errors) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, and $(t,x) \in [0,T) \times \mathbb{R}^d_+$. Let $u(t,x)$ be the option price given by* (7)*. Let $h : \mathbb{R}^d_+ \to \mathbb{R}$ be the CPWA function given by* (8)*. Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1,\infty)$. For every $\eta \in (0,1)$, let $M_{d,\eta} \in [1,\infty)$ be given by* (221)*. For every $n, m \in \mathbb{N}$ satisfying*

$$n \ge 1 + \log_2(M_{d,\varepsilon/2}), \tag{247}$$

$$m \ge \log_2(C_2^2 d^2 (\varepsilon/2)^{-1}) \tag{248}$$

let $\widetilde{u}_{n,m,t,x}$ be the truncated quadrature solution given as in (238)*. Then*

$$|u(t,x) - \widetilde{u}_{n,m,t,x}| \le \varepsilon. \tag{249}$$

Proof. By (247), it holds that

$$M := 2^{n-1} \ge 2^{n_{d,\varepsilon}-1} \ge M_{d,\varepsilon/2}.$$

Let $\widetilde{u}_{n,t,x}$ be the truncated solution given by (237). By Proposition 4.4 (with $\varepsilon \leftarrow \varepsilon/2$ and $M \leftarrow 2^{n-1}$ in the notation of Proposition 4.4), it follows that

$$|u(t,x) - \widetilde{u}_{n,t,x}| \le \varepsilon/2. \tag{250}$$

Moreover, by (248), it holds that $C_2^2 d^2 2^{-m} \le \varepsilon/2$. Hence, by Proposition 4.5, it follows that

$$|\widetilde{u}_{n,t,x} - \widetilde{u}_{n,m,t,x}| \le \varepsilon/2. \tag{251}$$

Thus, (249) follows from triangle inequality. □

4.3 Step 3: Approximation error bounds for payoff function

Lemma 4.7 (Sublinear property of the max-function) *Let $\varepsilon > 0$, $n \in \mathbb{N}$, and let $(a_i)_{i=1}^n, (\tilde{a}_i)_{i=1}^n \subset \mathbb{R}$ satisfy for all $i = 1, \ldots, n$:*

$$|a_i - \tilde{a}_i| \le \varepsilon. \tag{252}$$

Then,

$$|\max_{i=1,\ldots,n}\{a_i\} - \max_{i=1,\ldots,n}\{\tilde{a}_i\}| \le \varepsilon. \tag{253}$$

Proof. Let $i \in \{1,\ldots,n\}$ be arbitrary. The fact that $\tilde{a}_i \le \max_{j=1,\ldots,n}\{\tilde{a}_j\}$ and (252) imply that

$$a_i - \max_{j=1,\ldots,n}\{\tilde{a}_j\} \le a_i - \tilde{a}_i \le |a_i - \tilde{a}_i| \le \varepsilon. \tag{254}$$

Since i was arbitrarily chosen, taking maximum over $i = 1, \ldots, n$ yields

$$\max_{i=1,\ldots,n}\{a_i\} - \max_{j=1,\ldots,n}\{\tilde{a}_j\} \le \varepsilon. \tag{255}$$

Repeating the argument by symmetry concludes (253). □

Proposition 4.8 (Approximating payoff function) *Let $d \in \mathbb{N}$, $r, T \in (0, \infty)$, $(t, x) \in [0, T) \times \mathbb{R}_+^d$, $n_1 \in \mathbb{N} \cap \{2, 3, \ldots\}$, and $m_1 \in \mathbb{N}_0$. Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be the CPWA function given by (8). i.e.*

$$h(\boldsymbol{x}) = \sum_{k=1}^{K} \xi_k \max\{\boldsymbol{a}_{k,l} \cdot \boldsymbol{x} + b_{k,l} : l = 1, \ldots, I_k\}.$$

Let Assumption 2.4 hold with corresponding constant $C_2 \in [1, \infty)$, and let $n_2 \in \mathbb{N} \cap \{2, 3, \ldots\}$ be defined by

$$n_2 := 1 + \lceil \log_2(C_2) \rceil. \tag{256}$$

For every $m_2 \in \mathbb{N}_0$ define the function $[\cdot]_{m_2} : \mathbb{R} \to 2^{-m_2}\mathbb{Z}$ by $[x]_{m_2} := \frac{\lfloor 2^{m_2} x \rfloor}{2^{m_2}}$, $x \in \mathbb{R}$. For every $m_2 \in \mathbb{N}_0$, $k = 1, \ldots, K$, and $l = 1, \ldots, I_k$, define $\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l} = (\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l,1}, \cdots, \widetilde{\boldsymbol{a}}_{n_2,m_2,k,l,d}) \in \mathbb{R}^d$ and $\widetilde{b}_{n_2,m_2,k,l} \in \mathbb{R}$ by

$$\begin{aligned} \widetilde{\boldsymbol{a}}_{n_2,m_2,k,l,i} &:= [(\boldsymbol{a}_{k,l})_i]_{m_2}, \quad i = 1, \ldots, d, \\ \widetilde{b}_{n_2,m_2,k,l} &:= [b_{k,l}]_{m_2}, \end{aligned} \tag{257}$$

and define the function $\widetilde{h}_{n_2,m_2} : \mathbb{R}^d \to \mathbb{R}$ by

$$\widetilde{h}_{n_2,m_2}(\boldsymbol{x}) := \sum_{k=1}^{K} \xi_k \max\{\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l} \cdot \boldsymbol{x} + \widetilde{b}_{n_2,m_2,k,l} : l = 1, \ldots, I_k\}. \tag{258}$$

Let $\widetilde{u}_{n_1,m_1,t,x} \in \mathbb{R}$ be the truncated quadrature solution given as in (238). i.e.

$$\widetilde{u}_{n_1,m_1,t,x} := e^{-r(T-t)} \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} h(\boldsymbol{j}) p_{\boldsymbol{j},m_1}.$$

For every $m_2 \in \mathbb{N}_0$ let $\widetilde{u}_{n_1,m_1,n_2,m_2,t,x} \in \mathbb{R}$ be the truncated quadrature solution with an approximated payoff function given by

$$\widetilde{u}_{n_1,m_1,n_2,m_2,t,x} := e^{-r(T-t)} \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{h}_{n_2,m_2}(\boldsymbol{j}) p_{\boldsymbol{j},m_1} \tag{259}$$

Then, for every $m_2 \in \mathbb{N}_0$ it holds that $(\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l}, \widetilde{b}_{n_2,m_2,k,l}) \in \mathbb{K}^{d+1}_{n_2,m_2}$ and that

$$|\widetilde{u}_{n_1,m_1,t,x} - \widetilde{u}_{n_1,m_1,n_2,m_2,t,x}| \leq C_2 d^2 2^{n_1 - m_2}. \tag{260}$$

Proof. By Assumption 2.4, it holds that

$$\forall k = 1, \ldots, K, \ \forall l = 1, \ldots, I_K, \ \forall i = 1, \ldots, d : \quad |(\boldsymbol{a}_{k,l})_i|, |b_{k,l}| \leq C_2. \tag{261}$$

Hence, by Definition 3.1, (257), and (258), it follows that $(\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l}, \widetilde{b}_{n_2,m_2,k,l}) \in \mathbb{K}^{d+1}_{n_2,m_2}$. Furthermore, observe that

$$\forall c > 0 : \quad |c - [c]_{m_2}| \leq 2^{-m_2}. \tag{262}$$

Hence, for all $k = 1, \ldots, K$, $l = 1, \ldots, I_k$, and $\boldsymbol{x} \in \mathbb{R}^d_+$, it follows that

$$|\boldsymbol{a}_{k,l} \cdot \boldsymbol{x} + b_{k,l} - (\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l} \cdot \boldsymbol{x} + \widetilde{b}_{n_2,m_2,k,l})| \leq (d+1) 2^{-m_2} \max\{1, \max\{(\boldsymbol{x})_i : i = 1, \ldots, d\}\}. \tag{263}$$

Moreover, since $\mathbb{K}_{n_1,m_1} \subset [-2^{n_1-1}, 2^{n_1-1}]$ (c.f. Definition 3.1), it follows for all $k = 1, \ldots, K$, $l = 1, \ldots, I_k$ that

$$\forall \boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+} : \quad |\boldsymbol{a}_{k,l} \cdot \boldsymbol{j} + b_{k,l} - (\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l} \cdot \boldsymbol{j} + \widetilde{b}_{n_2,m_2,k,l})| \leq (d+1) 2^{n_1-1} 2^{-m_2}. \tag{264}$$

Hence, by Lemma 4.7, it holds for all $k = 1, \ldots, K$ that

$$|\max\{\boldsymbol{a}_{k,l} \cdot \boldsymbol{j} + b_{k,l} : l = 1, \ldots, I_k\} - \max\{\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l} \cdot \boldsymbol{j} + \widetilde{b}_{n_2,m_2,k,l} : l = 1, \ldots, I_k\}| \leq (d+1) 2^{n_1-1} 2^{-m_2}. \tag{265}$$

Hence, by Assumption 2.4, it follows that

$$\forall \boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+} : \quad |h(\boldsymbol{j}) - \widetilde{h}_{n_2,m_2}(\boldsymbol{j})| \leq K(d+1) 2^{n_1-1} 2^{-m_2} \leq C_2 d^2 2^{n_1-m_2}. \tag{266}$$

Furthermore, since $e^{-r(T-t)} \leq 1$ and

$$0 < \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} p_{\boldsymbol{j},m_1} = \int_{[0,2^{n_1-1}]^d} p(y, T; x, t) dy \leq 1,$$

we conclude that

$$|\widetilde{u}_{n_1,m_1,t,x} - \widetilde{u}_{n_1,m_1,n_2,m_2,t,x}| \leq C_2 d^2 2^{n_1-m_2+1} e^{-r(T-t)} \cdot \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} p_{\boldsymbol{j},m_1} \leq C_2 d^2 2^{n_1-m_2}. \tag{267}$$

□

Corollary 4.9 (Truncation and quadrature with approximated payoff errors) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, and $(t,x) \in [0,T) \times \mathbb{R}_+^d$. Let $u(t,x)$ be the option price given by (7). Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be the CPWA function given by (8). Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1,\infty)$, and let $n_2 := 1 + \lceil \log_2(C_2) \rceil$. For every $\eta \in (0,1)$, let $M_{d,\eta} \in [1,\infty)$ be given by (221). For every $n_1, m_1, m_2 \in \mathbb{N}$ satisfying*

$$n_1 \geq 1 + \log_2(M_{d,\varepsilon/3}), \tag{268}$$

$$m_1 \geq \log_2(C_2^2 d^2 (\varepsilon/3)^{-1}), \tag{269}$$

$$m_2 \geq 1 + \log_2(M_{d,\varepsilon/3}) + \log_2(C_2 d^2 (\varepsilon/3)^{-1}), \tag{270}$$

let $\widetilde{u}_{n_1,m_1,n_2,m_2,t,x} \in \mathbb{R}$ be the truncated quadrature solution with an approximated payoff function be given by (259)*. Then we have that*

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,t,x}| \leq \varepsilon. \tag{271}$$

Proof. Let $\tilde{u}_{n_1,m_1,t,x}$ be the quadrature solution given by (238). By (268), (269), and Corollary 4.6 (with $\varepsilon \leftarrow 2\varepsilon/3$ in the notation of Corollary 4.6), it follows that

$$|u(t,x) - \widetilde{u}_{n_1,m_1,t,x}| \leq 2\varepsilon/3. \tag{272}$$

Moreover, by Proposition 4.8 (with $m_2 \leftarrow m_2$ in the notation of Proposition 4.8) and (270), it follows that

$$|\widetilde{u}_{n_1,m_1,t,x} - \widetilde{u}_{n_1,m_1,n_2,m_2,t,x}| \leq C_2 d^2 2^{n_1 - m_2} \leq \varepsilon/3. \tag{273}$$

Thus, the conclusion follows from the triangle inequality.

□

4.4 Step 4: Distribution loading error bounds

Proposition 4.10 (Distribution loading errors) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, and $(t,x) \in [0,T) \times \mathbb{R}_+^d$. Let $u(t,x)$ be the option price given by (7). Let $h : \mathbb{R}_+^d \to \mathbb{R}$ be the CPWA function given by (8). Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1,\infty)$, and let $n_2 := 1 + \lceil \log_2(C_2) \rceil$. For every $\eta \in (0,1)$, let $M_{d,\eta} \in [1,\infty)$ be given by (221) and for every $n_1, m_1 \in \mathbb{N}$ let $\{\widetilde{p}_{\boldsymbol{j},\eta} : \boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}\} \subset [0,1]$ satisfy*

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\eta} = 1 \tag{274}$$

and

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} |\widetilde{p}_{\boldsymbol{j},\eta} - \gamma^{-1} p_{\boldsymbol{j},m_1}| \leq \frac{\eta}{C_2^2 d^2 2^{n_1+1}}, \tag{275}$$

where for all $\boldsymbol{j} = (j_1, \ldots, j_d) \in \mathbb{K}^d_{n_1,m_1,+}$,

$$p_{\boldsymbol{j},m_1} := \int_{Q_{\boldsymbol{j},m_1}} p(y,T;x,t)dy, \quad Q_{\boldsymbol{j},m_1} := [j_1, j_1 + 2^{-m_1}) \times \cdots \times [j_d, j_d + 2^{-m_1}), \tag{276}$$

and

$$\gamma := \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} p_{\boldsymbol{j},m_1} \in (0,1). \tag{277}$$

Moreover, for every $n_1, m_1, m_2 \in \mathbb{N}$ satisfying

$$n_1 \geq 1 + \log_2(M_{d,\varepsilon/4}), \tag{278}$$

$$m_1 \geq \log_2(C_2^2 d^2 (\varepsilon/4)^{-1}), \tag{279}$$

$$m_2 \geq 1 + \log_2(M_{d,\varepsilon/4}) + \log_2(C_2 d^2 (\varepsilon/4)^{-1}), \tag{280}$$

let $\widetilde{h}_{n_2,m_2} : \mathbb{R}^d \to \mathbb{R}$ be given by (258), and let $\widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x} \in \mathbb{R}$ be the truncated quadrature solution with approximated payoff and loaded distribution given by

$$\widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x} := \gamma e^{-r(T-t)} \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/4} \widetilde{h}_{n_2,m_2}(\boldsymbol{j}), \tag{281}$$

Then,

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x}| \leq \varepsilon. \tag{282}$$

Proof. Let $\widetilde{u}_{n_1,m_1,n_2,m_2,t,x} \in \mathbb{R}$ be the quadrature solution with an approximated payoff function be given by (259). Note that by Corollary 4.9 (with $\varepsilon \leftarrow 3\varepsilon/4$ in the notation of Corollary 4.9), it holds that

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,t,x}| \leq 3\varepsilon/4. \tag{283}$$

Moreover, by Lemma 4.2 and (266), it holds for every $\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}$ that

$$\begin{aligned}
|\widetilde{h}_{n_2,m_2}(\boldsymbol{j})| &\leq |h(\boldsymbol{j}) - \widetilde{h}_{n_2,m_2}(\boldsymbol{j})| + |h(\boldsymbol{j})| \\
&\leq C_2 d^2 2^{n_1-m_2} + C_2^2 d(1 + \|\boldsymbol{j}\|_1) \\
&\leq C_2 d^2 2^{n_1-m_2} + C_2^2 d(1 + d2^{n_1-1}) \\
&\leq C_2 d^2 2^{n_1-m_2} + C_2^2 d^2 2^{n_1} \\
&\leq C_2^2 d^2 2^{n_1+1}.
\end{aligned} \tag{284}$$

Hence, by (259) and (281), using (275), the fact that $0 < \gamma, e^{-r(T-t)} \leq 1$, and the above estimate, we have

$$\begin{aligned}
|\widetilde{u}_{n_1,m_1,n_2,m_2,t,x} - \widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x}| &\leq \gamma e^{-r(T-t)} \cdot \max_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} |\widetilde{h}_{n_2,m_2}(\boldsymbol{j})| \cdot \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} |\widetilde{p}_{\boldsymbol{j},\varepsilon/4} - \gamma^{-1} p_{\boldsymbol{j},m_1}| \\
&\leq \varepsilon/4.
\end{aligned} \tag{285}$$

Thus, the conclusion follows from triangle inequality. □

4.5 Step 5: Rotation error bounds

Proposition 4.11 (Rotation error) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, and $(t,x) \in [0,T) \times \mathbb{R}^d_+$. Let $u(t,x)$ be the option price given by (7). Let $h : \mathbb{R}^d_+ \to \mathbb{R}$ be the CPWA function given by (8). Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1,\infty)$, and let $n_2 := 1 + \lceil \log_2(C_2) \rceil$. For every $\eta \in (0,1)$ let $M_{d,\eta} \in [1,\infty)$ be given by (221), for every $n_1, m_1, m_2 \in \mathbb{N}$ let $\{\widetilde{p}_{\boldsymbol{j},\eta} : \boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}\} \subset [0,1]$ satisfy*

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\eta} = 1 \tag{286}$$

and

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} |\widetilde{p}_{\boldsymbol{j},\eta} - \gamma^{-1} p_{\boldsymbol{j},m_1}| \leq \frac{\eta}{C_2^2 d^2 2^{n_1+1}}, \tag{287}$$

where for all $\boldsymbol{j} = (j_1, \ldots, j_d) \in \mathbb{K}^d_{n_1,m_1,+}$,

$$p_{\boldsymbol{j},m_1} := \int_{Q_{\boldsymbol{j},m_1}} p(y,T;x,t)dy, \quad Q_{\boldsymbol{j},m_1} := [j_1, j_1 + 2^{-m_1}) \times \cdots \times [j_d, j_d + 2^{-m_1}), \tag{288}$$

and

$$\gamma := \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} p_{\boldsymbol{j},m_1} \in (0,1), \tag{289}$$

let $\mathfrak{s}_{d,\eta} \in (0,\infty)$ be defined by

$$\mathfrak{s}_{d,\eta} := \sqrt{\frac{\eta}{(C_2^2 d^2 2^{n_1+1})^3}}, \tag{290}$$

let $\widetilde{h}_{n_2,m_2} : \mathbb{R}^d \to \mathbb{R}$ be given by (258), and let $a_{n_1,n_2,m_1,m_2,\eta} \in [0,1]$ be the amplitude given by

$$a_{n_1,n_2,m_1,m_2,\eta} = \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\eta} \sin^2\left(\frac{\mathfrak{s}_{d,\eta} \widetilde{h}_{n_2,m_2}(\boldsymbol{j})}{2} + \frac{\pi}{4}\right). \tag{291}$$

Moreover, for every $n_1, m_1, m_2 \in \mathbb{N}$ satisfying

$$n_1 \geq 1 + \log_2(M_{d,\varepsilon/5}), \tag{292}$$

$$m_1 \geq \log_2(C_2^2 d^2 (\varepsilon/5)^{-1}), \tag{293}$$

$$m_2 \geq 1 + \log_2(M_{d,\varepsilon/5}) + \log_2(C_2 d^2 (\varepsilon/5)^{-1}), \tag{294}$$

let $\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} \in \mathbb{R}$ be the truncated quadrature solution with approximated payoff and loaded distribution with rotation given by

$$\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} := \mathfrak{s}^{-1} \gamma e^{-r(T-t)} (2a - 1), \tag{295}$$

where here

$$\mathfrak{s} := \mathfrak{s}_{d,\varepsilon/5}, \qquad \textit{and} \qquad a =: a_{n_1,n_2,m_1,m_2,\varepsilon/5}.$$

Then, the following holds:

(i)

$$\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} = \mathfrak{s}^{-1}\gamma e^{-r(T-t)} \sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5} \sin\Big(\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})\Big). \tag{296}$$

(ii)

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x}| \leq \varepsilon. \tag{297}$$

Proof. First, recall the trigonometric identity that for all $x \in \mathbb{R}$

$$\sin^2(\frac{x}{2}+\frac{\pi}{4}) = 1-\cos^2(\frac{x}{2}+\frac{\pi}{4}) = 1-\frac{1}{2}(1+\cos(x+\pi/2)) = \frac{1}{2}+\frac{1}{2}\sin(x). \tag{298}$$

This, (291),(295), and the fact that $\sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5} = 1$ imply that

$$\begin{aligned}
\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} &= \mathfrak{s}^{-1}\gamma e^{-r(T-t)} \sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5}\Big[2\sin^2\Big(\frac{\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})}{2}+\frac{\pi}{4}\Big)-1\Big] \\
&= \mathfrak{s}^{-1}\gamma e^{-r(T-t)} \sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5} \sin\Big(\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})\Big),
\end{aligned}$$

which proves Item (i). Next, for the proof of Item (ii), note that by Taylor expansion, one has for any $x \in [-1,1]$ the estimate

$$|\sin(x)-x| \leq \Big(\tfrac{|x|^3}{3!}+\tfrac{|x|^5}{5!}+\tfrac{|x|^7}{7!}+\cdots\Big) \leq |x|^3\big(e-[1+\tfrac{1}{1!}+\tfrac{1}{2!}]\big) \leq |x|^3. \tag{299}$$

Moreover, since $|\widetilde{h}_{n_2,m_2}(\boldsymbol{j})| \leq C_2^2 d^2 2^{n_1+1}$ (c.f. (284)), by (290), it holds for all $\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}$ that

$$|\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})| \leq \sqrt{\varepsilon/5} \leq 1. \tag{300}$$

This, (299), (290), and the fact that $|\widetilde{h}_{n_2,m_2}(\boldsymbol{j})| \leq C_2^2 d^2 2^{n_1+1}$ hence ensure for all $\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}$ that

$$\mathfrak{s}^{-1}\big|\sin\Big(\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})\Big)-\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})\big| \leq \mathfrak{s}^{-1}|\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})|^3 = \mathfrak{s}^2|\widetilde{h}_{n_2,m_2}(\boldsymbol{j})|^3 \leq \varepsilon/5. \tag{301}$$

Let here $\widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x} \in \mathbb{R}$ be the truncated quadrature solution with approximated payoff and loaded distribution given by

$$\widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x} := \gamma e^{-r(T-t)} \sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5}\widetilde{h}_{n_2,m_2}(\boldsymbol{j}).$$

This, (301), (296), and the fact that

$$0 < \gamma e^{-r(T-t)} \sum_{\boldsymbol{j}\in\mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/5} \leq 1$$

imply that

$$|\widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x} - \widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x}| \leq \varepsilon/5. \tag{302}$$

Furthermore, by Proposition (4.10) (with $\varepsilon \leftarrow 4\varepsilon/5$ in the notation of Proposition (4.10)), it holds that

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,p,t,x}| \leq 4\varepsilon/5. \tag{303}$$

Hence, the conclusion follows from the triangle inequality. □

4.6 Step 6: Quantum amplitude estimation error bounds

Proposition 4.12 (Combined errors) *Let $\varepsilon \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, and $(t,x) \in [0,T) \times \mathbb{R}^d_+$. Let $u(t,x)$ be the option price given by (7). Let $h : \mathbb{R}^d_+ \to \mathbb{R}$ be the CPWA function given by (8). Let Assumption 2.2 and Assumption 2.4 hold with respective constants $C_1, C_2 \in [1,\infty)$, and let*

$$n_2 := 1 + \lceil \log_2(C_2) \rceil \tag{304}$$

For every $\eta \in (0,1)$, let $M_{d,\eta} \in [1,\infty)$ be given by (221). Let $n_{1,d,\varepsilon}, m_{1,d,\varepsilon}, m_{2,d,\varepsilon} \in (0,\infty)$ be defined by

$$n_{1,d,\varepsilon} := 1 + \log_2(M_{d,\varepsilon/6}), \tag{305}$$

$$m_{1,d,\varepsilon} := \log_2(C_2^2 d^2 (\varepsilon/6)^{-1}), \tag{306}$$

$$m_{2,d,\varepsilon} := 1 + \log_2(M_{d,\varepsilon/6}) + \log_2(C_2 d^2 (\varepsilon/6)^{-1}). \tag{307}$$

Moreover, for every $n_1, m_1, m_2 \in \mathbb{N}$ satisfying $n_1 \geq n_{1,d,\varepsilon}$, $m_1 \geq m_{1,d,\varepsilon}$, and $m_2 \geq m_{2,d,\varepsilon}$, let $\{\widetilde{p}_{\boldsymbol{j},\varepsilon/6} : \boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}\} \subset [0,1]$ satisfy

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/6} = 1 \tag{308}$$

and

$$\sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} |\widetilde{p}_{\boldsymbol{j},\varepsilon/6} - \gamma^{-1} p_{\boldsymbol{j},m_1}| \leq \frac{\varepsilon}{6 C_2^2 d^2 2^{n_1+1}}, \tag{309}$$

where for all $\boldsymbol{j} = (j_1, \ldots, j_d) \in \mathbb{K}^d_{n_1,m_1,+}$,

$$p_{\boldsymbol{j},m_1} := \int_{Q_{\boldsymbol{j},m_1}} p(y,T;x,t)dy, \quad Q_{\boldsymbol{j},m_1} := [j_1, j_1 + 2^{-m_1}) \times \cdots \times [j_d, j_d + 2^{-m_1}), \tag{310}$$

and

$$\gamma := \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} p_{\boldsymbol{j},m_1} \in (0,1), \tag{311}$$

let $\mathfrak{s} \equiv \mathfrak{s}_{d,\varepsilon/6} \in (0,\infty)$ be defined by

$$\mathfrak{s} \equiv \mathfrak{s}_{d,\varepsilon/6} := \sqrt{\frac{\varepsilon/6}{(C_2^2 d^2 2^{n_1+1})^3}}, \tag{312}$$

let $\tilde{h}_{n_2,m_2} : \mathbb{R}^d \to \mathbb{R}$ be given by (258), let $a \equiv a_{n_1,n_2,m_1,m_2,\varepsilon/6} \in [0,1]$ be the amplitude given by

$$a \equiv a_{n_1,n_2,m_1,m_2,\mathfrak{s},\varepsilon/6} := \sum_{\boldsymbol{j} \in \mathbb{K}^d_{n_1,m_1,+}} \widetilde{p}_{\boldsymbol{j},\varepsilon/6} \sin^2\left(\frac{\mathfrak{s}\widetilde{h}_{n_2,m_2}(\boldsymbol{j})}{2} + \frac{\pi}{4}\right), \tag{313}$$

let $\hat{a} \in [0,1]$ satisfy

$$|a - \hat{a}| \leq \frac{\varepsilon \mathfrak{s}}{12}, \tag{314}$$

and let $\widetilde{U}_{t,x}$ be the approximated solution given by

$$\widetilde{U}_{t,x} := \mathfrak{s}^{-1} \gamma e^{-r(T-t)} (2\hat{a} - 1). \tag{315}$$

Then,

$$|u(t,x) - \widetilde{U}_{t,x}| \leq \varepsilon. \tag{316}$$

Proof. Let here $\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} \in \mathbb{R}$ be the truncated quadrature solution with approximated payoff and loaded distribution with rotation given by

$$\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} := \mathfrak{s}^{-1} \gamma e^{-r(T-t)} (2a - 1).$$

By Proposition 4.11 item (ii) (with $\varepsilon \leftarrow 5\varepsilon/6$ in the notation of Proposition 4.11), it holds that

$$|u(t,x) - \widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x}| \leq 5\varepsilon/6. \tag{317}$$

Using $0 < \gamma e^{-r(T-t)} \leq 1$ and (314), it follows that

$$|\widetilde{u}_{n_1,m_1,n_2,m_2,p,a,t,x} - \widetilde{U}_{t,x}| \leq 2\mathfrak{s}^{-1}|a - \hat{a}| \leq \varepsilon/6. \tag{318}$$

Hence, we conclude (316). ☐

5 Quantum Algorithm 1 and Proof of Theorem 2.22

In this section, we present Algorithm 1 outlined in Section 2.4.1 and provide the proof of Theorem 2.22.

Algorithm 1: Quantum algorithm for pricing European options with CPWA payoffs

Input: $\varepsilon \in (0,1)$, $\alpha \in (0,1)$, $d \in \mathbb{N}$, $r, T \in (0,\infty)$, $(t,x) \in [0,T) \times \mathbb{R}_+^d$, covariance matrix $\boldsymbol{C}_d \in \mathbb{R}^{d\times d}$, and CPWA function

$$\mathbb{R}_+^d \ni x \mapsto h(x) = \sum_{k=1}^{K} \xi_k \max\{\boldsymbol{a}_{k,l} \cdot \boldsymbol{x} + b_{k,l} : l = 1, \dots, I_k\} \in \mathbb{R}$$

Output: $\widetilde{U}_{t,x} \in \mathbb{R}$

1 Set $C_1, C_2, C_3 \in [1,\infty)$ to be the constants given by Assumption 2.2, Assumption 2.4, and Assumption 3.16, respectively.

2 Set

$$n_1 := \lceil n_{1,d,\varepsilon} \rceil, \quad n_2 := 1 + \lceil \log_2(C_2) \rceil, \quad m_1 := \lceil m_{1,d,\varepsilon} \rceil, \quad m_2 := \lceil m_{2,d,\varepsilon} \rceil,$$

where $n_{1,d,\varepsilon}, m_{1,d,\varepsilon}, m_{2,d,\varepsilon}$ are defined in (305)-(307) in Proposition 4.12.

3 Set

$$N = (192), \quad \gamma = (311), \quad \mathfrak{s} = (312), \quad \text{and} \quad \widetilde{\boldsymbol{a}}_{n_2,m_2,k,l}, \, \widetilde{b}_{n_2,m_2,k,l} = (257) \ \text{ for } \ k = 1, \dots K, \ l = 1, \dots I_k.$$

4 Construct probability distribution quantum circuit $\mathcal{P} \equiv \mathcal{P}_{d,\varepsilon}$ using Assumption 3.16 (with $n \leftarrow n_1$, $m \leftarrow m_1$, $\varepsilon \leftarrow \frac{\varepsilon}{6C_2^2 d^2 2^{n_1+1}}$ in the notation of Assumption 3.16).

5 Construct CPWA payoff with rotation quantum circuit $\mathcal{R}_h$ given by Proposition 3.22 (with $s \leftarrow \mathfrak{s}$, $a_{k,l,j} \leftarrow \mathrm{E}_{n_2,m_2}(\widetilde{\boldsymbol{a}}_{n_2,m_2,k,l,j})$, $b_{k,l} \leftarrow \mathrm{E}_{n_2,m_2}(\widetilde{b}_{n_2,m_2,k,l})$ for $k = 1, \dots, K$, $l = 1, \dots, I_k$, $j = 1, \dots, d$ in the notation of Proposition 3.22).

6 Construct the quantum circuit $\mathcal{A} = \mathcal{R}_h(\mathcal{P} \otimes I_2^{\otimes(N-d(n_1+m_1))})$ using the quantum circuits $\mathcal{R}_h$ and $\mathcal{P}$.

7 Set $\widehat{a} = \frac{a_u - a_l}{2}$ using the output $[a_l, a_u]$ from the modified iterative quantum amplitude estimation algorithm [27, Algorithm 1 Modified IQAE] (with $\varepsilon \leftarrow \frac{\varepsilon\mathfrak{s}}{12}$, $\alpha \leftarrow \alpha$, $N_{\text{shots}} \leftarrow 1$, and $\mathcal{A} \leftarrow \mathcal{A}$ in the notation of [27, Algorithm 1]).

8 Return $\widetilde{U}_{t,x} := \mathfrak{s}^{-1}\gamma e^{-r(T-t)}(2\hat{a} - 1)$.

Proof of Theorem 2.22. First, let $n_1, n_2, m_1, m_2, N, \gamma, \mathfrak{s}$ be defined as in line 2–3 of Algorithm 1, and set $n := n_1 + n_2$ and $m := m_1 + m_2$. Let $\boldsymbol{h} : \mathbb{F}_{n_1,m_1}^d \to \mathbb{F}_{n+d+K+1+m}$ be defined as in (190), and let $p := d(2n_2 + 2m_2 + 3)$ and $N, \{q_k\}_{k=1}^K \in \mathbb{N}$ be given by (192) from Proposition 3.22. By Assumption 3.16, it holds that

$$\mathcal{P} |0\rangle_{d(n_1+m_1)} = \sum_{\boldsymbol{i} \in \mathbb{F}_{n_1,m_1,+}^d} \sqrt{\widetilde{p}_i}\, |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1}. \tag{319}$$

Hence, together with Proposition 3.22, the circuit $\mathcal{A} := \mathcal{R}_h(\mathcal{P} \otimes I_2^{\otimes(N-d(n_1+m_1))})$ satisfies

$$\begin{aligned}
\mathcal{A} |0\rangle_N &= \sum_{\boldsymbol{i} \in \mathbb{F}_{n_1,m_1,+}^d} \sqrt{\widetilde{p}_i}\, |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |\text{anc}\rangle_{q_1+\cdots+q_K+2K(n+m+d+5)-1} \left[\cos\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big) |0\rangle + \sin\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big) |1\rangle\right] \\
&= \sum_{\boldsymbol{i} \in \mathbb{F}_{n_1,m_1,+}^d} \sqrt{\widetilde{p}_i} \cos\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big) |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |\text{anc}\rangle_{q_1+\cdots+q_K+2K(n+m+d+5)-1} |0\rangle \\
&\quad + \sum_{\boldsymbol{i} \in \mathbb{F}_{n_1,m_1,+}^d} \sqrt{\widetilde{p}_i} \sin\big(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2\big) |i_1\rangle_{n_1+m_1} \cdots |i_d\rangle_{n_1+m_1} |\text{anc}\rangle_{q_1+\cdots+q_K+2K(n+m+d+5)-1} |1\rangle \\
&=: \sqrt{1-a}\, |\psi_0\rangle_{N-1} |0\rangle + \sqrt{a}\, |\psi_1\rangle_{N-1} |1\rangle,
\end{aligned} \tag{320}$$

where as in Proposition 3.22, $\bar{f} : \mathbb{F}_{n+d+K+1,m} \to \mathbb{R}$ is defined by $\bar{f}(i) = f \circ \mathrm{D}_{n+d+K+1,m}(i)$ and $f(x) = \mathfrak{s}x + \frac{\pi}{2}$, and $a \in [0,1]$ is given by

$$a := \sum_{\boldsymbol{i} \in \mathbb{F}_{n_1,m_1,+}^d} \widetilde{p}_i \sin^2(\bar{f}(\boldsymbol{h}(\boldsymbol{i}))/2). \tag{321}$$

By Proposition 3.22 and Proposition 4.8, we note that the function $\widetilde{h}_{n_2,m_2}$ given in (258) coincides with the function $\mathrm{D}_{n+d+K+1,m}(\boldsymbol{h})$ when restricted to the domain $\mathbb{F}_{n_1,m_1}^d$. Using this and Proposition 4.12 (with $\varepsilon \leftarrow$

$\frac{\varepsilon}{6C_2^2 d^2 2^{n_1+1}}$ in the notation of Assumption 3.16), we have

$$a = \sum_{\boldsymbol{i} \in \mathbb{F}^d_{n_1,m_1,+}} \widetilde{p}_i \sin^2\left(\frac{\mathfrak{s}\mathrm{D}_{n+d+K+1,m}(\boldsymbol{h}(\boldsymbol{i}))}{2} + \frac{\pi}{4}\right) = a_{n_1,n_2,m_1,m_2,\mathfrak{s},\varepsilon/6}, \tag{322}$$

where $a_{n_1,n_2,m_1,m_2,\mathfrak{s},\varepsilon/6}$ is defined in (313). By Proposition 2.20, the output $\widehat{a}$ from line 7 of Algorithm 1 satisfies the bound

$$|a - \widehat{a}| \le \varepsilon\mathfrak{s}/12, \quad \text{with probability at least } 1-\alpha. \tag{323}$$

Thus, the estimate (57) follows from Proposition 4.12. Next, we count the total number of qubits and elementary gates used to construct circuit $\mathcal{A}$. Let $M_{d,\varepsilon/6}$ be the constant given by (221), and note that

$$M_{d,\varepsilon/6} = 6\mathfrak{c}d^{\frac{5}{2}}\varepsilon^{-1}. \tag{324}$$

Moreover, recall that for any $v \in \mathbb{R}$, one has $\lceil v \rceil \le v+1$. Hence, by (305)-(307) and the bound on $M_{d,\varepsilon/6}$, we have the following bounds

$$n_1 = \lceil n_{1,d,\varepsilon} \rceil \le 2 + \log_2(M_{d,\varepsilon/6}) = 2 + \log_2(2 \cdot 3\mathfrak{c}d^{\frac{5}{2}}\varepsilon^{-1}), \tag{325}$$

$$n_2 \le 2 + \log_2(C_2) \le 2 + \log_2(\mathfrak{c}^{\frac{1}{2}}), \tag{326}$$

$$m_1 = \lceil m_{1,d,\varepsilon} \rceil \le 1 + \log_2(C_2^2 d^2 (\varepsilon/6)^{-1}) \le 1 + \log_2(2 \cdot 3\mathfrak{c}d^2\varepsilon^{-1}), \tag{327}$$

$$m_2 = \lceil m_{2,d,\varepsilon} \rceil \le 2 + \log_2(M_{d,\varepsilon/6}) + \log_2(C_2 d^2 (\varepsilon/6)^{-1}) \le 2 + \log_2(2^2 3^2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{9}{2}} \varepsilon^{-2}). \tag{328}$$

Furthermore,

$$n+m+1 = n_1+n_2+m_1+m_2+1 \le 8 + \log_2(2^4 3^4 \mathfrak{c}^4 d^9 \varepsilon^{-4}) = \log_2(2^7 3^4 \mathfrak{c}^4 d^9 \varepsilon^{-4}). \tag{329}$$

By Proposition 3.22 and the fact that $\mathcal{A} = \mathcal{R}_h(\mathcal{P} \otimes I_2^{\otimes N - d(n_1+m_1)})$, the quantum circuit $\mathcal{A}$ uses N qubits, where N is given by (192). Using the upper bound (208) for N, Assumption 2.4, and (329), we thus have the following bound on the number of qubits used for the circuit $\mathcal{A}$

$$\begin{aligned} N &\le 23K \cdot \max_{k=1,\dots,K} I_k \cdot d(n+m+1) \\ &\le 23C_2 d^2 (n+m+1) \\ &\le 23C_2 d^2 \log_2(2^7 3^4 \mathfrak{c}^4 d^9 \varepsilon^{-4}) \\ &\le 23C_2 d^2 (\log_2(2^7 3^4 \mathfrak{c}^4) + 9\log_2(d\varepsilon^{-1})) \\ &\le 23C_2 d^2 (\log_2(2^7 3^4 \mathfrak{c}^4) + 9)(1 + \log_2(d\varepsilon^{-1})) \\ &= 23C_2 \log_2(2^{16} 3^4 \mathfrak{c}^4) d^2 (1 + \log_2(d\varepsilon^{-1})) \\ &\le \mathfrak{C} d^2 (1 + \log_2(d\varepsilon^{-1})). \end{aligned} \tag{330}$$

Next, we count the number of elementary gates used to construct the quantum circuit $\mathcal{A}$, which will be denoted by $N_{\mathcal{A}}$. By Assumption 3.16, the number of elementary gates used to construct $\mathcal{P}$ is at most (117) with ($n \leftarrow n_1$, $m \leftarrow m_1$, $\varepsilon \leftarrow \frac{\varepsilon}{6C_2^2 d^2 2^{n_1+1}}$ in the notation of Assumption 3.16). Hence, using (325) and (327), the number of elementary gates used to construct $\mathcal{P}$ is bounded by

$$\begin{aligned} & C_3 (n_1+m_1)^{C_3} d^{C_3} (\log_2(6\varepsilon^{-1} C_2^2 d^2 2^{n_1+1}))^{C_3} \\ &= C_3 (n_1+m_1)^{C_3} d^{C_3} (\log_2(6C_2^2 d^2 \varepsilon^{-1}) + n_1 + 1))^{C_3} \\ &\le C_3 (3 + \log_2(2^2 3^2 \mathfrak{c}^2 d^{\frac{9}{2}} \varepsilon^{-2}))^{C_3} d^{C_3} (\log_2(2 \cdot 3\mathfrak{c}d^2\varepsilon^{-1}) + 3 + \log_2(2 \cdot 3\mathfrak{c}d^{\frac{5}{2}}\varepsilon^{-1}))^{C_3} \\ &= C_3 d^{C_3} (\log_2(2^5 3^2 \mathfrak{c}^2 d^{\frac{9}{2}} \varepsilon^{-2}))^{2C_3} \\ &\le C_3 d^{C_3} (\log_2(2^5 3^2 \mathfrak{c}^2) + 5\log_2(d\varepsilon^{-1}))^{2C_3} \\ &\le C_3 d^{C_3} (\log_2(2^5 3^2 \mathfrak{c}^2) + 5)^{2C_3} (1 + \log_2(d\varepsilon^{-1}))^{2C_3} \\ &= C_3 (\log_2(2^{10} 3^2 \mathfrak{c}^2))^{2C_3} d^{C_3} (1 + \log_2(d\varepsilon^{-1}))^{2C_3}. \end{aligned} \tag{331}$$

As in (330), by Proposition 3.22, Assumption (2.4), and (329), the number of elementary gates used to construct

$\mathcal{R}_h$ is at most

$$\begin{aligned} & 15262K^3 \max\{I_1,\dots,I_k\}^3 d^4 (n+m+1)^4 \\ & \leq 15262(C_2 d)^3 d^4 (\log_2(2^7 3^4 \mathfrak{c}^4 d^9 \varepsilon^{-4}))^4 \\ & \leq 15262 C_2^3 d^7 (\log_2(2^7 3^4 \mathfrak{c}^4) + 9\log_2(d\varepsilon^{-1}))^4 \\ & \leq 15262 C_2^3 d^7 (\log_2(2^7 3^4 \mathfrak{c}^4) + 9)^4 (1+\log_2(d\varepsilon^{-1}))^4 \\ & = 15262 C_2^3 (\log_2(2^{16} 3^4 \mathfrak{c}^4)^4 d^7 (1+\log_2(d\varepsilon^{-1}))^4. \end{aligned} \tag{332}$$

Hence, by (331) and (332), the number of elementary gates used to construct quantum circuit $\mathcal{A}$ is at most

$$\begin{aligned} N_{\mathcal{A}} & \leq C_3(\log_2(2^{10}3^2\mathfrak{c}^2))^{2C_3} d^{C_3}(1+\log_2(d\varepsilon^{-1}))^{2C_3} + 15262 C_2^3(\log_2(2^{16}3^4\mathfrak{c}^4)^4 d^7(\log_2(1+d\varepsilon^{-1}))^4 \\ & \leq 2\cdot 15262 C_2^3 C_3 (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{7,C_3\}}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}}. \end{aligned} \tag{333}$$

Next, we count the number of elementary gates used in line 7 of Algorithm 1, which by Remark 2.21 Item 2. coincides with the number of elementary gates used to construct the quantum circuit $\mathcal{Q}^{k_t}\mathcal{A}$ in the Modified IQAE algorithm. Note that this number is also the number of elementary gates used in Algorithm 1. Using (312) and (325), the number $\mathfrak{s}^{-1}$ is bounded by

$$\begin{aligned} \mathfrak{s}^{-1} & = \left(6\varepsilon^{-1}(C_2^2 d^2 2^{n_1+1})^3\right)^{\frac{1}{2}} \\ & \leq \sqrt{6}\varepsilon^{-\frac{1}{2}} C_2 d (2^{3+\log_2(6\mathfrak{c}d^{\frac{5}{2}}\varepsilon^{-1})})^{3/2} \\ & = \sqrt{6}\varepsilon^{-\frac{1}{2}} C_2 d 2^{\frac{9}{2}} (6\mathfrak{c}d^{\frac{5}{2}}\varepsilon^{-1})^{\frac{3}{2}} \\ & = 2^{\frac{13}{2}} 3^2 C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-2}. \end{aligned} \tag{334}$$

Thus, by using Proposition 2.20 Item 3. (with $\mathcal{A} \leftarrow \mathcal{A}$, $\varepsilon \leftarrow \varepsilon\mathfrak{s}/12$, $n \leftarrow N-1$, and $N \leftarrow N_{\mathcal{A}}$ in the Notation of Proposition 2.20) together with (330) and (333), we conclude that the number of elementary gates used in Algorithm 1 is bounded by

$$\begin{aligned} & \frac{\pi}{4\frac{\varepsilon\mathfrak{s}}{12}}(8N^2+23+N_{\mathcal{A}}) \\ & \leq 2^{\frac{13}{2}} 3^3 \pi C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-3}\big[23 + 8(23C_2\log_2(2^{16}3^4\mathfrak{c}^4) d^2(1+\log_2(d\varepsilon^{-1})))^2 \\ & \qquad + 2\cdot 15262 C_2^3 C_3(\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{7,C_3\}}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}}\big] \\ & \leq 2^{\frac{13}{2}} 3^3 \pi C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-3}\big[23 + 8(23C_2)^2 + 2\cdot 15262 C_2^3 C_3\big] \\ & \qquad \cdot (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{7,C_3\}}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}} \\ & \leq 2^{\frac{13}{2}} 3^3 2^2 C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-3} \cdot 34779 C_2^3 C_3 \\ & \qquad \cdot (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{7,C_3\}}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}} \\ & \leq 2^{\frac{13}{2}} 3^3 2^2 C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-3} 2^{16} C_2^3 C_3 (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{7,C_3\}}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}} \\ & \leq 2^{25} 3^3 C_2^4 C_3 \mathfrak{c}^{\frac{3}{2}} (\log_2(2^{16}3^4\mathfrak{c}^4))^{\max\{4,2C_3\}} d^{\max\{12,5+C_3\}} \varepsilon^{-3}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}} \\ & = \mathfrak{C} d^{\max\{12,5+C_3\}} \varepsilon^{-3}(1+\log_2(d\varepsilon^{-1}))^{\max\{4,2C_3\}}. \end{aligned} \tag{335}$$

Lastly, we count the number of applications on $\mathcal{A}$. Using (47) (with $\varepsilon \leftarrow \varepsilon\mathfrak{s}/12$ and $\alpha \leftarrow \alpha$ in the notation Proposition 2.20) and bound for $\mathfrak{s}^{-1}$ (c.f. (334)), the number of applications on $\mathcal{A}$ is at most

$$\tfrac{62\cdot 12}{\varepsilon\mathfrak{s}} \ln\left(\tfrac{21}{\alpha}\right) \leq 62\cdot 12\cdot 2^{\frac{13}{2}} 3^2 C_2 \mathfrak{c}^{\frac{3}{2}} d^{\frac{19}{4}} \varepsilon^{-3} \ln\left(\tfrac{21}{\alpha}\right) \leq \mathfrak{C} d^5 \varepsilon^{-3} \ln\left(\tfrac{21}{\alpha}\right). \tag{336}$$

□

Acknowledgment

Financial support by the Nanyang Assistant Professorship Grant (NAP Grant) *Machine Learning based Algorithms in Finance and Insurance* and the grant NRF2021-QEP2-02-P06 is gratefully acknowledged.

References

[1] Scott Aaronson and Patrick Rall. "Quantum approximate counting". In: *Simplified.* (2019).

[2] Yves Achdou and Olivier Pironneau. *Computational methods for option pricing.* SIAM, 2005.

[3] J. Aitchison and J.A.C. Brown. *The Lognormal Distribution.* Cambridge University Press, 1957.

[4] J J Álvarez-Sánchez, J V Álvarez-Bravo, and L M Nieto. "A quantum architecture for multiplying signed integers". In: *Journal of Physics: Conference Series* 128 (2008), p. 012013. DOI: 10.1088/1742-6596/128/1/012013.

[5] Dong An, Noah Linden, Jin-Peng Liu, Ashley Montanaro, Changpeng Shao, and Jiasu Wang. "Quantum-accelerated multilevel Monte Carlo methods for stochastic differential equations in mathematical finance". In: *Quantum* 5 (2021), p. 481.

[6] Juan Miguel Arrazola, Timjan Kalajdzievski, Christian Weedbrook, and Seth Lloyd. "Quantum algorithm for nonhomogeneous linear partial differential equations". In: *Physical Review A* 100.3 (2019), p. 032306.

[7] Christian Beck, Sebastian Becker, Patrick Cheridito, Arnulf Jentzen, and Ariel Neufeld. "Deep splitting method for parabolic PDEs". In: *SIAM Journal on Scientific Computing* 43.5 (2021), A3135–A3154.

[8] Richard E. Bellman. *Dynamic programming.* Princeton University Press, Princeton, NJ, 1957.

[9] Julius Berner, Philipp Grohs, and Arnulf Jentzen. "Analysis of the generalization error: Empirical risk minimization over deep artificial neural networks overcomes the curse of dimensionality in the numerical approximation of Black–Scholes partial differential equations". In: *SIAM Journal on Mathematics of Data Science* 2.3 (2020), pp. 631–657.

[10] Fischer Black and Myron Scholes. "The pricing of options and corporate liabilities". In: *Journal of political economy* 81.3 (1973), pp. 637–654.

[11] Phelim P Boyle. "Options: A monte carlo approach". In: *Journal of financial economics* 4.3 (1977), pp. 323–338.

[12] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. "Quantum amplitude amplification and estimation". In: *Contemporary Mathematics* 305 (2002), pp. 53–74.

[13] R.E. Bryant and D.R. O'Hallaron. *Computer Systems: A Programmer's Perspective.* Prentice Hall, 2003. ISBN: 9780131784567.

[14] G. Campolieti and R.N. Makarov. *Financial Mathematics: A Comprehensive Treatment.* Textbooks in Mathematics. CRC Press, 2014. ISBN: 9781439892435.

[15] Shouvanik Chakrabarti, Rajiv Krishnakumar, Guglielmo Mazzola, Nikitas Stamatopoulos, Stefan Woerner, and William J Zeng. "A threshold for quantum advantage in derivative pricing". In: *Quantum* 5 (2021), p. 463.

[16] M. Chiani, D. Dardari, and M. K. Simon. "New exponential bounds and approximations for the computation of error probability in fading channels". In: *IEEE Transactions on Wireless Communications* 2.4 (2003), pp. 840–845. DOI: 10.1109/TWC.2003.814350.

[17] Andrew M Childs, Jin-Peng Liu, and Aaron Ostrander. "High-precision quantum algorithms for partial differential equations". In: *Quantum* 5 (2021), p. 574.

[18] Michael G Crandall, Hitoshi Ishii, and Pierre-Louis Lions. "User's guide to viscosity solutions of second order partial differential equations". In: *Bulletin of the American mathematical society* 27.1 (1992), pp. 1–67.

[19] Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin, and David Petrie Moulton. "A new quantum ripple-carry addition circuit". In: (2004). arXiv: quant-ph/0410184 [quant-ph].

[20] Cirq Developers. *Cirq*. Version v1.1.0. See full list of authors on Github: https://github .com/quantumlib/Cirq/graphs/contributors. Dec. 2022. DOI: 10.5281/zenodo.7465577.

[21] João F Doriguello, Alessandro Luongo, Jinge Bao, Patrick Rebentrost, and Miklos Santha. "Quantum algorithm for stochastic optimal stopping problems with applications in finance". In: *17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022).* Schloss Dagstuhl-Leibniz-Zentrum für Informatik. 2022.

[22] Thomas Draper. "Addition on a Quantum Computer". In: (Sept. 2000).

[23] D.S. Dummit and R.M. Foote. *Abstract Algebra.* Wiley, 2003. ISBN: 9780471433347.

[24] Daniel J Egger, Claudio Gambella, Jakub Marecek, Scott McFaddin, Martin Mevissen, Rudy Raymond, Andrea Simonetto, Stefan Woerner, and Elena Yndurain. "Quantum computing for finance: State-of-the-art and future prospects". In: *IEEE Transactions on Quantum Engineering* 1 (2020), pp. 1–24.

[25] Dennis Elbrächter, Philipp Grohs, Arnulf Jentzen, and Christoph Schwab. "DNN expression rate analysis of high-dimensional PDEs: Application to option pricing". In: *Constructive Approximation* 55.1 (2022), pp. 3–71.

[26] Filipe Fontanela, Antoine Jacquier, and Mugad Oumgari. "A quantum algorithm for linear PDEs arising in finance". In: *SIAM Journal on Financial Mathematics* 12.4 (2021), SC98–SC114.

[27] Shion Fukuzawa, Christopher Ho, Sandy Irani, and Jasen Zion. "Modified Iterative Quantum Amplitude Estimation is Asymptotically Optimal". In: *arXiv preprint arXiv:2208.14612* (2022).

[28] Manfred Gilli, Dietmar Maringer, and Enrico Schumann. *Numerical methods and optimization in finance.* Academic Press, 2019.

[29] Dmitry Grinko, Julien Gacon, Christa Zoufal, and Stefan Woerner. "Iterative quantum amplitude estimation". In: *npj Quantum Information* 7.1 (2021), pp. 1–6.

[30] Philipp Grohs, Fabian Hornung, Arnulf Jentzen, and Philippe Von Wurstemberger. "A proof that artificial neural networks overcome the curse of dimensionality in the numerical approximation of Black-Scholes partial differential equations". In: *arXiv preprint arXiv:1809.02362* (2018).

[31] Lov Grover and Terry Rudolph. "Creating superpositions that correspond to efficiently integrable probability distributions". In: (Sept. 2002).

[32] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search." In: *STOC.* Ed. by Gary L. Miller. ACM, 1996, pp. 212–219. ISBN: 0-89791-785-5.

[33] Jiequn Han, Arnulf Jentzen, and Weinan E. "Solving high-dimensional partial differential equations using deep learning". In: *Proceedings of the National Academy of Sciences* 115.34 (2018), pp. 8505–8510.

[34] Steven Herbert. "Quantum Monte Carlo integration: the full advantage in minimal circuit depth". In: *Quantum* 6 (2022), p. 823.

[35] Zbyněk Šidák. "Rectangular Confidence Regions for the Means of Multivariate Normal Distributions". In: *Journal of the American Statistical Association* 62.318 (1967), pp. 626–633. DOI: 10.1080/01621459.1967.10482935. eprint: https://doi.org/10.1080/01621459.1967.10482935.

[36] Antoine Jacquier, Oleksiy Kondratyev, Alexander Lipton, and Marcos Lopez de Prado. *Quantum Machine Learning and Optimisation in Finance: On the Road to Quantum Advantage*. Packt Publishing Ltd, 2022.

[37] Emanuel Knill. "Approximation by quantum circuits". In: *arXiv preprint quant-ph/9508006* (1995).

[38] Kenji Kubo, Koichi Miyamoto, Kosuke Mitarai, and Keisuke Fujii. "Pricing multi-asset derivatives by variational quantum algorithms". In: *arXiv preprint arXiv:2207.01277* (2022).

[39] Noah Linden, Ashley Montanaro, and Changpeng Shao. "Quantum vs. classical algorithms for solving the heat equation". In: *Communications in Mathematical Physics* 395.2 (2022), pp. 601–641.

[40] D.C. Marinescu. *Classical and Quantum Information*. Elsevier Science, 2011. ISBN: 9780123838759.

[41] Robert C Merton. "Theory of rational option pricing". In: *The Bell Journal of economics and management science* (1973), pp. 141–183.

[42] Ashley Montanaro. "Quantum speedup of Monte Carlo methods". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 471.2181 (2015), p. 20150301. DOI: 10.1098/rspa.2015.0301. eprint: https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.2015.0301.

[43] Ashley Montanaro and Sam Pallister. "Quantum algorithms and the finite element method". In: *Physical Review A* 93.3 (2016), p. 032324.

[44] Ariel Neufeld, Antonis Papapantoleon, and Qikun Xiang. "Model-free bounds for multi-asset options using option-implied information and their exact computation". In: *Management Science* (2022).

[45] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176.

[46] Román Orús, Samuel Mugel, and Enrique Lizaso. "Quantum computing for finance: Overview and prospects". In: *Reviews in Physics* 4 (2019), p. 100028.

[47] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik, and Jeremy L O'brien. "A variational eigenvalue solver on a photonic quantum processor". In: *Nature communications* 5.1 (2014), pp. 1–7.

[48] Kirill Plekhanov, Matthias Rosenkranz, Mattia Fiorentini, and Michael Lubasch. "Variational quantum amplitude estimation". In: *Quantum* 6 (2022), p. 670.

[49] Patrick Rall and Bryce Fuller. "Amplitude Estimation from Quantum Signal Processing". In: *arXiv preprint arXiv:2207.08628* (2022).

[50] Sergi Ramos-Calderer, Adrián Pérez-Salinas, Diego García-Martín, Carlos Bravo-Prieto, Jorge Cortada, Jordi Planaguma, and José I Latorre. "Quantum unary approach to option pricing". In: *Physical Review A* 103.3 (2021), p. 032414.

[51] Pooja Rao, Kwangmin Yu, Hyunkyung Lim, Dasol Jin, and Deokkyu Choi. "Quantum amplitude estimation algorithms on IBM quantum devices". In: *Quantum Communications and Quantum Imaging XVIII*. Vol. 11507. SPIE. 2020, pp. 49–60.

[52] Patrick Rebentrost, Brajesh Gupt, and Thomas R. Bromley. "Quantum computational finance: Monte Carlo pricing of financial derivatives". In: *Phys. Rev. A* 98 (2 2018), p. 022321. DOI: 10.1103/PhysRevA.98.022321.

[53] Patrick Rebentrost and Seth Lloyd. "Quantum computational finance: quantum algorithm for portfolio optimization". In: *arXiv preprint arXiv:1811.03975* (2018).

[54] Lidia Ruiz-Perez and Juan Carlos Garcia-Escartin. "Quantum arithmetic with the quantum Fourier transform". In: *Quantum Information Processing* 16.6 (2017). ISSN: 1573-1332. DOI: 10.1007/s11128-017-1603-1.

[55] Mehdi Saeedi and Massoud Pedram. "Linear-depth quantum circuits for n-qubit Toffoli gates with no ancilla". In: *Physical Review A* 87.6 (2013), p. 062318.

[56] Engin Şahin. "Quantum arithmetic operations based on quantum fourier transform on signed integers". In: *International Journal of Quantum Information* 18.06 (2020), p. 2050035.

[57] Nikitas Stamatopoulos, Daniel J Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen, and Stefan Woerner. "Option pricing using quantum computers". In: *Quantum* 4 (2020), p. 291.

[58] Yohichi Suzuki, Shumpei Uno, Rudy Raymond, Tomoki Tanaka, Tamiya Onodera, and Naoki Yamamoto. "Amplitude estimation without phase estimation". In: *Quantum Information Processing* 19.2 (2020), pp. 1–17.

[59] A tA v et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2021. DOI: 10.5281/zenodo.2573505.

[60] Vlatko Vedral, Adriano Barenco, and Artur Ekert. "Quantum networks for elementary arithmetic operations". In: *Physical Review A* 54.1 (1996), 147–153. ISSN: 1094-1622. DOI: 10.1103/physreva.54.147.

[61] Chu-Ryang Wie. "Simpler quantum counting". In: *arXiv preprint arXiv:1907.08119* (2019).

[62] Stefan Woerner and Daniel J. Egger. "Quantum risk analysis". In: *npj Quantum Information* 5.1 (2019). ISSN: 2056-6387. DOI: 10.1038/s41534-019-0130-6.

[63] Yunpeng Zhao, Haiyan Wang, Kuai Xu, Yue Wang, Ji Zhu, and Feng Wang. "Adaptive Algorithm for Quantum Amplitude Estimation". In: *arXiv preprint arXiv:2206.08449* (2022).

[64] Christa Zoufal, Aurélien Lucchi, and Stefan Woerner. "Quantum Generative Adversarial Networks for learning and loading random distributions". In: *npj Quantum Information* 5.1 (2019), p. 103. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0223-2.