UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques
i Informàtica

GRADO DE MATEMÁTICAS

Trabajo final de grado

THE MATHEMATICS OF QUANTUM AMPLITUDE ESTIMATION ALGORITHM IN QUANTUM COMPUTING

Autor: José Antonio Hidalgo Castillo

Director: Dr. Nahuel Norberto Statuto Perez
Realizado en: Departament de Matemàtiques
i Informàtica

Barcelona, January 13, 2026

Abstract

This work establishes the mathematical and physical framework necessary to rigorously analyze the computational advantages of Quantum Amplitude Estimation (QAE) algorithm. We begin by defining the underlying linear algebra structures—specifically finite-dimensional Hilbert spaces, linear operators, and tensor products—to provide the necessary justification for Dirac notation via the Riesz-Fréchet representation theorem and to formulate the fundamental postulates of quantum mechanics. Building upon this theoretical basis, we theoretically demonstrate that QAE achieves a quadratic speedup over classical Monte Carlo methods, specifically reducing the query complexity required to achieve an additive error ϵ from $\mathcal{O}(1/\sqrt{M})$ to $\mathcal{O}(1/M)$, where M is the number of quantum samples. Furthermore, we analyze techniques to boost the success probability of the algorithm to arbitrary confidence levels. Finally, we apply this algorithmic framework to financial risk management to estimate the Value at Risk (VaR) and Economic Capital Requirement (ECR) of a credit portfolio.

Keywords: Hilbert Spaces, Operator, Qubits, Gates, Measurements, Quantum Amplitude Estimation, Value at Risk.

Resumen

Este trabajo establece el marco matemático y físico necesario para analizar rigurosamente las ventajas computacionales del algoritmo de Estimación de Amplitud Cuántica (QAE). Comenzamos definiendo las estructuras subyacentes del álgebra lineal (específicamente los espacios de Hilbert de dimensión finita, los operadores lineales y los productos tensoriales) para proporcionar la justificación necesaria para la notación de Dirac mediante el teorema de representación de Riesz-Fréchet y para formular los postulados fundamentales de la mecánica cuántica. Con base en esta base teórica, demostramos teóricamente que QAE logra una aceleración cuadrática sobre los métodos clásicos de Monte Carlo, específicamente reduciendo la complejidad de la consulta requerida para lograr un error aditivo ϵ de $\mathcal{O}(1/\sqrt{M})$ a $\mathcal{O}(1/M)$, donde M es el número de muestras cuánticas. Además, analizamos técnicas para aumentar la probabilidad de éxito del algoritmo a niveles de confianza arbitrarios. Finalmente, aplicamos este marco algorítmico a la gestión del riesgo financiero para estimar el Valor en Riesgo (VaR) y el Requerimiento de Capital Económico (ECR) de una cartera de crédito.

Palabras clave: Espacios de Hilbert, Operadores, Qubits, Puertas, Mediciones, Estimación de Amplitud Cuántica, Valor en Riesgo.

2020 Mathematics Subject Classification. 81P68, 81P10, 91G60, 68Q12, 46C05

Agradecimientos

La realización de este Trabajo Final de Grado supone la culminación de una etapa académica llena de retos y aprendizajes, un hito que no habría sido posible alcanzar sin el apoyo de las personas que me han acompañado en el camino.

En primer lugar, quisiera expresar mi más sincero agradecimiento a mi tutor, Nahuel, por su inestimable guía. Agradezco profundamente su lectura atenta y su feedback constructivo a lo largo de todo el proceso. Sus observaciones críticas y sugerencias detalladas han sido fundamentales para desenmarañar la complejidad técnica de este proyecto y pulir el resultado final. Sin su orientación constante, no habría sido posible llevar a buen puerto esta investigación.

De manera muy especial, quiero dar las gracias a mi madre. Gracias por haber apostado incondicionalmente por mi educación y por brindarme el apoyo necesario, tanto moral como material, para que hoy pueda estar escribiendo estas líneas. Este logro es también tuyo.

Finalmente, quiero dedicar un reconocimiento a todos los amigos y compañeros que he tenido la suerte de conocer a lo largo de estos años de carrera universitaria. Gracias por los momentos compartidos y por haberme motivado, de una forma u otra, a seguir adelante y superar las exigencias del grado. Ojalá poder mencionaros a todos vosotros en una sola página.

Contents

Chapter 1

Introduction

The purpose of this chapter is to introduce the reader to the fundamental context of this work, providing the necessary foundations to understand the problem and the subsequent methodology.

1.1 Contextualization

The history of information processing is currently undergoing a fundamental discontinuity, marking a departure from the classical paradigms that have governed computation since the mid-20th century [1]. While classical computing relies on the deterministic manipulation of binary bits—states restricted to definitive zeros or ones—quantum computing harnesses the counter-intuitive principles of quantum mechanics, specifically superposition and entanglement, to process information in ways that are physically impossible for classical computers [2].

This technological evolution was first conceptualized by Richard Feynman in 1981, who argued that simulating quantum systems (which grow exponentially in complexity) is intractable for classical computers, necessitating a machine built of quantum mechanical elements [3]. Consequently, this revolution is not merely an incremental improvement in processing speed, but constitutes a shift in the underlying complexity classes of solvable problems, promising to redefine industries ranging from materials science to the financial sector [4].

Narrowing the focus from hardware to software, the power of quantum computing is actualized through specific algorithms that offer provable computational advantages over best-known classical methods [5]. The most famous of these is Shor's Algorithm, which utilizes the Quantum Fourier Transform (QFT) to factor large integers in polynomial time ($\mathcal{O}((\log N)^3)$), thereby posing a theoretical existential threat to RSA cryptography and secure internet communications [6]. Beyond cryptography, the Quantum Phase Estimation (QPE) algorithm serves as a versatile backbone for various applications, including Quantum Principal Component Analysis (QPCA) in machine learning and ground state energy estimation in chemistry [7].

Within the domain of computational finance, the general advantages of quantum algorithms are distilled into a specific tool known as Quantum Amplitude Estimation (QAE) [8]. QAE is an advanced iteration of Grover's search algorithm; however, rather than

simply identifying a target state, QAE estimates the amplitude (probability) of that state with high precision [9].

This capability is particularly relevant for modern financial engineering, which relies heavily on stochastic modeling to price complex financial derivatives and assess credit risk [10]. In these applications, financial institutions must simulate thousands of potential market scenarios—such as interest rate fluctuations or correlated loan defaults—to estimate fair pricing and potential losses [11]. Recent research by IBM has demonstrated that QAE can effectively replace the classical subroutines used in these simulations, specifically for tasks like derivative pricing and credit risk analysis, by mapping probability distributions directly onto quantum registers [12].

At the tip of the applications in credit risk analysis lies the specific metric of Value at Risk (VaR), the regulatory standard for measuring the maximum expected loss of a portfolio over a specific time horizon [13]. Currently, banks calculate VaR using classical Monte Carlo simulations, where the estimation error ϵ converges slowly at a rate of $\mathcal{O}(1/\sqrt{M})$, requiring massive computational clusters to achieve high precision [14].

However, by applying QAE to the calculation of VaR, it is possible to achieve a proven quadratic speedup. The estimation error in the quantum regime scales as $\mathcal{O}(1/M)$, meaning that to achieve a precision of 10^{-4}, a quantum computer requires roughly 10^4 operations compared to the 10^8 required by classical methods [15]. Therefore, this paper argues that Quantum Amplitude Estimation stands to revolutionize financial risk management by allowing institutions to calculate VaR and Conditional Value at Risk (CVaR) with exponentially greater efficiency than the classical Monte Carlo methods currently underpinning global financial stability [16].

1.2 Objectives and methodology

The primary objective of this work is to provide a mathematical framework for the quantum algorithm known as Quantum Amplitude Estimation (QAE) from [8], demonstrating a quadratic speedup with respect classical Monte Carlo, passing thus from algorithmic complexity $\mathcal{O}(1/\sqrt{M})$ to $\mathcal{O}(1/M)$ where M indicates the number of samples to reduce the estimate error ϵ [17]. To reach this conclusion effectively, this paper follows a strict bottom-up workflow that constructs the necessary mathematical and algorithmic tools.

Specifically, the specific goals of this work are organized as follows:

1. **Establishment of Hilbert spaces and Dirac Notation:** Within the first half of Chapter 2, we define finite-dimensional Hilbert spaces, aiming to prove the Riesz-Fréchet representation theorem (Theorem 2.5). This result allows us to properly introduce Dirac notation, the standard formalism in quantum mechanics [18]. Subsequently, we rigorously study the properties of this notation under the action of linear operators and tensor products.

2. **Formulation of Quantum Mechanics Postulates:** Within the second half of Chapter 2, we introduce the four fundamental postulates of quantum mechanics: State Space, Unitary Evolution, Composition of Systems, and Measurement [19]. These postulates allow us to interpret quantum circuits as operations within Hilbert spaces, providing the necessary physical and mathematical basis for the construction of quantum algorithms.

3. **Analysis of Quantum Amplitude Estimation (QAE):** In Chapter 3, we analyze the central quantum algorithm of this work, dissecting its mathematical underpinnings to demonstrate how it achieves a quadratic speedup over classical Monte Carlo methods for estimating probabilities. We rely on Theorem 3.9 to rigorously quantify the precision of the estimation and explore techniques to boost the success probability of the algorithm.

4. **Application to Financial Risk:** Finally, in Chapter 4, we apply the developed algorithm QAE to a specific financial context. We propose a quantum algorithm adapted from [12] to estimate the Value at Risk (VaR) of a portfolio, leveraging the previously proven speedup to address the computational inefficiency of simulating rare-event credit risks.

Chapter 2

Mathematical Framework

This chapter establishes the foundational structures necessary to rigorously describe and analyze quantum algorithms. We have organized this exposition into two distinct sections. In Section 2.1, we focus on the mathematical formalism, specifically defining finite-dimensional Hilbert spaces, linear operators, and tensor products. This section introduces the Dirac notation, which by Riesz-Fréchet representation theorem (Theorem 2.5) provides a powerful algebraic language for manipulating quantum states [5]. To maintain the fluidity of the exposition, proofs for results either considered elemental within linear algebra or to have mechanical calculations have been relegated to Appendix A.

Building upon this mathematical basis, Section 2.2 transitions to the physical framework of quantum computing [20]. Here, we formulate the fundamental postulates of quantum mechanics—State Space, Unitary Evolution, Composition of Systems, and Measurement [19]. These postulates serve to translate the abstract algebraic structures defined previously into the operational components of quantum computation, effectively defining the behavior of qubits, quantum gates, and measurement processes.

2.1 Hilbert spaces and Dirac notation

We define the Hilbert space as the complex vector space that provides the mathematical setting for quantum mechanics. Beyond the definition itself, the first objective is to prove the existence of an orthonormal basis. Establishing this existence is crucial, as it not only allows for significant simplifications, but also the proper introduction of Dirac notation.

Definition 2.1. *A finite-dimensional vector space $\mathcal{H}$ over the field of complex numbers $\mathbb{C}$ is a **Hilbert space** if it is endowed with an inner product, that is, a map*

$$\langle \cdot\,, \cdot \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$$

such that, for all $x, y, z \in \mathcal{H}$ and all $\lambda, \mu \in \mathbb{C}$, it satisfies the following three properties:

1. *(Conjugate symmetry) $\langle x,\, y\rangle = \overline{\langle y,\, x\rangle}$, where the horizontal bar of the right-hand side denotes the complex conjugate[1] of $\langle y,\, x\rangle$;*
2. *(Linearity in the second argument) $\langle x, \lambda y + \mu z\rangle = \lambda\langle x, y\rangle + \mu\langle x, z\rangle$*
3. *(Positive-definiteness) $\langle x,\, x\rangle \in \mathbb{R}_{\geq 0}$ and $\langle x,\, x\rangle = 0 \iff x = \mathbf{0}$.*

[1] The complex conjugate of any complex number $z = a + ib$, for some a and b real, is $\overline{z} = a - ib$.

By combining the two first properties and the additivity and multiplicativity of complex conjugates, one obtains the *conjugate-linearity* in the first argument:

$$\langle \lambda x + \mu y, z\rangle = \overline{\langle z, \lambda x + \mu y\rangle} = \overline{\lambda\langle z, x\rangle + \mu\langle z, y\rangle} = \overline{\lambda}\overline{\langle z, x\rangle} + \overline{\mu}\overline{\langle z, y\rangle} = \overline{\lambda}\langle x, y\rangle + \overline{\mu}\langle x, z\rangle$$

Additionally, since the complex conjugate of a real number is itself, the inner product is symmetric so long as its output is a real number: $\langle x, y\rangle \in \mathbb{R} \implies \langle x, y\rangle = \langle y, x\rangle$.

Before moving on, we will provide an example of a Hilbert space, according to this definition.

Example 2.2. Let $\mathcal{H} = \mathbb{C}^n$, which is known to be a vector space. For any two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, the *dot product* is defined as

$$\langle x, y\rangle = \sum_{i=1}^{n} \overline{x_i} y_i$$

The three properties are proven in Appendix A using elemental properties of complex numbers.

Unless $\mathcal{H} = \{\mathbf{0}\}$, the fact that $\mathcal{H}$ is finite-dimensional allows to select a basis $\{e_1, \ldots, e_n\}$ for some natural number n. As a result, every vector $x \in \mathcal{H}$ is uniquely represented as

$$x = z_1\, e_1 + \cdots + z_n\, e_n \quad \text{where } z_1, \ldots, z_n \in \mathbb{C}$$

We expected the elements of the basis to behave in a "suitable" way under the action of the inner product.

Definition 2.3. *Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of $\mathcal{H}$ and $x, y \in \mathcal{H}$ any two vectors such that $x \neq y$.*

*(a) x and y are **orthogonal** if $\langle x, y\rangle = 0$, and we denoted by $x \perp y$;*

*(b) x is a **unit vector** if $\langle x, x\rangle = 1$;*

*(c) $\mathcal{B}$ is an **orthogonal basis** if all its elements are orthogonal pair-wise;*

*(d) $\mathcal{B}$ is an **orthonormal basis** if it is orthogonal and all its elements are unit vectors.*

Due to the simplifications in calculations and the nature of quantum mechanics, it is crucial to be able to find an orthonormal basis given any initial basis $\mathcal{B}$ on a Hilbert space. For any vector $x \neq \mathbf{0} \in \mathcal{H}$, it is immediate to check $\dfrac{x}{\sqrt{\langle x, x\rangle}}$ is a unit vector. Thus, the challenge is actually finding an orthogonal basis.

Proposition 2.4. *If $\mathcal{H}$ is a Hilbert space, then it has an orthogonal basis.*

Using an orthogonal basis fundamentally streamlines mathematical operations because it provides a natural coordinate system where each axis represents a distinct, non-overlapping piece of information, which is critical for clarity in fields ranging from signal processing to quantum mechanics [21].

2.1.1 Dual vector spaces

Recall from linear algebra that the *dual vector space* $\mathcal{H}^*$ is the set of linear maps from $\mathcal{H}$ to $\mathbb{C}$. This algebraic structure puts us in a position to state a fundamental result that serves as the mathematical cornerstone for the formalism of quantum mechanics. By establishing a rigorous one-to-one correspondence between the vectors of a Hilbert space and the linear functionals of its dual space, the following theorem effectively bridges the gap between these two algebraic structures. This identification is of paramount importance, as it provides the necessary justification to introduce Dirac notation, a powerful and elegant language that unifies the treatment of quantum states and their associated linear maps.

Theorem 2.5 (Weak version of Riesz-Fréchet representation theorem)**.** *Let $\mathcal{H}$ be a Hilbert space with $\langle \cdot, \cdot \rangle$ as its inner product, and let $\mathcal{H}^*$ be its dual space. For every linear map $f \in \mathcal{H}^*$, there exists a unique vector $y \in H$ such that*

$$f(x) = \langle y, x \rangle \quad \textit{for all } x \in \mathcal{H}$$

Proof. We begin with the existence. Since $\mathcal{H}$ is finite-dimensional, we can select an orthonormal basis $\{e_1, \ldots, e_n\}$. We can express any $x \in \mathcal{H}$ using this basis as $x = \sum_{i=1}^{n} \langle e_i, x \rangle e_i$. Given any linear map $f : \mathcal{H} \to \mathbb{C}$,

$$f(x) = f\left(\sum_{i=1}^{n} \langle e_i, x \rangle e_i\right) = \sum_{i=1}^{n} \langle e_i, x \rangle f(e_i)$$

Considering the vector $y = \displaystyle\sum_{j=1}^{n} \overline{f(e_j)} e_j$, we also get

$$\langle y, x \rangle = \left\langle \sum_{j=1}^{n} \overline{f(e_j)} e_j, x \right\rangle = \sum_{j=1}^{n} \overline{\overline{f(e_j)}} \langle e_j, x \rangle = \sum_{j=1}^{n} f(e_j) \langle e_j, x \rangle$$

Comparing our two results, we observe $f(x) = \langle y, x \rangle$.

For the uniqueness, we assume there is a linear map $f \in \mathcal{H}^*$ such that $f(x) = \langle y, x \rangle = \langle y', x \rangle$ for all $x \in \mathcal{H}$. Particularly,

$$f(y - y') = \langle y, y - y' \rangle = \langle y', y - y' \rangle \implies \langle y - y', y - y' \rangle = 0$$

By positive-definiteness of the inner product, $y - y' = \mathbf{0} \implies y = y'$. □

Theorem 2.5 allows to introduce Dirac notation, which was invented by Paul Dirac [18] and we will develop throughout this current chapter. In this notation, the symbol identifying a vector x in a Hilbert space $\mathcal{H}$ is written inside a 'ket', and it looks something like $|x\rangle$. According to Theorem 2.5, we can make $|y\rangle$ correspond an unique $f_y \in \mathcal{H}^*$ such that $f_y(|x\rangle) = \langle |y\rangle, |x\rangle \rangle$ for all $|x\rangle \in \mathcal{H}$. Due to its uniqueness, Dirac notation suggests to simply denote f_y as $\langle y|$, which is a 'bra'. Thus, the 'bra-ket' $\langle y|x\rangle := \langle y|(|x\rangle)$ is simply a complex number, and can be seen as another way to denote the inner product of any two vectors in $\mathcal{H}$. Some properties arise from the Dirac notation.

Proposition 2.6 (Properties of Dirac notation under the Dual space)**.** *For any complex scalars $\lambda, \mu \in \mathbb{C}$, and vector $|x\rangle, |y\rangle \in \mathcal{H}$ we have*

1. $|\lambda x + \mu y\rangle = \lambda|x\rangle + \mu|y\rangle$
2. $\langle\lambda x + \mu y| = \overline{\lambda}\langle x| + \overline{\mu}\langle y|$
3. $|\psi\rangle = \lambda|x\rangle + \mu|y\rangle \iff \langle\psi| = \overline{\lambda}\langle x| + \overline{\mu}\langle y|$

In order to summarize what we have so far concerning this notation, we will provide an example based on reference [19].

Example 2.7. Let $\mathcal{H}$ be a 2-dimensional Hilbert space which has $\{|0\rangle, |1\rangle\}$ as an orthonormal basis. The elements $|0\rangle, |1\rangle$ are in $\mathcal{H}$ and are not necessarily related to either the complex numbers 0 and 1 or the null vector $\mathbf{0}$. We want to show the vectors

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

form an orthonormal basis too. By Proposition 2.6 we get

$$\langle+|0\rangle = \left(\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\right)|0\rangle = \frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 1|0\rangle) = \frac{1}{\sqrt{2}}(1+0) = \frac{1}{\sqrt{2}} = \langle+|1\rangle$$
$$\langle-|0\rangle = \left(\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)\right)|0\rangle = \frac{1}{\sqrt{2}}(\langle 0|0\rangle - \langle 1|0\rangle) = \frac{1}{\sqrt{2}}(1-0) = \frac{1}{\sqrt{2}} = -\langle-|1\rangle$$

By these identities, it becomes easy to check

$$\langle+|+\rangle = \frac{1}{\sqrt{2}}(\langle+|0\rangle + \langle+|1\rangle) = \frac{1}{\sqrt{2}} \cdot 2\langle+|0\rangle = 1$$
$$\langle-|-\rangle = \frac{1}{\sqrt{2}}(\langle-|0\rangle - \langle-|1\rangle) = \frac{1}{\sqrt{2}} \cdot 2\langle+|0\rangle = 1$$
$$\langle-|+\rangle = \frac{1}{\sqrt{2}}(\langle-|0\rangle + \langle-|1\rangle) = \frac{1}{\sqrt{2}} \cdot 0 = 0 = \langle+|-\rangle$$

We will continue developing the notation on the subsequent subsections, when new objects may enter in conflict with it.

2.1.2 Operators

In this subsection, we adapt the concept of operator to the Dirac notation, which excels when manipulating such objects and their associated matrices. We are particularly interested in establishing not only a way to express them, but also the existence and uniqueness of the adjoint operator $T^\dagger$. Furthermore, we will conclude by defining operators that are fundamental in the quantum mechanics framework —specifically unitary operators and orthogonal projectors— and analyzing their most relevant properties.

Under the Dirac notation, we showed $\langle\phi|\psi\rangle$ is actually the action of a vector in $\mathcal{H}$ under a linear map $\mathcal{H} \to \mathbb{C}$, thus it returns a complex number. Now we are interested in giving a meaning to the 'ket-bra' $|\psi\rangle\langle\phi|$. Given any vector $|\chi\rangle \in \mathcal{H}$, by the notation we have developed so far, it is natural to define

$$(|\psi\rangle\langle\phi|)|\chi\rangle := (\langle\phi|\chi\rangle)|\psi\rangle \tag{2.1.1}$$

Observe the right-hand side is a scalar multiplying the vector $|\psi\rangle$, thus the action of a vector under $|\psi\rangle\langle\phi|$, which is commonly referred as the *outer product* to contrast the inner product $\langle\psi|\phi\rangle$, returns another vector.

Recall from linear algebra that a *linear operator* (or simply operator) on a vector space V is a linear map $T : V \to V$ from the vector space to itself. For any vector $|x\rangle$ (or x), we will denote $T|x\rangle$ (or Tx) instead of $T(|x\rangle)$ (or $T(x)$). Thus, $|\psi\rangle\langle\phi|$ can be interpreted as a linear operator on $\mathcal{H}$. In fact, the following theorem strengthens their relation [19].

Theorem 2.8. *Let $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be an orthonormal basis on a Hilbert space $\mathcal{H}$. Then every linear operator T on $\mathcal{H}$ can be written as*

$$T = \sum_{i,j=1}^{n} T_{i,j}|e_i\rangle\langle e_j| \tag{2.1.2}$$

where $T_{i,j} = \langle e_i|T|e_j\rangle := (\langle e_i|T)|e_j\rangle = \langle e_i|(T|e_j\rangle)$.

Proof. Since T is a linear map, it is sufficient to prove Eq. (2.1.2) by evaluating only the elements of the orthonormal basis such as $|e_k\rangle$, for $1 \leq k \leq n$. On the one hand, we can express $T|e_k\rangle = \sum_{j=1}^{n} \lambda_j|e_j\rangle$ for some $\lambda_1, \ldots \lambda_n \in \mathbb{C}$. On the other hand,

$$\left(\sum_{i,j=1}^{n} T_{i,j}|e_i\rangle\langle e_j|\right)|e_k\rangle = \sum_{i,j=1}^{n} T_{i,j}(|e_i\rangle\langle e_j|)|e_k\rangle = \sum_{i,j=1}^{n} T_{i,j}(\langle e_j|e_k\rangle)|e_i\rangle = \sum_{i=1}^{n} T_{i,k}|e_i\rangle$$

Since

$$T_{i,k} = \langle e_i|(T|e_k\rangle) = \langle e_i|(\sum_{j=1}^{n} \lambda_j|e_j\rangle) = \sum_{j=1}^{n} \lambda_j(\langle e_i|e_j\rangle) = \lambda_i$$

then both expressions coincide and *Eq.* (2.1.2) is satisfied when evaluating $|e_k\rangle$. □

During the proof, we got $T|e_k\rangle = \sum_{i=1}^{n} T_{i,k}|e_i\rangle$ for any elements of an orthonormal basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$. Thus, under this basis, the matrix associated with T has the coefficient $T_{i,j} = \langle e_i|(T|e_j\rangle)$ in the i^{th} row and the j^{th} column.

Example 2.9. Let $\mathcal{H}$ be a 2-dimensional Hilbert space, $\{|0\rangle, |1\rangle\}$ an orthonormal basis, and H an operator such that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, which are the same vectors from Example 2.7. Hence,

$$T_{1,1} = \langle 0|H|0\rangle = \frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 1|0\rangle) = \frac{1}{\sqrt{2}} = T_{1,2} = T_{2,1}$$
$$T_{2,2} = \langle 1|H|1\rangle = \frac{1}{\sqrt{2}}(\langle 1|0\rangle - \langle 1|1\rangle) = -\frac{1}{\sqrt{2}}$$

By Equation Eq. (2.1.2), the operator can be expressed as

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

Under that basis, the matrix representation of H is $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

In order to state properly crucial properties of Dirac notation with operators, we must introduce the following definition:

Definition 2.10. *Let T be an operator of a Hilbert space $\mathcal{H}$. The operator $T^\dagger$ on $\mathcal{H}^*$ is said to be the **adjoint of** T if*

$$\langle x|Ty\rangle = \langle T^\dagger x|y\rangle \quad \textit{for all } |x\rangle, |y\rangle \in \mathcal{H}$$

In simpler terms, the adjoint $T^\dagger$ is the operator that does the "same job" as T, but on the other side of the inner product. The adjoint of any operator exists and is unique, as stated in the following theorem.

Theorem 2.11. *Let T be a linear operator on a Hilbert space $\mathcal{H}$. Then the adjoint of T exists and is unique. Furthermore, under an orthonormal basis, the matrix associated with the adjoint $T^\dagger$ is the complex conjugate transpose (also called the Hermitian conjugate) of the matrix associated with T in that basis.*

It is worth commenting Dirac notation plays a crucial role within the proof of this theorem. The existence of the adjoint ensures important properties for this work. We start stating the ones concerning the Dirac notation.

Proposition 2.12 (Properties of Dirac notation under operators)**.** *Let $\mathcal{H}$ be a Hilbert space. For any operator T and any vector $|x\rangle$ we have*

1. $|Tx\rangle = T|x\rangle \quad$ *for all* $|x\rangle \in \mathcal{H}$
2. $\langle x|T = \langle T^\dagger x| \quad$ *for all* $\langle x| \in \mathcal{H}^*$

Proof. The first property is vacuously true, since T maps vectors to vectors in the same Hilbert space. For the second property, one simply considers $(\langle x|T)|y\rangle = \langle x|(T|y\rangle) = \langle x|Ty\rangle = \langle T^\dagger x|y\rangle = (\langle T^\dagger x|)|y\rangle$. □

Other relevant properties that derive from Theorem 2.11 and the definition of adjoint of a operator are summarized in the following corollary.

Corollary 2.13. *Let S and T be operators on a Hilbert space $\mathcal{H}$, and $\lambda \in \mathbb{C}$. Then*

1. $(T^\dagger)^\dagger = T$
2. $(ST)^\dagger = T^\dagger S^\dagger$
3. $(S + \lambda T)^\dagger = S^\dagger + \overline{\lambda} T^\dagger$

We conclude this subsection defining some operators which are fundamental in the quantum mechanics framework.

Definition 2.14. *Let U and P be operators on a Hilbert space $\mathcal{H}$.*

*(a) U is **unitary** if it has an inverse operator U^{-1} such that $U^\dagger = U^{-1}$;*

*(b) P is an **orthogonal projector** if $PP = P$ and $P^\dagger = P$.*

Although we will discuss their implications applied into quantum mechanics on subsequent chapters, there is one important result from linear algebra involving orthogonal projectors that is worth stating.

Proposition 2.15. *Let P be an orthogonal projector on a Hilbert space $\mathcal{H}$ and define $P^\perp = I - P$ where I is the identity operator. Then*

$$\langle Px|P^\perp y\rangle = 0 \quad \text{for all } |x\rangle, |y\rangle \in \mathcal{H}$$

Furthermore, $\mathcal{H}$ is the direct sum of the images of P and $P^\perp$, that is

$$\mathcal{H} = \mathrm{Im}(P) \oplus \mathrm{Im}(P^\perp)$$

Proof. For the first part, by the properties of an orthogonal projector

$$\langle Px|P^\dagger x\rangle = \langle x|P^\dagger(I-P)|x\rangle = \langle x|(P^\dagger - P^\dagger P)|x\rangle = \langle x|(P-P)|x\rangle = 0$$

For the second part, it is sufficient to show that for $|x\rangle \in \mathcal{H}$ there are $|x_1\rangle \in \mathrm{Im}(P)$ and $|x_0\rangle \in \mathrm{Im}(P^\perp)$ such that $|x\rangle = |x_1\rangle + |x_0\rangle$, since the first part within the proof ensures $\mathrm{Im}(P) \cap \mathrm{Im}(P^\perp) = \{\mathbf{0}\}$. Nevertheless, the existence follows immediately if we consider $|x_1\rangle = P|x\rangle$ and $|x_0\rangle = P^\perp|x\rangle$. □

2.1.3 Tensor products

In this subsection, we define the tensor product as a rigorous way of combining vector spaces, vectors, or linear maps. In quantum mechanics, this concept is fundamental as it allows us to study the action of individual objects as a unified whole. We will focus on understanding how the mathematical structures we have developed so far behave under this operation. This new space is essential because it contains states that describe all possible correlations and interactions between the objects, including complex states [21].

Definition 2.16. *Let $V_1, \ldots, V_n$ be finite-dimensional vector spaces (not necessarily Hilbert spaces) over the same field such that $\mathcal{B}_j = \{|e_1^j\rangle, \ldots, |e_{n_j}^j\rangle\}$ is a basis of V_j for each $j = 1, \ldots, n$. Then the **tensor product space** $V_1 \otimes \cdots \otimes V_n$ is a new vector space whose elements are called **tensors** and such that*

$$\mathcal{B}_\otimes = \{|e_{i_1}^1\rangle \otimes \cdots \otimes |e_{i_n}^n\rangle \ : \ 1 \le i_j \le n_j \text{ for each } j = 1, \ldots, n\}$$

is a basis under the lexicographic order.

Additionally, by uniquely representing any vectors $|x_j\rangle \in V_j$ for each $j = 1, \ldots, n$ as

$$|x_j\rangle = \sum_{i_j=1}^{n_j} \lambda_{i_j}^j |e_{i_j}^j\rangle,$$

*the **pure tensor of** $|x_1\rangle, \ldots, |x_n\rangle$ is a vector in $V_1 \otimes \cdots \otimes V_n$ defined as*

$$|x_1\rangle \otimes \cdots \otimes |x_n\rangle := \sum_{i_1=1}^{n_1} \cdots \sum_{i_n=1}^{n_n} (\lambda_{i_1}^1 \cdots \lambda_{i_n}^n)(|e_{i_1}^1\rangle \otimes \cdots \otimes |e_{i_n}^n\rangle)$$

By this definition of tensor product space[2], it is immediate that its dimension is the cardinal of $\mathcal{B}_\otimes$, hence

$$N = \dim(V_1 \otimes \cdots \otimes V_n) = \prod_{j=1}^{n} \dim(V_j) \tag{2.1.3}$$

and it is isomorphic to $\mathbb{C}^N$.

Example 2.17. Let $V_j = \mathbb{C}$ for all $1 \le j \le n$. A basis of V_j is $\{z^{(j)}\}$ so long as $z^{(j)} \neq 0$. By Eq. (2.1.3) we obtain $\dim(V^1 \otimes \cdots \otimes V^n) = 1$. Thus the tensor product space is isomorphic to $\mathbb{C}$. A natural isomorphism would be the one that maps pure tensors $x_1 \otimes \cdots \otimes x_n$ to $x_1 \cdots x_n$. By this isomorphism, we can interpret the operator $\otimes$ as the multiplication of complex numbers, which is naturally multilinear due to its properties.

[2]More generally, the tensor product space is usually defined as a vector space that satisfies certain "universal property".

Moving on, in the case of pure tensors, the way they are defined implies

$$\operatorname{span}(B_{\otimes}) = \operatorname{span}\{|x_1\rangle \otimes \cdots \otimes |x_n\rangle \ : \ |x_1\rangle \in V_1, \ldots, |x_n\rangle \in V_n\}$$

Equivalently, every tensor is generated by pure tensors.

Additionally, it ensures the operation $\otimes$ is *multilinear*; that is, it is linear in each one of its arguments:

$$|x_1\rangle \otimes \cdots \otimes |\lambda_j x_j + \mu_j y_j\rangle \otimes \cdots \otimes |x_n\rangle = |x_1\rangle \otimes \cdots \otimes |\lambda_j x_j\rangle \otimes \cdots \otimes |x_n\rangle + |x_1\rangle \otimes \cdots \otimes |\mu_j y_j\rangle \otimes \cdots \otimes |x_n\rangle$$

for each $j = 1, \ldots, n$. In the case $n = 2$, that is, $V_1 \otimes V_2$, we refer to the term *multilinear* as *bilinear*.

Now, to avoid overloading the notation, we will restrict ourselves to tensor product spaces of the form $V_1 \otimes V_2$, but the results are extended to any tensor, $V_1 \otimes \cdots \otimes V_n$, with ease. We will also drop the Dirac notation for now, since the tensor product space does not have a structure of a Hilbert space yet. Hence, our next goal is to find a proper inner product for it.

If $\langle \cdot, \cdot \rangle_{\mathcal{H}_1}$ and $\langle \cdot, \cdot \rangle_{\mathcal{H}_2}$ are the respective inner products of some Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, then we define for pure tensors the map

$$\begin{aligned} \langle \cdot, \cdot \rangle : (\mathcal{H}_1 \otimes \mathcal{H}_2) \times (\mathcal{H}_1 \otimes \mathcal{H}_2) &\longrightarrow \mathbb{C} \\ (x_1 \otimes x_2, y_1 \otimes y_2) &\mapsto \langle x_1, y_1 \rangle_{\mathcal{H}_1} \langle x_2, y_2 \rangle_{\mathcal{H}_2} \end{aligned} \tag{2.1.4}$$

Since pure tensors span the whole tensor product space, we can extend this map by linearity in the second argument and conjugate-linearity in the first one.

Theorem 2.18. *Under the same notation, $\mathcal{H}_1 \otimes \mathcal{H}_2$ is a Hilbert space endowed with the map defined on Eq.* (2.1.4)*. Furthermore, if $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, then $\mathcal{B}_{\otimes}$ is an orthonormal basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$ under that map.*

Although Theorem 2.18 allows us to recover Dirac notation, it is recommended to introduce first the definition of the tensor product of linear maps and then state the relevant properties involving the former with the latter.

Definition 2.19. *Let V_1, V_2, W_1, W_2 be finite-dimensional vector spaces over the same field and $S : V_1 \to W_1$, $T : V_2 \to W_2$ linear maps. The* ***tensor product of*** *S* ***and*** *T is said to be the linear map $S \otimes T : V_1 \otimes V_2 \to W_1 \otimes W_2$ such that*

$$(S \otimes T)|x_1 \otimes x_2\rangle := S|x_1\rangle \otimes T|x_2\rangle \quad \text{for all pure tensors } |x_1 \otimes x_2\rangle \in V_1 \otimes V_2$$

and extended linearly to all vectors of $V_1 \otimes V_2$.

Observe the tensor product of those linear maps is well-defined, since S and T are linear and $\otimes$ preserves these linearities. By this definition, it is a good moment to state the previously mentioned properties.

Proposition 2.20 (Properties of Dirac notation under tensor products)**.** *Let $\lambda, \mu \in \mathbb{C}$ and*

1. $|(\lambda x_1 + \mu y_1) \otimes x_2\rangle = \lambda |x_1 \otimes x_2\rangle + \mu |y_1 \otimes x_2\rangle$

2. $|x_1 \otimes (\lambda x_2 + \mu y_2)\rangle = \lambda|x_1 \otimes x_2\rangle + \mu|x_1 \otimes y_2\rangle$
3. $\langle(\lambda x_1 + \mu y_1) \otimes x_2| = \overline{\lambda}\langle x_1 \otimes x_2| + \overline{\mu}\langle y_1 \otimes y_2|$
4. $\langle x_1 \otimes (\lambda x_2 + \mu y_2)| = \overline{\lambda}\langle x_1 \otimes x_2| + \overline{\mu}\langle x_1 \otimes y_2|$
5. $|x_1 \otimes x_2\rangle\langle y_1 \otimes y_2| = |x_1\rangle\langle x_2| \otimes |y_1\rangle\langle y_2|$

Proof. For properties 1-4, it is sufficient to apply the bilinearity of the tensor product and similar arguments as the ones from Proposition 2.6.

For the last property, for any pure tensor $z_1 \otimes z_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$

$$(|x_1 \otimes x_2\rangle\langle y_1 \otimes y_2|)|z_1 \otimes z_2\rangle = \langle y_1 \otimes y_2|z_1 \otimes z_2\rangle|x_1 \otimes x_2\rangle = (\langle y_1|z_1\rangle_{\mathcal{H}_1}\langle y_2|z_2\rangle_{\mathcal{H}_2})|x_1 \otimes x_2\rangle,$$
$$(|x_1\rangle\langle y_1| \otimes |x_2\rangle\langle y_2|)|z_1 \otimes z_2\rangle = |x_1\rangle\langle y_1|z_1\rangle \otimes |x_2\rangle\langle y_2|z_2\rangle = (\langle y_1|z_1\rangle_{\mathcal{H}_1}\langle y_2|z_2\rangle_{\mathcal{H}_2})|x_1 \otimes x_2\rangle$$

Since both expressions coincide in the case of pure tensors, and the latter are generated by pure tensors, we have proved the expression. □

For simplicity, we can denote $|x\rangle|y\rangle := |x \otimes y\rangle$, or even $|xy\rangle := |x \otimes y\rangle$ for any vectors $|x\rangle \in \mathcal{H}_1$, $|y\rangle \in \mathcal{H}_2$. For consistency with the inner product, we would then denote $\langle x|\langle y| := \langle x \otimes y|$ or $\langle xy| := \langle x \otimes y|$. We will use this simplifications of the notation in the coming chapters particularly.

To conclude this framework involving Hilbert spaces, we want to show a fundamental identity that relates it with the notion of the adjoint and the inverse of an operator.

Proposition 2.21. *Let $S : \mathcal{H}_1 \to \mathcal{H}_1$ and $T : \mathcal{H}_2 \to \mathcal{H}_2$ be linear operators on Hilbert spaces. Then the adjoint*

$$(S \otimes T)^\dagger = S^\dagger \otimes T^\dagger \tag{2.1.5}$$

Furthermore, if both S and T are invertible, then $S \otimes T$ is also invertible and it is expressed as

$$(S \otimes T)^{-1} = S^{-1} \otimes T^{-1} \tag{2.1.6}$$

2.2 Quantum Computing

In this section, we transition from the mathematical structures established in the previous chapter to the physical framework of quantum computing. We introduce the fundamental postulates of quantum mechanics—State Space, Unitary Evolution, Composition of Systems, and Measurement—which govern the behavior of quantum systems and provide the theoretical foundation for transforming abstract algebraic concepts into physical realities. We begin by defining the qubit as the fundamental unit of information, associating it with state vectors in Hilbert spaces, and subsequently explore the dynamics of closed systems via unitary operators, the structure of composite systems through tensor products, and the probabilistic nature of measurement.

2.2.1 Qubits

A qubit is the fundamental unit of information in quantum computing, analogous to the classical bit but governed by the principles of quantum mechanics. Unlike a bit, which can only take the values 0 or 1, a qubit can exist in a superposition of states, enabling forms of computation impossible in classical systems [5].

To properly understand what a qubit is and why it behaves the way it does, we need to explain the **postulates** which give rise to quantum mechanics, because qubits are not abstract mathematical constructs—they arise directly from the physical behavior of quantum systems such as electrons, photons or atoms. These postulates will be formulated according to reference [19].

Quantum mechanics is the branch of physics that describes the behavior of matter and energy at very small scales, where classical physics fails [20]. In turn, a quantum system is any physical system whose behavior is governed by the laws of quantum mechanics, rather than classical physics [20]. In practice, this means the system is small enough, isolated enough, or controlled enough that uniquely quantum properties become relevant [20]. The first postulate gives us a mathematical way to represent such systems.

Postulate 2.22 (State Space Postulate)**.** *The state of a quantum system is described by a unit vector in a Hilbert space $\mathcal{H}$.*

Remark 2.23. The Hilbert space mentioned within the postulates is interpreted through the general definition from real-analysis textbooks instead of the one we have provided on this paper. Thus, it might be an infinite-dimensional vector space. Nevertheless, in the context of quantum computing, we usually restrict to finite dimensions. Particularly, we work with 2-dimensional Hilbert spaces.

By the State Space Postulate, if we think of a quantum system whose state can only occupy two independent quantum states, such as the presence or absence of a photon in a particular location, then it can be mathematically described by a two-dimensional Hilbert space $\mathcal{H}$ [19]. In such space, we could consider $\{|0\rangle, |1\rangle\}$ as a basis, and assign each state to each element of it. For instance, continuing with the example of the photon, we could associate its 'absence' state with $|0\rangle$, while its 'presence' state with $|1\rangle$. By the same postulate, both elements $|0\rangle$ and $|1\rangle$ are unit vectors. Furthermore, they are orthogonal. If that was not the case, then there would be some non-null "'part"' of one of the states that is generated by the other. However, this would not make sense physically, since they must be independent [20]. As a result, the basis is orthonormal.

From the previous paragraph, we can encode a *qubit* (or quantum bit) through a quantum 2-state system by assigning the basis $\{|0\rangle, |1\rangle\}$ from a 2-dimensional Hilbert space. Such basis is often called *computational basis*. This is analogous to what is done for classical computation. For a classical computer, the two-level system may be the voltage level on a wire, assigning the bit (or classical bit) '0' to the absence of voltage and '1' to its presence. The main difference with respect qubits is that the latter may be in a *superposition* of the two states. That is, if we associate a qubit to the vector $|\psi\rangle$ representing the state of the system, usually called the *state vector*, then

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where the complex coefficients α and β are often called the *amplitudes* of the basis states $|0\rangle$ and $|1\rangle$ respectively. Due to this association, from now on we will consider the terms "qubits" and "state vectors" as synonyms.

While the state vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a point in a complex two-dimensional Hilbert space, the normalization constraint $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$ allows for a more intuitive geometric representation. Specifically, the state of a qubit can be uniquely parameterized

by two real angles, $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$, as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

This transformation maps the possible states of a qubit onto the surface of a unit sphere in $\mathbb{R}^3$, known as the Bloch Sphere.

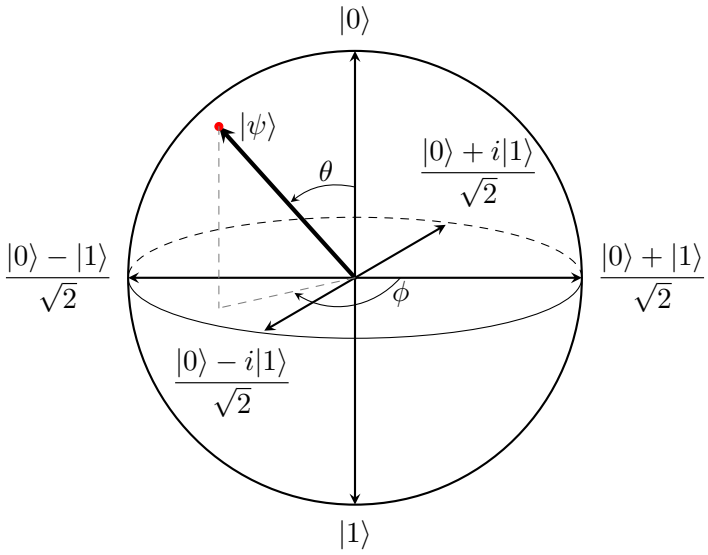


Figure 2.1: Representation of the Bloch Sphere. Source: own elaboration.

2.2.2 Quantum gates on a single qubit

Any physical system changes in time, including quantum ones. The next postulate describes the evolution of such a system when it is closed. By *closed quantum system* we mean a quantum system that evolves without exchanging energy, particles, or information with its surroundings, meaning it is perfectly isolated from any external influence [5].

Postulate 2.24 (Unitary Evolution Postulate)**.** *The time-evolution of the state of a closed quantum system is described by a unitary operator. That is, for any evolution of the closed system there exists a unitary operator U such that if the initial state of the system is $|\psi_0\rangle$ then after the evolution the state of the system will be*

$$|\psi_1\rangle = U|\psi_0\rangle$$

By this postulate and the definitions of unitary and adjoint operator, we obtain

$$\langle\psi_1|\psi_1\rangle = \langle U\psi_0|U\psi_0\rangle = \langle U^\dagger U\psi_0|\psi_0\rangle = \langle\psi_0|\psi_0\rangle = 1$$

since $|\psi_0\rangle$ must be a unit vector. Hence, unitary operators not only map unit vectors to unit vectors, but they also reinforce the State Space Postulate.

Additionally, the composition of unitary operators U and V is also a unitary operator. Indeed, if $W = UV$ then by Corollary 2.13

$$W^{-1} = (UV)^{-1} = V^{-1}U^{-1} = V^\dagger U^\dagger = (UV)^\dagger = W^\dagger$$

Thus the evolution of a closed quantum system might be actually expressed as a composition of unitary operators.

In quantum computing, we refer to a unitary operator U acting on a single qubit as a *1-qubit quantum gate*, or simply *gate* if it does not give rise to confusion. As a consequence, no information is lost inside a closed system: evolution is reversible, and the new vector state can be still represented on the Bloch Sphere.

The Unitary Evolution Postulate implies that, in a closed quantum system, we can theoretically control a qubit through the implementation of specific unitary operators. This gives rise to the concept of *quantum circuits*, which is a visual way of representing a sequence of objects, featuring gates, to manipulate them. For one single qubit whose state $|\psi\rangle$ evolves through $U_1, U_2, \ldots, U_n$ gates, we can illustrate the circuit like in Figure 2.2.

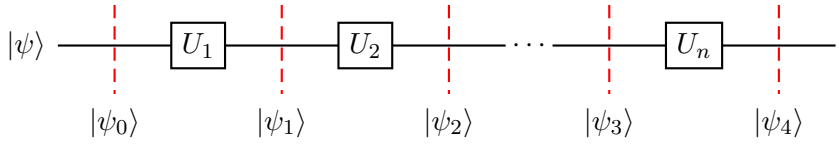


Figure 2.2: Quantum circuit with a single qubit. Source: own elaboration.

In Figure 2.2, the vertical dashed lines help us to indicate the different sections of the quantum circuit and how the qubit changes in each one. Starting from the left, the first section indicates the initial state $|\psi_0\rangle = |\psi\rangle$. In the next one, we have applied the unitary gate U_1; thus $|\psi_1\rangle = U_1|\psi_0\rangle$. From here, it follows with ease that in the next section $|\psi_2\rangle = U_2|\psi_1\rangle$. Between section $|\psi_2\rangle$ and $|\psi_3\rangle$ we have used the composition of gates, which we know is unitary, $U = U_{n-1}\cdots U_4U_3$; thus $|\psi_3\rangle = U|\psi_2\rangle$. Finally, U_n yields the final state $|\psi_4\rangle$. Equivalently,

$$|\psi_4\rangle = U_nU_{n-1}\cdots U_2U_1|\psi_0\rangle$$

Example 2.25. Consider the qubit $|\psi_0\rangle = |0\rangle$, which is an element from the computational basis, and the operator H from Example 2.9. Since H is unitary, it may act as gate. In fact, H is called *Hadamard gate*. Now we consider a quantum circuit consisting of $|0\rangle$ and two Hadamard gates.

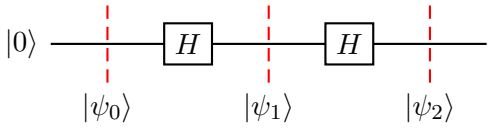


Figure 2.3: Two Hadamard gates. Source: own elaboration.

Since we now the matrix representation of H from Example 2.9, we can calculate the state vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ with ease.

$$|\psi_1\rangle = H|\psi_0\rangle = H|0\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \equiv |+\rangle$$

$$|\psi_2\rangle = H|\psi_1\rangle \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \equiv |0\rangle$$

where $|+\rangle$ is the vector (state) from Example 2.7.

2.2.3 Quantum gates on multiple qubits

So far we have discussed the postulates for the case of a single system only, in particular a qubit. If we want to study potentially useful quantum computations we will need to understand how quantum mechanics works for systems composed of several qubits interacting with each other. This brings us to our third postulate [19].

Postulate 2.26 (Composition of Systems Postulate)**.** *When two quantum systems are treated as one combined system, the state space of the combined quantum system is the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of the state spaces $\mathcal{H}_1, \mathcal{H}_2$ of the component subsystems. If the first system is in the state $|\psi_1\rangle$ and the second system in the state $|\psi_2\rangle$, then the state of the combined system is*

$$|\psi_1\psi_2\rangle := |\psi_1\rangle \otimes |\psi_2\rangle$$

The implications of this postulate extend beyond the mere additive combination of qubits. The resulting tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ contains a far broader class of vectors. Specifically, a state in the combined system is said to be *entangled* if it cannot be decomposed into a pure tensor product of individual subsystem states. As a consequence, the two of them are generally correlated [20].

Example 2.27. The state vector $|+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, known as a *Bell state*, is actually entangled. To maintain the logical flow of this section, we show this property in Example 2.34, and how it affects measurements significantly.

One can apply the Composition of Systems Postulate to show that the state space of the system composed of n distinct subsystems is naturally isomorphic to the tensor product space of the state spaces of the n subsystems [5]. Therefore, in the context of quantum computing, we can perfectly represent the state space consisting of n qubits as

$$\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n \tag{2.2.1}$$

where $\mathcal{H}_j$ is the state space of the j^{th} qubit. A Hilbert space like the one from Eq. (2.2.1) is said to be a *n-qubit register*, since it describes the behavior of n qubits. By Eq. (2.1.3), an $n-$qubit register is 2^n-dimensional.

Recalling the computational basis $\{|0\rangle, |1\rangle\}$ from a $1-$ qubit register and the definition of tensor product space, we have that

$$\{|j_{n-1}\rangle \cdots |j_1\rangle|j_0\rangle := |j_{n-1} \cdots j_1 j_0\rangle \ : \ j_{n_1}, \ldots, j_1, j_0 = 0, 1\} \tag{2.2.2}$$

is a basis on an $n-$qubit register. The set Eq. (2.2.2) is said to be the *computational basis* for an $n-$qubit register.

Example 2.28. On a 3-qubit register, $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ is its computational basis.

In quantum computing, we refer to a unitary operator U acting on n qubits as a *n-qubit quantum gate*, or simply *gate* if it does not give rise to confusion. This suggests we can construct quantum circuits for multiple qubits. However, we need to determine if quantum circuits such as the following are compatible with the Unitary Evolution Postulate:

On the one hand, it is clear

$$|\psi_0\rangle = |q_3\rangle|q_2\rangle|q_1\rangle|q_0\rangle =: |q_3\, q_2\, q_1\, q_0\rangle$$

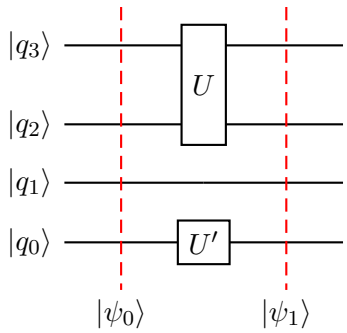


Figure 2.4: Quantum circuit with four qubits and two gates. Source: own elaboration.

On the other hand, we need to apply each gate with the corresponding qubits to obtain

$$|\psi_1\rangle = U(|q_3\rangle|q_2\rangle)\,|q_1\rangle\,U'|q_0\rangle = (U \otimes I \otimes U')(|q_3\rangle|q_2\rangle|q_1\rangle|q_0\rangle) = (U \otimes I_1 \otimes U')|\psi_0\rangle$$

where I_1 denotes the identity matrix applied on a single qubit. Thus, the quantum circuit from Figure 2.4 does not violate the Unitary Evolution Postulate if and only if the operator $U \otimes I_1 \otimes U'$ is unitary.

Example 2.29. Consider the quantum circuit on Figure 2.5.

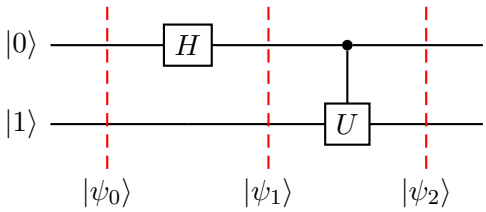


Figure 2.5: Quantum circuit with two qubits. Source: own elaboration.

First of all, we have $|\psi_0\rangle = |01\rangle$. Then, between the vector states $|\psi_0\rangle$ and $|\psi_1\rangle$ there is only a Hadamard gate acting on the qubit from the 1^{st} subregister, that is, $|0\rangle$; thus $|\psi_1\rangle = (H \otimes I_1)|01\rangle = |+\rangle|1\rangle$.

Between $|\psi_1\rangle$ and $|\psi_2\rangle$ we have a quantum gate acting on both qubits. Specifically, this gate is called *controlled–U gate with control on the i^{th} subregister and target on the j^{th} subregister* (or simply *controlled–U gate*), where U is an arbitrary $1-$qubit quantum gate. If denoting the operator as $CU_{i,j}$, or even as CU when confusion may not arise, then it acts on each element of the basis of the tensor product state $\mathcal{H}_i \otimes \mathcal{H}_j$ as

$$CU|00\rangle = |00\rangle, \quad CU|01\rangle = |01\rangle, \quad CU|10\rangle = |1\rangle U|0\rangle, \quad CU|11\rangle = |1\rangle U|1\rangle$$

In simpler terms, CU acts as an identity operator on both qubits when the i^{th} one is in the state $|0\rangle$, and the gate U acts on the j^{th} qubit when the i^{th} one is in the state $|1\rangle$. Therefore,

$$\begin{aligned} |\psi_2\rangle = CU|\psi_1\rangle = CU|+\rangle|1\rangle = \frac{1}{\sqrt{2}}CU(|0\rangle + |1\rangle)|1\rangle \\ = \frac{1}{\sqrt{2}}CU(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |1\rangle U|1\rangle) \end{aligned}$$

2.2.4 Measurements

Ultimately we will be interested on measuring some properties of the quantum system, and so at some point we must allow the system to interact with the measurement apparatus of some observer. When this happens the original system is no longer closed, and the Unitary Evolution Postulate is no longer appropriate for describing its evolution. The evolution of the state of a system during a measurement process is not unitary, and we add this additional postulate to describe such processes [19].

Postulate 2.30 (Measurement Postulate)**.** *A measurement in a quantum system can be performed through a set of operators $\{M_i\}$ on the state space $\mathcal{H}$, indexed by the possible outcomes i, such that*

$$\sum_i M_i^\dagger M_i = I \tag{2.2.3}$$

where I is the identity operator.

For any such set of operators, which are called ***measurement operators****, if the state vector $|\psi\rangle$ is measured, then with probability*

$$p(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle$$

outputs outcome i and after the measurement leaves the state vector as

$$|\psi_i\rangle = \frac{M_i|\psi\rangle}{\sqrt{p(i)}}$$

From this postulate, some little observations are necessary. First of all, Eq. (2.2.3) guarantees the sum of the probabilities $p(i)$ is one. Secondly, $|\psi_i\rangle$ is indeed a unit vector. Finally, if $p(i) = 0$ we never get the outcome i and there is no need to renormalize the state, since $0 = p(i) = \langle M_i\psi_i|M_i\psi_i\rangle$ implies $M_i\psi_i = \mathbf{0}$.

Yet this begs the question if a set of measurement operators exist, at least in the context of quantum computing. That gives rise to the next result, which ensures the existence if the state space is a Hilbert space as we defined it.

Proposition 2.31. *Let $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be an orthonormal basis on a (finite-dimensional) state space $\mathcal{H}$. Then*

$$\{|e_1\rangle\langle e_1|, \ldots, |e_n\rangle\langle e_n|\}$$

is a set of orthogonal projectors which satisfy Eq. (2.2.3)*.*

Proof. As a consequence of Theorem 2.8, the matrix of $|e_i\rangle\langle e_i|$ under the basis is all zeros except 1 in the entry of i^{th} row and i^{th} column. Thus,

$$(|e_i\rangle\langle e_i|)(|e_i\rangle\langle e_i|) = |e_i\rangle\langle e_i|$$

Additionally, by Theorem 2.11 the matrix of adjoint of the operator is the same as the operator, since the Hermitian conjugate matrix of a symmetric matrix with real coefficients is itself. Therefore, $(|e_i\rangle\langle e_i|)^\dagger = |e_i\rangle\langle e_i|$ and it follows $|e_i\rangle\langle e_i|$ is an orthogonal projector. Finally, by Theorem 2.8 again and the definition of orthogonal projector, the set satisfies Eq. (2.2.3). □

As an immediate consequence, for a $1-$qubit register we have

$$M_0 = |0\rangle\langle 0|, \quad M_1 = |1\rangle\langle 1| \tag{2.2.4}$$

form a set of measurement operators, given the computational basis. In this case, we say that the measurement is performed in the computational basis. Moreover, as convention we assign the labels depending on the outcome of the measurement

- classical bit '0' if state $|0\rangle$ is obtained,
- classical bit '1' if state $|1\rangle$ is obtained.

The term "classical bit" is used due to the collapse of the qubit in one and only one of the two states after the measurement under Eq. (2.2.4). Specifically, for a qubit in state $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ we have probability

$$p(0) = \langle q|M_0^\dagger M_0|q\rangle = \langle q|M_0|q\rangle = \alpha\langle q|0\rangle = \alpha\overline{\alpha} = |\alpha|^2$$

of getting the classic bit 0 after measurement, leaving it in state $|q_0\rangle = \frac{\alpha}{|\alpha|}|0\rangle$. As we can see there is only state $|0\rangle$ after the measurement. Analogously, with probability $p(i) = |\beta|^2$ we get classical bit 1 and $|q_1\rangle = \frac{\beta}{|\beta|}|1\rangle$ after the measurement.

Example 2.32. If a qubit in state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is measured, the math shows it has a 50% chance of yielding '0' and a 50% chance of yielding '1'. Observe that after the measurement, the original superposition is destroyed, and the qubit remains in the observed state $|0\rangle$ or $|1\rangle$.

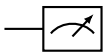


Figure 2.6: Quantum circuit representation of measurement of a single qubit. Source: own elaboration.

On the other hand, measurements within an $n-$qubit register for $n > 1$, that is, a system with multiple qubits, can be performed in two different ways: either totally or locally. For this work, we will only use local measurements, thereby we will only explain them. Nevertheless, total measurements are induced with ease from the latter.

First of all, observe

$$\{M_j = |j\rangle\langle j| \ : \ |j\rangle \text{ is in the computational basis}\} \tag{2.2.5}$$

is a set of measurements operators by Eq. (2.31). As convention, we assign the label classical bit 'j' if state $|j\rangle$ is obtained. Note that in an $n-$qubit register $|j\rangle = |j_{n-1}\cdots j_1 j_0\rangle$ where $j_i \in \{0, 1\}$, thus classical bit $j = j_{n-1}\cdots j_1 j_0$. From classical computing, classical $n-$bits represent uniquely the set of positive integers $\{0, 1, \ldots, 2^n - 1\}$ by

$$j_{n-1}2^{n-1} + \cdots + j_1 2^1 + j_0 2^0 \tag{2.2.6}$$

Therefore, for $0 \leq j < 2^n$, we will assume $|j\rangle \equiv |j_{n-1}\cdots j_1 j_0\rangle$ in an $n-$qubit register.

Example 2.33. In a $2-$qubit register, we apply total measurements through

$$M_{00} = |00\rangle\langle 00|, \ M_{01} = |01\rangle\langle 01|, \ M_{10} = |10\rangle\langle 10|, \ M_{11} = |11\rangle\langle 11|$$

By Eq. (2.2.6) this implies M_{00} measures classical bit '0', M_{01} '1', M_{10} '2', and M_{11} '3'.

Moving on, with respect partial measurements, we only measure the state of some qubits individually. Formally, express the $n-$qubit register as in Eq. (2.2.1):

$$\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{i_1} \otimes \cdots \otimes \mathcal{H}_{i_k} \otimes \cdots \otimes \mathcal{H}_n$$

where $\mathcal{H}_{i_1}, \ldots, \mathcal{H}_{i_k}$ are $1-$qubit subregisters where we want to perform a measurement. For each $j = 1, \ldots, k$, we can individually perform a measurement on $\mathcal{H}_{i_j}$ through the measurement operators $M_0^{i_j} = |0\rangle\langle 0|$ and $M_1^{i_j} = |1\rangle\langle 1|$. Then to perform a measurement on the whole $n-$qubit register we apply the set consisting of the measurement operators

$$M_{j_1 \cdots j_k}^{i_1 \cdots i_k} = I_1 \otimes \cdots \otimes M_{j_1}^{i_1} \otimes \cdots \otimes M_{j_k}^{i_k} \otimes \cdots \otimes I_n$$

where $j_1, \ldots, j_k = 0, 1$ and I_l is the identity operator on $\mathcal{H}_l$. Indeed they are measurement operators, since $M_0^{i_j} = |0\rangle\langle 0|$ and $M_1^{i_j} = |1\rangle\langle 1|$ are orthogonal projectors, implying that

$$\sum_{j_1, \ldots, j_k} (M_{j_1 \cdots j_k}^{i_1 \cdots i_k})^\dagger M_{j_1 \cdots j_k}^{i_1 \cdots i_k} = \sum_{j_1, \ldots, j_k} M_{j_1 \cdots j_k}^{i_1 \cdots i_k} = I_1 \otimes \cdots \otimes I_{i_1} \otimes \cdots \otimes I_{i_k} \otimes \cdots \otimes I_n = I$$

Although this set of measurement operators may seem abstract, in practice they are intuitive.

Example 2.34. Consider the quantum circuit on Figure 2.7.

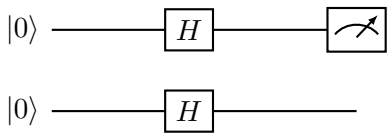


Figure 2.7: Quantum circuit with a partial measurement. Source: own elaboration.

The initial state is $|00\rangle$. After the Hadamard gates on both subregisters, we obtain the Bell state

$$|+\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

First we want to show $|+\rangle$ is a entangled state. Assume $|+\rangle$ is a product state $|\psi_A\rangle \otimes |\psi_B\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$ for complex scalars a, b, c, d. Expansion yields $ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$, necessitating $ac = bd = 1/\sqrt{2}$ and $ad = bc = 0$. The constraint $ad = 0$ implies either $a = 0$ or $d = 0$ by the zero-product property of the complex field $\mathbb{C}$. If $a = 0$, then $ac = 0$, contradicting $ac = 1/\sqrt{2}$; conversely, if $d = 0$, then $bd = 0$, contradicting $bd = 1/\sqrt{2}$. Since $|+\rangle$ cannot be decomposed into a pure tensor product.

At the end of the circuit, we want to measure only the first subregister. Since it is a partial measurement, we apply the measurement operators

$$M_0 = |0\rangle\langle 0| \otimes I, \quad M_1 = |1\rangle\langle 1| \otimes I$$

where we have omitted some subscripts and superscripts to simplify the notation. With probability $p(0) = \langle +|M_0|+\rangle = \frac{1}{2}$ we obtain the state $|0\rangle$ after measurement. Similarly, we obtain the state $|1\rangle$ with a probability $p(1) = 1/2$. Observe that we not only have two possible outcomes, but in the case of a Bell state the measurement of one of the qubits subregisters determines the other.

Chapter 3

Quantum Amplitude Estimation

In this chapter, we apply the mathematical and physical framework established in Chapter 2 to develop a specific quantum algorithm. We focus on moving from the abstract postulates of quantum mechanics to concrete, algorithmic steps that can be analyzed for complexity and error.

Formally, a quantum algorithm is a procedure performed on a quantum computer, typically realized as a sequence of unitary gates and measurements. These algorithms are designed to exploit the structure of Hilbert space to solve computational problems —such as estimating the mean of a random variable— with a query complexity significantly lower than that of the best possible classical algorithms [17].

We begin by systematically developing the Quantum Amplitude Estimation (QAE) algorithm from [8], dissecting its mathematical foundation where the estimation of an amplitude is transformed into an eigenvalue estimation problem. Subsequently, we analyze the precision of its estimations and the probability to bound them at a certain error, which will turn into the main result of the whole paper: Theorem 3.9. As a consequence, we will be able not only to confirm QAE offers a quadratic speedup over Classical Monte Carlo, but also a logarithmic bound to boost the success probability of this quantum algorithm.

3.1 The Grover operator

In this section, we present and study all the objects we need, which are taken mainly from [8]. In first place, let $\mathcal{A}$ be a quantum algorithm acting on an $n-$qubit register such that it uses no measurements. This implies evolution remains unitary, and we can reverse the algorithm through $\mathcal{A}^{-1}$. Secondly, let $|\Psi\rangle = \mathcal{A}|0\rangle$. It is important to remark that we have denoted $|0\rangle$ instead of $|0^{\otimes n}\rangle := |0\overset{n}{\cdots}0\rangle$ for simplicity. Lastly, let P be an orthogonal projector acting on the same $n-$qubit register. The aim of QAE is to estimate $a := \langle\Psi|P|\Psi\rangle$, and its brilliance stems from turning this problem into a problem of estimating eigenvectors of a certain operator $\mathbf{Q}$. In this section we will mathematically justify how a certain angle θ_a is able to estimate $a := \langle\Psi|P|\Psi\rangle$. The link between the two objects is the Grover operator

$$\mathbf{Q} := \mathbf{Q}(\mathcal{A}, P) := \mathcal{U}\mathcal{V} \quad \text{where } \mathcal{U} = 2|\Psi\rangle\langle\Psi| - I,\ \mathcal{V} = I - 2P \tag{3.1.1}$$

Both $\mathcal{U}$ and $\mathcal{V}$ are unitary operators. Indeed, for the latter we have

$$\mathcal{V}^\dagger = I^\dagger - 2P^\dagger = I - 2P = \mathcal{V}$$

By the properties of orthogonal projectors, we obtain $\mathcal{V}^2 = I$, implying $\mathcal{V}^\dagger = I$. A similar argument can be applied to $\mathcal{U}$ if we show $|\Psi\rangle\langle\Psi|$ is an orthogonal projector too. However, this can be done with ease: Proposition 2.4 ensures an orthonormal basis containing $|\Psi\rangle = \mathcal{A}|0\rangle$ which is a unit vector, and Theorem 2.8 gives us an associated matrix of $|\Psi\rangle\langle\Psi|$ similar to the identity matrix except for an -1 instead of a 1, making immediate to show it is actually an orthogonal projector by Theorem 2.11. Therefore $\mathbf{Q}$ is also unitary, since it is the composition of unitary operator.

The usefulness of $\mathbf{Q}$ stems from its simple action on the subspace $\mathcal{H}_\Psi$ spanned by the vectors $|\Psi_1\rangle := P|\Psi\rangle$ and $|\Psi_0\rangle = P^\perp|\Psi\rangle$, where $P^\perp$ is used to denote the same operator as in Proposition 2.15.

Lemma 3.1. *Under the same notation,*

$$\begin{aligned}\mathbf{Q}|\Psi_1\rangle &= (1-2a)|\Psi_1\rangle - 2a|\Psi_0\rangle\\ \mathbf{Q}|\Psi_0\rangle &= 2(1-a)|\Psi_1\rangle - (1-2a)|\Psi_0\rangle\end{aligned}$$

Proof. On the one hand, by the fact $|\Psi_1\rangle = P^2|\Psi\rangle = P|\Psi_1\rangle$ we obtain

$$\mathbf{Q}|\Psi_1\rangle = \mathcal{U}\mathcal{V}|\Psi_1\rangle = \mathcal{U}(|\Psi_1\rangle - 2P|\Psi_1\rangle) = \mathcal{U}(|\Psi_1\rangle - 2|\Psi_1\rangle) = -(2(\langle\Psi|\Psi_1\rangle)|\Psi\rangle - |\Psi_1\rangle)$$

By Proposition 2.15, we have $|\Psi\rangle = |\Psi_1\rangle + |\Psi_0\rangle$ and $\langle\Psi_1|\Psi_0\rangle = 0$; thus

$$\langle\Psi|\Psi_1\rangle = \langle\Psi_1|\Psi_1\rangle = \langle\Psi|P|\Psi\rangle =: a$$

Continuing the calculations,

$$\mathbf{Q}|\Psi_1\rangle = -(2a|\Psi\rangle - |\Psi_1\rangle) = -2a(|\Psi_1\rangle + |\Psi_0\rangle) + |\Psi_1\rangle = (1-2a)|\Psi_1\rangle - 2a|\Psi_0\rangle$$

On the other hand,

$$\begin{aligned}\mathbf{Q}|\Psi_0\rangle &= \mathcal{U}(|\Psi_0\rangle - 2P|\Psi_0\rangle) = \mathcal{U}(|\Psi_0\rangle - 2P|\Psi - \Psi_1\rangle) = \mathcal{U}(|\Psi_0\rangle \cancel{-2|\Psi_1\rangle + 2|\Psi_1\rangle})\\ &= 2(\langle\Psi|\Psi_0\rangle)|\Psi\rangle - |\Psi_0\rangle\end{aligned}$$

Observe

$$\langle\Psi|\Psi_0\rangle = \cancel{\langle\Psi_1|\Psi_0\rangle} + \langle\Psi_0|\Psi_0\rangle = \langle\Psi|P^\perp|\Psi\rangle = \langle\Psi|\Psi\rangle - \langle\Psi|P|\Psi\rangle = 1-a \tag{3.1.2}$$

since $P^\perp = I - P$ is an orthogonal projector. By elementary algebra, the second identity can be also proved. □

Observe Eq. (3.1.2) not only implies $\langle\Psi_0|\Psi_0\rangle = 1-a$, but also that $0 \leq a \leq 1$. Two simple yet important consequences are given rise. Firstly, by positive-definiteness $\dim(\mathcal{H}_\Psi) = 2$ if and only if $a \neq 0, 1$. If $a = j$ then $\mathcal{H}_\Psi = \operatorname{span}\{|\Psi_i\rangle\}$ where j is either 0 or 1. Secondly, a is uniquely represented by an angle $0 \leq \theta_a \leq \pi/2$ as

$$\sin^2(\theta_a) = a = \langle\Psi|P|\Psi\rangle \tag{3.1.3}$$

The angle θ_a will help us characterizing special eigenvalues of $\mathbf{Q}$, making us understand better the latter operator, as shown on the following result.

Proposition 3.2. *Under the same notation, if* $0 < a < 1$*, then* $\mathcal{H}_\Psi$ *has an orthonormal basis consisting of two eigenvectors of* $\mathbf{Q}$

$$|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{a}}|\Psi_1\rangle \pm \frac{i}{\sqrt{1-a}}|\Psi_0\rangle\right) \tag{3.1.4}$$

with associated eigenvalues $\lambda_\pm = e^{\pm i2\theta_a}$*.*

Proof. To find the eigenvectors, we must solve the eigenvalue equation $\mathbf{Q}|\Psi\rangle = \lambda|\Psi\rangle$. We can represent this problem using linear algebra in the basis $\{|\Psi_1\rangle, |\Psi_0\rangle\}$. On that basis, by Lemma 3.1, the matrix

$$\mathcal{Q} = \begin{pmatrix}(1-2a) & 2(1-a)\\ -2a & (1-2a)\end{pmatrix}$$

describes perfectly the action of $\mathbf{Q}$ restricted to the subspace $\mathcal{H}_\Psi$.

First we find the eigenvalues (λ) by solving the characteristic equation

$$\det\begin{pmatrix}(1-2a)-\lambda & 2(1-a)\\ -2a & (1-2a)-\lambda\end{pmatrix} = 0 \implies \lambda^2 - 2(1-2a)\lambda + 1 = 0$$

By Eq. (3.1.3), $a = \sin^2(\theta_a)$ 4 and $1 - 2a = 1 - 2\sin^2(\theta_a) = \cos(2\theta_a)$. Substituting this in:

$$\lambda^2 - 2\cos(2\theta_a)\lambda + 1 = 0$$

Using the quadratic formula,

$$\begin{aligned}\lambda_\pm &= \frac{2\cos(2\theta_a) \pm \sqrt{4\cos^2(2\theta_a) - 4}}{2} = \cos(2\theta_a) \pm \sqrt{\cos^2(2\theta_a) - 1}\\ &= \cos(2\theta_a) \pm \sqrt{-\sin^2(2\theta_a)} = \cos(2\theta_a) \pm i\sin(2\theta_a) = e^{\pm i2\theta_a}\end{aligned}$$

Now we find the eigenvector $|\Psi_\pm\rangle \equiv (z_1, z_0)$ under the basis for each eigenvalue. For the case $\lambda_+ = e^{i2\theta_a}$ we solve $(Q - \lambda_+ I)|\Psi_+\rangle = \mathbf{0}$:

$$\begin{pmatrix}(1-2a) - e^{i2\theta_a} & 2(1-a)\\ -2a & (1-2a) - e^{i2\theta_a}\end{pmatrix}\begin{pmatrix}z_1\\ z_0\end{pmatrix} = \begin{pmatrix}0\\ 0\end{pmatrix}$$

We choose to manipulate the second row for simplicity:

$$-2a(z_1) + ((1-2a) - e^{i2\theta_a})(z_0) = 0 \implies -2az_1 = i\sin(2\theta_a)z_0$$

Using $a = \sin^2(\theta_a)$ and $\sin(2\theta_a) = 2\sin(\theta_a)\cos(\theta_a)$:

$$\begin{aligned}-2\sin^2(\theta_a)z_1 = i(2\sin(\theta_a)\cos(\theta_a))z_0 &\implies -\sin(\theta_a)z_1 = i\cos(\theta_a)z_0\\ \implies \frac{z_1}{z_0} = \frac{i\cos(\theta_a)}{-\sin(\theta_a)} &= \frac{i\sqrt{1-a}}{-\sqrt{a}}\end{aligned}$$

Thus the eigenvector $|\Psi_+\rangle$ is proportional to $(i\sqrt{1-a}, -\sqrt{a})$ in coordinates. By multiplying the latter by the scalar $\frac{-i}{\sqrt{a(1-a)}}$ we obtain the former.

The case $\lambda_- = e^{-i2\theta_a}$ is solved analogously to the first case. Finally, the fact that $\{|\Psi_+\rangle, |\Psi_-\rangle\}$ is an orthonormal basis is immediate by the identities

$$\langle\Psi_1|\Psi_0\rangle = 0,\ \langle\Psi_1|\Psi_1\rangle = a,\ \langle\Psi_0|\Psi_0\rangle = 1 - a$$

. □

For $0 < a < 1$, Eq. (3.1.4) allows us to express $|\Psi\rangle = \mathcal{A}|0\rangle$ in the eigenvector basis as

$$\mathcal{A}|0\rangle = -\frac{i}{\sqrt{2}}(e^{i\theta_0}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle) \tag{3.1.5}$$

It is now immediate that after k applications of operator $\mathbf{Q}$, the state is

$$\mathbf{Q}^k|\Psi\rangle = \frac{-i}{\sqrt{2}}\left(e^{(2k+1)i\theta_a}|\Psi_+\rangle - e^{-(2k+1)i\theta_a}|\Psi_-\rangle\right) \tag{3.1.6}$$

For $a = 0 \iff \theta_a = 0$, we have $|\Psi_1\rangle = \mathbf{0}$ and $\mathbf{Q}|\Psi_0\rangle = |\Psi_0\rangle = \mathbf{Q}^k|\Psi_0\rangle$ by Lemma 3.1. Thus $\lambda_\pm = e^{\pm i2\theta_a}$ is the only eigenvalue of $\mathbf{Q}$ restricted to $\mathcal{H}_\Psi$ with associated eigenvectors $|\Psi_\pm\rangle = \pm i\frac{\sqrt{2}}{2}|\Psi_0\rangle$. This election of eigenvectors is made in order to be consistent with Eq. (3.1.5) and Eq. (3.1.6).

Similarly, for $a = 1 \iff \theta_a = \pi/2$, we have $|\Psi_0\rangle = \mathbf{0}$ and $\mathbf{Q}|\Psi_1\rangle = -|\Psi_1\rangle$ by Lemma 3.1, implying $\mathbf{Q}^k|\Psi_1\rangle = (-1)^k|\Psi_1\rangle$. Thus $\lambda_\pm = e^{\pm i2\theta_a}$ is the only eigenvalue of $\mathbf{Q}$ restricted to $\mathcal{H}_\Psi$ with associated eigenvectors $|\Psi_\pm\rangle = \frac{\sqrt{2}}{2}|\Psi_1\rangle$. This election of eigenvectors is made in order to be consistent with Eq. (3.1.5) and Eq. (3.1.6) too.

In conclusion, for all $0 \leq a \leq 1$ the problem of estimating $a = \sin^2(\theta_a)$, where $0 \leq \theta_a \leq \pi/2$, can be turned into a problem of estimating θ_a, taking advantage of the fact that any eigenvalue of operator $\mathbf{Q}$ restricted to the subspace $\mathcal{H}_\Psi$ is of the form $e^{\pm i2\theta_a}$. This gives rise to the following quantum algorithm, which is QAE.

Algorithm 1: Quantum Amplitude Estimation [8]

Input: A quantum algorithm $\mathcal{A}$ which uses no measurements such that $|\Psi\rangle = \mathcal{A}|0^{\otimes n}\rangle$, and an orthogonal projector P, both acting on a same $n-$qubit register; and another $m-$qubit register.

(i) Initialize both registers to the state $|0^{\otimes m}\rangle\mathcal{A}|0^{\otimes n}\rangle$,

(ii) Apply the quantum Fourier Transform $\mathcal{F}_m$ to the first register,

(iii) Apply the controlled sequence $\Lambda_{m,n}(\mathbf{Q})$ where $\mathbf{Q}$ is defined as in Eq. (3.1.1),

(iv) Apply the inverse of the quantum Fourier Transform, $\mathcal{F}_m^{-1}$ to the first register,

(v) Measure the first register and label the outcome $|y\rangle$,

(vi) Output $\hat{a} = \sin^2\left(\pi\frac{y}{M}\right)$.

The quantum Fourier Transform (QFT) mentioned in step 2 of Algorithm 1 is an operator which acts in the computational basis of an $m-$qubit register as

$$\mathcal{F}_m : |x\rangle \longmapsto \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1} e^{2\pi ixy/M}|y\rangle \quad \text{where } M = 2^m \text{ and } x \in \{0, \ldots, M-1\} \tag{3.1.7}$$

In this context, the QFT can be seen as a generalization of the $1-$qubit Hadamard gate, since it maps $|0\rangle$ to the state vector $\frac{1}{\sqrt{M}}(|0\rangle + \cdots + |M-1\rangle)$, where each state is equiprobable.

On the other hand, the controlled sequence is an operator which generalizes the concept of controlled gates. Given a unitary gate U acting on an $n-$qubit subregister, it takes an

$m-$qubit subregister as a control (*control subregister*) and applies k iterations of U on the targeted $n-$qubit subregister (*target subregister*). Specifically, $\Lambda_{m,n}(U)$ is defined by

$$\Lambda_{m,n}(U) = \sum_{j=0}^{M-1} |j\rangle\langle j| \otimes U^j \quad \text{where } M = 2^m \text{ and } j \in \{0 \dots, M-1\} \tag{3.1.8}$$

Note that if $|\Phi\rangle$ is an eigenvector of $\mathbf{U}$, its eigenvalue must have modulus 1, thus is of the form $e^{2\pi i\omega}$ for some $0 \leq \omega < 1$, since U is unitary. Then $\Lambda_{m,n}(\mathbf{U})$ maps $|j\rangle|\Phi\rangle$ to $e^{2\pi i\omega j}|j\rangle|\Phi\rangle$.

Before moving on, it is crucial to verify both operators are unitary to ensure Algorithm 1 is well-defined. That is what we show in the following result.

Proposition 3.3. *Under the same notation, the QFT $\mathcal{F}_m$ and the controlled sequence $\Lambda_{m,n}(U)$ are unitary operators. As a consequence, the inverse of the quantum Fourier Transform, $\mathcal{F}_m^{-1}$, exists.*

Proof. The easiest way to prove both operators are unitary is to show that they preserve the orthonormality of their respective computational bases. In the case of QFT, let $|\psi_x\rangle = \mathcal{F}_m|x\rangle$ and $|\psi_z\rangle = \mathcal{F}_m|z\rangle$, both $|x\rangle$ and $|z\rangle$ from the computational basis. We want to calculate the inner product $\langle\psi_z|\psi_x\rangle$. By the Dirac notation

$$|\psi_x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle \qquad \langle\psi_z| = \frac{1}{\sqrt{M}} \sum_{t=0}^{M-1} e^{-2\pi i \frac{zt}{M}} \langle t|$$

Observe $|\psi_x\rangle = |\psi_z\rangle$ if and only if $x = z$. Therefore, we obtain

$$\langle\psi_z|\psi_x\rangle = \frac{1}{M} \sum_{t=0}^{M-1} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M}(xy-zt)} \langle t|y\rangle = \frac{1}{M} \sum_{y=0}^{M-1} r^y$$

where $r = e^{2\pi i(x-z)/M}$, thus we have a geometric series. If $x = z$, then $r = 0$, implying $\langle\psi_z|\psi_x\rangle = (1/M)M = 1$. If $x \neq z$, then we can apply the formula of a geometric series $\frac{1-r^M}{1-r}$ to obtain

$$\langle\psi_z|\psi_x\rangle = \frac{1}{M} \frac{1 - e^{2\pi i(x-z)}}{1 - e^{2\pi i(x-z)/M}}$$

Since $x - z$ is an integer $e^{2\pi i(x-z)} = 1$, implying the inner product is 0.

For the case of $\Lambda_{m,n}(U)$, by properties of the adjoint we obtain

$$\Lambda_{m,n}(U)^\dagger = \sum_{j=0}^{M-1} |j\rangle\langle j| \otimes (U^\dagger)^j$$

For the operator to be unitary, and simplifying the notation, we must show that $\Lambda^\dagger\Lambda = I$. Indeed,

$$\Lambda^\dagger\Lambda = \left(\sum_k |k\rangle\langle k| \otimes (U^\dagger)^k\right) \left(\sum_j |j\rangle\langle j| \otimes U^j\right) = \sum_{j=0}^{M-1} |j\rangle\langle j| \otimes I = I_{control} \otimes I_{target} = I$$

where 'control' labels the $m-$*qubit* subregister and 'target' the $n-$qubit subregister. □

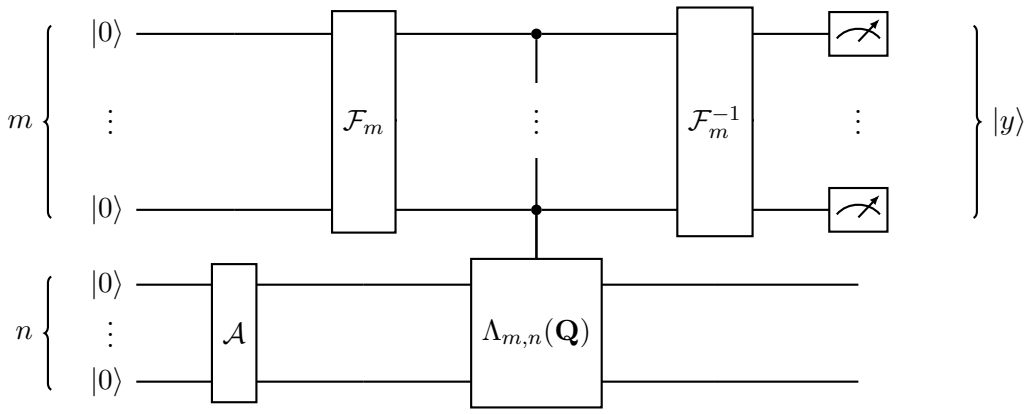


Figure 3.1: Quantum circuit for steps 1-5 of Algorithm 1. As a whole, it represents the operation $\left((\mathcal{F}_m^{-1} \otimes I_n)\Lambda_{m,n}(\mathbf{Q})(\mathcal{F}_m \otimes I_n)(I_m \otimes \mathcal{A})\right)|0^{\otimes m}\rangle|0^{\otimes n}\rangle$ before the measurement of $|y\rangle$. Source: own elaboration.

The major inconvenient of Algorithm 1 is that it is not deterministic, that is, not always gives the same output $\hat{a}$ in step 6. The reason of this event is because in step 5 we label outcome $|y\rangle$ as y, which is an integer from 0 to $2^m - 1$. Nevertheless, $\theta_a \neq \pi y/M$ in general. Thus errors on the estimations are practically unavoidable.

We conclude this section by analyzing the output of the Quantum Amplitude Estimation algorithm for a specific quantum algorithm $\mathcal{A}$. This concrete example will serve as a fundamental reference point throughout the remainder of this chapter; specifically, we will revisit and rigorously develop it in the subsequent sections, applying the mathematical tools and error bounds that we will introduce to validate the precision of the estimation.

Example 3.4. Consider the following algorithm that uses no measurements:

$$\mathcal{A} = R_Y(\theta_1) \otimes R_Y(\theta_2) \otimes R_Y(\theta_3) \otimes R_Y(\theta_4) \tag{3.1.9}$$

In first place, it is important to note this algorithm needs an $4-$qubit register ($n = 4$). We can also see it visually on Figure 3.2

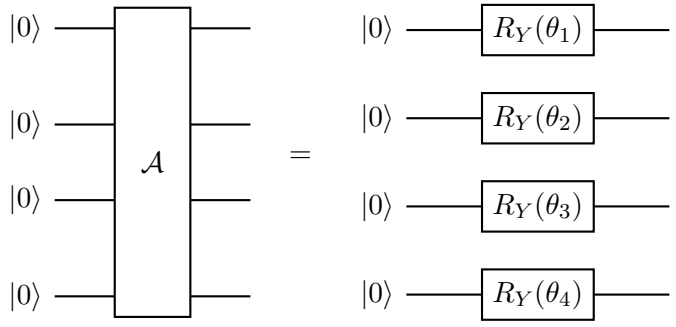


Figure 3.2: Quantum circuit of $\mathcal{A} = R_Y(\theta_1) \otimes R_Y(\theta_2) \otimes R_Y(\theta_3) \otimes R_Y(\theta_4)$. Source: own elaboration.

Secondly, the operator displayed is the single-qubit rotation gate $R_Y(\theta_k)$, which describes a rotation around the Y-axis by an angle θ_k. Since we will construct a similar operator

in Chapter 4, it is important to explain it a bit in detail. We can interpret in its matrix form as

$$R_Y(\theta_k) \equiv \begin{pmatrix} \cos\left(\frac{\theta_k}{2}\right) & -\sin\left(\frac{\theta_k}{2}\right) \\ \sin\left(\frac{\theta_k}{2}\right) & \cos\left(\frac{\theta_k}{2}\right) \end{pmatrix} \quad \text{for } k = 1, 2, 3, 4.$$

For this example (and the subsequent ones from this chapter), we will assume

$$(\theta_1, \theta_2, \theta_3, \theta_4) = (0.1,\ 0.2,\ 0.14,\ 0.16) \quad \text{and} \quad P = I \otimes I \otimes I \otimes |1\rangle\langle 1| \tag{3.1.10}$$

By the structure of P, it is clear we want to obtain the probability of measuring a '1' on the last qubit. Since in this case $\mathcal{A}$ results in a product state where each qubit is independently rotated, to obtain the probability it is sufficient to analyze $R_Y(\theta_4) = R_Y(0.16)$. Applying this to the state $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$:

$$|\psi_{\text{last}}\rangle = R_y(0.16)|0\rangle \equiv \begin{pmatrix} \cos(0.08) & -\sin(0.08) \\ \sin(0.08) & \cos(0.08) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(0.08) \\ \sin(0.08) \end{pmatrix}$$

Therefore, if $|\Psi\rangle = (R_Y(\theta_1) \otimes R_Y(\theta_2) \otimes R_Y(\theta_3) \otimes R_Y(\theta_4))|0000\rangle$, the probability of measuring a 1 on this qubit is

$$a = \langle\Psi|P|\Psi\rangle = \langle\psi_{\text{last}}|(|1\rangle\langle 1|)|\psi_{\text{last}}\rangle = \sin^2(0.08) \approx 0.638636\%$$

In this example, we will assume $m = 2$ for Algorithm 1. Thus, in step 5, we can only get as classical bits

$$y = 0 \equiv 00,\ y = 1 \equiv 01,\ y = 2 \equiv 10,\ y = 3 \equiv 1$$

which implies that in step 6 we will get as output respectively

$$\hat{a}_0 = \sin^2\left(\frac{0\pi}{2^2}\right) = 0,\ \hat{a}_1 = \sin^2\left(\frac{\pi}{4}\right) = 0.5 = \hat{a}_3,\ \hat{a}_2 = \sin^2\left(\frac{\pi}{2}\right) = 1$$

Measuring the errors of each estimation, we obtain

$$|a - \hat{a}_0| \approx 0.00638636,\ |a - \hat{a}_1| = |a - \hat{a}_3| \approx 0.49361364,\ |a - \hat{a}_2| \approx 0.99361364$$

As a conclusion, if $m = 2$, we would prefer to obtain as estimation $\hat{a}_0$ rather than the others, since it is the one that offers the minimum error.

3.2 Error minimization

This section is motivated by Example 3.4, where we obtained different outputs as estimations of Algorithm 1 (QAE) which offer different magnitudes of error with respect to the actual probability a. Here we develop the necessary tools which will culminate in Theorem 3.9, which not only ensures a huge probability of the estimations minimizing the error, but also a significant reduction when increasing the number of qubits from the $m-$qubit register. The results of this section are mainly based in [8].

It is important to note that errors in our estimate $\hat{\theta}_a = \pi y/M$ for θ_a translate into errors in our estimate $\hat{a} = \sin^2(\hat{\theta}_a)$ for a, as described in the next lemma.

Lemma 3.5. *Let $a = \sin^2(\theta_a)$ and $\hat{a} = \sin^2(\hat{\theta}_a)$ with $0 \leq \theta_a, \hat{\theta}_a \leq 2\pi$ then*

$$|\hat{\theta}_a - \theta_a| \leq \varepsilon \quad \Longrightarrow \quad |\hat{a} - a| \leq 2\varepsilon\sqrt{a(1-a)} + \varepsilon^2$$

Proof. For $\varepsilon \geq 0$, using standard trigonometric identities, we obtain

$$\sin^2(\theta_a + \varepsilon) - \sin^2(\theta_a) = \sqrt{a(1-a)}\sin(2\varepsilon) + (1-2a)\sin^2(\varepsilon) \text{ and}$$
$$\sin^2(\theta_a) - \sin^2(\theta_a - \varepsilon) = \sqrt{a(1-a)}\sin(2\varepsilon) + (2a-1)\sin^2(\varepsilon).$$

The inequality follows directly. □

By this lemma, we can shift to the error analysis of the angles. Hence, we need to define some objects involving them.

Definition 3.6. *For any integer $M = 2^m > 0$ and real number $0 \leq \omega < 1$, we define the state vector*

$$|\mathcal{S}_m(\omega)\rangle := \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \omega y} |y\rangle$$

Additionally, for any two real numbers $\omega_0, \omega_1 \in \mathbb{R}$, we define

$$d(\omega_0, \omega_1) := \min_{z \in \mathbb{Z}} \{|z + \omega_1 - \omega_0|\}$$

On the one hand, $|\mathcal{S}_m(\omega)\rangle$ is a state vector which encodes the angle $2\pi\omega$ in the amplitudes on equiprobable quantum states. Moreover, observe that for all $x \in \{0, \ldots, M-1\}$ we have the relation

$$\mathcal{F}_m |x\rangle = |\mathcal{S}_m(x/M)\rangle \tag{3.2.1}$$

On the other hand, for $\omega_0, \omega_1 \in \mathbb{R}$, $2\pi d(\omega_0, \omega_1)$ represents the length of the shortest arc on the unit circle going from $e^{2\pi i \omega_0}$ to $e^{2\pi i \omega_1}$. From its definition it immediately follows that $0 \leq d(\omega_0, \omega_1) \leq 1/2$. The following lemma establishes a crucial relation between these two recently defined concepts.

Lemma 3.7. *For $0 \leq \omega_0 < 1$ and $0 \leq \omega_1 < 1$ let $\Delta = d(\omega_0, \omega_1)$. If $\Delta = 0$ we have $|\langle \mathcal{S}_m(\omega_0) | \mathcal{S}_m(\omega_1)\rangle|^2 = 1$. Otherwise*

$$|\langle \mathcal{S}_m(\omega_0) | \mathcal{S}_m(\omega_1)\rangle|^2 = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)}$$

Proof. Note that if $\Delta = 0$, then $\omega_0 = \omega = 1$, thus $|\mathcal{S}m(\omega_0)\rangle = |\mathcal{S}m(\omega_1)\rangle$. Since every state vector is a unit vector, $|\langle \mathcal{S}_m(\omega_0) | \mathcal{S}_m(\omega_1)\rangle|^2 = 1$.

If $\Delta \neq 0$ then

$$\begin{aligned} |\langle \mathcal{S}_m(\omega_0) | \mathcal{S}_m(\omega_1)\rangle|^2 &= \left| \left(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{-2\pi i \omega_0 y} \langle y| \right) \left(\frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \omega_1 y} |y\rangle \right) \right|^2 \\ &= \frac{1}{M^2} \left| \sum_{y=0}^{M-1} e^{2\pi i \Delta y} \right|^2 = \frac{1}{M^2} \left| \frac{1 - e^{2\pi i \Delta M}}{1 - e^{2\pi i \Delta}} \right|^2 = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)} \end{aligned}$$

For the last equality we have factored out $e^{\pi i \Delta M}$ on the numerator and $e^{\pi i \Delta}$ on the denominator, and have used Euler's identity $e^{-ix} - e^{ix} = -2i\sin(x)$ where $x \in \mathbb{R}$. □

Consider the problem of estimating ω where $0 \leq \omega < 1$, given the state $|\mathcal{S}_m(\omega)\rangle$. If $\omega = x/M$ for some integer $0 \leq x < M$, then $\mathbf{F}_m^{-1}|\mathcal{S}_m(x/M)\rangle = |x\rangle$ by definition, and thus we have an exact estimator. If $M\omega$ is not an integer, then observing $\mathbf{F}_m^{-1}|\mathcal{S}_m(\omega)\rangle$ still provides a good estimation of ω [8], as shown in the following result.

Proposition 3.8. *Let X be the discrete random variable corresponding to the classical result of measuring $\mathcal{F}_m^{-1}|\mathcal{S}_m(\omega)\rangle$ in the computational basis. If $M\omega$ is an integer then* $\text{Prob}(X = M\omega) = 1$. *Otherwise, letting $\Delta = d(\omega, x/M)$,*

$$\text{Prob}(X = x) = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)} \leq \frac{1}{(2M\Delta)^2}$$

Furthermore,

$$\text{Prob}(d(X/M, \omega) \leq 1/M) \geq \frac{8}{\pi^2} \approx 0.81$$

Proof. By letting $|\Phi\rangle = \mathcal{F}_m^{-1}|\mathcal{S}_m(\omega)\rangle$, we obtain

$$\text{Prob}(X = x) = \langle\Phi|(|x\rangle\langle x|)|\Phi\rangle = |\langle x|\Phi\rangle|^2$$

Since $\mathcal{F}_m$ is unitary, $x \in \{0, \ldots, M-1\}$, and by Eq. (3.2.1), we then have

$$\text{Prob}(X = x) = |\langle x|F_m^{-1}|\mathcal{S}_m(\omega)\rangle|^2 = |\langle F_m x|\mathcal{S}_m(\omega)\rangle|^2 = |\langle S_m(x/M)|S_m(\omega)\rangle|^2$$

If $x = M\omega$, then Lemma 3.7 implies $\text{Prob}(X = x) = 1$. Otherwise, by the Lemma 3.7 again,

$$\text{Prob}(X = x) = \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)} \leq \frac{1}{M^2 \sin^2(\Delta\pi)}$$

To obtain another upper bound, we can minimize $\sin(\Delta\pi)$ by using Jordan's inequality:

$$\sin(y) \geq \frac{2}{\pi} y \quad \forall y \in [0, \pi/2]$$

which can be easily proved by the fact that $\sin(y)$ is a concave function on the interval $[0, \pi/2]$[1]. Since $0 \leq \Delta \leq 1/2$, Jordan's inequality proves the first part.

For the last part, observe the inequality $d(X/M, \omega) \leq 1/M$ is equivalent to $d(X, M\omega) \leq 1$. If $M\omega$ is an integer, then $\text{Prob}(d(X/M, \omega) \leq 1/M) = 1$ since $M\omega$ is a value of X. Otherwise, the only two integers from X that satisfy the inequality are $\lfloor M\omega \rfloor$ and $\lceil M\omega \rceil$, where $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ denote the floor and ceiling function respectively. Since these two values are integers from X

$$\begin{aligned} \text{Prob}(d(X/M, \omega) \leq 1/M) &= \text{Prob}(X = \lfloor M\omega \rfloor) + \text{Prob}(X = \lceil M\omega \rceil) \\ &= \frac{\sin^2(M\Delta\pi)}{M^2 \sin^2(\Delta\pi)} + \frac{\sin^2\left(M\left(\frac{1}{M} - \Delta\right)\pi\right)}{M^2 \sin^2\left(\left(\frac{1}{M} - \Delta\right)\pi\right)} \end{aligned} \tag{3.2.2}$$

where for the last equality we have applied the first part of the result with $\Delta = d(\omega, \lfloor M\omega \rfloor/M)$, implying $d(\omega, \lceil M\omega \rceil/M) = 1/M - \Delta$ since $\lfloor M\omega \rfloor < M\omega < \lceil M\omega \rceil$.

[1] Indeed, its second derivative, $-\sin(y)$ is negative for all $y \in [0, \pi/2]$, implying its concavity. Since $f(y) = \frac{2}{\pi} y$ is geometrically the line which connects points $(0, 0)$ and $(\pi/2, 1)$, by the concavity it must be less or equal that $\sin(y)$ on the closed interval.

According to [8], Eq. (3.2.2) attains its minimum at $\Delta = 1/(2M)$ when $0 \leq \Delta \leq 1/M$ for $M > 2$. Hence, substituting $\Delta = \frac{1}{2M}$ into the probability formula yields

$$\text{Prob}(d(X/M, \omega) \leq 1/M) \geq \frac{1}{M^2 \sin^2(\frac{\pi}{2M})} + \frac{1}{M^2 \sin^2(\frac{\pi}{2M})} = \frac{2}{M^2 \sin^2(\frac{\pi}{2M})}$$

By using the fact that $\sin(y) \leq y$ for all $y < 0$

$$\text{Prob}(d(X/M, \omega) \leq 1/M) \geq \frac{2}{M^2 \sin^2(\frac{\pi}{2M})} \geq \frac{2}{M^2(\frac{\pi}{2M})^2} = \frac{8}{\pi^2}$$

For $M = 1, 2$, $\text{Prob}(d(X/M, \omega) < 1/M) = 1 \geq 8/\pi^2$ since $0 \leq d(\omega_0, \omega_1) \leq 1/2$ for all $\omega_0, \omega_1 \in \mathbb{R}$. □

We are now in a position to synthesize the mathematical tools developed throughout this section —specifically the trigonometric error propagation from Lemma 3.5 and the probabilistic bounds derived in Proposition 3.8— to formally state the fundamental result of this work. By combining these findings, we can move beyond the analysis of isolated components to rigorously quantify the global accuracy of the Quantum Amplitude Estimation algorithm, establishing a direct link between the physical resources employed and the precision achieved.

The following theorem encapsulates the core computational advantage of this method. It explicitly demonstrates that the estimation error is suppressed as the dimension of the auxiliary register $M = 2^m$ increases, allowing us to minimize the error to an arbitrary degree simply by adding qubits to the control register. Crucially, this result confirms that such high precision is attained with a robust success probability that remains strictly bounded from below, independent of the system's size.

Theorem 3.9. *In the same way as we have defined it, Algorithm 1 outputs $\hat{a}$, an estimate of $a = \langle\Psi|P|\Psi\rangle$, such that*

$$|\hat{a} - a| \leq 2\pi \frac{\sqrt{a(1-a)}}{M} + \frac{\pi^2}{M^2} \tag{3.2.3}$$

with probability at least $8/\pi^2$, using exactly M evaluations of the Grover operator $\mathbf{Q}$.

Proof. After step 1, by Eq. (3.1.5), we obtain

$$|0\rangle\mathcal{A}|0\rangle = \frac{-i}{\sqrt{2}}|0\rangle \left(e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle\right)$$

After applying $\mathcal{F}_m$ from step 2, we have the state vector

$$-\frac{i}{\sqrt{2M}} \sum_{j=0}^{M-1} |j\rangle \left(e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle\right)$$

After applying $\Lambda_{m,n}(\mathbf{Q})$ from step 3, by Eq. (3.1.6) we have

$$\begin{aligned}
&-\frac{i}{\sqrt{2M}}\sum_{j=0}^{M-1}|j\rangle\mathbf{Q}^j\left(e^{i\theta_a}|\Psi_+\rangle - e^{-i\theta_a}|\Psi_-\rangle\right)\\
&= -\frac{i}{\sqrt{2M}}\sum_{j=0}^{M-1}|j\rangle\left(e^{i\theta_a}e^{2ij\theta_a}|\Psi_+\rangle - e^{-i\theta_a}e^{-2ij\theta_a}|\Psi_-\rangle\right)\\
&= -e^{i\theta_a}\frac{i}{\sqrt{2M}}\sum_{j=0}^{M-1}e^{2ij\theta_a}|j\rangle|\Psi_+\rangle + e^{i\theta_a}\frac{i}{\sqrt{2M}}\sum_{j=0}^{M-1}e^{-2ij\theta_a}|j\rangle|\Psi_-\rangle\\
&= -e^{i\theta_a}\frac{i}{\sqrt{2M}}\left[\left|\mathcal{S}_m\left(\frac{\theta_a}{\pi}\right)\right\rangle|\Psi_+\rangle - \left|\mathcal{S}_m\left(1-\frac{\theta_a}{\pi}\right)\right\rangle|\Psi_-\rangle\right]
\end{aligned}$$

For the last equality, we have used the identities $2ij\theta_a = 2\pi ij\theta_a/\pi$ and $\exp(-2ij\theta_a) = \exp(-2\pi ij\theta_a/\pi + 2\pi ij)$. Also observe that $\left|\mathcal{S}_m\left(\frac{\theta_a}{\pi}\right)\right\rangle$ and $\left|\mathcal{S}_m\left(1-\frac{\theta_a}{\pi}\right)\right\rangle$ are well defined since we established $0 \le \theta_a \le \pi/2$.

After applying $\mathcal{F}_m^{-1}$ from step 4, we obtain the state vector

$$-e^{i\theta_a}\frac{i}{\sqrt{2M}}\left[\left(\mathcal{F}_m^{-1}\left|\mathcal{S}_m\left(\frac{\theta_a}{\pi}\right)\right\rangle\right)|\Psi_+\rangle - \left(\mathcal{F}_m^{-1}\left|\mathcal{S}_m\left(1-\frac{\theta_a}{\pi}\right)\right\rangle\right)|\Psi_-\rangle\right]$$

Since after a measurement in the computational basis we always obtain an integer between 0 and $M-1$, if either $\mathcal{F}_m^{-1}\left|\mathcal{S}_m\left(\frac{\theta_a}{\pi}\right)\right\rangle$ or $\mathcal{F}_m^{-1}\left|\mathcal{S}_m\left(1-\frac{\theta_a}{\pi}\right)\right\rangle$ is a decimal number, we will have different probabilities of obtaining different outcomes after step 5.

If we measure the first component, we get an outcome y such that $y/M \approx \frac{\theta_a}{\pi}$, by Eq. (3.2.1). Otherwise, if we measure the second component, we effectively measure a value y' such that $y'/M \approx 1 - \frac{\theta_a}{\pi}$. Note this corresponds to an outcome of $M-y$ relative to the first case. However, since $\sin^2(x) = \sin^2(\pi - x)$ for all $x \in \mathbb{R}$, both outcomes yield the same estimate. Indeed,

$$\hat{a} = \sin^2\left(\pi\frac{y}{M}\right) = \sin^2\left(\pi\left(1-\frac{y}{M}\right)\right) = \sin^2\left(\pi\frac{M-y}{M}\right)$$

Since the final calculated probability of obtaining $\hat{a}$ is identical in both cases, we can simply assume we measured $|y\rangle$ given the state $F_M^{-1}|\mathcal{S}_M(\frac{\theta_a}{\pi})\rangle$. By Proposition 3.8, we have a probability of $8/\pi^2$ of getting $d(y/M, \theta_a/\pi) \le 1/M$. Since $0 \le y/M$, $\theta_a/\pi \le 1$, we obtain

$$\left|\frac{y}{M} - \frac{\theta_a}{\pi}\right| = d\left(\frac{y}{M}, \frac{\theta_a}{\pi}\right) \le \frac{1}{M} \implies \left|\pi\frac{y}{M} - \theta_a\right| \le \frac{\pi}{M}$$

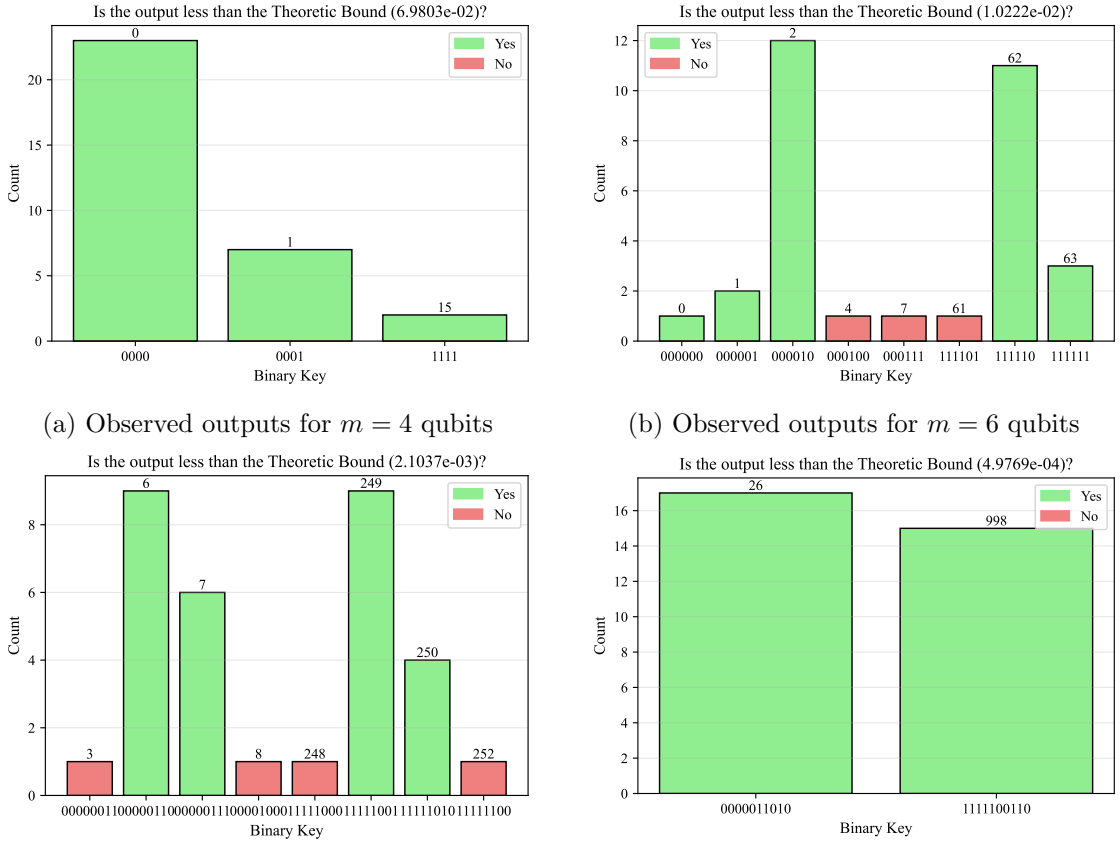
Since our estimate $\hat{\theta}_a = \pi\frac{y}{M}$, we obtain the bound $|\hat{\theta}_a - \theta_a| \le \frac{\pi}{M}$. Consequently, by setting $\varepsilon = \frac{\pi}{M}$ and invoking Lemma 3.5 we can obtain the desired upper bound.

Finally, the fact that Algorithm 1 uses exactly M evaluations of operator $\mathbf{Q}$ follows directly from the definition of the operator $\Lambda_{m,n}(\mathbf{Q})$ used in step 3. □

Having established the theoretical upper bounds for the estimation error and the associated success probability, we now turn to a practical verification of these results. In the following example, which serves as a direct continuation of Example 3.4, we apply the conditions of Theorem 3.9 to the specific algorithmic setup previously introduced. This numerical analysis will allow us to rigorously test the validity of the derived bounds and

to explicitly observe the asymptotic decay of the error as the dimension of the evaluation register M increases.

Example 3.10. We are still assuming $\mathcal{A}$ is defined in the same way as in Eq. (3.1.9) with the same parameters as in Eq. (3.1.10). The main difference is that now we want to analyze the frequency of output estimations for $m = 4, 6, 8, 10$. Data processing and figure generation were performed using scripts developed in Python 3.13.5 and Qiskit 2.2.3 [22].



(a) Observed outputs for $m = 4$ qubits

(b) Observed outputs for $m = 6$ qubits

(c) Observed outputs for $m = 8$ qubits

(d) Observed outputs for $m = 10$ qubits

Figure 3.3: Frequency distribution of QAE outputs over $N = 32$ independent runs for register sizes $m \in \{4, 6, 8, 10\}$. Green bars indicate estimates satisfying the error bound of Theorem 3.9, while red bars represent those outside the theoretical limit. Source: own elaboration.

We perform the Algorithm 1 $N = 32$ independent times for different amounts of $m \in \{4, 6, 8, 10\}$ qubits on the measurement register. The results are summarized in Figure 3.3, where the horizontal axis represents the observed output y (displayed in binary format with its decimal equivalent above the bar) and the vertical axis represents the frequency of that specific outcome. A bar is colored green if the resulting estimate $\hat{a}$ satisfies the following bound almost identical to the error bound Eq. (3.2.3),

$$\frac{1}{2M} + \frac{\pi^2}{M^2} \tag{3.2.4}$$

and red otherwise, since $\frac{1}{2} \lesssim 2\pi\sqrt{a(1-a)}$ when $a \approx 0.638636\%$ (the actual probability in

this case). We use in the example this bound instead of Eq. (3.2.3) for numerical stability.

For the cases of $m = 4$ and $m = 10$ (Figure 3.3a and Figure 3.3d respectively), we observe a robust behavior where every single execution of the algorithm successfully yields an estimate within the theoretical bounds. Specifically, for $m = 4$, the outputs $y \in \{0, 1, 15\}$ accumulate frequencies of 23, 7, and 2 respectively, totaling the 32 runs with a 100% success rate. Similarly, for $m = 10$, the outputs concentrate exclusively on $y = 26$ and $y = 998$, again achieving a 100% success rate. These empirical results far exceed the theoretical lower bound for success probability established: $P_{succ} \geq 8/\pi^2 \approx 81.06\%$.

In the experiments with $m = 6$ and $m = 8$ (Figure 3.3b and Figure 3.3c respectively), we observe the appearance of "red" bars, indicating instances where the estimation error exceeded the theoretical threshold. For $m = 6$, we record failures at outputs $y \in \{4, 7, 61\}$ with a frequency of 1 each, resulting in 3 total failures against 29 successes. This corresponds to an empirical success probability of $29/32 \approx 90.6\%$. For $m = 8$, failures occur at outputs $y \in \{3, 8, 248, 252\}$, again with a frequency of 1 each, yielding 4 failures and 28 successes. This results in a success rate of $28/32 = 87.5\%$.

Crucially, in all scenarios tested, the empirical success probability remains strictly greater than the lower bound of $8/\pi^2$ guaranteed by Theorem 3.9. This confirms that while the algorithm is probabilistic and susceptible to projection errors, the probability of these errors is bounded. Furthermore, the results illustrate the relationship between the precision and the register size $M = 2^m$: as we increase m, the "theoretical bound" Eq. (3.2.4) displayed in the histograms decreases rapidly (from $\approx 6.98 \times 10^{-2}$ at $m = 4$ to $\approx 4.98 \times 10^{-4}$ at $m = 10$), yet the probability of finding the estimate within this tightening window remains consistently high.

To further validate the asymptotic behavior derived in Theorem 3.9, we compare the theoretical upper bound Eq. (3.2.3) against the actual estimation error $|\hat{a} - a|$ across a range of $m-$qubit registers for measure where $m \in \{1, \ldots, 20\}$. The results are visualized in Figure 3.4.

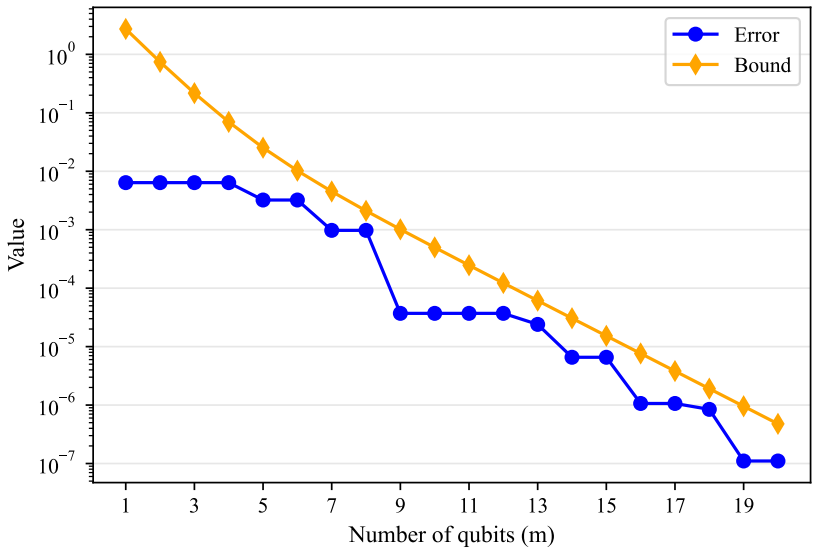


Figure 3.4: Comparison of the empirical estimation error $|\hat{a} - a|$ (blue) versus the theoretical upper bound derived in Theorem 3.9 (orange) as a function of the number of evaluation qubits m. Source: own elaboration.

Three key observations emerge from this numerical experiment. First, the actual error consistently respects the derived inequality, remaining strictly below the theoretical bound for all values of m. Second, the theoretical bound exhibits a linear decay on the logarithmic scale, confirming the exponential suppression of error with respect to the number of qubits m. Finally, the empirical error displays a characteristic step-like behavior rather than a smooth monotonic decrease. This phenomenon is a direct consequence of the discretization of the outcome space; as M increases, the grid of possible estimates y/M refines, but the distance between the true value a and the nearest grid point does not necessarily decrease at every increment of m. Nevertheless, the global trend confirms that increasing the qubit register size is an effective strategy for achieving high-precision estimates.

3.3 Quadratic speedup over Monte Carlo

In this section, we formalize the computational advantage of QAE presented on Theorem 3.9 by analyzing its asymptotic behavior compared to classical Monte Carlo methods. To establish a rigorous comparison of the convergence rates, we first introduce the Big-O notation, which provides the necessary mathematical language to describe how the query complexity scales with the required precision [23]. By applying this formalism to the error bounds derived previously, we will demonstrate the quadratic speedup that characterizes the quantum approach.

Definition 3.11. *Let $f(n)$ and $g(n)$ be functions mapping non-negative integers to non-negative real numbers. We say that $f(n)$ is in $\mathcal{O}(g(n))$ if and only if:*

$$\exists C > 0, \exists n_0 > 0 \text{ such that } \forall n \geq n_0, 0 \leq f(n) \leq Cg(n)$$

Strictly speaking, $\mathcal{O}(g(n))$ defines a set of functions. Therefore, the mathematically correct notation is $f(n) \in \mathcal{O}(g(n))$. However, by convention and abuse of notation, we will write it as $f(n) = \mathcal{O}(g(n))$.

With the definition of asymptotic behavior established, we can now rigorously quantify the convergence rate of the Quantum Amplitude Estimation algorithm. In the following example, we apply the Big-O notation to the explicit error bound derived in Eq. (3.2.3). Our objective is to formally demonstrate that the estimation error scales as $\mathcal{O}(1/M)$, hence providing the mathematical justification for the superior query complexity of the quantum approach compared to classical methods [5].

Example 3.12. Consider the function $f(M) = 2\pi\frac{\sqrt{a(1-a)}}{M} + \frac{\pi^2}{M^2}$ from Eq. (3.2.3). We want to prove $f(M) = \mathcal{O}\left(\frac{1}{M^2}\right)$. If $M_0 = 1$ we have $M^2 \geq M$ for all $M \geq M_0$, and consequently $\frac{1}{M^2} \leq \frac{1}{M}$. We can bound the original expression by replacing $\frac{1}{M^2}$ with $\frac{1}{M}$:

$$f(M) = \frac{2\pi\sqrt{a(1-a)}}{M} + \frac{\pi^2}{M^2} \leq \frac{2\pi\sqrt{a(1-a)}}{M} + \frac{\pi^2}{M} = \frac{1}{M}\left(2\pi\sqrt{a(1-a)} + \pi^2\right)$$

Since the term in parentheses is a constant relative to M, let $C = 2\pi\sqrt{a(1-a)} + \pi^2$. The inequality holds for all $M \geq M_0$, thus $f(M) = \mathcal{O}\left(\frac{1}{M}\right)$.

Having formally derived the asymptotic behavior of QAE, it is crucial to contextualize this result within the broader landscape of stochastic estimation. Since Monte Carlo approximation constitute the classical algorithm for industry standard for valuing financial

derivatives and assessing risk [11], it serves as the ideal comparison object for evaluating the practical utility of our quantum approach [4]. We will briefly define the classical approximation and state an expression for the Root Mean Square Error (RMSE) of this algorithm, whose proof can be found in [24].

Definition 3.13. *Let $X, X_1, \ldots, X_M$ be real-valued independent and identically distributed (i.i.d.) random variables such that its expected value $\mathbb{E}[|X|] < \infty$ and its variance $\mathrm{Var}[X] < \infty$. The **Monte Carlo approximation** of $\mu := \mathbb{E}[X]$ is defined as the random variable*

$$\hat{\mu}_M := \frac{1}{M} \sum_{i=1}^{M} X_i \tag{3.3.1}$$

The well-known *strong law of large numbers* in probability theory ensures that increasing the number of samples (M) in Eq. (3.3.1) ensures the convergence $\hat{\mu}_M \to \mu$ [24].

Proposition 3.14. *Let $\hat{\mu}_M$ be the Monte Carlo approximation of μ for any $M \in \mathbb{N}$. Then the RMSE of $\hat{\mu}_M$ is*

$$RMSE(\hat{\mu}_M) := \sqrt{\mathbb{E}[(\hat{\mu}_M - \mu)^2]} = \mathcal{O}\left(\frac{1}{\sqrt{M}}\right)$$

To validate the theoretical speedup derived in this section, we will return to the specific problem configuration from Example 3.4. In this comparative analysis, we contrast the asymptotic behavior of the estimation error obtained via QAE against the RMSE characteristic of classical Monte Carlo methods. Our primary objective is to empirically verify the distinct scaling laws governing these approaches, explicitly demonstrating the divergence between the classical $\mathcal{O}(1/\sqrt{M})$ regime and the quantum $\mathcal{O}(1/M)$ convergence rate as the computational resources increase.

Example 3.15. We are still assuming $\mathcal{A}$ is defined in the same way as in Eq. (3.1.9) with the same parameters as in Eq. (3.1.10). We compare the convergence properties of Algorithm 1 against classical Monte Carlo by plotting the absolute estimation error $|\hat{a} - a|$ as a function of the number of samples M, where M ranges over powers of two from 2^1 to 2^{20}. The results are visualized in Figure 3.5.

The empirical data provides clear visual verification of the theoretical speedup derived in Section 3.3. The QAE error (blue) follows a steep descent consistent with a slope of -1 on the logarithmic scale, validating the $\mathcal{O}(1/M)$ convergence rate. We observe once again the characteristic step-like behavior inherent to the quantization of the angle estimation, yet the global trend strictly adheres to the theoretical bound. In contrast, the Monte Carlo error (orange) exhibits a significantly shallower decay, fluctuating around a slope of -0.5, which characterizes the slower $\mathcal{O}(1/\sqrt{M})$ convergence.

Crucially, the quadratic speedup is definitively present. As the number of samples increases, the gap between the two curves widens substantially; for instance, at 2^{19} samples, the quantum algorithm achieves a precision orders of magnitude superior to its classical counterpart. This divergence empirically confirms that QAE requires quadratically fewer resources to achieve a target precision ϵ, or conversely, yields a quadratically smaller error for a fixed computational budget.

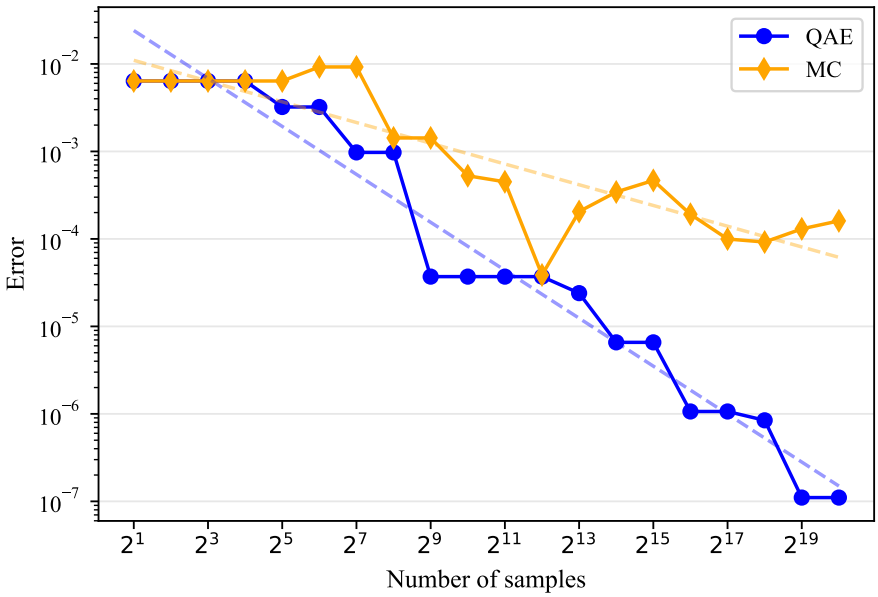


Figure 3.5: Comparison of estimation error $|\hat{a} - a|$ for QAE (blue) and Monte Carlo (orange) versus sample count M. The distinct slopes empirically validate the quadratic speedup of the quantum algorithm. Source: own elaboration.

3.4 Boosting the success probability

Although Theorem 3.9 establishes a specific error bound for our estimate, it guarantees success with a constant probability of approximately 0.81. In practical financial contexts, where high reliability is paramount, this confidence level is often insufficient. To address this limitation, we aim to amplify the success probability to an arbitrary level $1 - \delta$ by repeating the algorithm independently N times and taking the median of the resulting estimates. Consequently, our immediate goal is to derive a bound on N that ensures the median estimate remains within the desired precision ϵ with high probability.

This necessity leads us to introduce the following lemma, whose prove can be found in [25]. This fundamental result from probability theory will serve as the crucial tool for the subsequent proposition, allowing us to prove that the failure probability decays exponentially with the number of repetitions.

Lemma 3.16 (Hoeffding's Inequality)**.** *Let $X_1, \ldots, X_n$ be independent random variables such that $0 \leq X_i \leq 1$ for all $i = 1, \ldots, n$. If we denote $S_n = \sum_{i=1}^{n} X_i$, then for $0 < t < 1 - \frac{\mathbb{E}[S_n]}{n}$*

$$\text{Prob}\left(\frac{S_n}{n} - \frac{\mathbb{E}[S_n]}{n} \geq t\right) \leq \exp(-2nt^2)$$

Proposition 3.17. *Let $\mathcal{A}$ be a (classical or quantum) algorithm aiming to estimate a quantity μ, whose output $\hat{\mu}$ satisfies $|\mu - \hat{\mu}| \leq \epsilon$ with probability at least $1 - \gamma$, for some fixed failure probability $\gamma < \frac{1}{2}$. For any desired target failure probability $\delta > 0$, let the algorithm $\mathcal{A}$ be repeated N independent times, where N satisfies:*

$$N \geq \frac{\ln(1/\delta)}{2(1/2 - \gamma)^2} \tag{3.4.1}$$

Then, the median of these N estimates is accurate to within ϵ with probability at least $1-\delta$.

Proof. Let X_i be an indicator where $X_i = 1$ if the i-th run is "bad" (outside the range $|\hat{\mu} - \mu| \leq \epsilon$) and 0 otherwise. The median fails if the sum

$$S_N = \sum_{i=1}^{N} X_i \geq N/2 \iff \frac{S_N}{N} - \gamma \geq \frac{1}{2} - \gamma$$

Since $P(X_i = 1) = \gamma < 1/2$, one can obtain with ease that $\mathbb{E}[S_N]/N = \gamma$. Hence, we can invoke Hoeffding's Inequality for $t = \frac{1}{2} - \gamma$ to obtain

$$\text{Prob}\left(\frac{S_N}{N} - \gamma \geq t\right) \leq \exp\left(-2N\left(\frac{1}{2} - \gamma\right)^2\right)$$

We require this failure probability to be at most δ:

$$\exp\left(-2N\left(\frac{1}{2} - \gamma\right)^2\right) \leq \delta$$

By taking the natural logarithm and multiplying by -1 on both sides we obtain the desired inequality. □

We conclude this section by applying Eq. (3.4.1) to determine the computational cost required to ensure high reliability. Suppose we demand a success probability of 99.75%, which corresponds to a target failure probability of $\delta = 0.0025$. Recalling Theorem 3.9, the failure probability of a single QAE run is bounded by $\gamma \leq 1 - 8/\pi^2 \approx 0.19$. Substituting these values into the inequality derived in the proposition yields:

$$N \geq \frac{\ln(1/0.0025)}{2(0.5 - 0.19)^2} = \frac{\ln(400)}{2(0.31)^2} \approx 31.1$$

Therefore, by strictly rounding up, we determine that repeating the algorithm $N = 32$ times and taking the median is sufficient to satisfy the reliability requirement. Crucially, because this factor N depends only on the desired confidence level and not on the precision ϵ, the total query complexity of the Quantum Monte Carlo method remains $\mathcal{O}(1/M)$.

Example 3.18. The data from Figure 3.3 explicitly corroborates the effectiveness of the probability-boosting strategy derived in Proposition 3.17. Recall that by setting $N = 32$, we aimed to ensure that the median estimate satisfies the error bound with a probability of at least 99.75%. For the median to fail, the number of erroneous estimates (red bars) would need to exceed $N/2 = 16$. In our experiments, the maximum number of failures observed is merely 4, falling well below the critical threshold. Consequently, the median of these 32 independent runs successfully converges to a value within the theoretical error bound in every case, demonstrating that the calculated redundancy is sufficient to satisfy high-reliability requirements.

Chapter 4

Application to Credit Risk

Having established the rigorous mathematical foundation of Quantum Amplitude Estimation (QAE) in Chapter 3, we now turn our attention to its practical utility within the financial sector. The analysis conducted previously culminated in Theorem 3.9, a pivotal result that explicitly bounds the estimation error and guarantees a quadratic speedup over classical Monte Carlo methods. In this chapter, we leverage this theoretical advantage to address a specific and computationally demanding problem: the analysis of credit risk [13].

We organize this application into three sections. First, we formally define the financial metrics of interest, specifically Value at Risk (VaR) and Economic Capital Requirement (ECR), framing them as rare-event simulation problems where classical convergence is notoriously slow [12]. Adapted from the previous reference, we construct a specialized quantum circuit that encodes the loss distribution of a portfolio into the quantum state, allowing us to utilize QAE as a subroutine to evaluate the cumulative distribution function with the high precision guaranteed by Theorem 3.9. Finally, we validate this framework through a numerical experiment, empirically demonstrating that the quantum algorithm achieves the predicted accuracy and reliability essential for modern risk management.

4.1 Risk metrics

In this section, we formally define the specific financial metrics that serve as the target of our estimation: Value at Risk (VaR) and Economic Capital Requirement (ECR). While the expected loss provides a measure of the central tendency of the performance of a financial company's portfolio, effective risk management requires a rigorous quantification of extreme adverse events located in the "tails" of the loss distribution [13]. Consequently, we introduce the mathematical framework for these metrics and specify the simplified portfolio model—characterized by independent default probabilities—upon which we will deploy our quantum algorithm.

Definition 4.1. *Let $(L_1, \dots, L_K) \in \mathbb{R}^K_{\geq 0}$ be the random vector which represents the loss of the k^{th} asset on a financial institution's portfolio for all $k = 1, \dots, K$. If we denote as $\mathcal{L} = \sum_{k=1}^{K} L_k$ the total loss of the portfolio, the **Value at Risk (VaR)** for a given a confidence level $\alpha \in [0, 1]$ is*

$$\mathrm{VaR}_\alpha[\mathcal{L}] := \inf_{x \geq 0} \{x \mid \mathrm{Prob}(\mathcal{L} \leq x) \geq \alpha\} \tag{4.1.1}$$

Additionally, the ***Economic Capital Requirement (ECR)*** *at confidence level* α *is*

$$\mathrm{ECR}_\alpha[\mathcal{L}] := \mathrm{VaR}_\alpha[\mathcal{L}] - \mathbb{E}[\mathcal{L}] \tag{4.1.2}$$

VaR serves as the regulatory standard for quantifying the maximum expected loss of a portfolio over a specific horizon, specifically targeting extreme adverse events located in the "tails" of loss distributions. The ECR defines the additional capital reserves an institution must maintain beyond expected losses to ensure continued solvency during periods of high default risk. Together, these fundamental metrics provide the mathematical framework necessary for financial institutions to assess stability and manage rare-event risks.

For simplification, we will only consider the ECR related to default risk, that is, the loss that occurs when an obligor does not fulfill the payment of an associated passive, and which is an active of the firm. Additionally, we assume that all losses are independent, thus the loss of each asset can be expressed as $L_k = \lambda_k X_k$, where λ_k is a positive integer and $X_k \in \{0, 1\}$ is a Bernoulli random variable with probability p_k for all $k = 1, \ldots, K$. Equivalently, with probability $\mathrm{Prob}(X_k = 1) = p_k$ we get a default for the k^{th} asset whose amount is λ_k, which is also the amount that the institution losses[1].

From all these assumptions, it is clear that $\mathbb{E}[\mathcal{L}] = \sum_{k=1}^{K} \lambda_k p_k$, due to the linearity of the expected value, and can be calculated it using classical computers. Thus, the challenge from Eq. (4.1.2) is to calculate $\mathrm{VaR}_\alpha[\mathcal{L}]$, which usually requires Monte Carlo simulations.

4.2 Quantum algorithm

In this section, we construct a quantum algorithm to estimate VaR based on the previous assumptions. Its key will be to use QAE as a subroutine to evaluate the cumulative distribution function (CDF) of the total loss $\mathcal{L}$, that is, $\mathrm{Prob}(\mathcal{L} \leq x)$ for a given $x \geq 0$.

In fact, the problem can be reduced to the construction of a quantum algorithm $\mathcal{A}$ which uses no measurements on a $(n+1)-$qubit register such that

$$|\Psi\rangle = \mathcal{A}|0^{\otimes(n+1)}\rangle = \sqrt{1-a}|\Psi_0\rangle_n|0\rangle + \sqrt{a}|\Psi_1\rangle_n|1\rangle \tag{4.2.1}$$

where $|\Psi_0\rangle_n, |\Psi_1\rangle_n \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ are two orthogonal state vectors, and $a = \mathrm{Prob}(\mathcal{L} \leq x)$.

By applying the orthogonal projector $P = I_n \otimes |1\rangle\langle 1|$, which measures if we get a '1' on the last qubit register, one can show $a = \langle\Psi|P|\Psi\rangle$. Thus, by Theorem 3.9, Algorithm 1 will output an estimation of a whose error is bounded by Eq. (3.2.3), which we know equals to $\mathcal{O}(1/M)$ where $M = 2^m$ is the $2-$power of a $m-$qubit register, and with probability at least $8/\pi^2$. Furthermore, by Eq. (3.4.1), repeating the quantum algorithm times and taking the median result boosts the success probability logarithmically. Finally, by applying a bisection search, one can find the smallest x_α to calculate $\mathrm{VaR}_\alpha[\mathcal{L}]$.

Before moving on the construction of $\mathcal{A}$, it is also important to remark that the confidence level α is usually set to be close to one, that is, $\alpha^- \to 1$. By the definition of Eq. (4.1.1), when $a = \mathrm{Prob}(\mathcal{L} \leq x) \approx \alpha$, we can replace in Eq. (3.2.3) a to α to get a better error bound for QAE. In particular, if $\alpha = 99.9\%$, then the error bound is approximately

$$\frac{1}{5M} + \frac{\pi^2}{M^2} \tag{4.2.2}$$

[1] In [12] they generalize these assumptions to a more realistic ones which give rise to the *Gaussian conditional independence model*.

which is an advantage compared to classical Monte Carlo, since it only then depends on M.

In order to construct $\mathcal{A}$, we need three unitary operators: $\mathcal{P}$, $\mathcal{S}$ and $\mathcal{C}$. Firstly, we use $\mathcal{P}$ to assign the probabilities $p_1, \ldots, p_k$ of defaulting on their respective asset. Specifically, we define this operator on a $K-$qubit register as

$$\mathcal{P} = R_Y(\theta_1) \otimes \cdots \otimes R_Y(\theta_K) \quad \text{where } R_Y(\theta_k) \equiv \begin{pmatrix} \cos\left(\frac{\theta_k}{2}\right) & -\sin\left(\frac{\theta_k}{2}\right) \\ \sin\left(\frac{\theta_k}{2}\right) & \cos\left(\frac{\theta_k}{2}\right) \end{pmatrix} \tag{4.2.3}$$

on the $1-$qubit register computational basis $\{|0\rangle, |1\rangle\}$, where $\theta_k = 2\arcsin(\sqrt{p_k})$ for all $k = 1, \ldots, K$. By trigonometric properties, it can be proved with ease that

$$R_Y(\theta_k)|0\rangle = \sqrt{1-p_k}|0\rangle + \sqrt{p_k}|1\rangle$$

Thus the probability of measuring '1' on the $k-$qubit subregister is the same as the probability of getting a default of the k^{th} asset.

Secondly, $\mathcal{S}$ computes the total loss into a n_S-qubit register. It is called *weighted sum operator* and, while being unitary, satisfies that

$$\mathcal{S}|x_1 \cdots x_K\rangle|0^{\otimes n_S}\rangle = |x_1 \cdots x_K\rangle|\lambda_1 x_1 + \cdots + \lambda_K x_K\rangle_{n_S} \tag{4.2.4}$$

where $x_k \in \{0, 1\}$. To represent all the possible values of $\lambda_1 x_1 + \cdots + \lambda_K x_K$ (which are sums and multiplications of positive integers) we set $n_S = \lfloor \log_2(\lambda_1 + \cdots + \lambda_K) \rfloor + 1$. Depending on the values of the weights, ancilla qubits may be necessary to temporarily store the carries during addition operations. An efficient implementation of $\mathcal{S}$ needs at most $\lfloor \log_2(n_S) \rfloor$ of them [15].

Lastly, $\mathcal{C}$ flips an ancilla qubit from $|0\rangle$ to $|1\rangle$ if and only if $\mathcal{L} = \lambda_1 x_1 + \cdots + \lambda_K x_K \leq x$. More formally, $\mathcal{C}$ acts on a $(n_S + 1)-$qubit register as

$$\mathcal{C} : |i\rangle_{n_S}|0\rangle \mapsto \begin{cases} |i\rangle_{n_S}|1\rangle & \text{if } i \leq x, \\ |i\rangle_{n_S}|0\rangle & \text{otherwise.} \end{cases} \tag{4.2.5}$$

After applying all these operators, it can be seen with ease that the composition of these three operators gives us Eq. (4.2.1) when inputting $|0^{\otimes(K+n_S+1)}\rangle$. Figure 4.1 summarizes this idea, and we can also describe the quantum algorithm as a whole in Algorithm 2.

Algorithm 2: Quantum algorithm for VaR [12]

Input: A $K-$qubit register, n_S-qubit register, a $1-$qubit register, a $m-$qubit register, and the orthogonal projector $I_n \otimes |1\rangle\langle 1|$ acting on the $(K + n_S + 1)-$qubit register.

(i) Initialize all registers to the state $|0^{\otimes K}\rangle|0^{\otimes n_S}\rangle|0\rangle$,

(ii) Apply the operator $\mathcal{P}$ from Eq. (4.2.3) to the first register,

(iii) Apply the operator $\mathcal{S}$ from Eq. (4.2.4) to the first two registers,

(iv) Apply the operator $\mathcal{C}$ from Eq. (4.2.5) to the last two registers,

(v) Apply steps 2 - 6 of Algorithm 1 with $\mathcal{A} = (I_K \otimes \mathcal{C})(\mathcal{S} \otimes I)(\mathcal{P} \otimes I_{n_S+1})$, $P = I_n \otimes |1\rangle\langle 1|$ and the $m-$qubit register.

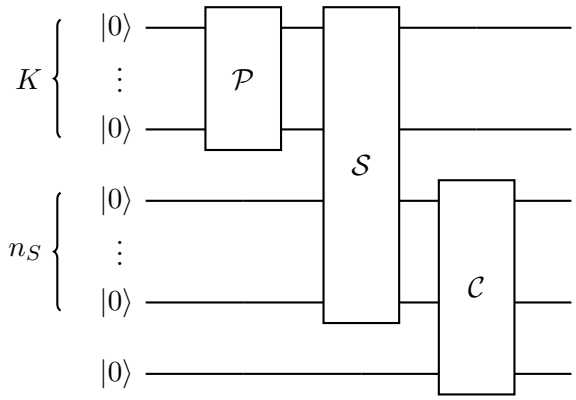


Figure 4.1: Implementation of $\mathcal{A}$ as the composition $(I_K \otimes \mathcal{C})(\mathcal{S} \otimes I)(\mathcal{P} \otimes I_{n_S+1})$. For simplification, implementation of the ancilla qubits is not shown. Source: own elaboration.

4.3 Numerical experiment

In this section we will use a numerical example to verify all the bounds and probabilities for qae and the proposed algorithm $\mathcal{A}$. Data processing and figure generation were performed using scripts developed in Python 3.13.5 and Qiskit 2.2.3 [22].

Asset (k)	**Loss Given Default (λ_k)**	**Default Probability (p_k)**
1	4	0.10
2	1	0.20
3	5	0.15
4	2	0.05
5	3	0.10

Table 4.1: Problem parameters for the illustrative example with $K = 5$ assets under the independence assumption.

To validate the efficacy of the proposed quantum framework, we implement Algorithm 2 in conjunction with a classical bisection search to estimate the Value at Risk for the portfolio defined in Table 4.1. We set a high confidence level of $\alpha = 99.9\%$ and $m = 9$ qubits for measuring the output with higher precision, necessitating the resolution of the extreme tail of the loss distribution. Additionally, for every bisection step, we run Algorithm 2 $N = 32$ times and extract the median result to boost the success probability to at least 99.75%, as showed at the end of Section 3.4. The results of this iterative process are visualized in Figure 4.2.

The search procedure initiates at $x = 7$ (labeled as step 1), where the quantum algorithm estimates a cumulative probability of approximately 0.968670. Since this value is strictly below the target threshold (indicated by the red dashed line), the algorithm infers that the VaR must be located in the upper range of the domain. Consequently, the second iteration evaluates $x = 11$ (step 2), yielding an estimate of ≈ 0.998645. Although this result indicates a high probability, there might be a higher $x > 11$ which satisfies the condition $\text{Prob}(\mathcal{L} \leq x) \leq 0.999$, implying that it is not $\text{VaR}_{99.9\%}[\mathcal{L}]$.

Proceeding to the upper bound, the third iteration tests $x = 13$ (step 3), resulting in a probability effectively ≈ 0.999962, which clearly surpasses the bound. Since we are using $m = 9$ qubits for measuring estimations, if the actual probability $a \geq 99.9\%$, by

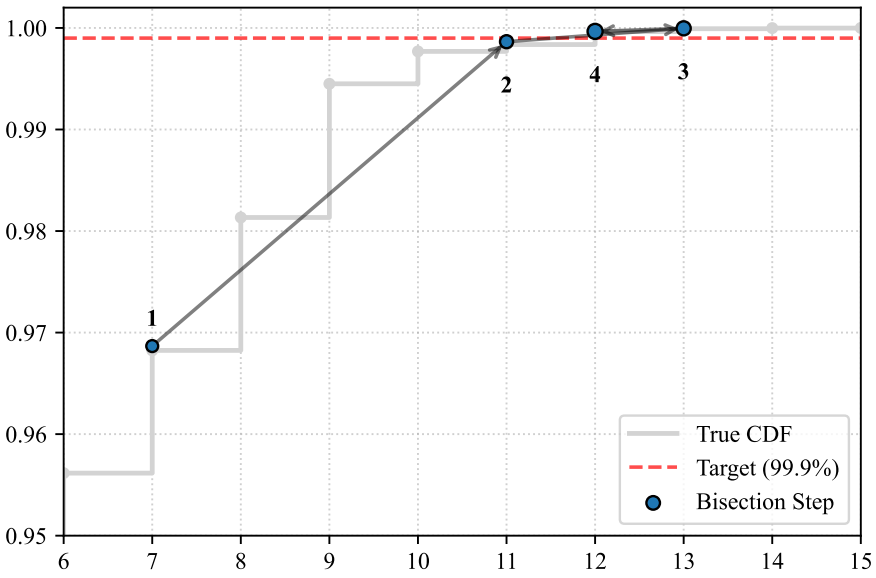


Figure 4.2: Iterative estimation of $\mathrm{VaR}_{99.9\%}[\mathcal{L}]$ using QAE with bisection search. The process identifies the minimal loss threshold $x = 12$ (step 4) where the cumulative probability exceeds the target confidence level (red dashed line). Source: own elaboration.

Theorem 3.9 and Eq. (4.2.2)

$$|\hat{a} - a| \leq \frac{1}{5 \cdot 2^m} + \frac{\pi^2}{(2^m)^2} \approx 4.2827 \times 10^{-4}$$

Thus we have at least the first third decimals of our estimated probability correct, motivating us to make a fourth iteration of bisection search.

For $x = 12$ (step 4) we obtain a estimated probability ≈ 0.999661. Given that $x = 11$ was insufficient, we identify the transition point and conclude that

$$\mathrm{VaR}_{99.9\%}[\mathcal{L}] := \inf_{x \geq 0} \{x \mid \mathrm{Prob}(\mathcal{L} \leq x) \geq 99.9\%\} = 12$$

Furthermore, the close alignment between the quantum estimates and the true CDF empirically confirms the precision of Algorithm 2 in mapping the portfolio's loss profile.

On the other hand, unlike the estimation of Value at Risk, the computation of the expected loss $\mathbb{E}[\mathcal{L}]$ does not require the deployment of quantum algorithms, since it remains computationally efficient for classical processors even as the portfolio size K scales. Applying this property to our specific numerical example, we utilize the risk parameters provided in Table 4.1 to calculate the expected value explicitly:

$$\mathbb{E}[\mathcal{L}] = \sum_{k=1}^{5} \lambda_k p_k = 4(0.10) + 1(0.20) + 5(0.15) + 2(0.05) + 3(0.10) = 1.75$$

Finally, having determined both the Value at Risk and the expected loss, we can rigorously quantify the Economic Capital Requirement as defined in Eq. (4.1.2). Substituting the derived values $\mathrm{VaR}_{99.9\%}[\mathcal{L}] = 12$ and $\mathbb{E}[\mathcal{L}] = 1.75$, we obtain

$$\mathrm{ECR}_{99.9\%}[\mathcal{L}] = 12 - 1.75 = 10.25$$

Chapter 5

Conclusions

This work has established a comprehensive mathematical and physical framework to analyze the computational advantages of quantum algorithm Quantum Amplitude Estimation (QAE). By rigorously bridging the gap between abstract linear algebra and quantum computing, we have demonstrated that this algorithm offers a provable speedup over the classical method known as Monte Carlo. The journey from the axiomatic definition of a Hilbert space to the precise estimation of the error reveals not only the theoretical elegance of Quantum Amplitude Estimation (QAE) but also its disruptive potential in computational finance.

Chapter 2 established that the efficacy of quantum algorithms stems from the algebraic structures of quantum systems. By applying the Riesz-Fréchet theorem (Theorem 2.5) to finite-dimensional Hilbert spaces, we justified the vector-dual vector isomorphism of Dirac notation—a necessity for modeling unitary evolution. This framework defined the role of unitary and orthogonal projectors, alongside tensor products ($\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$) for managing correlated vector spaces.

Translating these algebraic concepts into the four Postulates of Quantum Mechanics allows for the interpretation of quantum circuits as linear operations. The State Space postulate defines qubits as Hilbert space elements, while the Composition postulate utilizes tensor products to enable non-classical correlations. These non-factorable states provide the parallelism that distinguishes quantum computing from classical processing. Furthermore, the Unitary Evolution and Measurement postulates formalize norm-preserving gates and the probabilistic observation of qubits via orthogonal projectors, respectively.

In Chapter 3, we dissected the Quantum Amplitude Estimation (QAE) algorithm, transforming the probabilistic problem of amplitude estimation into a deterministic spectral analysis problem. The core of this analysis was the construction of the Grover operator. By explicitly deriving the spectrum obtained in Eq. (3.1.5), we proved that the target probability is encoded in the eigenvalues of the operator. This insight allowed us to utilize the unitary gate known as Quantum Fourier Transform (QFT) to extract the phase and, consequently, the amplitude.

The central achievement of this theoretical analysis was the derivation of Theorem 3.9. We explicitly bounded the estimation error as a function of the number of query qubits m proving that

$$|\hat{a} - a| \leq 2\pi \frac{\sqrt{a(1-a)}}{2^m} + \frac{\pi^2}{2^{2m}}$$

This inequality provides the rigorous mathematical justification for the quadratic speedup. Through asymptotic analysis in Section 3.3, we demonstrated that the query complexity required to achieve a precision scales $\mathcal{O}(1/\sqrt{M})$ as for QAE, in stark contrast to the scaling $\mathcal{O}(1/M)$ of classical Monte Carlo.

This theoretical advantage was empirically validated through the extensive numerical experiments conducted. The comparative error analysis visualized in Figure 3.5 serves as definitive empirical proof of the speedup. The QAE error curve (blue) follows a steep descent consistent with a slope of on the logarithmic scale, strictly adhering to the bound. Conversely, the classical Monte Carlo error (orange) exhibits the shallower slope of characteristic of convergence. We observed that as the sample size increases, the divergence between the two methods widens by orders of magnitude, confirming that quantum algorithms can achieve high-precision estimates with significantly fewer computational resources.

Furthermore, we addressed the probabilistic nature of the algorithm. While Theorem 3.9 guarantees a constant success probability ($8/\pi^2$), this might be insufficient for critical real-world applications. We demonstrated via Proposition 3.17 that the success probability can be boosted to an arbitrary confidence level through independent repetitions and median selection. Our numerical results in Figure 3.3 corroborated this, showing that with repetitions, the median estimate converged to the true value within the theoretical error bounds in 100% of the trials for 4 and 10 qubits, surpassing even the strict theoretical requirements for a 99.75% confidence level.

Finally, in Chapter 4, we successfully translated these theoretical advantages into a practical solution for Credit Risk Analysis. We identified Value at Risk (VaR) and the Economic Capital Requirement (ECR) as the critical metrics for risk management. The calculation of these metrics inherently involves the estimation of cumulative probabilities in the "tails" of loss distributions—rare events that are computationally expensive to simulate classically due to the slow convergence of Monte Carlo methods.

We constructed a specialized quantum circuit in Algorithm 2 utilizing three specific operators:

- **Probability Loading $\mathcal{P}$:** To encode default probabilities into qubit amplitudes.
- **Weighted Sum $\mathcal{S}$:** To compute the total portfolio loss into a quantum register.
- **Comparator $\mathcal{C}$:** To flag loss events exceeding a threshold.

By integrating this circuit with QAE and a classical bisection search, we demonstrated the ability to map the portfolio's Cumulative Distribution Function (CDF) with high precision. The numerical experiment in Section 4.3 yielded a VaR of 12 and an ECR of 10.25, derived from a process where the quantum estimates aligned almost perfectly with the analytical CDF, as visualized in Figure 4.2.

The implications of this result are profound. The ability of QAE to provide precise, quadratically faster risk estimates means that financial institutions could calculate capital requirements more accurately and frequently.

In conclusion, this thesis argues that Quantum Amplitude Estimation stands not merely as a theoretical curiosity, but as a mathematically sound mechanism to revolutionize financial engineering.

Bibliography

[1] Paul Benioff. "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". In: *Journal of statistical physics* 22.5 (1980), pp. 563–591.

[2] David Deutsch. "Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117.

[3] Richard P Feynman. "Simulating physics with computers". In: *Feynman and computation*. cRc Press, 2018, pp. 133–153.

[4] John Preskill. "Quantum computing in the NISQ era and beyond". In: *Quantum* 2 (2018), p. 79.

[5] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[6] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[7] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum principal component analysis". In: *Nature physics* 10.9 (2014), pp. 631–633.

[8] Gilles Brassard et al. "Quantum amplitude amplification and estimation". In: *arXiv preprint quant-ph/0005055* (2000).

[9] Yohichi Suzuki et al. "Amplitude estimation without phase estimation: Y. Suzuki et al." In: *Quantum Information Processing* 19.2 (2020), p. 75.

[10] Adam Bouland et al. "Prospects and challenges of quantum finance". In: *arXiv preprint arXiv:2011.06492* (2020).

[11] Paul Glasserman. *Monte Carlo methods in financial engineering*. Vol. 53. Springer, 2004.

[12] Daniel J Egger et al. "Credit risk analysis using quantum computers". In: *IEEE transactions on computers* 70.12 (2020), pp. 2136–2145.

[13] Darrell Duffie and Jun Pan. "An overview of value at risk". In: *Journal of derivatives* 4.3 (1997), pp. 7–49.

[14] Stefan Woerner and Daniel J Egger. "Quantum risk analysis". In: *npj Quantum Information* 5.1 (2019), p. 15.

[15] Nikitas Stamatopoulos et al. "Option pricing using quantum computers". In: *Quantum* 4 (2020), p. 291.

[16] Dylan Herman et al. "A survey of quantum computing for finance". In: *arXiv preprint arXiv:2201.02773* (2022).

[17] 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.

[18] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. 27. Oxford university press, 1981.

[19] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. OUP Oxford, 2006.

[20] David J Griffiths and Darrell F Schroeter. *Introduction to quantum mechanics*. Cambridge university press, 2018.

[21] Jun John Sakurai and Jim Napolitano. *Modern quantum mechanics*. Cambridge University Press, 2020.

[22] José Antonio Hidalgo Castillo. *tfg_qiskit_qae*. `https://github.com/jantohidalca/tfg_qiskit_qae`. Visited on 15-12-2025. Commit: 6a1d043. 2025.

[23] Thomas H Cormen et al. *Introduction to algorithms*. MIT press, 2022.

[24] Nicholas Metropolis and Stanislaw Ulam. "The monte carlo method". In: *Journal of the American statistical association* 44.247 (1949), pp. 335–341.

[25] Wassily Hoeffding. "Probability inequalities for sums of bounded random variables". In: *Journal of the American statistical association* 58.301 (1963), pp. 13–30.

Appendix A

Proofs from Results of Linear Algebra

Proof of Example 2.2. 1. $\overline{\langle y,\, x\rangle} = \overline{\sum_{i=1}^{n} \overline{y_i} x_i} = \sum_{i=1}^{n} \overline{\overline{y_i}\, x_i} = \sum_{i=1}^{n} \overline{x_i} y_i = \langle x, y\rangle$

2. $\langle x, \lambda y + \mu z\rangle = \sum_{i=1}^{n} \overline{x_i}(\lambda y_i + \mu z_i) = \lambda \sum_{i=1}^{n} \overline{x_i} y_i + \mu \sum_{i=1}^{n} \overline{x_i} z = \lambda\langle x, y\rangle + \mu\langle x, z\rangle$;

3. by representing x_i as $x_i = a_i + ib_i$, one obtains $\overline{x_i} x_i = a_i^2 + b_i^2 \geq 0 \implies \langle x,\, x\rangle \in \mathbb{R}_{\geq 0}$. Moreover, if $\langle x,\, x\rangle = 0$ and $\overline{x_i} x_i > 0$ for some i, we would have a contradiction. Therefore, $\overline{x_i} x_i = 0$ for all i, so $x = \mathbf{0}$.

□

Proof of Proposition 2.4. Since $\mathcal{H}$ is finite-dimensional, let $n = \dim(\mathcal{H})$. By the definition of finite dimensionality, there exists a basis of vectors $\{e_1, \ldots, e_n\}$ which are linearly independent and span $\mathcal{H}$.

We construct for all $k = 1, \ldots, n$ the vectors

$$u_k = e_k - \sum_{i=1}^{k-1} \frac{\langle u_i, e_k\rangle}{\langle u_i, u_i\rangle} u_i$$

We first show by induction that $\operatorname{span}\{e_1, \ldots, e_k\} = \operatorname{span}\{u_1, \ldots, u_k\}$ for any $1 \leq k \leq n$. In case it is true, proving $\{u_1, \ldots, u_n\}$ is a basis is immediate by cardinality. For the base case $k = 1$, it is vacuously true. We now assume $\operatorname{span}\{e_1, \ldots, e_{k-1}\} = \operatorname{span}\{u_1, \ldots, u_{k-1}\}$. Since $\sum_{i=1}^{k-1} \frac{\langle u_i, e_k\rangle}{\langle u_i, u_i\rangle} u_i \in \operatorname{span}\{u_1, \ldots, u_{k-1}\} = \operatorname{span}\{e_1, \ldots, e_{k-1}\}$ by the induction hypothesis, u_k is generated by e_k and the latter span. Thus, $u_k \in \operatorname{span}\{e_1, \ldots, e_k\}$, which is a basis, showing $\operatorname{span}\{u_1, \ldots, u_n\} \subseteq \operatorname{span}\{e_1, \ldots, e_n\}$. Analogously, by the relation $e_k = u_k + \sum_{i=1}^{k-1} \frac{\langle u_i, e_k\rangle}{\langle u_i, u_i\rangle} u_i$, we obtain the other inclusion.

We use induction again to show the elements of $\{u_1, \ldots, u_n\}$ are orthogonal pair-wise for any $1 \leq k \leq n$. The base $k = 1$ continues to be vacuously true, since there are no

orthogonal vectors with respect to u_1. Now we must show $\langle u_m, u_k\rangle = 0$ for any $m < k$.

$$\langle u_m, u_k\rangle = \left\langle u_m, e_k - \sum_{i=1}^{k-1} \frac{\langle u_i, e_k\rangle}{\langle u_i, u_i\rangle} u_i \right\rangle$$

By the second property of the inner product,

$$\langle u_m, u_k\rangle = \langle u_m, e_k\rangle - \sum_{i=1}^{k-1} \frac{\langle u_i, e_k\rangle}{\langle u_i, u_i\rangle} \langle u_m, u_i\rangle$$

By our induction hypothesis, $u_m \perp u_i$ for all $i \neq m$. Thus,

$$\langle u_m, u_k\rangle = \langle u_m, e_k\rangle - \frac{\langle u_m, e_k\rangle}{\langle u_m, u_m\rangle} \langle u_m, u_m\rangle = 0,$$

implying $u_m \perp u_k$ for all $m < k$.

It remains to show $u_k \neq \mathbf{0}$, which can be proved with ease: if $u_k = \mathbf{0}$, then e_k would be a linear combination of $u_1, \ldots, u_{k-1}$, contradicting they are linearly independent. □

Proof of Proposition 2.6. The first property is immediate by the axioms of vector space. For the second property, given any $|z\rangle \in \mathcal{H}$,

$$(\langle \lambda x + \mu y|)|z\rangle = \langle \lambda x + \mu y|z\rangle = \overline{\lambda}\langle x|z\rangle + \overline{\mu}\langle y|z\rangle = (\lambda\langle x| + \mu\langle y|)|z\rangle$$

Since both linear maps give the same value for every $|z\rangle$, they are the same.

For the last property, we start with the left-to-right direction. For any $|\phi\rangle \in \mathcal{H}$, one obtains

$$\langle \psi|\phi\rangle = \langle |\phi\rangle, |\psi\rangle\rangle = \overline{\lambda}\langle |\phi\rangle, |x\rangle\rangle + \overline{\mu}\langle |\phi\rangle, |y\rangle\rangle = \overline{\lambda}\langle x|\phi\rangle + \overline{\mu}\langle y|\phi\rangle = (\overline{\lambda}\langle x| + \overline{\mu}\langle y|)(|\phi\rangle)$$

Thus, $\langle\psi|$ and $\overline{\lambda}\langle x| + \overline{\mu}\langle y|$ must be the same linear map. For the converse, by considering $\langle\phi| \in \mathcal{H}^*$,

$$\langle \phi|\psi\rangle = \overline{\langle \psi|\phi\rangle} = \overline{(\overline{\lambda}\langle x| + \overline{\mu}\langle y|)|\psi\rangle} = \overline{\overline{\lambda}\langle x|\phi\rangle + \overline{\mu}\langle y|\psi\rangle} = \lambda\langle\psi|x\rangle + \mu\langle\psi|y\rangle = \langle\phi|\lambda x + \mu y\rangle$$

By a similar argument we used to prove the uniqueness of Theorem 2.5 and the previous two properties, the converse can be proved. □

Proof of Theorem 2.11. We start with the existence. Let $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be an orthonormal basis. Under its action, we can represent any two vectors as

$$|x\rangle = \sum_k \lambda_k |e_k\rangle \qquad |y\rangle = \sum_l \mu_l |e_l\rangle$$

Observe we have denoted $\sum_k$ instead of $\sum_{k=1}^n$. This is to avoid overloading the notation with all the subindices that will appear within the proof.

Given any linear operator T, by Theorem 2.8 we can express it as

$$T = \sum_{i,j} T_{i,j} |e_i\rangle\langle e_j|$$

where $T_{i,j}$ is the coefficient in the i^{th} row and j^{th} column of its associated matrix. We also consider the operator

$$T^\dagger = \sum_{i,j} = \overline{T}_{j,i}|e_i\rangle\langle e_j|$$

Note the associated matrix with $T^\dagger$ is the Hermitian conjugate of the one related to T. On the one hand,

$$\begin{aligned}\langle x|Ty\rangle = \langle x|T|y\rangle &= \langle x| \left(\sum_{i,j} T_{i,j}|e_i\rangle\langle e_j|\right)\left(\sum_l \mu_l|e_l\rangle\right) \\ &= \langle x| \left(\sum_{i,j,l} \mu_l T_{i,j}|e_i\rangle\langle e_j|e_l\rangle\right) = \langle x| \left(\sum_{i,j} \mu_j T_{i,j}|e_i\rangle\right)\end{aligned}$$

By Proposition 2.6, we know $\langle x| = \sum_k \overline{\lambda_k}\langle e_k|$. Thus,

$$\langle x|Ty\rangle = \left(\sum_k \overline{\lambda_k}\langle e_k|\right)\left(\sum_{i,j} \mu_j T_{i,j}|e_i\rangle\right) = \sum_{i,j,k} \overline{\lambda_k}\mu_j T_{i,j}\langle e_k|e_i\rangle = \sum_{i,j} \overline{\lambda_i}\mu_j T_{i,j} \tag{A.0.1}$$

On the other hand,

$$\begin{aligned}\langle y|T^\dagger x\rangle = \langle y|T^\dagger|x\rangle &= \langle y| \left(\sum_{i,j} \overline{T}_{j,i}|e_i\rangle\langle e_j|\right)\left(\sum_k \lambda_k|e_k\rangle\right) \\ &= \langle y| \left(\sum_{i,j,k} \lambda_k \overline{T}_{j,i}\langle e_i|\langle e_j|e_k\rangle\right) = \langle y| \left(\sum_{i,j} \lambda_j \overline{T}_{j,i}|e_i\rangle\right)\end{aligned}$$

Again, by Proposition 2.6, we know $\langle y| = \sum_l \overline{\mu_l}\langle e_l|$. Thus,

$$\langle y|T^\dagger x\rangle = \left(\sum_l \overline{\mu_l}\langle e_l|\right)\left(\sum_{i,j} \lambda_j \overline{T}_{j,i}|e_i\rangle\right) = \sum_{i,j,l} \overline{\mu_l}\lambda_j \overline{T}_{j,i}\langle e_l|e_i\rangle = \sum_{i,j} \overline{\mu_i}\lambda_j \overline{T}_{j,i} \tag{A.0.2}$$

By the properties of the inner product

$$\langle T^\dagger x|y\rangle = \overline{\langle y|T^\dagger x\rangle} = \sum_{i,j} \mu_i \overline{\lambda_j} T_{j,i} \tag{A.0.3}$$

Thus, Eq. (A.0.1) and Eq. (A.0.3) coincide, implying $T^\dagger$ is an adjoint of T whose associated matrix is Hermitian conjugate.

For the uniqueness, suppose there are two adjoints operators of T, denoted by $T_1^\dagger$ and $T_2^\dagger$. Hence,

$$\langle T_1^\dagger x|y\rangle = \langle x|Ty\rangle = \langle T_2^\dagger x|y\rangle \implies \langle (T_1^\dagger - T_2^\dagger)x|y\rangle = 0$$

for all $|x\rangle, |y\rangle \in \mathcal{H}$. By a similar argument we used to prove the uniqueness of Theorem 2.5, we can finish the proof. □

Proof of Theorem 2.18. We need to prove the three properties of the inner product. We begin with conjugate symmetry. On pure tensors

$$\overline{\langle x_1 \otimes x_2, y_1 \otimes y_2\rangle} = \overline{\langle x_1, y_1\rangle_{\mathcal{H}_1}\langle x_2, y_2\rangle_{\mathcal{H}_2}} = \langle y_1, x_1\rangle\langle y_2, x_2\rangle = \langle y_1 \otimes y_2, x_1 \otimes x_2\rangle$$

If we now consider $x = \sum_i x_i \otimes x_i'$ and $y = \sum_j y_j \otimes y_j'$, by the bilinear extension

$$\langle x, y\rangle = \sum_{i,j} \langle x_i \otimes x_i', y_j \otimes y_j'\rangle = \sum_{i,j} \overline{\langle y_j \otimes y_j', x_i \otimes x_i'\rangle} = \overline{\langle y, x\rangle}$$

To prove the linearity in the second argument, it is sufficient to do so for the case of pure tensors, due to extension of the map Eq. (2.1.4) for any tensor. Given $\lambda, \mu \in \mathbb{C}$, by the bilinearity of $\otimes$,

$$\begin{aligned}\langle x_1 \otimes x_2, (\lambda y_1 + \mu y_1') \otimes y_2\rangle &= \langle x_1, \lambda y_1 + \mu y_1'\rangle_{\mathcal{H}_1} \langle x_2, y_2\rangle_{\mathcal{H}_2} \\ &= (\lambda \langle x_1, y_1\rangle_{\mathcal{H}_1} + \mu \langle x_1, y_1'\rangle) \langle x_2, y_2\rangle_{\mathcal{H}_2} \\ &= \lambda \langle x_1 \otimes x_2, y_1 \otimes y_2\rangle + \mu \langle x_1 \otimes x_2, y_1' \otimes y_2\rangle\end{aligned}$$

Similarly, $\langle x_1 \otimes x_2,\, y_1 \otimes (\lambda y_2 + \mu y_2')\rangle = \lambda \langle x_1 \otimes x_2, y_1 \otimes y_2\rangle + \mu \langle x_1 \otimes x_2, y_1 \otimes y_2'\rangle$

It remains to prove the positive-definiteness. Let $e_i, e_k \in \mathcal{B}_1$ and $f_j, f_l \in \mathcal{B}_2$. By the assumption of being both orthonormal,

$$\langle e_i \otimes f_j, e_k \otimes f_l\rangle = \langle e_i, e_k\rangle \langle f_j, f_l\rangle = \begin{cases} 1, & \text{if } i = k \text{ and } j = l \\ 0, & \text{otherwise} \end{cases}$$

If we verify the positive-definiteness, then it is immediate that $\mathcal{B}_\otimes$ is a orthonormal basis. For that, we represent $x \in \mathcal{H}_1 \otimes \mathcal{H}_2$ as $x = \sum_{i,j} \lambda_{i,j}(e_i \otimes f_j)$. Hence,

$$\begin{aligned}\langle x, x\rangle &= \left\langle \sum_{k,l} \lambda_{kl}(e_k \otimes f_l),\, \sum_{i,j} \lambda_{ij}(e_i \otimes f_j) \right\rangle \\ &= \sum_{i,j} \sum_{k,l} \lambda_{ij}\, \overline{\lambda_{kl}}\, \langle e_i \otimes f_j,\, e_k \otimes f_l\rangle = \sum_{i,j} |\lambda_{ij}|^2 \quad \geq 0\end{aligned}$$

Moreover, $\langle x, x\rangle = 0$ if and only if all the coefficients $\lambda_{ij} = 0$ which means $x = \mathbf{0}$. □

Proof of Proposition 2.21. We start showing the first identity in the case of pure tensors $x_1 \otimes x_2,\, y_1 \otimes y_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$:

$$\begin{aligned}\langle x_1 \otimes x_2 | (S \otimes T)(y_1 \otimes y_2)\rangle &= \langle x_1 \otimes x_2 | Sy_1 \otimes Ty_2\rangle = \langle x_1 | Sy_1\rangle_{\mathcal{H}_1} \langle x_2 | Sy_2\rangle_{\mathcal{H}_2} \\ &= \langle S^\dagger x_1 | y_1\rangle_{\mathcal{H}_1} \langle T^\dagger x_2 | y_2\rangle_{\mathcal{H}_2} = \langle S^\dagger x_1 \otimes T^\dagger x_2 | y_1 \otimes y_2\rangle \\ &= \langle (S^\dagger \otimes T^\dagger)(x_1 \otimes x_2) | y_1 \otimes y_2\rangle\end{aligned}$$

By using the linearity in the second argument, the conjugate-linearity in the first one and the fact that every tensor is generated by pure tensors, we can prove the identity from above for all $|x\rangle, |y\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Finally, Theorem 2.11 guarantees us $S^\dagger \otimes T^\dagger$ is the unique adjoint of $S \otimes T$.

By a similar argument about linearity, it is sufficient to prove the second identity for the case of pure tensors. Since for any $|x \otimes y\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ the equations

$$\begin{aligned}(S^{-1} \otimes T^{-1})(S \otimes T)|x \otimes y\rangle &= S^{-1}S|x\rangle \otimes T^{-1}T|y\rangle = |x\rangle \otimes |y\rangle, \\ (S \otimes T)(S^{-1} \otimes T^{-1})|x \otimes y\rangle &= SS^{-1}|x\rangle \otimes TT^{-1}|y\rangle = |x\rangle \otimes |y\rangle\end{aligned}$$

coincide, we have proved what we wanted. □