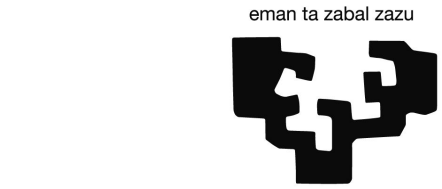


Universidad del País Vasco
Euskal Herriko Unibertsitatea

Máster Universitario en Modelización e Investigación Matemática, Estadística y Computación 2020/2021

Trabajo Fin de Máster

Quantum Genetic Algorithms, Applications and Convergence Analysis

---

Rubén Ibarrondo López

Tutor/es
Dr. Mikel Sanz

Lugar y fecha de presentación prevista

Summary

The ability to control quantum phenomena, such as quantum superposition and interference, has led to a new computational paradigm known as quantum computation, which allows us to design algorithms with dramatic advantages over classical computers. However, whether quantum computation can provide any advantage to evolutionary algorithms, and more precisely, to genetic algorithms (GAs), remains as an open question. Mainly, the development of a fully-quantum GA is hampered by both theoretical constraints, such as the impossibility of perfectly cloning or erasing quantum information, and technical limitations due to the difficulty of the analysis of a huge heuristic quantum algorithm without access to a quantum computer. In this work, we propose a new completely-quantum genetic algorithm (QGA) and we thoroughly analyze its components and performance by means of numerical simulations and quantum-channel techniques. These methods allow us to extract valuable conclusions about the behavior of the algorithm, including its convergence, without the requirement to execute it in a quantum computer. Besides, they make possible to compare the performance of different subroutines in the replication procedure. This proposal paves the way for a new bioinspired optimization quantum algorithm which, additionally, can be straightforwardly parallelized among different processors.

Resumen

El control de fenómenos cuánticos, como la superposición o las interferencias cuánticas, ponen a nuestro alcance un nuevo paradigma computacional conocido como computación cuántica, que nos permite diseñar algoritmos con ventajas vertiginosas frente a los basados en la computación clásica. Sin embargo, aún es incierto si la computación cuántica puede ofrecer una ventaja significativa para los algoritmos evolutivos, y en concreto, para los algoritmos genéticos (GA). Los obstáculos principales en esta línea son tanto teóricos, como la imposibilidad de clonar o borrar información cuántica idealmente, como técnicos, dada la complejidad del análisis heurístico de un algoritmo que aún no podemos ejecutar en un ordenador cuántico. En este trabajo, proponemos un algoritmo genético cuántico (QGA) y estudiamos a fondo sus componentes mediante el uso de simulaciones numéricas y análisis basado en técnicas de canales cuánticos. Estas nos permiten extraer conclusiones valiosas sobre el funcionamiento del algoritmo, incluyendo su convergencia, sin la necesidad de ejecutarlo en un ordenador cuántico. Asimismo, nos posibilitan realizar una comparación de distintas subrutinas para el replicado. Nuestra propuesta sienta las bases para un nuevo algoritmo bioinspirado cuántico, y demás, podría ser paralizada en distintos procesadores cuánticos de menor tamaño.

Contents

Introduction

From the vacuum-tube computer to the state of the art electronic processors, classical computers apply Boolean functions to process information encoded in bits. A classical processing unit with n bits is able to represent 2^n different states, which can be used to encode and run a wide variety of classical algorithms. Conversely, the state space of a quantum processing unit with n *qubits* (the quantum counterpart of bits) is exponentially larger, as the state of a qubit also admits any *superposition* of the states of a classical bit. This exponentially larger computational space, however, is subjected to the laws of quantum mechanics, which constrain the operations that can be employed to design quantum algorithms. For instance, in contrast with classical information, an unknown quantum state cannot be exactly replicated into another system. Therefore, the additional resources and constraints imposed by quantum mechanics make the development and analysis of algorithms for quantum processors extremely challenging.

The implementation in quantum processors of bioinspired algorithms, which are computational tools that mimic natural processes, has recently attracted much attention. In particular, genetic algorithms (GAs) mimic the natural selection process in Nature in order to find resilient solutions to a constrained optimization problem. As GAs provide an outstandingly robust approach, they are often used when the definition of the fitness criteria is complex within the constraints of the problem and the implementation of other optimization methods is cumbersome. Consequently, the implementation of a GA in a quantum processor has been considered as a potential source of new heuristic optimization methods. The ambiguity in the extension of classical GAs to quantum ones has led to the development of different quantum versions [1, 2, 3] and, in particular, to our contribution with the QGA proposed in this work. In this manuscript, we provide a thorough description of each subroutine composing the algorithm and a numerical-analytical analysis of its performance for certain cases. Eventually, to be considered of real interest, any quantum GA has to overcome its classical counterpart and other quantum optimization algorithms in a relevant application. However, the analysis of more complex and relevant applications or a fair comparison with its classical counterpart is left for future work.

Regarding previous approaches, we can classify the proposals in three research lines (as elaborated in Section 2.2). First, the algorithms based on the quantum-inspired genetic algorithm (QIGA) proposed by Narayanan and Moore in 1996 [4]. This algorithm was initially proposed to be run in a classical computer and it was afterwards adapted to be run in a quantum computer. Anyway, the QIGA obtains no advantage from the quantum hardware [1, 3], thus the QIGA and its variants

should be regarded as quantum-inspired classical algorithms. Secondly, Rylander et al. proposed a quantum genetic algorithm which was based on a representation that used quantum superposition and entanglement [5]. Although they claim that this representation may provide a greater searching power, this conclusion is to our knowledge yet unsupported [1]. Finally, the approaches based upon the reduced quantum genetic algorithm (RQGA), which employs a single quantum register to represent all the population (the set of individuals which are optimized in the GA) by means of quantum superposition [6]. This algorithm has been adapted to include all the genetic operators with classical subroutines [7], and quantum subroutines [8]. This approach employs quantum searching algorithms to enhance the selection procedure of the GA. However, it is unclear if the genetic operators are conversely contributing to enhance the searching capability of quantum searching algorithms [1].

In this thesis, we pursue the analysis of the quantum genetic algorithm proposed by R. Ibarrondo in his bachelor thesis [9]. That project was devoted to the design of a novel quantum genetic algorithm (QGA), which was able to be run in a quantum computer, providing a potential advantage. For this master thesis, we have developed the tools to analyse the performance of this algorithm and also enhanced its description so that it clearly distinguishes the fundamental structure from the parts that can be adapted in further variants. We employ those tools to compare the performance of some variants of the algorithm, e.g. skipping the mutation subroutine or employing different pseudo-cloning methods, and applying them to a wide variety of problem cases. Additionally, we validated a method based on quantum channel analysis to show the convergence of the method, understand its behavior and predict its performance. Although we note some potential advantages against its classical counterpart, proving that the QGA outperforms the classical GA and other quantum optimization techniques requires further research which cannot be approached without first understanding the characteristics of the QGA. Therefore, in this project, we have focused on analysing the fundamental properties of the QGA and left the quest for proving advantage for future work.

The theoretical foundation required to develop this work lies on the roots of physics and electronic engineering curricula. We regard as indispensable the solid background in basic linear algebra, quantum mechanics, and programming and numerical techniques for physics which are acquired in these studies. Linear algebra is the core of quantum information and quantum computations, since it is essential to deal with quantum states and quantum processes, both analytically and numerically. Additionally, quantum mechanics is required in order to understand the physical process underneath the algebraic representation. Finally, programming and numerical techniques are present in the validation and analysis of the results. Additionally, some subjects studied in the *Máster en Modelización e Investigación Matemática, Estadística y Computación* provide a wider background in this areas and a more fundamental comprehension of their mathematical foundation. For instance, the contents studied about bioinspired algorithms, about both genetic algorithms and particle swarm optimization, have played an important role for the understanding of the algorithm and the development of the analytical approach. Additionally, the subject about statistical modelling has provided a fundamental statistical background to understand (or, maybe, not to

missunderstand) the numerical results.

This manuscript is structured in three chapters, apart from the introduction and the conclusion. In the first Chapter, we revisit the mathematical formalism of quantum mechanics which is relevant for the work and briefly summarize the fundamental concepts of quantum computation. In the second Chapter, we first provide a sort description of a typical genetic algorithm and a review of the state of the art in the design of genetic algorithms adapted to quantum hardware. Afterwards, we introduce our quantum genetic algorithm and analyse each of its building blocks. Finally, in the third Chapter, we show the analytical results obtained through quantum channel analysis and numerical results from computational simulations. Both successfully validate the performance of the algorithm as an optimization algorithm for a wide variety of problem cases and are used to compare different variants. All in all, we expect that the algorithm studied in this work and the tools employed in the last Chapter, can encourage research in this new family of quantum genetic algorithms in the quest for a GA that takes advantage of quantum hardware.

Chapter 1

Introduction to quantum computation

Quantum mechanics describes the physics at the scale of atoms. In contrast with classical mechanics, quantum mechanics allows for unintuitive phenomena, such as quantum superposition and quantum entanglement. At the end of the twentieth century, a novel computational paradigm known as quantum computation was proposed based on the astonishing properties of quantum mechanics. In this chapter, we review the fundamental concepts of quantum mechanics, as well as some useful tools from quantum computation and quantum information, which will be relevant to understand the core of this work, covered in Chapters 2 and 3.

This introductory chapter is mainly addressed to readers who are not familiar with quantum mechanics and quantum computation. Firstly we re-examine the fundamental postulates of quantum mechanics, reviewing the concepts of quantum state, physical observables, physical measurements, density operators and time evolution of a state (Section 1.1). Then, we revisit some important consequences derived from the aforementioned principles to work with mixed states (Section 1.2). Finally,we introduce the fundamentals of quantum computation, explaining the concepts of qubit, quantum gate, and quantum measurement, and revisiting the quantum circuit notation (Section 1.3).

1.1 Overview of quantum mechanics

In this section, we introduce the the mathematical formalism employed in quantum mechanics. This formalism is built upon a set of postulates introducing the concepts of quantum state, quantum measurements, and the time propagator which defines the state evolution. The wording of each postulate may differ according to the source, however all of them have the same meaning in essence. Here, we have synthesized the statements from Ref. [10] and Ref. [11], adapting the wording to quantum information and quantum computing in general, and to the context of this work in particular. For an interested reader, Ref. [11] delivers a mathematically formal description of the foundations of quantum mechanics.

1.1.1 The state of a quantum system

In the mathematical formalisation of quantum mechanics, the first postulate defines the mathematical objects we use to describe the state of a quantum system: quantum states. These mathematical entities will provide afterwards a way to perform probabilistic predictions of the outcomes of any measurement.

Postulate I *Any physical system can be related to a complex and separable Hilbert space $\mathcal{H}$. The pure state of a physical system in a particular time t corresponds to a unit ray, denoted by $|\psi(t)\rangle_R$, in that Hilbert space. In particular, a vector $|\psi(t)\rangle$ of the ray $|\psi(t)\rangle_R$ is known as the* state vector *or* ket.

As we will see in the following postulates, the requirement for the physical systems to be described by complex and separable Hilbert spaces will prove to be key to build a proper description of quantum phenomena. In particular, after Postulate III we will emphasize the equivalence of unit vectors in the same unit ray, i.e. that only differ by a phase, when it comes to describing observable magnitudes.

Often finding the appropriate $\mathcal{H}$ associated to a particular quantum system is a difficult task. Fortunately, in quantum computation and quantum information, we focus on state spaces composed of *qubit*s. The qubit is a two-dimensional quantum system (see Section 1.3.1 for further details). Due to the subjacent vector space structure, any qubit state can be described as a linear combination of two orthonormal vectors comprising a basis. In general, in physics it is chosen a certain quantum axis, called z axis, which defines a canoncial basis whose vectors are denoted by $|0\rangle$ and $|1\rangle$. Thus, an arbitrary state can be described by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1.1}$$

with $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$, due to the normalization condition $\langle\psi|\psi\rangle = 1$.

To conclude, let us summarize the typical notation and terminology used in this context. For two states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$, where $\mathcal{H}$ stands for the Hilbert space of the system, we write the scalar product by $\langle\psi_2|\psi_1\rangle$, which is taken to be linear in the right-hand side vector and anti-linear in the left-hand side vector, that is

$$\langle\psi_2|\alpha\psi + \beta\psi'\rangle = \alpha\,\langle\psi_2|\psi\rangle + \beta\,\langle\psi_2|\psi'\rangle\,, \tag{1.2}$$

$$\langle\psi_2|\psi_1\rangle = \langle\psi_1|\psi_2\rangle^*\,, \tag{1.3}$$

with $\alpha, \beta \in \mathbb{C}$ and * denoting complex conjugation. This allows us to define of the symbol $\langle\psi|$, known as *bra*, which describes the functional

$$\langle\psi| : \ |\psi'\rangle \to \langle\psi|\psi'\rangle\,, \tag{1.4}$$

which can be shown to be related to the ket $|\psi\rangle$. If we wish to represent the operation of a linear operator A acting on a state $|\psi\rangle$ of the Hilbert space of the system, we just write $A\,|\psi\rangle$ and $\langle\psi'|A|\psi\rangle$ for its scalar product with other state $|\psi'\rangle$. The adjoint of such operator is the denoted by $A^\dagger$ when it exists.

Finally, when we write a state $|\psi\rangle$ as a linear combination

$$|\psi\rangle = \sum_i \alpha_i\,|\psi_i\rangle\,, \tag{1.5}$$

we say that $|\psi\rangle$ is a *superposition of states* $|\psi_i\rangle$ with respective *amplitudes* α_i. For instance, the state of a qubit has been represented as the superposition of $|0\rangle$ and $|1\rangle$, with amplitudes α and β. Although it is common for the states $|\psi_i\rangle$ to be orthonormal, this terminology is also used in more general cases. As I will fundamentally make use of finite dimensional Hilbert spaces, composed of qubits, the states are also typically represented by column vectors with the amplitudes of the state for a particular orthonormal basis.

1.1.2 Description of physical observables

When it comes to retrieving information about a state, scientist define physical quantities which can be observed in the system. In the following postulate, physically observable quantities are introduced as operators in the Hilbert space of the system.

Postulate II *The observables of a physical system are represented as lineal self-adjoint operators acting on the Hilbert space of the physical system.*

As stated before, we will focus on finite dimensional Hilbert spaces. As these operators can be represented by Hermitian matrices, physicist usually call them Hermitian operators. Hermitian operators satisfy $A = A^\dagger$, which particularly implies that they admit a spectral decomposition. Below, we state the spectral decomposition theorem and then I provide its description for the case of Hermitian operators.

Theorem 1 (Spectral decomposition) *Let A be a normal operator, which satisfy $AA^\dagger = A^\dagger A$, acting on a vector space V. Then there exists an orthonormal basis for V diagonalizing A. Conversely, any diagonalizable operator, which can be diagonalised in this manner, is normal.*

Let us state the eigenvalue equation as

$$A\,|\lambda\rangle = \lambda\,|\lambda\rangle\,, \tag{1.6}$$

with eigenvalues λ and respective normalized eigenvectors $|\lambda\rangle$, let $\sigma(A)$ denote the set of eigenvalues of A. One can show that eigenvectors corresponding to different eigenvalues are orthogonal and that the eigenvalues must be real. Moreover, one can define states $|\lambda, i\rangle$ forming an orthonormal basis of the eigenspace corresponding to the eigenvalue λ, where i ranges from 1 to the multiplicity of λ denoted $m(\lambda)$. Therefore, the set of all $|\lambda, i\rangle$ forms an orthonormal basis of the Hilbert space associated to the system. Thus, any state $|\psi\rangle$ can be expressed as a superposition of such vectors

$$|\psi\rangle = \sum_{\lambda\in\sigma(A)} \sum_{i=1}^{m(\lambda)} a_{\lambda,i}\,|\lambda, i\rangle\,, \quad a_{\lambda,i} \equiv \langle\lambda, i|\psi\rangle\,. \tag{1.7}$$

Consequently, the action of the observable on the system can be described by

$$A\,|\psi\rangle = \sum_{\lambda\in\sigma(A)} \sum_{i=1}^{m(\lambda)} a_{\lambda,i} A\,|\lambda, i\rangle = \sum_{\lambda\in\sigma(A)} \sum_{i=1}^{m(\lambda)} a_{\lambda,i}\lambda\,|\lambda, i\rangle = \sum_{\lambda\in\sigma(A)} \lambda \sum_{i=1}^{m(\lambda)} a_{\lambda,i}\,|\lambda, i\rangle\,. \tag{1.8}$$

If we define the projector in state $|\lambda, i\rangle$ with the notation $|\lambda, i\rangle\langle\lambda, i|$ one can also define the proyector in the eigenspace corresponding to λ by

$$M_\lambda \equiv \sum_{i=1}^{m(\lambda)} |\lambda, i\rangle\langle\lambda, i| \,, \tag{1.9}$$

then it is straightforward to show that the observable admits a decomposition of the form

$$A = \sum_{\lambda \in \sigma(A)} \lambda M_\lambda, \tag{1.10}$$

which represents the spectral decomposition of observable A.

1.1.3 Measurement of physical observables

Once physical magnitudes have been defined as operators, we can mathematically define the probability of obtaining a given value for each magnitude.

Postulate III *The outcome of a measurement of an observable A must be one of its eigenvalues λ. Moreover, the probability of obtaining the value λ in a physical system in the normalized pure state $|\psi\rangle$ is given by*

$$P(\lambda, \psi) = \langle\psi|M_\lambda|\psi\rangle \,. \tag{1.11}$$

It is straightforward to check that these values satisfy the desired properties for a probability distribution, precisely, $P(\lambda, \psi) \in [0, 1]$ and $\sum_\lambda P(\lambda, \psi) = 1$, as $\sum_\lambda M_\lambda = \mathbb{I}$. Employing the representation of the state used in Eq. 1.7 the probability can be easily shown to be

$$P(\lambda, \psi) = \sum_{i=1}^{m(\lambda)} |\langle\lambda, i|\psi\rangle|^2 = \sum_{i=1}^{m(\lambda)} |a_{\lambda,i}|^2. \tag{1.12}$$

From this representation one can clearly see why it is stated in Postulate I that any vector in the same ray $|\psi\rangle_R$ results in the same probability distribution for its outcomes. Indeed, vector states described with amplitudes $a_{\lambda,j}$ or $e^{i\theta}a_{\lambda,j}$ yield exactly the same result. This is usually also rephrased stating that normalised vectors that only differ by a *global phase*, say $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$, have identical physical meaning.

As an important conclusion of this postulate the expected value of observable A can be obtained

$$\langle A\rangle_\psi = \sum_{\lambda \in \sigma(A)} \lambda P(\lambda, \psi) = \sum_{\lambda \in \sigma(A)} \lambda \langle\psi|M_\lambda|\psi\rangle = \langle\psi|A|\psi\rangle \,. \tag{1.13}$$

Conversely, the effect of a measurement in a quantum state is described in the following postulate.

Postulate IV *The state resulting from measuring observable A having obtained eigenvalue λ is*

$$|\psi_\lambda\rangle = \frac{M_\lambda |\psi\rangle}{\sqrt{\langle\psi|M_\lambda|\psi\rangle}}. \tag{1.14}$$

This process is commonly known as the *collapse* of the state vector, as it is projected into the eigenspace of the obtained output loosing the superposition terms in other eigenspaces.

Frequently we will refer to *measuring in a particular orthonormal basis* $\{|m\rangle\}$. This is a common expression, meaning a measurement of an observable which is diagonal in that basis and whose eigenvalues have multiplicity 1. This ensures that once the system is measured there is a one-to-one correspondence between the outcome of the measurement and the vector state after collapsing. This terminology will prove useful for quantum computation (Section 1.3.2). For example, measuring a qubit in the $\{|0\rangle, |1\rangle\}$ basis, means to use the projectors $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$ to obtain the probabilities of measuring each state in a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

$$P(0,\psi) = \langle\psi|M_0|\psi\rangle = |\alpha|^2, \quad P(1,\psi) = \langle\psi|M_1|\psi\rangle = |\beta|^2. \tag{1.15}$$

This result illustrates a relation between the probability and the amplitude of a state. In general, for a state described as a superposition of an orthonormal basis as $|\psi\rangle = \sum_m a_m |m\rangle$, the probability of obtaining each state is $|a_m|^2$. In general, the probability of measuring an arbitrary state $|\phi\rangle$ by means of a projective measurement in the state $|\psi\rangle$, is given by

$$P(\phi,\psi) = |\langle\phi|\psi\rangle|^2. \tag{1.16}$$

Now that we have introduce these postulates concerning pure states, it is a suitable moment to introduce the treatment for mixed states.

1.1.4 The density operator

Until now, we have only considered pure states, which can be represented by normalised vectors in the Hilbert space associated to the physical system. Let us introduce the mathematical representation used for states when one wants to express uncertainty about the state, known as mixed quantum state.

Definition 1 *A mixed state of a physical system may be described by a* density operator *(or* density matrix *for the finite dimensional case) defined as*

$$\rho \equiv \sum_i w_i |\psi_i\rangle\langle\psi_i|, \tag{1.17}$$

where w_i represent the probability of finding the system in the pure state $|\psi_i\rangle$, with $\sum_i w_i = 1$. We call $\{w_i, |\psi_i\rangle\}$ an ensemble of pure states *and note that the pure states are not required to be orthonormal.*

This operator shows some important properties:

- ρ is a self-adjoint operator, $\rho^\dagger = \rho$,
- ρ is a positive operator, $\rho \geq 0$,
- the trace of ρ is 1, $\mathrm{tr}(\rho) = 1$, and $\mathrm{tr}(\rho^2) \leq 1$.

These properties ensure first that ρ is a valid observable of a physical system. Second, that all of its eigenvalues are non-negative and, third, that they add up to one. By virtue of the Theorem 1, we can diagonalize ρ in the basis formed by its eigenvectors, labelled $|\phi_j\rangle$, whose eigenvalues, q_j, must satisfy $q_j \geq 0$ and $\sum_j q_j = 1$. Hence, the spectral decomposition of ρ is

$$\rho = \sum_j q_j \, |\phi_j\rangle\langle\phi_j| = \sum_q q M_q, \tag{1.18}$$

where M_q again represents the projection on the eigenspace of eigenvalue q. Although this representation is similar to the one given in the definition, it brings in the fact that we can represent any mixed state as an ensemble of orthonormal pure states $\{q_i, |\phi_i\rangle\}$, which was not required for $\{w_i, |\psi_i\rangle\}$.

We shall also note that a pure state is a particular case of a mixed state, which has a single pure state in the ensemble with probability one, $\rho = |\psi\rangle\langle\psi|$. Moreover, it can be shown that only pure states satisfy $\rho^2 = \rho$ and $\mathrm{tr}(\rho^2) = 1$. Hence, for any mixed state $\mathrm{tr}(\rho^2) < 1$. In the other hand, the maximally mixed state in a d-dimensional Hilbert space is the state represented by the ensemble $\{\frac{1}{d}, |\phi_i\rangle\}$, expressed in any orthogonal basis. The latter state represents absolute uncertainty on the state of the system and it is usually represented as $\mathbb{I}/d$, where $\mathbb{I}$ represents the identity operator. We will see other examples for qubit states in Section 1.3.2.

On the basis of Postulate II, the density operator formalism provides with convenient ways to compute the probability of a measurement λ from the spectrum of an observable A, its expected value and the state after obtaining output λ are

$$\begin{aligned} P(\lambda, \rho) &= \mathrm{tr}(\rho M_\lambda), \\ \langle A \rangle_\rho &= \mathrm{tr}(\rho A), \\ \rho_\lambda &= \frac{M_\lambda \rho M_\lambda}{\mathrm{tr}(\rho M_\lambda)}. \end{aligned}$$

Additionally, there is a compact manner to represent the state of a physical system after a measurement with an *unknown* output. In particular, one can state an equivalent result for Postulate IV: The mixed state resulting from the measurement of observable A in state ρ is given by

$$\rho_A = \sum_\lambda M_\lambda \rho M_\lambda, \tag{1.19}$$

where M_λ is the projector on the eigenspace of A with eiganvalue λ. In particular, if the initial state is a pure state the final state is $\rho_A = \sum_\lambda M_\lambda \, |\psi\rangle\langle\psi| \, M_\lambda$, which would be a mixed state if and only if $|\psi\rangle$ is not an eigenstate of A.

We must underline the virtues of the density operator approach: the description of physical systems whose pure state is not known with certainty, and the description of subsystems of a composite physical system. I will deepen on these applications in Section 1.2.

1.1.5 Time evolution of a system

Finally, we introduce the postulate which describes the dynamics of a quantum system. That its, describes the evolution of the state in terms of the well known Schödinger equation.

Postulate V *The state of a system remains pure provided that it is kept isolated, particularly if there is no measurement performed on it. If that is the case, one can find in each unit ray* $|\psi(t)\rangle_R$ *a state vector* $|\psi(t)\rangle$ *whose evolution is given by the* Schrödinger equation

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = H(t)\,|\psi(t)\rangle\,, \tag{1.20}$$

where the operator $H(t)$ *is the Hamiltonian of the system.*

The Hamiltonian of a system may explicitly depend on time in general. However, if it is constant, we write just H and we may refer to it as the *energy* operator of the system.

One can easily show that the evolution of the state of a system in terms of a density matrix is given by

$$i\hbar\frac{\mathrm{d}\rho(t)}{\mathrm{d}t} = [H(t), \rho(t)]. \tag{1.21}$$

An important property of the Schrödinger equation is that it preserves the norm of the state vector. Thus, as the equation is lineal, the integration of this equation in a range t_0, t must lead to an isometric lineal operator $U(t_0, t)$ satisfying

$$|\psi(t)\rangle = U(t_0, t)\,|\psi(t_0)\rangle\,, \tag{1.22}$$

which we call the *evolution operator*. Moreover, it can be also shown that the domain and image of $U(t_0, t)$ is $\mathcal{H}$, which considered with the fact that it is isometric implies that it must also be unitary. Thus it satisfies

$$U^{-1}(t_0, t) = U^{\dagger}(t_0, t). \tag{1.23}$$

In turn, one can show that the evolution of a mixed state is given by $\rho(t) = U(t_0, t)\rho(t_0)U^{\dagger}(t_0, t)$.

In particular, if we only consider time-independent Hamiltonians, Eq. 1.20 can be straightforwardly integrated to obtain

$$U(t_0, t) = \exp[-i(t - t_0)H/\hbar], \tag{1.24}$$

which has the distinctive property that the evolution operator only depends on the time elapsed and not in the initial time t_0. We typically use symbols like $U(\Delta t)$ or simply U, when we refer to evolutionary processes whose time laps are known.

In particular, for finite dimensional Hilbert spaces, H is given by a Hermitian matrix and U by a unitary matrix which can be obtained by $U = \exp[-i\Delta t H/\hbar]$. This fact is a cornerstone in quantum computation, as it shows that the evolution of a vector state of a n-qubit system can can be described by unitary matrices. This, in particular implies that the computation process performed must be reversible and must obey some important constraints. In quantum computation, the importance of the Hamiltonian is substituted by the representation of quantum evolution processes by unitary transformations.

Finally, let us omit the sixth postulate due to its lack of relevance on this work. Indeed, this postulate is used for the canonical quantization of observables, in particular generalized coordinates and their conjugate momenta, and it will not be used in this work.

1.2 Important results from quantum mechanics

The postulates of quantum mechanics have already been introduced, together with some of their physical implications. In this section we aim at introducing further conclusions, which are particularly relevant for our work with genetic algorithms, and some useful tools to understand them.

Firstly, we present a exciting property of quantum states of composite systems, quantum entanglement. Afterwards, we employ density operators to describe parts of a composite system. Then, we enunciate the no-cloning and no-deleting theorems, two core results in quantum information that constrain the action of copying and erasing information in quantum computers. In the following subsection, we define two relevant distance measures for quantum states. Finally, we introduce the quantum channel formalism for the description of almost arbitrary quantum processes.

1.2.1 Entanglement and the Schmidt decomposition

According to Postulate I, one can associate any physical system to a Hilbert space, but it does not tell us how to choose this space. However, there is a natural choice to describe composite systems, once the Hilbert spaces associated to the constituent systems are known. The Hilbert space, $\mathcal{H}$, of a composite physical system is the tensor product of Hilbert spaces of the spaces of its subsystems, $\mathcal{H}_1, \ldots, \mathcal{H}_n$, that is

$$\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n. \tag{1.25}$$

Moreover, if each constituent system is in state vector $|\psi_i\rangle \in \mathcal{H}_i$, then the state vector $|\psi\rangle \in \mathcal{H}$ of the composite system is given by $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Let us label $|u_{i,j}\rangle$ the vectors from an orthonormal basis of each $\mathcal{H}_i$, with j ranging from 1 to $d_i \equiv \dim \mathcal{H}_i$. Now, recall that we can build the set of vectors with the form $|u_{1,j_1}\rangle \otimes \cdots \otimes |u_{n,j_n}\rangle$, with $j_i = 1, \ldots, d_i$, to form an orthonormal basis for $\mathcal{H}$, the composite system. In particular, for two systems with finite dimensional Hilbert spaces, one with basis $\{|1\rangle, \ldots, |N\rangle\}$, and other one with basis $\{|1\rangle, \ldots, |M\rangle\}$, the composite system has a basis formed by $|i\rangle \otimes |j\rangle$ with $1 \leq i \leq N$ and $1 \leq j \leq M$.

It is commonplace to take the shorthand $|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle |\psi_2\rangle = |\psi_1\psi_2\rangle$, as this notation can not be confused with any possible vector product. As an example, consider a two-qubit system and assume that each qubit is prepared in an arbitrary state similar to Eq. 1.63, the joint state is given by

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) && (1.26)\\ &= \alpha_1\alpha_2 |0\rangle |0\rangle + \beta_1\alpha_2 |1\rangle |0\rangle + \alpha_1\beta_2 |0\rangle |1\rangle + \beta_1\beta_2 |1\rangle |1\rangle && (1.27)\\ &= \alpha_1\alpha_2 |00\rangle + \beta_1\alpha_2 |10\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\beta_2 |11\rangle , && (1.28) \end{aligned}$$

where we have used the distributive property of the tensor product of vectors of Hilbert spaces.

Nevertheless, not all states of a two-qubit system can be described in this manner. For instance, consider the following two-qubit state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{1.29}$$

one can easily show from Eq. 1.28 that there are no single qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$ whose tensor product results in this one. In general, a pure state of a composite system is called *separable* if it satisfies that $|\psi\rangle \neq |\psi_1\rangle |\psi_2\rangle$ for some state vector pair $|\psi_1\rangle$ and $|\psi_2\rangle$ of the component systems, and *entangled* otherwise. Therefore, two qubits in an entangled state cannot be described in terms of individual systems, i.e. they must be described as a whole. The astonishing fact is that entanglement holds even when the composite systems are far away from each other, hence quantum mechanics forces their description as a unique system even if they are unable to interact due to the distance. This property, intrinsic of quantum systems, is puzzling at first sight, but it is extremely useful when it comes to performing quantum computation, and most importantly for quantum communication and cryptography.

The *Schmidt decomposition* provides a convenient way to represent pure states of composite system with two subsystems.

Theorem 2 (Schmidt decomposition) *Let $|\psi\rangle$ be a pure state of a composite system, with associated Hilbert space $\mathcal{H}_a \otimes \mathcal{H}_b$. Let us assume that $n \leq m$, where n and m are the dimensions of $\mathcal{H}_a$ and $\mathcal{H}_b$ respectively. Then, there exist two orthonormal bases $|i_a\rangle \in \mathcal{H}_a$, with $i_a = 1, \ldots, n$, and $|i_b\rangle \in \mathcal{H}_b$, with $i_b = 1, \ldots, m$, such that*

$$|\psi\rangle = \sum_{i=1}^{n} \lambda_i |i_a\rangle |i_b\rangle , \tag{1.30}$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as Schmidt coefficients.

The proof of this theorem stems from the singular value decomposition of complex matrices, which also provides the result that the Schmidt coefficients are unique up to reordering, although the vectors $|i_a\rangle$ and $|i_b\rangle$ may vary. In particular, the number of λ_i values which are strictly positive, $d \leq \min(n, m)$, is known as the *Schmidt number* or *Schmidt rank*. One can show that the Schmidt number does not vary under local unitary transformations on the individual systems $\mathcal{H}_1$ and $\mathcal{H}_2$, thus it is possible to find a decomposition satisfying $|\psi\rangle = \sum_{i=1}^{d} \lambda_i |i_a\rangle |i_a\rangle$. Note that $d = 1$ if and only if the state is separable, whereas it is entangled for any $d > 1$.

Let us note that the Schmidt decomposition can be formulated in a similar manner for mixed states. However, the concept of entanglement and separability becomes less clear for mixed states, because one must distinguish classical correlations from purely quantum entanglement. This makes the characterization of their entanglement extraordinarily difficult and, as we do not require it for this manuscript, we are omitting its formal description. In Section 1.2.4, we superficially describe a general separable mixed state merely as an instance that illustrates the limitations of the entanglement witness covered in that section.

1.2.2 Density operator of subsystems

Suppose that ρ^{AB} is the density operator describing the state of a composite system, comprising two physical systems A and B, represented by Hilbert spaces

$\mathcal{H}_a$ and $\mathcal{H}_b$. Now let us assume that we have only access to system A, then what is the appropriate density operator ρ^A in $\mathcal{H}_a$ physically compatible with ρ^{AB}? That is, what is the density operator describing the state of the subsystem A if we discard subsystem B? In this section we review the definition answering this question and its justification.

Definition 2 *Let ρ^{AB} be a density operator describing the composite system AB. We define the* reduced density operator *for system A by*

$$\rho^A \equiv \mathrm{tr}_B(\rho^{AB}), \tag{1.31}$$

where tr_B is the partial trace over system B, which is the map of operators defined by

$$\mathrm{tr}_B(\rho^{AB}) = \sum_{i=1}^{m} (\mathbb{I}_A \otimes \langle i|_B)\rho^{AB}(\mathbb{I}_A \otimes |i\rangle_B), \tag{1.32}$$

where m is the dimension of $\mathcal{H}_b$, $|i\rangle_B$ is any basis of $\mathcal{H}_b$ and $\mathbb{I}_A$ is the identity on $\mathcal{H}_a$.

The reason for the partial trace to be present in the definition of the reduced density operator for a subsystem is the fact that it preserves all statistic information about any measurement on system A. More precisely, for any observable M on system A it is possible to extend it to AB by

$$M' = M \otimes \mathbb{I}_B, \tag{1.33}$$

where $\mathbb{I}_B$ is the identity operator acting on system B. On the basis of this extension, it is our goal to ensure that

$$\mathrm{tr}\big(M\rho^A\big) = \mathrm{tr}\big(M'\rho^{AB}\big), \tag{1.34}$$

that is, it yields the same expected value for any observable M on A. It is clear that the partial trace defined above satisfies this property, and it can be shown that it is the unique map achieving it for any M [10].

The reduced density matrix has the intuitive property that given $\rho^{AB} = \rho \otimes \sigma$, with ρ an operator on $\mathcal{H}_a$ and σ an operator on $\mathcal{H}_b$, the reduced density matrices obtained via partial trace are $\rho^A = \rho$ and $\rho^B = \sigma$. In particular, if the states ρ and σ represent pure states, then ρ^{AB} represents a pure and separable state, and the resulting operators ρ^A and ρ^B describe also pure sates. However, a joint pure state ρ^{AB} does not necessarily produce reduced density operators representing pure states. In fact, this property is strictly related to entanglement.

If ρ^{AB} represents a pure state, it can be described employing Schmidt decomposition of the pure state (which should not be confused with the Schmidt decomposition of a mixed state)

$$|\Psi_{AB}\rangle = \sum_{i=1}^{d} \lambda_i |a_i\rangle |b_i\rangle , \tag{1.35}$$

$$\rho^{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}| = \sum_{i=1}^{d}\sum_{j=1}^{d} \lambda_i\lambda_j |a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j| , \tag{1.36}$$

where $|a_i\rangle$ and $|b_i\rangle$ are states from an orthonormal basis in $\mathcal{H}_a$ and $\mathcal{H}_b$ respectively, and d is the Schmidt number, implying that $\lambda_i > 0$. Now, the reduced density operator for system A can easily be computed

$$\rho^A = \mathrm{tr}_B(\rho^{AB}) = \sum_{i=1}^{d}\sum_{j=1}^{d} \lambda_i\lambda_j \, |a_i\rangle\langle a_j| \, \mathrm{tr}(|b_i\rangle\langle b_j|) \tag{1.37}$$

$$= \sum_{i=1}^{d}\sum_{j=1}^{d} \lambda_i\lambda_j \, |a_i\rangle\langle a_j| \, \langle b_i|b_j\rangle = \sum_{i=1}^{d} \lambda_i^2 \, |a_i\rangle\langle a_j| \, . \tag{1.38}$$

Recalling that $\sum_{i=1}^{d} \lambda_i = 1$, one can easily show that $\mathrm{tr}\big(\rho^A\big) = 1$ and $\mathrm{tr}\big((\rho^A)^2\big) \leq 1$, which is known as the *purity* of the system because the equality $\mathrm{tr}\big((\rho^A)^2\big) = 1$ only holds for a Schmidt decomposition with a single term, that is for $d = 1$ with $\lambda_1 = 1$. In other words, the reduced density operator can only represent a pure state if ρ^{AB} is separable in the first place.

1.2.3 The no-cloning and no-deleting theorems

Postulate V imposes the limitation that only unitary transformation can be applied to isolated quantum systems. Notably, this implies the impossibility of performing some operations with quantum information which are ordinary with classical information, such as copying or erasing. Here we review the result obtained by W. K. Wootters and W. H. Zurek who proved the impossibility of a perfect cloning procedure [12], currently known as the no-cloning theorem. Although we focus on pure states and unitary evolutions, it can be proven that mixed states can neither be perfectly cloned and that allowing non-unitary operations, such as measurements, does not change this limitation [10].

First, let us introduce the desired (yet unachievable) procedure. We are given two physical systems with equal dimensions, and assume one of the systems is in an unknown state $|\psi\rangle$, which we want to copy in the second subspace, which is a known blanck state $|e_0\rangle$. For a perfect quantum copying protocol, we should be able to overwrite the second system and transform the joint state $|\psi\rangle\,|e_0\rangle$ into $|\psi\rangle\,|\psi\rangle$.

Let us assume that there exists a unitary transformation U, satisfying

$$U\,|\psi\rangle\,|e_0\rangle = |\psi\rangle\,|\psi\rangle\,, \tag{1.39}$$

which may depend on the reference state $|e_0\rangle$, but must be independent of the unknown state $|\psi\rangle$. If so, the unitary U could also be applied to any other arbitrary state $|\phi\rangle$ in a similar manner, $U\,|\phi\rangle\,|e_0\rangle = |\phi\rangle\,|\phi\rangle$.

On the other hand, by using the property that under a unitary transformation the inner product is preserved, the inner product for both the initial states and the states after applying the cloning operation U are equal, which leads to

$$\langle\psi|\phi\rangle \overbrace{\langle e_0|e_0\rangle}^{1} = \langle\psi|\phi\rangle\,\langle\psi|\phi\rangle \;\Rightarrow\; \langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \;\Rightarrow\; \langle\psi|\phi\rangle = 0 \text{ or } 1. \tag{1.40}$$

This proves that two arbitrary states cannot be cloned with a single unitary operator, unless either they are the same or they are orthonormal, which establishes the following.

Theorem 3 *There is no unitary transformation U acting on $\mathcal{H} \otimes \mathcal{H}$, that given some reference state vector $|e_0\rangle$ and any arbitrary state vector $|\psi\rangle$ in $\mathcal{H}$ satisfy*

$$U |\psi\rangle |e_0\rangle = |\psi\rangle |\psi\rangle . \tag{1.41}$$

Nevertheless, this theorem naturally leads to the question of which is the optimal imperfect cloning protocol. For example, the proof provided above does not forbid perfectly cloning any state in an orthonormal basis.

Exploring the limits of an imperfect cloning process has motivated multiple investigations [13]. Some looking for cloning systems that worked with similar fidelity for any input state, called universal quantum cloning machines [14]. Others focusing on the idea of cloning only part of the quantum information of a state, known in the bibliography as partial quantum cloning [15, 16]. We cover the topic of quantum pseudo-cloning subroutines in Section 2.6.1.

However, perfect cloning has been wrongly assumed to exist in the past, resulting in unfeasible protocols. A well known example was provided by N. Herbert, who proposed a method for faster-than-light communication by means of entanglement if perfect cloning were allowed [17]. This astonishing application could jeopardise the compatibility of quantum mechanics with special relativity. However, Herbert's communication protocol required a perfect cloning transformation in the receptor system, in order to retrieve the transmitted information. Without that mechanism, the communication protocol was unable to figure out conclusive information about the input. The example of faster-than-light communication reminds the important role of this theorem when it comes to assuming the existence of a feasible transformation for a quantum state.

A similar result was found forbidding reversible erasure of quantum states [18]. In general, the action of irreversibly erasing a quantum state can be attained by swapping it with a reference state in an ancillary system and discarding that part. Whereas the reversible erasure can be described by

$$|\psi\rangle |\psi\rangle |A\rangle \rightarrow |\psi\rangle |e_0\rangle |A_\psi\rangle , \tag{1.42}$$

where $|A_\psi\rangle$ is the final state of the ancillary system, which may depend on the erased state. On the basis of linearity of quantum mechanics, the **quantum no-deleting theorem** states that this transformation can only be achieved for any state by the swap operation between the second copy and the ancillary system, implying that the only universal erasure operation is the irreversible erasure. Therefore, two copies of an unknown state cannot be used to delete one of them reversibly.

1.2.4 Quantifying entanglement: von Neumann entropy

In the context of quantum information theory, entropy quantifies the uncertainty about the state of a physical system.

Definition 3 *Let ρ be the quantum state of a system, von Neumann defined its* entropy *to be*

$$S(\rho) \equiv -\operatorname{tr}(\rho \log \rho), \tag{1.43}$$

where the logarithm is taken in base two (as usual in information science). The entropy can be easily calculated once the spectrum of ρ, $\sigma(\rho)$, is known,

$$S(\rho) \equiv -\operatorname{tr}(\rho \log \rho) = -\sum_{\lambda \in \sigma(\rho)} m(\lambda)\lambda \log \lambda, \tag{1.44}$$

where we take $0 \log 0 = 0$ and $m(\lambda)$ is the multiplicity of λ.

Note that in the definition of the entropy can be given in terms of the eigenvalues due to the basis independence of the trace function [10]. Distinctly, the representation in terms of the spectrum of ρ allows us to straightforwardly compute the von Neumann entropy of an arbitrary pure state and the maximally mixed state. The pure state has a single non-zero eigenvalue equal to 1, thus $S(|\psi\rangle\langle\psi|) = 0$, and a maximally mixed state has a single eigenvalue $1/d$ with multiplicity d, where d is the dimension of the Hilbert space, thus its entropy is $S(\mathbb{I}/d) = \log d$. In fact, the von Neumann entropy lies within the interval $0 \leq S(\rho) \leq \log d$, with the lower bound only holding for pure states and the upper bound for the maximally mixed state.

The von Neumann entropy possesses a bunch of mathematical properties, however, we will narrow down to the ones related to quantifying entanglement in a bipartite system. Let us consider a composite system, with associated Hilbert space $\mathcal{H}_a \otimes \mathcal{H}_b$, and a pure state described by $|\psi\rangle$. Then, employing the Schmidt decomposition in Theorem 2, it can be shown that the entropy of the reduced density operators of both subsystem matches, which we label S_{red},

$$S_{\text{red}} \equiv S(\rho^A) = S(\rho^B). \tag{1.45}$$

Moreover, as a consequence of the Schmidt decomposition, the reduced density operators for each subsystem are pure if state $|\psi\rangle$ is separable ($S_{\text{red}} = 0$), and mixed otherwise ($S_{\text{red}} > 0$). Consequently, S_{red} is considered a good witness of the entanglement of a pure state $|\psi\rangle$ in a bipartite system [19]. Indeed, the lowest value is obtained for a separable state, $S_{\text{red}} = 0$, and the highest for the case where the reduced density operators are maximally mixed, $S_{\text{red}} = \log d$ where $d = \min(\dim(\mathcal{H}_a), \dim(\mathcal{H}_b))$. S_{red} quantifies entanglement in terms of the uncertainty emerging from considering each subsystem separately instead of as a whole, i.e. for a separable state there is no loss of information, but the description of an entangled state only in terms of its parts is incomplete.

Nevertheless, if the composite system is in a mixed state in general $S(\rho^A) \neq S(\rho^B)$. At least, the joint entropy satisfies the following inequalities [10]

$$S(\rho^{AB}) \leq S(\rho^A) + S(\rho^B), \tag{1.46}$$

$$S(\rho^{AB}) \geq \left|S(\rho^A) - S(\rho^B)\right|. \tag{1.47}$$

The first inequality, known as subadditivity inequality for von Neumann entropy, holds with equality if and only if both subsystems are uncorrelated, which is not a synonym for unentangled. An uncorrelated state can be represented as $\rho^{AB} = \rho^A \otimes \rho^B$ which shows clearly that they are separable states. This leads to the definition of a *correlation* degree for bipartite systems, given by

$$\frac{1}{2}\big(S(\rho^A) + S(\rho^B) - S(\rho^{AB})\big), \tag{1.48}$$

which is zero for uncorrelated states, and strictly positive otherwise. We ought to normalise it in order to obtain equivalent results to S_{red} for the case of a pure state.

Nevertheless, the correlation degree in Eq. 1.48 is not an appropriate magnitude to strictly quantify entanglement. Roughly speaking, a correlation between two physical subsystems may be classical or due to quantum entanglement, and the correlation measure intertwines them. Strictly speaking, an arbitrary separable state can be described by a classical probability ensemble of tensor product states $\{p_i, |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|\}$,

$$\rho_{sep} = \sum_i p_i \, |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i| \,, \tag{1.49}$$

where $\{|a_i\rangle\} \subset \mathcal{H}_a$ and $\{|b_i\rangle\} \subset \mathcal{H}_b$ are not necessarily orthonormal sets [19]. This state, may be prepared separately, without quantum entanglement, allowing classical communication in the preparation of the state of each subsystem. For instance, the preparation of each subsystem may depend in a common classical stochastic variable. Such a process results in a state with classical correlation between states $|a_i\rangle$ and $|b_i\rangle$, but not entanglement. To see the difference, compare with the Schmidt decomposition of an entangled pure state from Eq. 1.30 in the form of a density operator,

$$|\psi\rangle\langle\psi| = \sum_{i=1}^{d} \sum_{j=1}^{d} \lambda_i \lambda_j \, |a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j| \,. \tag{1.50}$$

Quantifying the entanglement of a mixed state is an active area of research, and there are many sophisticated techniques but they are out of the scope of this work [19]. For our purposes, correlation degree will be a sufficiently informative magnitude. In the state resulting from the quantum genetic algorithm described in Chapter 2, any classical correlation arises from projective measurements of previously entangled states. In Chapter 3, we are interested in measuring the consequences of entanglement during the whole algorithm, therefore, the correlation measure proposed in this section will prove insightful.

1.2.5 Distance measures for density operators

In this section, we review two methods to quantify the distance between density operators, namely, the trace distance and the fidelity.

Definition 4 *The* trace distance *between density operators ρ and σ acting on the same Hilbert space is defined as*

$$D(\rho, \sigma) \equiv \frac{1}{2} \operatorname{tr} |\rho - \sigma|, \tag{1.51}$$

where $|A| \equiv \sqrt{A^\dagger A}$ is the spectral norm.

It is clear from the definition that D is non-negative for any input states and that it is symmetric. Moreover, it can be easily proved that, in the domain of density operators, it satisfies the triangle inequality and that $D(\rho, \sigma) = 0$ if and only if $\rho = \sigma$. Therefore, the function D can be considered a proper distance function. Additionally, we will frequently make use of the following measure:

Definition 5 *The* fidelity *between density operators ρ and σ acting on the same Hilbert space is defined as*

$$F(\rho, \sigma) \equiv \mathrm{tr}^2 \sqrt{\rho^{1/2} \sigma \rho^{1/2}}. \tag{1.52}$$

Roughly speaking, the fidelity ranges from 0 for totally orthogonal states to 1 for identical states. Although it is a established method for comparing quantum states, one must keep in mind that it is not a distance metric in the mathematical sense. For example, the triangle inequality is not satisfied. However, it can be shown that F is symmetric, $F(\rho, \sigma) = F(\sigma, \rho)$ for any pair of density matrices.

If $\rho = |\psi\rangle\langle\psi|$ the fidelity reduces to

$$F(\rho, \sigma) = \mathrm{tr}^2 \sqrt{|\psi\rangle\langle\psi| \, \sigma \, |\psi\rangle\langle\psi|} = \mathrm{tr}^2 (\sqrt{\langle\psi|\sigma|\psi\rangle} \, |\psi\rangle\langle\psi|) = \langle\psi|\sigma|\psi\rangle \,, \tag{1.53}$$

which is the probability to measure state $|\psi\rangle$ in σ. Moreover, if additionally $\sigma = |\phi\rangle\langle\phi|$, then $F(\rho, \sigma) = |\langle\psi|\phi\rangle|^2$.

Interestingly, both trace distance and fidelity are invariant under unitary transformations on their arguments,

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma) \quad \text{and} \quad F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma). \tag{1.54}$$

As unitary transformations describe the evolution of isolated systems, we can conclude that if two arbitrary states, ρ and σ, evolve according to the same unitary transformation, U, the initial and the final distance between those states is the same. In other words, the distance between two quantum states is constant if they undergo the same isolated process.

1.2.6 Quantum channels

On the basis of Postulate V, we have focused on unitary transformations of quantum states, both for pure states and for density operators. These transformations perfectly describe quantum evolutions restricted to isolated physical systems. In this sense, quantum channels generalize the description to a wider variety of phenomena. The term quantum channel refers to physical systems which interact with an environment, including measurements, noise or other external stochastic interactions. Quantum channels are described by means of *quantum operations*, which can describe the most general transformation a quantum state ρ can undergo,

$$\rho \to \rho' = \mathcal{E}(\rho), \tag{1.55}$$

where $\mathcal{E}$ is a map from the set of density operators acting on the input state space, $\mathcal{H}$, to the set of density operator on the output state space, $\mathcal{H}'$. More precisely, quantum operations must satisfy the following conditions to preserve their physical meaning.

Definition 6 *Let $\mathcal{H}$ and $\mathcal{H}'$ be two Hilbert spaces. A map $\mathcal{E}$ from linear operators on $\mathcal{H}$ to linear operators on $\mathcal{H}'$ is called a* quantum operation *if it satisfies the following conditions.*

1. *For any density operator ρ acting on $\mathcal{H}$, we obtain* $0 \leq \mathrm{tr}[\mathcal{E}(\rho)] \leq 1$.

2. *$\mathcal{E}$ is a convex-linear map on the set of density operators.*

3. *$\mathcal{E}$ is a completely positive map.*

The first condition supports the interpretation that $\mathrm{tr}[\mathcal{E}(\rho)]$ reflects the probability of the quantum process to happen. If the quantum operation provides a complete description of the quantum channel, then $\mathcal{E}$ should also be a trace preserving map, $\mathrm{tr}[\mathcal{E}(\rho)] = 1$ for any density matrix ρ. Although it is convenient to allow for non trace-preserving maps, which provide partial descriptions of quantum channels, from now on we will consider trace-preserving maps.

Another physical requirement accounts for the second condition. If the initial density operator is selected from an ensemble $\{p_i, \rho_i\}$, we expect the output ensemble to be $\{p_i, \mathcal{E}(\rho_i)\}$, for a trace preserving map. That is,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i), \tag{1.56}$$

which describes the condition for a convex-linear map, because $\sum_i p_i = 1$ and $p_i \geq 0$.

The third condition ensures that we obtain a valid density matrix in the output. That is, for any positive operator A acting on the initial state space $\mathcal{H}$, one should obtain in the outcome a positive operator $\mathcal{E}(A)$ acting on the final state space $\mathcal{H}'$.

The following theorem provides a useful characterization for quantum operations.

Theorem 4 *A quantum operation $\mathcal{E}$ acting from linear operators on $\mathcal{H}$ to linear operators on $\mathcal{H}'$ admits an* operator-sum representation *of the form*

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{1.57}$$

for a set of linear operators $\{E_k\}$ acting from $\mathcal{H}$ to $\mathcal{H}'$, and satisfying $\sum_k E_k^\dagger E_k \leq \mathbb{I}$. The operators $\{E_k\}$ are known as the Kraus operators.

In particular, if $\mathcal{E}$ is a trace preserving map the condition for the operators transforms into $\sum_k E_k^\dagger E_k = \mathbb{I}$. Let us now analyze in this context the two processes described in Postulate IV and Postulate V. In the first case, the density operator resulting from the measurement of an observable with eigenvalues λ was shown to be $\mathcal{E}(\rho) = \sum_\lambda M_\lambda \rho M_\lambda$. The set of projection operators in the eigenspaces, $\{M_\lambda\}$, are the Kraus operators of this quantum channel. In the second case, a system under a unitary transformation can be described with a single Kraus operator which is the unitary operator of the process, thus $\mathcal{E}(\rho) = U\rho U^\dagger$.

Now, we are interested in reviewing a method to obtain the operator-sum representation for a quantum process. Here we elaborate on the common case of a physical system interacting with an environment, where $\mathcal{H} = \mathcal{H}'$ can be assumed. The general method implies first extending the physical system to include the environment, then applying a unitary evolution to the joint system, and finally

tracing out the environment. Let ρ be the initial state of the system and ρ_{env} the initial state of the environment and assume the joint system undergoes a unitary evolution U, then the resulting state of the system is

$$\mathcal{E}(\rho) = \text{tr}_{\text{env}}[U(\rho \otimes \rho_{\text{env}})U^\dagger]. \tag{1.58}$$

Now, let us assume that the initial state of the environment can be described by a reference state $\rho_{\text{env}} = |e_0\rangle\langle e_0|$ and employ an orthonormal basis $\{|e_k\rangle\}$ in the Hilbert space of the environment. Then,

$$\mathcal{E}(\rho) = \sum_k \mathbb{I} \otimes \langle e_k| \left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger\right] \mathbb{I} \otimes |e_k\rangle \tag{1.59}$$

$$= \sum_k E_k \rho E_k^\dagger, \tag{1.60}$$

where $E_k \equiv (\mathbb{I}\otimes\langle e_k|)U(\mathbb{I}\otimes|e_0\rangle)$ are the Kraus operators acting on the Hilbert space of the system. It can be shown that there is no loss of generality in assuming $|e_0\rangle\langle e_0|$ for the environment, due to a technique known as purification [10]. Moreover, although this method described for equal initial and final Hilbert spaces, it can be generalized to $\mathcal{H} \neq \mathcal{H}'$.

The operator sum representation provides a straightforward method to describe the quantum channel resulting from the composition of quantum channels. Let $\mathcal{E}$ be a quantum channel from $\mathcal{H}$ to $\mathcal{H}'$ with Kraus operators $\{E_k\}_{k=1}^K$, and $\mathcal{T}$ a quantum channel from $\mathcal{H}'$ to $\mathcal{H}''$ with Kraus operators $\{T_l\}_{l=1}^L$, then the quantum channel $\mathcal{T} \circ \mathcal{E}$ from $\mathcal{H}$ to $\mathcal{H}''$ has Kraus operators $\{T_l E_k\}$, with $1 \leq k \leq K$ and $1 \leq l \leq L$. This will play an important role in obtaining the quantum channel representation of the quantum genetic algorithm from the analysis of its subroutines. In particular, if $\mathcal{E}$ acts from $\mathcal{H}$ to $\mathcal{H}$ we denote $\mathcal{E}^n = \mathcal{E} \circ \cdots \circ \mathcal{E}$ to the n composition of the map $\mathcal{E}$. The n composition of a quantum channel is key for the analysis of the convergence of the algorithm, as we illustrate now introducing the concept of fixed points.

Fixed points of channels, which are the density operators satisfying $\mathcal{E}(\rho) = \rho$, are *stationary states*. These states have the distinctive property that they remain invariant under the action of the quantum channel. One can always assume without loss of generality that every quantum operation $\mathcal{E}$ has spectral radius 1 and, at least, one stationary state $\mathcal{E}(\Lambda) = \Lambda$ associated to that eigenvalue [20, 21]. Moreover, if there are more than one linearly independent fixed point, i.e. eigenvalue 1 is degenerate, the eigenspace of stationary states is a convex set with at most d^2 extreme points, where d is de dimension of the Hilbert space on which the operator acts.

If there is a unique eigenvalue of the quantum operation $\mathcal{E}$ with absolute value equal to unity and the fixed point Λ is a positive definite operator ($\Lambda > 0$), then the quantum channel is said to be strongly irreducible and satisfies the property that there exists the limit

$$\lim_{n\to\infty} \mathcal{E}^n = \mathcal{E}^\infty, \tag{1.61}$$

where $\mathcal{E}^\infty(X) := \Lambda\,\text{tr}(X)$ [22], for density operators $\mathcal{E}^\infty(\rho) := \Lambda$. This property implies the convergence towards the fixed point of the infinite composition of the

quantum channel acting on any initial state. Moreover, in this case the convergence towards the stationary state occurs in an exponential manner $\exp(1/\lambda_2)$ [22], where λ_2 is the second greater eigenvalue of $\mathcal{E}$. In general, one cannot ensure that the infinite composition of quantum channels converges, neither that its range is the set of fixed points. However, that property arises frequently in quantum channels.

In order to obtain the stationary state of a quantum channel one must solve the eigenvalue equation $\mathcal{E}(\rho) = \lambda\rho$ for $\lambda = 1$. This can be straightforwardly solved employing the matrix representation of the equation. For instance, take the density matrix corresponding to ρ and the Kraus matrices corresponding to E_k, then the eigenvalue equation is

$$\sum_{k=1}^{K} E_k \rho E_k^\dagger = \lambda\rho \quad \Rightarrow \quad \left(\sum_{k=1}^{K} E_k^* \otimes E_k\right)\mathrm{vec}(\rho) = \lambda\mathrm{vec}(\rho), \tag{1.62}$$

where $\mathrm{vec}(\rho)$ denotes the vectorization of the matrix ρ, obtained by concatenating the columns of the matrix ρ in a single column, and E_k^* denotes the complex conjugate of E_k. The matrix equation arises from the vectorization property $\mathrm{vec}(ABC) = \big(C^T \otimes A\big)\mathrm{vec}(B)$.

1.3 Fundamentals of quantum computation

Quantum computation is a computational paradigm built upon the properties of quantum mechanics. This allows for encoding information in quantum states and performing computational procedures by transforming those states according to quantum dynamics. Those procedures are commonly known as quantum algorithms. Firstly, we formally define the qubit, which was already mentioned as an example of a physical system. Then, we review the concepts of quantum measurement and quantum gates. In this section, we also introduce the fundamental notation used to represent quantum procedures, i.e. the quantum circuit notation.

1.3.1 Quantum bits

The fundamental unit of information in classical computation is the bit, which is an abstraction of a physical system with two possible states, namely, 0 and 1. The qubit is its quantum counterpart, it is an abstraction of a physical system associated to a 2-dimensional Hilbert space. The preferred basis for such a system is the *computational basis*, composed of the orthonormal vectors $|0\rangle$ and $|1\rangle$. As introduced after Postulate I, the most general pure qubit state can be represented as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\,, \tag{1.63}$$

with θ and ϕ any real numbers in the range $[0, 2\pi)$. Here we have assumed the convention of a real amplitude for $|0\rangle$, motivated by the global phase equivalence. From now on, we will adopt the convention

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}. \tag{1.64}$$

In general, we employ n qubits to design quantum algorithms. Such a system is related to a 2^n-dimensional Hilbert space, whose computational basis is described by all the possible n-bit strings, $\{|00...00\rangle, |00...01\rangle, ..., |11...10\rangle, |11...11\rangle\}$. Bit strings are usually also denoted by the integer they represent in binary basis, i.e. $|00...00\rangle = |0\rangle, |00...01\rangle = |1\rangle, ..., |11...10\rangle = |2^n - 2\rangle, |11...11\rangle = |2^n - 1\rangle$. Therefore, we can write an arbitrary state for a n-qubit system as

$$|\psi\rangle = \sum_{i_1,\cdots,i_n=0,1} a_{i_1\cdots i_n} |i_1 \cdots i_n\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle , \tag{1.65}$$

with complex amplitudes a_i satisfying $\sum_i |a_i|^2 = 1$. Considering the global phase equivalence, a n-qubit pure state requires $2^n - 1$ complex amplitudes to be completely described.

The convention adopted for the column vector representation is

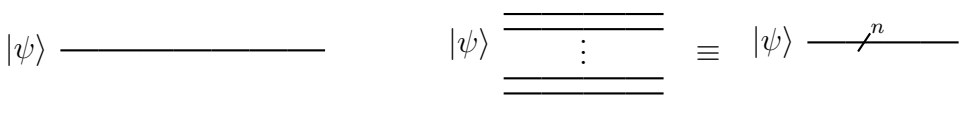
$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^n-1} \end{pmatrix}. \tag{1.66}$$

This is consistent with the description given in Section 1.2.1 for the computational basis for a two qubit system and the convention in Eq. 1.64, substituting the tensor product of state vectors with the Kronecker product of matrices for column vectors. For example,

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}. \tag{1.67}$$

Note that we obtain a column vector which is defined block-wise, where each block is constructed by the product of each element of the first vector with the second vector.

In quantum circuit notation, every qubit is represented by a horizontal wire, as in the diagram shown in Fig. 1.1, where time goes from left to right. n qubits are usually represented by n horizontal lines or by a single wire carrying n qubits, sometimes the slash is implicitly assumed.



(a) (b)

Figure 1.1: Circuit notation: a) wire carrying a single qubit, and b) n qubits or wire carrying n qubits, sometimes the slash is implicitly assumed.

1.3.2 Measurements

In the context of quantum computation, measurements commonly refer to measurements in a particular basis. According to Postulates III and IV, the probabilities of a state described as a linear combination in certain basis to be measured in one of the vectors of this basis are proportional to the absolute value of the corresponding amplitude squared and the state after the measurement collapses to the vector obtained. However, we usually represent the computational basis to represent the states of qubit-strings and we occasionally need to perform measurements in a different basis. In those cases, we shall employ the procedure described in Section 1.3.2 to compute the probabilities for each outcome of the measurement. The notation in quantum circuit diagrams for a measurement is depicted in Fig. 1.2.

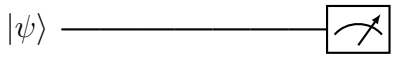


Figure 1.2: Circuit notation for a measurement.

As an instance of a measurement of a single qubit in the computational basis, $\{|0\rangle, |1\rangle\}$, note that the probability of obtaining $|0\rangle$ and $|1\rangle$ in the qubit state described in Eq. 1.63 are $\cos^2\frac{\theta}{2}$ and $\sin^2\frac{\theta}{2}$, respectively. If the output obtained corresponds to $|0\rangle$, then the state collapses to $|0\rangle$, while if the output corresponds to $|1\rangle$ it collapses to $|1\rangle$. This property is satisfied for an arbitrary n-qubit state, as described in Eq. 1.65, where the probability of obtaining output i is given by $|a_i|^2$.

We can represent the state after measuring in the $\{|0\rangle, |1\rangle\}$ basis and assuming the outcome of the measurement is unknown by the state ensemble $\left\{\left(\cos^2\frac{\theta}{2}, |0\rangle\right), \left(\sin^2\frac{\theta}{2}, |1\rangle\right)\right\}$ and, thus, by the density matrix

$$\rho = \cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| = \begin{pmatrix}\cos^2\frac{\theta}{2} & 0\\ 0 & \sin^2\frac{\theta}{2}\end{pmatrix}. \tag{1.68}$$

One can also measure in other basis. For example, take the states $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$, which clearly form an orthonormal basis in a 2-dimensional Hilbert space. In order to apply the procedure described after Postulate II, we must define the projection operators into the subspace related with each possible outcome, namely, $M_+ = |+\rangle\langle +|$ and $M_- = |-\rangle\langle -|$. Consequently, it is straightforward to compute the probability of obtaining each output by virtue of Postulate III, $p_+ = \langle\psi|M_+|\psi\rangle = |\langle +|\psi\rangle|^2 = (1+\cos\varphi\sin\theta)/2$, and $p_- = \langle\psi|M_-|\psi\rangle = |\langle -|\psi\rangle|^2 = (1-\cos\varphi\sin\theta)/2$, where p_+ and p_- denote the probability of obtaining $|+\rangle$ or $|-\rangle$. We can also represent the mixed state after the measurement with a density matrix,

$$\rho = M_+|\psi\rangle\langle\psi|M_+ + M_-|\psi\rangle\langle\psi|M_- \tag{1.69}$$

$$= p_+|+\rangle\langle +| + p_-|-\rangle\langle -| \tag{1.70}$$

$$= \begin{pmatrix}\frac{1}{2} & \cos\varphi\sin\theta\\ \cos\varphi\sin\theta & \frac{1}{2}\end{pmatrix}, \tag{1.71}$$

which is equivalent to the mixed state described by the state ensemble $\{(p_+, |+\rangle), (p_-, |-\rangle)\}$.

Additionally, one can also restrict its measurement to a subset of qubits. In this case we say that some qubits are measured in a particular basis. For example, take the general two qubit state described by four complex parameters a, b, c and d, with $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$,

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle\,. \tag{1.72}$$

Applying the usual procedure we define the projection operators into subspace of each qubit value, precisely, for the value 0 we get $M_0 = |0\rangle\langle 0| \otimes \mathbb{I}$ and for 1 $M_1 = |1\rangle\langle 1| \otimes \mathbb{I}$. Therefore, the probability of obtaining $|0\rangle$ in the first qubit is $\langle\psi|M_0|\psi\rangle = |a|^2 + |b|^2$ and $|1\rangle$ is $\langle\psi|M_1|\psi\rangle = |c|^2 + |d|^2$, and

$$\text{with output } |0\rangle \text{ the resulting state is } \frac{M_0\,|\psi\rangle}{\sqrt{\langle\psi|M_0|\psi\rangle}} = \frac{a\,|00\rangle + b\,|01\rangle}{\sqrt{|a|^2 + |b|^2}}, \tag{1.73}$$

$$\text{with output } |1\rangle \text{ the resulting state is } \frac{M_1\,|\psi\rangle}{\sqrt{\langle\psi|M_1|\psi\rangle}} = \frac{c\,|10\rangle + d\,|11\rangle}{\sqrt{|c|^2 + |d|^2}}. \tag{1.74}$$

Let me note that the probability of obtaining $|0\rangle$ (or $|1\rangle$) is also the addition of the probability of obtaining any of the states with value 0 (or 1) in that qubit. We can also represent the mixed state after the measurement with a density matrix,

$$\rho = (a\,|00\rangle + b\,|01\rangle)(a^*\,\langle 00| + b^*\,\langle 01|) + (c\,|10\rangle + d\,|11\rangle)(c^*\,\langle 10| + d^*\,\langle 11|) \tag{1.75}$$

$$= \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} a^* & b^* & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ c \\ d \end{pmatrix} \begin{pmatrix} 0 & 0 & c^* & d^* \end{pmatrix} = \begin{pmatrix} |a|^2 & ab^* & 0 & 0 \\ a^*b & |b|^2 & 0 & 0 \\ 0 & 0 & |c|^2 & c^*d \\ 0 & 0 & cd^* & |d|^2 \end{pmatrix}. \tag{1.76}$$

1.3.3 Quantum logic gates

Classical logic gates are Boolean functions describing operations performed in bit strings that yield a new bit string as a classical result. More formally, they take the form $f : \{0,1\}^k \to \{0,1\}^m$, where k indicates the number of input bits and m the number of output bits. A fundamental example of one of such functions is the AND(x, y) gate, which gets two input bits and returns a 1 if and only if both are 1, otherwise it returns a 0. This can be mathematically described employing Boolean algebra, but in computational science it is also common to use the truth table or the logic circuit representation of a function. In Fig 1.3, we show the truth tables for AND, OR and NOT gates, together with their logic circuit representation.

Quantum logic gates, or simply quantum gates, have to be implemented via unitary transformations, as described in Postulate V. Therefore, a n-qubit quantum logic gate can be represented by a unitary matrix U with shape $2^n \times 2^n$.

Classically, it can be shown that a small set of gates are sufficient to compute any Boolean function, for example the AND and NOT gates. A set with those properties is known as universal set for classical computation. Additionally, it can be shown that a finite set of quantum gates can be used to compute an

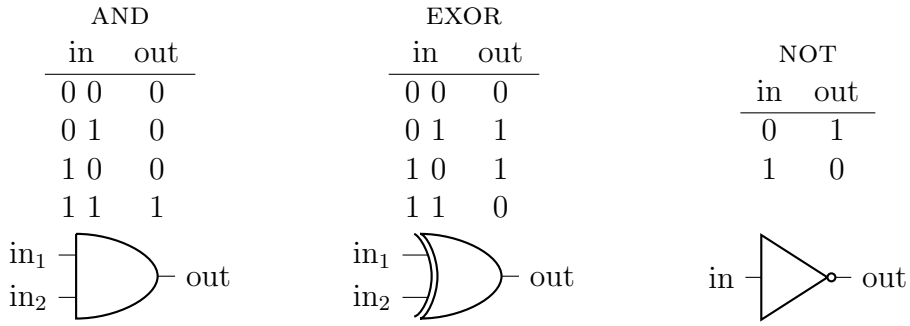


Figure 1.3: Truth tables and circuit representations for some classical gates.

arbitrary classical function [10], maybe discarding some of the output qubits. Hence, a quantum computer can simulate a classical computer and the other way around. Therefore, we can conclude that both have the same computational power. Moreover, one can find a finite set of quantum gates which can be used to replicate any other quantum gate with arbitrary accuracy, as proven in the Solovay-Kitaev theorem [10]. Even though these results regarding universality are of great importance for the implementability of quantum algorithms into physical quantum computers, we will not develop them in this introduction, since they are note necessary for this master thesis.

The general notation for a quantum gate U is depicted in Fig. 1.4. In circuit notation, gates are always applied to the state on the left and produce the state at the right. Hereunder, some important gates are introduced.

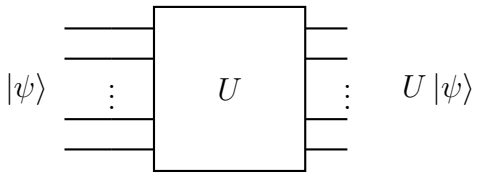


Figure 1.4: General n qubit quantum logic gate represented by unitary matrix U.

Single qubit gates

(a) (b)

Figure 1.5: Circuit notation examples for a) X gate, also known as NOT gate and b) Hadamard gate, H.

Quantum gates acting on a single-qubit are known as single-qubit gates. For a single qubit, the operation performed by the quantum evolution can be described by a 2×2 unitary matrix

$$U = \begin{pmatrix} \cos\theta & e^{i\varphi}\sin\theta \\ e^{i\gamma}\sin\theta & -e^{i(\varphi+\gamma)}\cos\theta \end{pmatrix}, \tag{1.77}$$

where θ, φ and γ represent real parameters in the interval $[0, 2\pi)$.

The classical NOT gate, described in Fig. 1.3, has its quantum counterpart represented with the Pauli-X matrix, which performs the transformation $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. In practice, the Pauli matrices are of great importance for quantum computation. Here, we list them as matrices in the computational basis

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{1.78}$$

Other important gates are the Hadamard gate (H), phase gate (S) and $\pi/8$ gate (T) listed below

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{1.79}$$

When we act with single qubit gates on several qubits, the whole unitary transformation can be described by the Kronecker product of the matrices representing each single qubit gate. For instance, if the set of single qubit transformations $\{U_1, U_2, \ldots, U_n\}$ describes each unitary transformation in a n-qubit system, the global system's unitary is $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$. Note that the identity transformation can be substituted when no gate is acting on a qubit. For instance, if in a two-qubit system the identity gate is applied in the first qubit and a Hadamard gate is applied in the second one, as expressed in Fig. 1.6, this can be described by

$$\mathbb{I} \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{1.80}$$

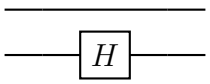


Figure 1.6: Circuit representation for $\mathbb{I} \otimes H$.

Two-qubit gates

Although single-qubit gates can act in different qubits, they operate separately in the Hilbert space of each qubit. Multi-qubit gates, in turn, act on the Hilbert space of the whole multi-qubit system. For instance, a two-qubit gate may transform a separable state into an entangled state, or vice-versa, while that is impossible with single-qubit gates.

Let us take the case of a two-qubit circuit aimed to change the value of the second qubit, target qubit, depending on the first one, control qubit. If the control qubit is in $|q_1\rangle = |0\rangle$ state, the other qubit will not be touched, while if it is in $|q_1\rangle = |1\rangle$ the target will be flipped, apply a X gate. This two-qubit gate is known as the controlled not or simply CNOT gate, and it can be written in the

computational basis ($\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ for $|q_1 q_2\rangle$) as

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{1.81}$$

and it is depicted in Fig. 1.7a in circuit notation. Note that, if we apply a CNOT gate on a two-qubit state which may initially be separable, as in Fig. 1.7a, we can get an entangled state. This is not possible with single qubit gates, as illustrated with an example in Fig. 1.7b.

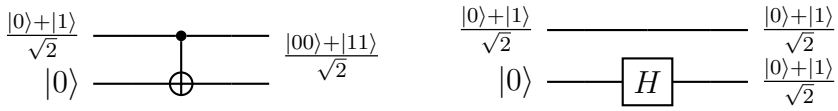


Figure 1.7: Difference between a) applying a controlled-not with a superpostion state in the control and b) applying a Hadamard gate in the target qubit. Note that in both cases a superposition is obtained in the output state, but only the CNOT creates an entanglement.

Other common two-qubit gate is the SWAP gate. This gate performs the operation $S_{1,2}|x\rangle|y\rangle = |y\rangle|x\rangle$ in the computational basis, $x, y \in \{0, 1\}$, and its matrix representation is

$$S_{1,2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.82}$$

When n-qubit systems are involved, the two-qubit swap operation $S_{i,j}$ describes the action of swapping qubits i and j,

$$S_{i,j}|x_1\rangle_1 \cdots |x_i\rangle_i \cdots |x_j\rangle_j \cdots |x_n\rangle_n = |x_1\rangle_1 \cdots |x_j\rangle_i \cdots |x_i\rangle_j \cdots |x_n\rangle_n. \tag{1.83}$$

We have only exposed those gates which play an important role in the development of the quantum genetic algorithm. Therefore, many important single qubit gates and multi-qubit gates have been omitted for the sake of concreteness.

1.4 Summary table

Concept	Description
Pure state	A normalized vector $\|\psi\rangle$ belonging to a Hilbert space $\mathcal{H}$ associated to a physical system, known as the *state vector* or *ket*.
Dual of a state	The functional $\langle\psi\|$ belonging to the dual space of $\mathcal{H}$ which associates to each vector state $\|\phi\rangle$ the result of the product $\langle\psi\|\phi\rangle$, known as the *bra* of a vector state $\|\psi\rangle$.
Density operator	$\rho \equiv \sum_i w_i \|\psi_i\rangle\langle\psi_i\|$, where w_i is the probability of finding the system in the vector state $\|\psi_i\rangle$.
Observable	Represented as lineal self-adjoint operator, A, acting on $\mathcal{H}$.
Spectral decomposition of A	$A = \sum_{\lambda\in\sigma(A)} \lambda M_\lambda$, where $\sigma(A)$ is the spectrum of A and M_λ is the projectors in the eigenspace associated to eigenvalue λ.
Measurement of A: outcomes	Outcomes must be one of the eigenvalues of A. The probability of obtaining λ in a vector state is $\langle\psi\|M_\lambda\|\psi\rangle$ and in a density operator $\mathrm{tr}(\rho M_\lambda)$.
Measurement: remaining state	If outcome λ is obtained, the remaining state is $M_\lambda \|\psi\rangle / \sqrt{\langle\psi\|M_\lambda\|\psi\rangle}$ for a vector state and $M_\lambda \rho M_\lambda / \mathrm{tr}(\rho M_\lambda)$ for a density operator.
Time evolution of an isolated system	Given an initial state $\|\psi_0\rangle$ and the unitary operator U describing the evolution, the final state is $\|\psi\rangle = U\|\psi_0\rangle$.
Quantum operation	It is a map $\mathcal{E}$ from linear operators on the Hilbert space $\mathcal{H}$ to linear operators on the Hilbert space $\mathcal{H}'$ satisfying that 1. $0 \le \mathrm{tr}[\mathcal{E}(\rho)] \le 1$ for any density operator ρ acting on $\mathcal{H}$. 2. $\mathcal{E}$ is a convex-linear map on the set of density operators. 3. $\mathcal{E}$ is a completely positive map.
Entanglement	Given $\mathcal{H}_1$ and $\mathcal{H}_2$, their joint state $\|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is separable if it can be expressed as $\|\psi\rangle = \|\psi_1\rangle\|\psi_2\rangle$ for $\|\psi_1\rangle \in \mathcal{H}_1$ and $\|\psi_2\rangle \in \mathcal{H}_2$, otherwise it is entangled.
Entropy	$S(\rho) \equiv -\mathrm{tr}(\rho \log_2 \rho)$
Trace distance	$D(\rho,\sigma) \equiv \frac{1}{2}\mathrm{tr}\|\rho-\sigma\|$, where $\|A\| \equiv \sqrt{A^\dagger A}$
Fidelity	$F(\rho,\sigma) \equiv \mathrm{tr}^2 \sqrt{\rho^{1/2}\sigma\rho^{1/2}}$
Qubit	A physical system associated to a 2-dimensional Hilbert space.
Quantum register	Physical system composed of n qubits.
Quantum gate	Unitary operation acting on the state of quantum registers.

Table 1.1: Summary of the concepts introduced in the first chapter. $\mathcal{H}$, $\mathcal{H}_1$ and $\mathcal{H}_2$ refer to Hilbert spaces associated to a physical system. ρ and σ refer to density operators, assumed to be acting on the same Hilbert space.

Chapter 2

A quantum genetic algorithm

Genetic Algorithms (GAs) are extremely successful bioinspired optimization algorithms which emulate the natural selection process. Merging GAs with quantum computation is an old ambition which has been considered as a potential source of new heuristic optimisation methods. However, only restricted results have been achieved up to now due to the limitations imposed by quantum mechanics for cloning or erasing information.

This chapter begins introducing classical GAs and their components (Section 2.1). Then, we introduce the outstanding challenges which hinder the development of a fully quantum genetic algorithm (QGA) and the attempts to achieve it so far (Section 2.2). Afterwards, we describe our proposal for a QGA, elaborating each of the subroutines, explaining their characteristics and introducing illustrative examples. The algorithm is divided into the selection subroutine (Section 2.5), the crossover subroutine (Section 2.6), and the mutation subroutine (Section 2.7).

2.1 Classical genetic algorithms

Classical genetic algorithms (GAs) are heuristic optimisation methods based on natural selection and the evolution of species. Before anything else, one needs to find a suitable encoding for the candidates to solutions, known as individuals, and an appropriate fitness criteria which grades each individual. Afterwards, a group of random individuals are generated forming the initial population. Then, the population is evolved for a finite number of generations until the improvement in the overall fitness is considered sufficient.

There are different forms to implement these algorithms and multiple modifications have been proposed since their original proposal. However, for the sake of simplicity, we will focus on a typical GA as referred in Refs. [23, 24] and depicted in Fig. 2.1. In particular, we will only consider binary encoding, that is, individuals are completely described by a finite bit string which is known as the *chromosome* of the individual.

The basic structure of the algorithm is described in the flow chart in Fig. 2.1. Initially, a random population with N individuals is generated before starting the evolution process to generate the first generation. Afterwards, after every generation a set of subroutines are applied. First, the fitness of each individual is evaluated and this information is used to select the individuals with highest

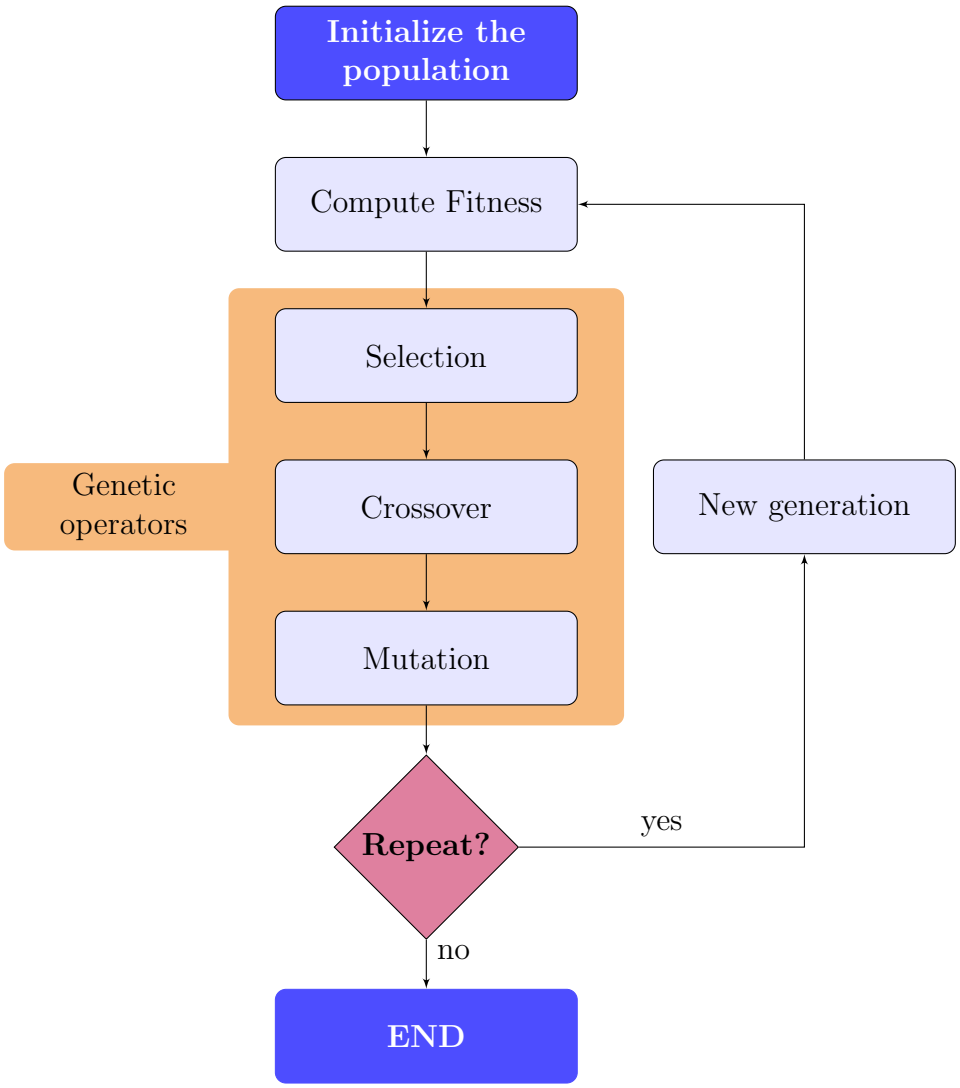


Figure 2.1: Flow diagram representation of a simple genetic algorithm.

fitness. Then, selected individuals are replicated and part of their bit strings are interchanged, resembling the sexual reproduction of living beings. Finally, bots can be randomly flipped (mutated) with a small probability p_m. In each generation, the number of individuals remains constant and the evolutionary process concludes either when a sufficiently good individual is found or when the maximum number of generations is reached.

2.1.1 Search space and fitness landscape

Let us introduce some commonplace terminology related with GAs, which will also be helpful for the understanding of the quantum counterpart. The *search space* of a particular GA refers to the whole set of possibilities for the encoding of the individuals. For instance, if we represent them with a n-bit string, the search space is composed of 2^n potential individuals. It is clear that the search space grows exponentially with the length of the bit-string.

The *fitness landscape* is the set of possible fitness achievable by the individuals.

Typically, we are unable to compute the whole fitness landscape. However, GAs often succeed at globally optimizing in the fitness landscape by computing only a small set of fitnesses [23].

2.1.2 The genetic operators

The genetic operators are the set of subroutines which are used to emulate the natural selection and sexual reproduction processes. Hereunder we focus in the most common approaches to implement these subroutines.

Selection. During this process, individuals are picked from the population to be part of the new offspring. In order to introduce the evolving pressure into the population, it must prioritize the best individuals. However, too strict selection methods could lead to rapidly converging generations that get stuck in local optima. There are two widespread approaches to accomplish selection, namely fitness proportional selection and elitist selection. The first one consists on selecting individuals randomly with a probability that is proportional to their relative fitness in the population. Whereas, the second one consists on straightforwardly selecting only the best individuals.

Crossover. This subroutine allows us to combine the values of the bit strings from different individuals. Typically, two parent individuals are chosen and their bit-strings are cut in the ith bit. Afterwards, the halves are interchanged mixing the starting and ending parts of different bit-strings, thus, resulting in two new individuals.

Mutation. The bit-flip operation known as mutation is the only operator which introduces new genetic information. As described above, each bit is mutated with probability p_m, which must be small, otherwise it may jeopardize the convergence of the GA. It is straightforward to see that mutations improving the performance of an individual tend to survive, while mutations that spoil their performance rapidly vanish.

2.2 Towards quantum genetic algorithms

During the past decades, merging genetic algorithms and quantum computation has been considered as a potential source of new heuristic optimization methods. The success of GAs solving classical optimization problems and the speed-up obtained by quantum algorithms in other fields have led to multiple publications in this direction [1, 2, 3]. Nevertheless, most of the effort has been focused on quantum inspired genetic algorithms, which are classical GAs that smartly adapt some concepts of quantum computation to promote new varieties of classical evolutionary techniques [4, 25, 26, 27, 28, 29, 30, 2]. In contrast, the algorithms pursuing quantum speed-up have achieved partial success in the implementation of a integral quantum proposal of a genetic algorithm, i.e. one performing the

genetic operators on a quantum state and satisfactorily implementing population evolution [5, 6, 7, 8].

In 1996, Narayanan and Moore proposed the first quantum inspired genetic algorithm (QIGA), which was completely conceived to be run in a classical computer [4]. Later, in the early 2000s, Han and Kim proposed a genetic quantum algorithm (GQA) adapting the QIGA, which represented the individuals employing qubit strings and the operations where performed with quantum gates [25, 26, 27]. The GQA has been further developed in latter publications [28, 29, 30, 2], and has even been proposed for particular optimization problems such as the Knapsack problem [27], PID tuning [31], and scheduling problems [32]. However, as noted by Sofge, the approach proposed by Han and Kim is infeasible in quantum hardware, since it disregards the implications of quantum measurements and the limitations of quantum cloning [1]. Therefore, the GQA is in fact a variation of the quantum inspired genetic algorithm. In fact, Roy et al. also noted this limitations of the GQA [2], and Lahoz-Beltra noted that these algorithms can be efficiently simulated in classical software, suggesting that they cannot lead to any quantum advantage [3].

In 2001, Rylander et al. proposed another quantum genetic algorithm, based on the principles of quantum superposition and quantum entanglement [5]. Their contribution consists in the introduction of the concepts of register individual and fitness registers. Both registers are in a superposition of chromosome-fitness pairs of the individuals, which means that the joint state of both registers is entangled. Although they claim that quantum superposition provides an increased searching power, probably resulting from better building blocks, this conclusion is considered unsupported [1].

In 2006, Udrescu et al. proposed an algorithm based on successful quantum searching algorithms and inspired by evolutionary computation [6]. This algorithm is called reduced quantum genetic algorithm (RQGA), because it employs a single register to represent the whole population by means of quantum superposition. The authors based on Grover's algorithm for searching in an unsorted list [33] in order to speed-up the selection process. Yet they conclude that there is no need of genetic operators like crossover or mutation, which has been used to argue that it is not truly a genetic algorithm [1]. Afterwards, Malossini et al. [7] proposed in 2008 the quantum genetic optimization algorithm (QGOA) which also employed quantum searching techniques, namely the Dür-Høyer algorithm for finding the minimum of an unsorted list [34]. This is employed to enhance the selection procedure but the crossover and mutation subroutines are classically processed. Lately, Saitoh et al. [8] proposed an algorithm based on RQGA and QGOA now including the crossover and mutation as quantum protocols. However, the role of the population in the evolutionary process dramatically differs from the usual role in classical GAs. Indeed, once the crossover and mutation are implemented by means of quantum procedures, the selection procedure is performed by Grover-BBHT search [35]. The latter requires projective measurements in order to find the maximum of an unsorted list, i.e. the individual with maximum fitness in this case. As a result, once this genetic operation is concluded, the individual with maximum fitness is the only information about the population that is retrieved from the state. Therefore, they initialize the population of the next generation

with that individual and a set of pseudo-randomly generated individuals. This results in a population evolution which could be deficient compared to classical GAs, due to the lack of memory of other individuals. Although SaiToh et al. propose an extension of their algorithm to mitigate this effect, it is not clear if the resulting algorithm performs comparably to classical GAs. In general, these algorithms pursue computational speed-up, but their evolutionary behaviour has not been sufficiently supported.

To summarise, those algorithms developed upon the Quantum-Inspired Genetic Algorithm are genetic algorithms which are not suitable for a quantum computer; whereas, other attempts stemming from truly quantum runnable principles achieve no probed success or take questionable advantage of genetic operators. Most of the previous approaches, are thoroughly revised in Softge's review [1], remarking the conclusions summarised in this paragraph. Although Lahoz-Beltra's later review includes some more recent algorithms [3], Softge's work is specially enlightening when it comes to understanding the state of the art of quantum genetic algorithms and it clearly highlights the respective relevant contributions.

Any attempt to create a quantum version of a genetic algorithm must overcome the obstacles related to the gap between classical information and quantum information. First, the no-cloning theorem obliges the quantum version to constrain itself to imperfect replication techniques, which opens a wide variety of selectable approximate cloning algorithms (Section 2.6.1). Second, the codification of the individuals and the definition of the fitness criteria are central topics in classical GAs. This problem is magnified by the more complex nature of quantum information, hence the possibilities for codification are greatly increased. Third, although quantum computers may access an exponentially larger search space during execution (compared to the number of qubits), their final output is restricted to the possible outcomes of measurements (which are of the size of the number of qubits). A final point is that the progress in classical genetic algorithms has been greatly boosted by the improvements in available computational power, due to their heuristic nature. In fact, formal analysis of their performance is limited to simplified versions [23]. The latter thought suggests that the area of quantum genetic algorithms may lack the boost of sufficiently powerful quantum hardware. Additionally, due to the heuristic nature of GAs, in order to compare their performance benchmark functions are employed, but this approach cannot be directly applicable to QGAs.

The quantum genetic algorithm introduced in this chapter (from now on we will refer to it using the abbreviation QGA) was started during my Bachelor Thesis [9]. There, we started the fundamentals of a novel fully-quantum genetic algorithm, which is the core of the algorithm developed here. In this work, we have substantially extended previous results and introduce new powerful tools based on the theory of quantum channels (completely positive trace preserving maps, see Section 1.2.6) to analyse the performance of these algorithms. Additionally, we have clarified the structure of QGAs, which allows us to clearly distinguish the fundamental parts from the ones that can be adapted in further works. Consequently, the aim of this work is finding potential advantages of QGAs, identifying the tunable features and critically studying their impact on the performance.

As stated below in Section 2.5.1, we expect that the main advantage of this algorithm over its classical counterpart is in the evaluation of the fitness criterion. However, in order to prove an overall speed-up one should also ensure that other subroutines of the algorithm and the final information retrieval can be implemented efficiently. Additionally, the QGA should also be compared with other optimization protocols based on quantum computers, not only with its classical counterpart. All in all, proving this in a general case, i.e with individuals of arbitrary length, is an extremely hard goal which will require further research. However, we expect that the algorithm proposed here and the tools developed in Chapter 3 will lead to a new perspective in the research on quantum genetic algorithms.

2.3 Overview of the quantum genetic algorithm

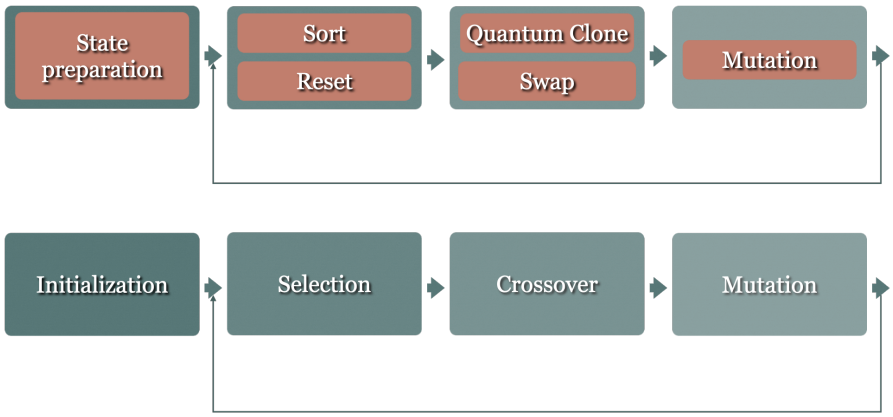


Figure 2.2: Comparison between the parts of the classical GA and the QGA. The mapping from the classical genetic operator to the quantum ones is not unique.

Figure 2.2 compares the structure of classical GAs with the one of QGAs, genetic operators are identified with three quantum subroutines. In essence, our proposal for QGA finds direct inspiration from classical GAs. However, this extension is not unique and may lead to different solutions.

With respect to the structure of this chapter, we initially describe the encoding used for the quantum individuals, as well as the relevant terminology in Section 2.4, which is afterwards summarized in Table 2.1. In the remaining sections, we describe the subroutines proposed for each genetic operator, discussing possible variations.

Selection is inspired by the classical elitist selection, i.e. only the best individuals survive. In Section 2.5, we discuss the quantum counterpart, which is implemented into two steps: first by sorting the individuals and then, by discarding the worst ones. Remarkably, we are able to perform the sorting operation without measuring the individuals to evaluate them, thus preserving their quantumness.

Section 2.6 is devoted to the analysis of the crossover subroutine, which face the constraints imposed by the no-cloning theorem and the methods to achieve partial cloning. Indeed, in Section 2.6.1 we review two paradigmatic methods for pseudo-cloning, whose impact on the performance of the QGA is later studied in Chapter 3.

Finally, in Section 2.7, we shortly review the importance of mutation, proposing to implement it by means of single qubit rotations. The necessity of this operation as a source of new information into the procedure is debatable in the quantum case, since the perturbing effect introduced by quantum measurements and approximated cloning may already play this role [5]. However, a careful discussion about this issue requires additional research and it is left for a future work.

Regarding previous QGAs, our approach in codification is similar to Rylander et al. [5], except that they overlook the possibility of considering solutions out of the computational basis, which restricts its computational power due to Gottesman–Knill theorem, and they require measuring the fitness of the individuals. On the other hand, Udrescu et al. [6], Malossini et al. [7], and SaiToh et al. [8] proposed a compact manner to employ a single register to store as a superposition all the individuals. However, we discarded this representation because this approach shows serious drawbacks. Additionally, this approach shows limitations for implementing satisfactory population evolution by means of quantum subroutines and jeopardizes the possibility of exploring states out of the computational basis. Although, Malossini et al. [7] prove a computational speed-up for their quantum enhanced genetic algorithm restricted to a particular type of fitness criteria, we did not prove it yet for our QGA. Nevertheless, it has been noted that the bottleneck of GAs is often the evaluation of the fitness criteria and not the application of genetic operators [1]. Here, we expect that our algorithm takes advantage of quantum subroutines with proved computational speed-up in the selection subroutine, mainly for the computation of fitness criteria.

2.4 Encoding and general procedure

Extending the classical picture, each individual is represented by the state of a qubit register, analogous to a bit string. There are n individuals stored in n independent registers, each of them comprising c qubits corresponding to their chromosome length. Previous works in QGAs have focused on solutions which can be classically represented with c bits [4, 7, 5], constraining the effective search space to individuals in the computational basis, which seriously limits its computational power due to Gottesman–Knill theorem. However, our approach allows for the whole Hilbert space associated to the register as the actual search space.

In order to analyse the QGA, it is useful to relate the fitness criteria with a cost function, which in turn can be related to a *problem Hamiltonian*, H_P. The problem Hamiltonian is defined so that it assigns higher expected energies to worst individuals, then the optimisation problem becomes a problem of finding low energy states, ideally the ground state (the state with the lowest energy). The fitness criterion is properly defined in a particular basis that we call the *problem basis*, $\{|u_k\rangle\}_{k=0}^{2^c-1}$, composed by the eigenstates of H_P and are assumed ordered

by their associate eigenvalues, $\lambda_k \leq \lambda_{k+1}$ where λ_k is the eigenvalue related to $|u_k\rangle$. These eigenvectors can theoretically be described by their coefficient in the computational basis, a_{kj}, satisfying the equation

$$|u_k\rangle = \sum_{j=0}^{2^c-1} a_{kj} |j\rangle , \tag{2.1}$$

where $|j\rangle$ represents the jth state in the computational basis. Let us define the problem unitary matrix by $(U_P)_{kj} = a^*_{jk}$, then

$$|u_k\rangle = U_P |k\rangle , \tag{2.2}$$

hence the problem is completely defined by U_P and the list of eigenvalues. Moreover, we will later show that, given a non-degenerate Hamiltonian, the problem is completely defined by U_P (Section 2.5.2).

In the following, we describe the state of the population in terms of the problem basis, in order to be clear about the action of each subroutine, but we shall remark that the knowledge of this basis is not required to implement the algorithm. Indeed, if the problem basis was required to be known beforehand, our optimization could be reformulated by mapping the problem basis to the computational basis. Whereas, if the problem basis was unknown, computing it could be equivalently hard to solving the problem itself. Instead, we only require an oracle that is able to compare states in the problem basis or able to evaluate their fitness. These are less demanding requirements, since it only demands to be able to perform controlled-U_P unitaries.

One can build a basis for the Hilbert space associated to n registers by combining the states of the problem basis employing the tensor product. This results in states with the form $|u_{k_1}\rangle_1 \otimes |u_{k_2}\rangle_2 \otimes ... \otimes |u_{k_n}\rangle_n$. Consequently, the state of the whole population, $|\psi_{\text{pop}}\rangle$, can be described as a linear combination of $p_{\max}$ different register-separable states in the problem basis,

$$|\psi_{\text{pop}}\rangle = \sum_{p=1}^{p_{\max}} b_p |u^p_{k_1}\rangle_1 \otimes |u^p_{k_2}\rangle_2 \otimes ... \otimes |u^p_{k_n}\rangle_n \tag{2.3}$$

$$= \sum_{p=1}^{p_{\max}} b_p \bigotimes_{r=1}^{n} |u^p_{k_r}\rangle_r , \tag{2.4}$$

where b_p are complex coefficients satisfying $\sum_p |b_p|^2 = 1$; and $|u^p_{k_r}\rangle_r$ denotes the k_r-th problem basis state, considered for the register r in the term p of the summation. Each term p in the summation describes a separable register state, whereas each $|u^p_{k_r}\rangle_r$ may be entangled. Altogether, $|\psi_{\text{pop}}\rangle$ may possibly be entangled among registers.

The proposed QGA is summarised in Algorithm 1 and the classical-quantum correspondence of the main terminology is in Table 2.1. As shown, first the registers are initialized in a random state, then the evolutionary process takes place. During each iteration of the loop, known as a generation, the registers are sorted, pseudo-cloned, recombined and mutated. In the following sections, we elaborate a specific subroutine for each of these steps.

Algorithm 1 Quantum genetic algorithm

$n \leftarrow number\_of\_registers$ ▷ assumed divisible by four
$c \leftarrow number\_of\_qubits\_per\_register$ ▷ assumed even
Initialize $|\psi_{\text{pop}}\rangle$ with a random state
repeat
    sort registers
    reset registers $n/2$ to n
    for $r = 1, 2, ..., n/2$ **do**
        pseudo-clone register r to register $n/2 + r$.
    for $i = 0, 1, ..., n/4 - 1$ **do**
        swap the last $c/2$ qubits of register $n/2 + 2 \cdot i + 1$, with the last $c/2$ qubits of register $n/2 + 2 \cdot i + 2$.
    mutate each qubit with probability p_m
until ending criteria is met

Element	GA	QGA
Chromosome (codification of an individual)	state of a c-bit string	state of a c-qubit register
Population	the state of n-bit strings	the state of n quantum registers, $\|\psi_{\text{pop}}\rangle$
Search space	Any combination of c bits, $\{0,1\}^c$	Hilbert space of a c-qubit register, $\mathcal{H}$
Fitness criteria	$f : \{0,1\}^c \to \mathbb{R}$	H_P Hamiltonian acting on $\mathcal{H}$

Table 2.1: Classical GA elements and QGA elements.

2.5 Selection subroutine

The selection subroutine is the only stimulus for the population to improve. Classically, a set of individuals are selected based on their fitness as parents of the next generation. The selection criterion must find a balance between selecting better individuals, so that the population is likely to improve, and ensuring a variety in the population, avoiding getting stuck in local optima.

Fitness-proportional selection is the most common method of performing selection in a classical GA [23]. The first step is to assign a probability to each individual, which is proportional to its relative fitness in the population. Afterwards, individuals are picked from a random sampling, where the same one can be picked more than once. The expected average fitness of the set of selected individuals is clearly better than the average value of the fitness of the initial population. Additionally, worse individuals have also a chance to be selected,

which promotes the exploration of the search space.

The point is that fitness-proportional selection requires evaluating the fitness function for every individual of the population in order to select them. The equivalent process in a quantum computer would require measuring the fitness of each individual, which usually destroys the superposition in the problem basis. In contrast, the sorting subroutine described below is able to preserve superposition for a larger number of cases, avoiding direct measurements of the fitness of the individuals.

The quantum selection subroutine proposed here is inspired by a classical selection procedure, calleds elitist selection. Classically, the individuals of the population are sorted according to their fitness. Afterwards, only the best individuals are selected. The size of the population is reduced in this step, but the original size is recovered after the crossover subroutine. Similarly, the selection subroutine in the QGA can be divided into two steps: sorting the individuals and discarding the individuals in the worst half of the population.

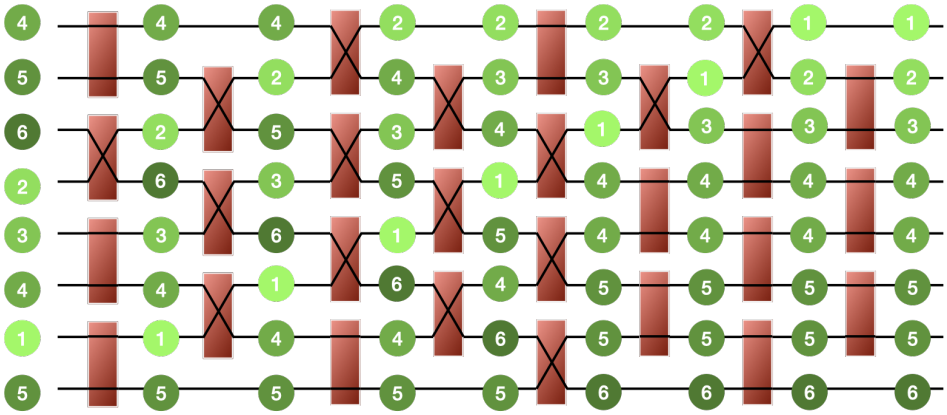


Figure 2.3: Diagram of the Bubble Sort algorithm for 8 elements. Red boxes represent the pairwise comparison which outputs always the lowest number in the upper position.

Sorting networks are protocols that sort the joint state of a n-register system [36]. For the sake of simplicity, we use the Bubble Sort algorithm, conceptually illustrated in Fig. 2.3. Although this sorting network is not asymptotically the best, it performs efficiently for a moderate number of registers, which perfectly suits our purpose. The Bubble Sort algorithm is composed of n layers, where the odd (even) ones sort consecutive register pairs starting from the first (second) performing $n/2$ comparisons ($n/2-1$ comparisons), hence requiring $\frac{n(n-1)}{2}$ comparisons. Each pairwise sort comprises a pairwise comparison and a controlled swap, which is activated if the comparison detects an unsorted pair. Figure 2.4 shows the circuit representation for a four-register sorting network. In the Figure, the controlled gate noted by CMP denotes the pairwise comparison and the controlled gate with two crosses denotes the controlled swap (Section 1.3.3).

In order to implement the sorting network, we need an oracle that can perform the comparison between registers, i.e. the controlled gate noted by CMP in Fig. 2.4.

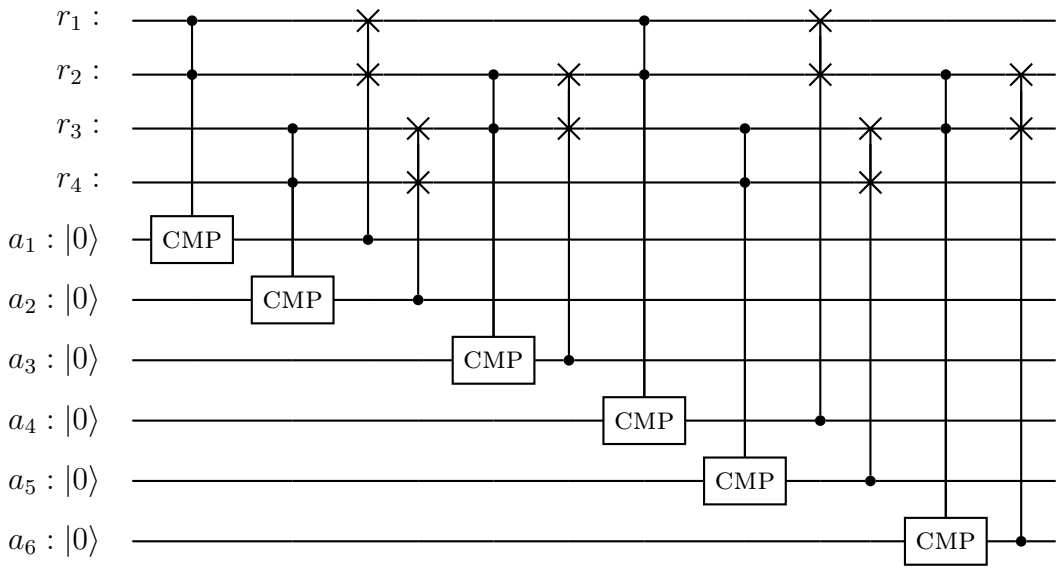


Figure 2.4: Circuit representation for the sorting subroutine with 4 registers, CMP denotes the operation of O_S on the ancillary qubits defined in Eq. 2.5.

We define the *sorting oracle*, O_S, as the unitary transformation

$$O_S \left|u_k\right\rangle \left|u_{k'}\right\rangle \left|0\right\rangle = \begin{cases} \left|u_k\right\rangle \left|u_{k'}\right\rangle \left|0\right\rangle & \text{if } \lambda_{k'} \leq \lambda_k, \\ \left|u_k\right\rangle \left|u_{k'}\right\rangle \left|1\right\rangle & \text{if } \lambda_{k'} > \lambda_k, \end{cases} \tag{2.5}$$

where $\left|u_k\right\rangle$ and $\left|u_{k'}\right\rangle$ are states in the problem basis, and λ_k and $\lambda_{k'}$ represent their eigenvalues. Once we have *marked* the ancillary qubit, we can perform a controlled swap to sort the pair. The control swap gate for two registers is

$$C_{\text{SWAP}} \left|x\right\rangle \left|y\right\rangle \left|c\right\rangle = \begin{cases} \left|x\right\rangle \left|y\right\rangle \left|c\right\rangle & \text{if } c = 0 \\ \left|y\right\rangle \left|x\right\rangle \left|c\right\rangle & \text{if } c = 1, \end{cases} \tag{2.6}$$

where $\left|x\right\rangle \left|y\right\rangle$ represents any separable pure state. Then, the pairwise sorting operator is defined by concatenating O_S and C_{SWAP}.

The state resulting from the sorting procedure is a superposition of sorted populations, possibly entangled with the ancillary qubits,

$$\left|\Psi\right\rangle = \sum_{p=1}^{p_{\max}} b_p \left|\psi_p\right\rangle \left|\sigma_p\right\rangle, \tag{2.7}$$

where $\left|\psi_p\right\rangle$ is the sorted state of the population denoted by p and $\left|\sigma_p\right\rangle$ the permutations performed to sort it. Note that the requirement for reversibility makes it impossible to find a unitary transformation that avoids the entanglement between the population registers and the ancillary qubits. However, ancillary qubits must be discarded in order to proceed with the algorithm, which physically implies measuring without knowing the output and is mathematically represented by computing the reduced density matrix for the population. Therefore, the output state is the reduced density matrix of the population resulting from state $\left|\Psi\right\rangle$,

$$\rho_{\text{sorted}} = \sum_{\sigma} \sum_{p=1}^{p_{\max}} \sum_{p'=1}^{p_{\max}} b_p b_{p'}^* \delta_{\sigma,\sigma_p} \delta_{\sigma,\sigma_{p'}} \left|\psi_p\right\rangle\!\left\langle\psi_{p'}\right|, \tag{2.8}$$

where the summation over σ iterates over all the possible permutations and δ_{σ,σ_p} is the Kronecker delta. The state is a mixture of pure states, which are in turn a quantum superposition of states with the same sorting permutations, $\sigma_p = \sigma_{p'}$.

In order to conclude the selection process, the subroutine must discard the states stored in the lowest registers ($r_{n/2}$ to r_n) and replace them with a reference state, $\rho_0^{\otimes n/2}$. We refer to this process as the *reset* of the lowest registers. The resulting state is the tensor product of the reduced density operator of the individuals that are kept and the reference state for the deleted individuals,

$$\rho_{\text{selected}} = \text{tr}_{\text{low}}(\rho_{\text{sorted}}) \otimes \rho_0^{\otimes n/2}. \tag{2.9}$$

Both, discarding ancillary qubits and resetting the lowest registers, may result in a loss of quantum superposition, which could imply dismissing good individuals. However, this approach provides an alternative method to a hypothetical unitary transformation preserving all the relevant information while discarding the undesired part, which is forbidden by the no-deleting theorem.

2.5.1 Designing the sorting oracle

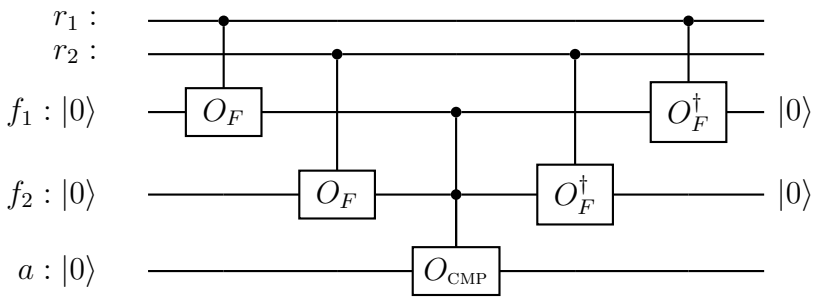


Figure 2.5: Circuit representation for the sorting oracle standard design. r_1 and r_2 are c-qubit registers storing the states of the individuals, f_1 and f_2 are t-qubit registers storing the eigenvalues of those individuals and a is a single qubit used to store the result of the comparison. O_F is the oracle expressed in Eq. 2.11, and O_{CMP} in Eq. 2.10.

Designing the optimal sorting oracle strongly depends on the problem Hamiltonian. Nevertheless, in order to account for the applicability of the algorithm, we provide a general structure that could be followed to develop such an oracle.

Firstly, let us note that arithmetic comparison in the computational basis has been implemented in quantum circuits [37], with computational complexity linear with the size of the input registers. The arithmetic comparison is then described by

$$O_{\text{CMP}} |i\rangle |j\rangle |0\rangle = |i\rangle |j\rangle |\text{CMP}(i,j)\rangle, \quad \text{CMP}(i,j) = \begin{cases} 0 & \text{if } j \leq i, \\ 1 & \text{if } i < j. \end{cases} \tag{2.10}$$

where $|i\rangle$ and $|j\rangle$ are states in the computational basis.

To make use of the O_{CMP} gate, we added a t-qubit fitness register associated to each individual register and we require the gate

$$O_F \left|u_k\right\rangle \left|0\right\rangle = \left|u_k\right\rangle \left|\tilde{\lambda}_k\right\rangle, \tag{2.11}$$

which computes a binary approximation $\tilde{\lambda}_k$ of the eigenvalue λ_k of the eigenstate $|u_k\rangle$, whose precision is limited by t. As a particular example, one could employ a phase estimation algorithm to perform this calculation [10], which is a well known quantum algorithm that can be used to estimate the eigenvalue of the eigenvector of an observable.

Finally, the fitness registers are contrasted employing the arithmetic comparing gate, and the computation performed by O_F can be reversed to avoid an undesired entanglement between the individual and fitness registers.

2.5.2 Simulation of the selection subroutine

The initial density operator ρ for the state of the population is represented by a density matrix with shape $2^{nc} \times 2^{nc}$. In order to operate with the ancillary qubits in the sorting subroutine, the density matrix ρ must be extended to $\rho \otimes |0\rangle\langle 0|$, where $|0\rangle\langle 0|$ is the zero state for a ancillary qubits represented by a $2^a \times 2^a$ matrix with zeros everywhere and a 1 in the $(1,1)$ position. Afterwards, we operate with the unitary matrix that represents the sorting circuit, which is a $2^{nc+a} \times 2^{nc+a}$ matrix Then, we compute the reduced density matrix for the population system recovering a $2^{nc} \times 2^{nc}$ density matrix, ρ_{sorted}.

Let U_{SORT} be the unitary matrix performing the sorting process in the joint system of the population and the ancillary qubits. Then,

$$\rho_{\text{sorted}} = \text{tr}_a[U_{\text{SORT}} \rho \otimes |0\rangle\langle 0| \, U_{\text{SORT}}^\dagger], \tag{2.12}$$

where tr_a represents the partial trace on the ancillary qubits. The unitary matrix U_{SORT} is constructed by concatenating the operation for each layer in the Bubble Sort circuit,

$$U_{\text{SORT}} = U_n U_{n-1} \cdots U_2 U_1, \tag{2.13}$$

where matrices U_i describe the process in each layer and can be divided into two groups. On the one hand, if i is *odd*, then U_i acts comparing consecutive register pairs starting from the first one, and stores the outputs in the ancillary qubits from $\frac{i-1}{2}(n-1)+1$ to $\frac{i-1}{2}(n-1)+\frac{n}{2}$. On the other hand, if i is *even*, then U_i acts comparing consecutive register pairs starting from the second one, and stores the outputs in the ancillary qubits from $\frac{i-2}{2}(n-1)+\frac{n}{2}+1$ to $\frac{i-2}{2}(n-1)+\frac{n}{2}+\frac{n-2}{2}$.

As the information in the ancillary qubits is not used after the sorting oracle and the controlled swap, either performing the partial trace operation right after the comparison and swap, or after completing the sorting network, are equivalent. Therefore, the ancillary qubits involved in the process U_i can be discarded right after the ith layer, because they are not involved in the subsequent layers. Employing this fact lowers the number of ancillary qubits required, from $\frac{n(n-1)}{2}$ to $\frac{n}{2}$, and enables us to simulate the process layer by layer assuming the matrices U_i act on the same ancillary qubits

$$\rho_i = \text{tr}_a[U_i \rho_{i-1} \otimes |0\rangle\langle 0| \, U_i^\dagger], \tag{2.14}$$

$$\text{with} \quad \rho_0 = \rho \quad \text{and} \quad \rho_{\text{sorted}} = \rho_n, \tag{2.15}$$

where ρ_i represents the density matrix after each layer in the sorting network. This method was used for the numerical simulation of the algorithm.

In order to efficiently simulate the comparison oracle, let us assume that we have the problem unitary matrix, U_P, introduced in Eq. 2.2 and that the problem Hamiltonian is non-degenerate (every eigenvalue has multiplicity one). These assumptions are not required to run the algorithm in a real quantum computer, but they reduce the computational cost of the simulation without a relevant loss of generality. Under these assumptions, we show that the pairwise comparison oracle, O_S, can be implemented as a basis transformation of O_{CMP},

$$O_S = [U_p \otimes U_p \otimes \mathbb{I}] O_{\text{CMP}} \left[U_p^\dagger \otimes U_p^\dagger \otimes \mathbb{I}\right]. \tag{2.16}$$

Let us show that Eq. 2.5 holds,

$$\begin{aligned}
O_S |u_k\rangle |u_{k'}\rangle |0\rangle &= [U_p \otimes U_p \otimes \mathbb{I}] O_{\text{CMP}} \left[U_p^\dagger \otimes U_p^\dagger \otimes \mathbb{I}\right] |u_k\rangle |u_{k'}\rangle |0\rangle && (2.17)\\
&= [U_p \otimes U_p \otimes \mathbb{I}] O_{\text{CMP}} |k\rangle |k'\rangle |0\rangle && (2.18)\\
&= [U_p \otimes U_p \otimes \mathbb{I}] \begin{cases} |k\rangle |k'\rangle |0\rangle & \text{if } k' \leq k \\ |k\rangle |k'\rangle |1\rangle & \text{if } k' > k, \end{cases} && (2.19)\\
&= \begin{cases} |u_k\rangle |u_{k'}\rangle |0\rangle & \text{if } \lambda_{k'} \leq \lambda_k \\ |u_k\rangle |u_{k'}\rangle |1\rangle & \text{if } \lambda_{k'} > \lambda_k, \end{cases}, && (2.20)
\end{aligned}$$

where the relation $\lambda_{k'} \leq \lambda_k \iff k' \leq k$ is satisfied due to $\lambda_k \neq \lambda_{k'}$ for $k \neq k'$.

Moreover, let $\tilde{U}_i$ be the unitaries describing the layers of the sorting network for the problem Hamiltonian whose $U_P = \mathbb{I}$, and $\tilde{U}_{\text{SORT}} = \tilde{U}_n \otimes \cdots \tilde{U}_1$. Then, due to the transformation of Eq. 2.16, the U_{SORT} for an arbitrary problem Hamiltonian with $U_P \neq \mathbb{I}$ can also be obtained by means of a basis transformation,

$$\begin{aligned}
U_i &= \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_i \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right], && (2.21)\\
U_{\text{SORT}} &= U_n U_{n-1} \cdots U_2 U_1 && (2.22)\\
&= \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_n \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_{n-1} \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] && (2.23)\\
&\quad \cdots \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_2 \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_1 \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] && (2.24)\\
&= \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_n \tilde{U}_{n-1} \cdots \tilde{U}_2 \tilde{U}_1 \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] && (2.25)\\
&= \left[U_p^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_{\text{SORT}} \left[(U_p^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right], && (2.26)
\end{aligned}$$

which shows that the unitary matrix describing any sorting network for a non-degenerate case is equivalent up to a change of basis. This can be used to accelerate the numerical simulation in a classical computer.

The latter also supports the relevance of the examples shown below, because we focus on cases with $U_P = \mathbb{I}$. Particularly, we consider two examples, one involving only two registers and another involving four registers.

Sorting network example 1. Consider the initial state

$$0.46 |00\ 10\rangle + 0.60 |00\ 11\rangle + 0.58 |01\ 00\rangle + 0.19 |01\ 01\rangle + 0.24 |01\ 11\rangle . \tag{2.27}$$

Notice that there are four components which are already sorted, namely $|00\ 10\rangle$, $|00\ 11\rangle$, $|01\ 01\rangle$, and $|01\ 11\rangle$, and one that is not sorted, $|01\ 00\rangle$. After the sorting network the final state is

$$0.663\,|\psi_0\rangle\langle\psi_0| + 0.337\,|\psi_1\rangle\langle\psi_1|\,, \quad \text{where} \tag{2.28}$$

$$|\psi_0\rangle = 0.56\,|00\ 10\rangle + 0.74\,|00\ 11\rangle + 0.23\,|01\ 01\rangle + 0.29\,|01\ 11\rangle\,, \tag{2.29}$$

$$|\psi_1\rangle = |00\ 01\rangle\,. \tag{2.30}$$

Note that the state undergoes a 'parallel sorting', in the sense that every computational basis state involved in the initial state is independently sorted.

Although the probability of each state does not describe the global state, it is an important characterization of the performance of the algorithm. Particularly, we are interested in obtaining the ground state with high probabilities, here $|00\rangle$. In Fig 2.6, we illustrate the evolution of the probability of every eigenstate in each register, represented by the width of the color bands. Precisely, the probability of $|00\rangle$ in the first register evolves from 0.57 to 0.91, and in the second register from 0.34 to zero; the probability of $|01\rangle$ evolves from 0.43 to 0.09 in the first register and from 0.04 to 0.37 in the second one; the probability of the $|10\rangle$ state remains zero in the first register and 0.21 in the second one; similarly, the probability of $|11\rangle$ remains zero in the first register and 0.42 in the second one.

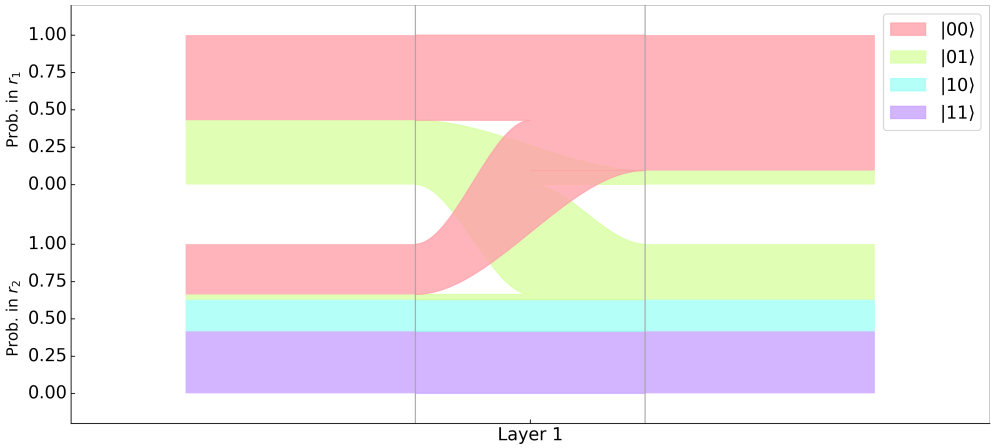


Figure 2.6: Evolution of the probability of the eigenstates of a non-degenerate problem Hamiltonian in the sorting subroutine with two registers. The initial state is given in Eq 2.27 and the final state in Eq. 2.28.

Sorting network, example 2. In Fig. 2.7, we show the evolution of the probabilities with four registers and a randomly generated initial state. The evolution of the probabilities, represented with the color bands, intuitively illustrates the complex underlying process. Indeed, it clearly shows that the probability of the ground state increases for the first register while decreases for the lower registers. Nevertheless, one must remember that this phenomenon is a consequence of the 'parallel sorting', as described in the previous example. For instance, if the sorting network is applied again to an already sorted state, the probability of the ground state in the first register is not further increased.

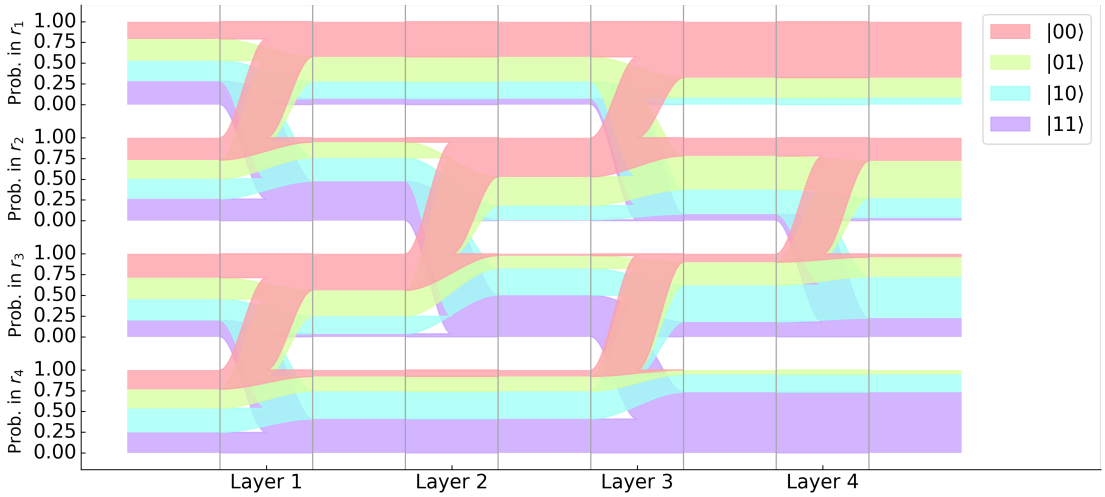


Figure 2.7: Evolution of the probability of the eigenstates of a non-degenerate problem Hamiltonian in the sorting subroutine with 4 registers.

2.6 Crossover subroutine

In this subroutine, the set of selected individuals is employed to produce a population for the next generation. In general, a selected individual can either be introduced without any variation into the next generation, or it can be combined with other individuals to produce a new one. Typically, we are interested in combining most of the individuals, while keeping some of them unchanged.

The genetic-information combining process is a perturbation carried out in the individuals, but its effect differs from the effect of the mutation. Mainly, crossover does not introduce new genetic information into the population, as it can only involve previously selected individuals. The crossover subroutine acts in the whole population and promotes the emergence of *families*. Families are sets of individuals whose genetic codes are similar. They are particularly interesting because the common pattern of surviving individuals is likely to obtain good fitness values while showing resilience against small variations. This feature is fundamental for GAs, as it produces an optimization algorithm that can robustly explore the search space.

When it comes to achieving a quantum counterpart of the crossover subroutine, the main obstacle is the no-cloning theorem (see Section 1.2.3). This fundamental result in quantum information forbids perfect replication of the individuals, which introduces limitations into the crossover process. Moreover, choosing a method to combine the quantum genetic information is not unique. We propose a quantum crossover subroutine comprising two steps: first, a partial cloning technique and then, performing swap gates between the lower registers.

A circuit diagram representing the process is shown in Fig. 2.8. Initially, half of the population (r_3 and r_4) are assumed to be in a reference state which can be overwritten, while the others (r_1 and r_2) store the selected individuals. Firstly, the registers with the selected individuals are partially cloned into the others. This is denoted in the figure by T_{QCM} and the information cloning is qualitatively illustrated by color replication. Partial cloning operations in quantum information are most

commonly known by the term approximated quantum cloning machines (QCM) and, in general, they are not necessarily unitary transformations, but quantum channels. Finally, half of the qubits of the lower registers are swapped.

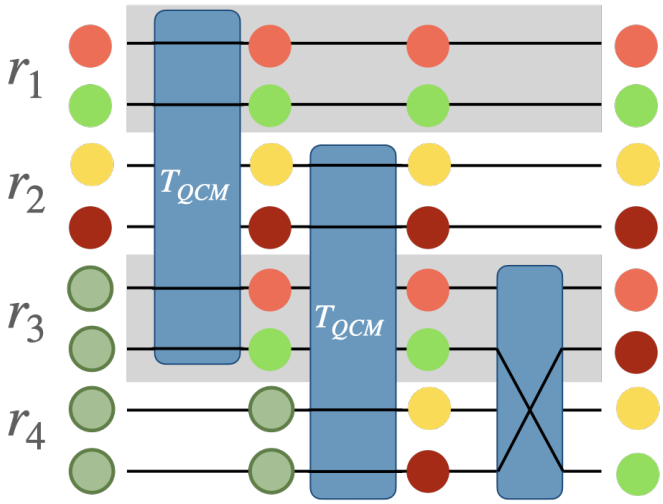


Figure 2.8: Illustrative scheme of the crossover subroutine. The gates named by T_{QCM} represent the quantum cloning operation and the last gate is the swap operation. The color indicate the qualitative content of each qubit, where green represents qubits in a reference state.

For the sake of clarity, let us first develop the crossover subroutine for the case in which T_{QCM} is a unitary transformation, U_{QCM}. The crossover unitary, U_{cross}, can be split into two parts: the cloning unitary, U_{clone}, and the swap unitary, U_{swap},

$$U_{\text{cross}} = U_{\text{swap}} U_{\text{clone}}. \tag{2.31}$$

In order to construct the operator U_{clone} for n registers, one uses as building block the operator U_{QCM} which acts on a two-register state space. More precisely, there is an input register storing the state to be copied, $|\psi\rangle$, and an overwrittable register in a reference state, $|0\rangle$. Then, the operator U_{QCM} transforms the joint state so that there is an approximate copy of the state $|\psi\rangle$ in both registers, i.e.

$$U_{\text{QCM}} |\psi\rangle |0\rangle = |\psi', \psi''\rangle , \tag{2.32}$$

where the output state, $|\psi', \psi''\rangle$, is not necessarily separable and the state in the first register may also differ from the initial one $|\psi\rangle$.

In the case of two registers, the cloning unitary is simply $U_{\text{clone}} = U_{\text{QCM}}$. However, if there are 4 registers, e.g. in state $|\psi_1\rangle |\psi_2\rangle |0\rangle |0\rangle$, one cannot simply define $U_{\text{clone}} = U_{\text{QCM}} \otimes U_{\text{QCM}}$, since this leads to

$$[U_{\text{QCM}} \otimes U_{\text{QCM}}] |\psi_1\rangle |\psi_2\rangle |0\rangle |0\rangle = U_{\text{QCM}} |\psi_1\rangle |\psi_2\rangle \otimes U_{\text{QCM}} |0\rangle |0\rangle , \tag{2.33}$$

since each U_{QCM} acts into two *consecutive* registers. In order to apply U_{QCM} for two qubits which are not consecutive, one must swap their positions. In Eq. 1.82, we introduced the swap unitary acting on qubits i and j, denoted by $S_{i,j}$. Here, we

use the notation S_{r_i,r_j} to describe the combined action of swapping each qubit of register r_i with the corresponding qubit in register r_j. Consequently,

$$U_{\text{clone}} = S_{r_2,r_3}[U_{\text{QCM}} \otimes U_{\text{QCM}}]S_{r_2,r_3}. \tag{2.34}$$

This process can straightforwardly be extended to n registers by reordering the registers, applying $(U_{\text{QCM}})^{\otimes n/2}$ and, finally, by reordering the registers back. The reordering is achieved by systematically swapping register $2k$ with register $2k + \frac{n}{2} - 1$ for $1 < k \leq \frac{n}{4}$, which is compactly expressed as

$$U_{\text{clone}} = S_R(U_{\text{QCM}})^{\otimes n/2}S_R, \tag{2.35}$$

where we define the reordering operator as

$$S_R = \prod_{k=1}^{n/4} S_{r_{2k},r_{2k+\frac{n}{2}-1}}. \tag{2.36}$$

Finally, the genetic-information combination operation is defined employing qubit swaps. One swaps qubits $c/2$ to c in register $\frac{n}{2} + 2i - 1$, with qubits $c/2$ to c in register $\frac{n}{2} + 2i$ from $i = 1$ to $i = \frac{n}{4}$, which results in

$$U_{\text{swap}} = \prod_{i=1}^{n/4}\prod_{j=\frac{c}{2}}^{c} S_{r_{\frac{n}{2}+2i-1}q_j,r_{\frac{n}{2}+2i}q_j}, \tag{2.37}$$

where $r_i + q_j$ denotes the index of the jth qubit in the ith register.

Therefore, the density matrix after the crossover subroutine is

$$\rho_{\text{cross}} = U_{\text{cross}}\rho U^{\dagger}_{\text{cross}}. \tag{2.38}$$

In a similar manner, when the QCM is represented by a quantum channel, T_{QCM}, the resulting density matrix is

$$\rho_{\text{cross}} = U_{\text{swap}}S_R T^{\otimes n/2}_{\text{QCM}}(S_R\rho S_R)S_R U_{\text{swap}}. \tag{2.39}$$

2.6.1 Quantum cloning machines

Let us consider a joint system $A - B$, such that, A initially is in an unknown state and B in a reference state. Then, a QCM is a quantum operation between A and B, which 'spreads' the quantum information of the state in A into the joint system AB. We only consider $1 \to 2$ QCMs, which take a single copy of a state and produce two approximated copies (the original one in A and the new one in B) [13].

This definition for a QCM is quite loose, because almost any interaction between A and B 'spreads' the quantum information of the state in A. However, we are interested in those interactions achieving high fidelities of the initial state in A for the final states in A and B. More precisely, let ρ_A and ρ_B be the reduced density operators of each system of the final state, and let $|\psi\rangle$ be the initial state of A, then the *single-copy fidelity* is

$$F_j(|\psi\rangle) = \langle\psi|\rho_j|\psi\rangle\,, \quad j = A, B. \tag{2.40}$$

Therefore, we are interested in those interactions that maximize these fidelities. Recall that $0 \leq F_j \leq 1$ and that the no-cloning theorem prevents us from finding a QCM achieving $F_A = F_B = 1$ for all $|\psi\rangle$.

There is a standard classification of QCMs in terms of their single-copy fidelities [13]:

- If F_A and F_B are independent of $|\psi\rangle$, the QCM is called universal (UQCM). Whereas if F_A or F_B vary with the input state, it is called non-universal or state-dependent.
- If all the final copies have the same fidelity, $F_A = F_B$, for all $|\psi\rangle$ the QCM is called symmetric.
- If the fidelity of the final copies are the maximal ones allowed by quantum mechanics, the QCM is called optimal. This classification can either be accounted for by the average fidelity, over all the possible input state, or the minimum fidelity obtained for any input state. The average fidelity and minimum fidelity often coincide for an optimal QCM.

When it comes to choosing a QCM for the crossover subroutine, one must carefully consider its properties and potential impact on the evolutionary process. Indeed, the variety of available QCMs is a potential path for the improvement of the algorithm in further studies. In Chapter 3, we take a step in this direction analysing two QCMs and comparing their impact on the overall performance of the QGA. The theoretical description of these two QCMs, known as the biomimetic cloning of quantum observables (BCQO) [16] and the optimal symmetric UQCM (UQCM in short) [14, 13], is summarized below. The choice of these two cloning methods was encouraged by their remarkable properties. Roughly speaking, BCQO provides a state-dependent result, which can even create perfect copies of certain states, whereas the UQCM provides a state-independent optimal result, although no state is perfectly cloned.

Biomimetic cloning of quantum observables (BCQO). This cloning method was introduced in Ref. [16]. Its main property is that it is able to perfectly replicate the statistics related with a complete set of commuting operators. More formally, for a given a reference state ρ_r and a quantum observable M, the cloning operator $U(\theta, \rho_r)$ is the operator satisfying

$$\mathrm{tr}[M\rho] = \mathrm{tr}\big[(M \otimes \mathbb{I})U\rho \otimes \rho_r U^\dagger)\big] = \mathrm{tr}\big[(\mathbb{I} \otimes M)U\rho \otimes \rho_r U^\dagger\big], \tag{2.41}$$

for any state ρ. That is, the expected value of M in the state ρ of the initial individual is the same as the expected value that is eventually obtained in any of the final individuals. If U satisfies Eq. 2.41 for the operator M, then it also holds for the complete set of observables commuting with M. This is a consequence of the well-known fact that a complete set of commuting operators can be simultaneously diagonalized in the same basis.

The unitary operator can be straightforwardly described in the basis diagonalizing the complete set of commuting operators, $\{|j\rangle\}_{j=1}^n$, and assuming

the reference state is $\rho_r = |1\rangle\langle 1|$,

$$x_{ni}\,|k\rangle = \begin{cases} |k+i-1\rangle & \text{if } k \leq n-i+1, \\ |k+i-1-n\rangle & \text{if } k > n-i+1, \end{cases} \qquad s_{ni} = |i\rangle\langle i|\,, \tag{2.42}$$

$$U_n = \sum_{i=1}^{n} s_{ni} \otimes x_{ni}, \tag{2.43}$$

where x_{ni} is a n-dimensional irreducible representation of the translation group, s_{ni} represents the projection into each subspace and U_n is the cloning unitary for BCQO. The operator U_n is the cloning operator, acting on the joint state space of two individuals, therefore, it acts on a n^2-dimensional space. It is described by its separate action on n subspaces of n dimensions, iterated over the index i, which is described by x_{ni}. This formula makes it straightforward to build the matrix for computational simulations.

The single copy fidelity, which is symmetric, for a pure state, $|\psi\rangle$, is

$$F(|\psi\rangle) = \sum_{j=1}^{n} |a_j|^4, \quad \text{for the state } |\psi\rangle = \sum_{j=1}^{n} a_j\,|j\rangle\,, \tag{2.44}$$

is clearly state-dependent. Indeed, the quality of the copy of a state strongly depends on its representation in therms of the basis $\{|j\rangle\}_{j=1}^{n}$. Particularly, the maximum value, $F = 1$, is obtained when only one component is one (the state is an eigenvector of M). Whereas the minimum value, $F = \frac{1}{n}$, is obtained for a uniform superposition, $|a_j| = \frac{1}{\sqrt{n}}$. As a matter of choice, we define the cloning unitary in the computational basis. Consequently, the information of the statistics of the computational basis is perfectly replicated and preserved. Whereas, other quantum information is spread onto the population and it is susceptible of disappearing after the selection process.

Optimal Symmetric UQCM (UQCM). This cloning machine was first proposed for the cloning of a single qubit [14], proving that it is possible to build a symmetric universal QCM achieving a single copy fidelity equal to 5/6. This method was proven to be optimal and it inspired a similar QCM for the multi-qubit case [13]. We only consider the case where the aim is to duplicate a single state, and we describe the UQCM in terms of density operators although the optimality is properly proven only for pure states [13].

Let $\mathcal{H}$ be the d-dimensional Hilbert space for each individual. Hence $\mathcal{H}^{\otimes 2}$ is the Hilbert space of the two individuals. The cloning subroutine is described as a quantum operation $T_{\text{UQCM}} : \mathcal{H} \to \mathcal{H}^{\otimes 2}$. Additionally, note that the image space can be restricted, because the output states should be symmetric with respect to the permutation of the individuals. In other words, the output states, ρ, must satisfy $\rho = S_{1,2}\rho S_{1,2}^{\dagger}$, with $S_{1,2}$ the swap operation between the first individual and the second. Let $\mathcal{H}_+^2$ be the subspace of $\mathcal{H}^{\otimes 2}$ formed by the symmetric states, and let S_+ be the projection operation onto $\mathcal{H}_+^2$,

$$S_+ \equiv \frac{1}{2}\big(\mathbb{I}^{\otimes 2} + S_{1,2}\big), \tag{2.45}$$

where $\mathbb{I}$ is the identity operation on $\mathcal{H}$.

Once these concepts have been introduced, the UQCM can be performed in two simple steps. Assuming that ρ is the state to copy, let us first take the trivial extension to $\mathcal{H}^{\otimes 2}$ by $\rho \to \rho \otimes \mathbb{I}$. Then, project the resulting state into the symmetric subspace $\mathcal{H}_+^2$, and normalize the result, i.e.

$$T_{\text{UQCM}}(\rho) = \frac{2}{d+1} S_+(\rho \otimes \mathbb{I}) S_+. \tag{2.46}$$

This operation can be extended to act on the joint state of two individuals, assuming an input state of the form $\rho \otimes \rho_0$, discarding and overwriting the reference state. In Section 3.1.1, we describe the process in the framework of quantum channels, providing the operator sum representation of T_{UQCM}.

The reduced density operator of has the form

$$\rho_1 = \rho_2 = \eta\rho + (1-\eta)\frac{\mathbb{I}}{d}, \quad \text{with} \quad \eta = \frac{1}{2}\frac{2+d}{1+d}. \tag{2.47}$$

Therefore, the single copy fidelity of the UQCM is

$$F = \frac{1}{2} + \frac{1}{1+d}, \tag{2.48}$$

which is clearly independent of the input state ρ.

2.6.2 Simulation of QCMs

The aim of this section is to provide a deeper comprehension of the crossover subroutine and its characteristics when employing each of the QCMs for the cloning. First, we analyze both QCMs for duplicating a single qubit. Afterwards, we propose some examples for a larger system. We provide in parallel the results for both cloning machines, employing subindex B for BCQO and U for the UQCM.

Assuming reference state $|0\rangle\langle 0|$ and that M is diagonalized in the computational basis, the unitary matrix implementing BCQO to clone a single qubit is

$$U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2.49}$$

which is equivalent to the CNOT gate, which can also be represented in braket notation as $U_2 = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$. Whereas, for UQCM we compute the S_+ matrix for a two-qubit system,

$$S_+ = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}. \tag{2.50}$$

Let $|\psi\rangle = a|0\rangle + b|1\rangle$ be the state to be cloned, then the initial joint state is $|\psi\rangle|0\rangle = a|00\rangle + b|10\rangle$ or represented by a density matrix

$$|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} |a|^2 & 0 & ab^* & 0 \\ 0 & 0 & 0 & 0 \\ a^*b & 0 & |b|^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.51}$$

Applying BCQO we obtain $U_2|\psi\rangle|0\rangle = a|00\rangle + b|11\rangle$ or in matrix form

$$\rho_B = \begin{pmatrix} |a|^2 & 0 & 0 & ab^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a^*b & 0 & 0 & |b|^2 \end{pmatrix}. \tag{2.52}$$

Therefore, the reduced density matrix for each individual and single copy fidelity are

$$\rho_{B1} = \rho_{B2} = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}, \quad F_B = |a|^4 + |b|^4. \tag{2.53}$$

These results for the UQCM are

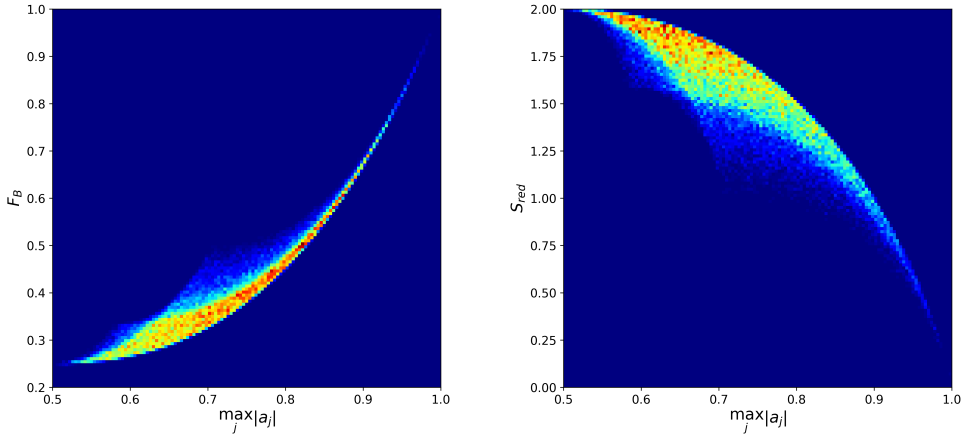
$$\rho_U = \frac{2}{3}\begin{pmatrix} |a|^2 & \frac{ab^*}{2} & \frac{ab^*}{2} & 0 \\ \frac{a^*b}{2} & \frac{1}{4} & \frac{1}{4} & \frac{ab^*}{2} \\ \frac{a^*b}{2} & \frac{1}{4} & \frac{1}{4} & \frac{ab^*}{2} \\ 0 & \frac{a^*b}{2} & \frac{a^*b}{2} & |b|^2 \end{pmatrix}, \tag{2.54}$$

$$\rho_{U1} = \rho_{U2} = \frac{2}{3}\begin{pmatrix} \frac{1}{4} + |a|^2 & ab^* \\ a^*b & \frac{1}{4} + |b|^2 \end{pmatrix}, \quad F_U = \frac{5}{6}. \tag{2.55}$$

Since $|a|^2 + |b|^2 = 1$, the fidelity for BCQO is in the interval $\frac{1}{2} \leq F_B \leq 1$, where 1 is only obtained for either $a = 1$ or $b = 0$, which correspond to $|0\rangle$ and $|1\rangle$. Moreover, these two cases are the only exceptions where the joint state after copying is still separable, any other initial state results in an entangled output state. The entanglement between both qubits has the consequence that information is lost when considering the reduced states of the qubits instead of the joint state. Nevertheless, it is entanglement what provides a means of flawlessly transferring the statistics in the computational basis, the diagonal terms of $|\psi\rangle\langle\psi|$. With regard to UQCM, it is clear that it always obtains $F_U = \frac{5}{6}$ and the output state is invariably a mixed state.

Concerning entanglement, one can quantify the correlation between the states of the registers with the techniques described in Section 1.2.4. Regarding the state resulting from BCQO, we obtain $S_{\text{red}} = |a|^2 \log |a|^2 + |b|^2 \log |b|^2$, which lies in the range 0 to 1. For the state resulting from UQCM, the entropy of the reduced state can be shown to be $S_{\text{red}} = \log \frac{6}{5^{5/6}} \approx 0.65$ and the entropy of the two-qubit state is $S = \log\left(\frac{4}{3}\right)^{1/3} \approx 0.14$. Hence, the correlation measure is $(2S_{\text{red}} - S)/2 = 0.58$, which indicates a highly correlated state.

Regarding the cloning of a two-qubit register, according to Eq. 2.48, the single copy fidelity for UQCM in this case is $\frac{7}{10} = 0.7$. The entropy of the join state is



(a) (b)

Figure 2.9: Two dimensional histograms describing a) the single copy fidelity and b) the reduced entropy obtained for BCQO for the duplication of two qubits, both in terms of the maximum absolute amplitude of the cloned state in the computational basis, i.e. the basis diagonalizing the set of commuting operators.

approximately 1.92, and the entropy for each of the individuals is 1.36. Hence, the correlation measure is 0.40, which is moderately correlated, considering that the entropy of a two-qubit system is at most 2.

Regarding BCQO, the fidelity is $F = \sum_j |a_k|^4$, and the reduced entropy is $-\sum_j |a_j| \log |a_j|$, which are state dependent and range from 0.25 to 1 and from 0 to 2 respectively. In order to obtain a visual representation of the performance, we generated 5×10^4 random pure states with real amplitudes, according to a Haar distribution employing the scipy Python library, whose algorithm is described in Ref. [38], and computed their single copy fidelities and their reduced entropy after duplication. It was assigned a *similarity* with the computational basis to every state, which is the magnitude of the largest absolute amplitude of the state in the computational basis, $\max_j |a_j|$. The greater this value, the closer the state to any of the states of the computational basis. Therefore, to every randomly generated state can be assigned two coordinates in a two dimensional plane. Figure 2.9a shows the two dimensional histogram of points for the single copy fidelity and Fig. 2.9b for the reduced entropy. One can clearly observe that the closer a state is from the computational basis, the better its fidelity is and the lower its reduced entropy. Therefore, this figures reinforce the idea that BCQO performs excellently for states close to the basis diagonalizing the set of commuting observables, and worse for those which are homogeneous linear combinations.

2.7 Mutation

This subroutine is essential to introduce new genetic information into the classical evolutionary process. The aim of this genetic operator is to slightly perturb some of the individuals, in order to facilitate the exploration of new areas in the search

space. Note that although the perturbation in the individual could be considered small, e.g. flipping a single bit, it can substantially vary its fitness. Anyway, the impact of the mutation operator should be sufficient to foster exploration, while not excessive to avoid jeopardizing the convergence.

Classically, the most usual method to carry out the mutation operator is to flip each bit according to a small probability p_m. Therefore, any bit has a chance to mutate although most of them probably remain unchanged. Consequently, the variation introduced by a mutation tends to survive and replicate only if its impact in the fitness is positive [23].

The analogous technique for the QGA is to apply a X gate on each qubit with probability p_m. However, this perturbation is dramatically limited, consider for example that it cannot introduce variations in the phase of a state. With the purpose of introducing other perturbations, we performed mutations employing randomly the X, Y or Z gate, in those qubits that were chosen to mutate.

In this work, we have specially focused on analyzing the performance of the sorting and the crossover subroutines, leaving behind important issues concerning mutation. For example, one could argue the quantum nature of the algorithm already introduces perturbations in the population, which may imply the irrelevance of mutation [5]. However, one should thoroughly inspect if those perturbations are enough to replicate general genetic dynamics. Moreover, classical mutation enables to access any region of the search space no matter the initial population, but this is not achieved combining X, Y and Z gates. Therefore, once the initial population is established, there are unreachable regions in the search space. Consequently, it is reasonable to consider if a universal set of quantum gates should be chosen and, more specifically, whether a two-qubit gate, such as the CNOT, should be introduced to enable mutations in the entanglement degree. These relevant questions require further research and therefore, they are left for future works.

Chapter 3

Analytic and numerical results

In this Chapter, we discuss the results of the numerical simulations of the QGA and frame them by employing quantum channel theory, including fixed points analysis. We have not focused on proving an explicit advantage against other approaches (either classical or quantum). Instead, our aim is to verify the performance of our QGA, validating its rapid exponential convergence and the accuracy of the outcome. This is based on the employment of quantum channel tools, especially related to their fixed points, which resulted to be a powerful analytical instrument for the analysis of these heuristic algorithms to prove the properties inferred after numerous simulations. Moreover, we also introduce the first steps comparing different variations of the cloning subroutine and the performance for different problem Hamiltonians.

Firstly, in the quantum channel analysis (Section 3.1), we provide the operator sum representation of every subroutine, discuss on their properties, and obtain their fixed points. Then, we describe the results obtained through numerical simulations of the QGA (Section 3.2). Afterwards, we compare the performance making use of two different cloning methods, specifically, the biomimetic cloning of quantum observables (BCQO) and the universal quantum cloning machine (UQCM). Finally, we provide a general discussion of the results (Section 3.3).

3.1 Quantum channel analysis of the QGA

As quantum algorithms often require no intermediate measurements or random unitary transformations, they can be implemented in isolated quantum systems and, thus, be described by unitary transformations. However, our QGA intrinsically does not fulfil these conditions and, thus, requires to be described in terms of quantum channels. Indeed, QGA always contains projective measurements to perform the selection according to the no-deleting theorem and probabilistic application of unitaries to perform random mutation. Moreover, the cloning operation is a quantum channel if is performed with the UQCM. Therefore, if one wants to describe the quantum genetic algorithm analytically, one needs describe the process employing quantum channels.

As described in Section 1.2.6, quantum channels are linear physical transformations mapping a quantum state into another. These transformations are described by completely positive trace-preserving linear maps, known as quantum

operations, acting in the set of density matrices associated to the system. Let $\mathcal{T}_G$ be the quantum operation describing the process of a single generation step of the quantum genetic algorithm. Then, a QGA iterated over N generations is described by the composition of N generation-step operations, $(\mathcal{T}_G)^N$. The number of generations is usually large, $N \gg 1$, therefore, one can consider the asymptotic limit of the QGA as a reliable description of its behaviour.

One of the important features of the asymptotic limit is the existence of fixed points towards the dynamics converge. Assuming the hypotheses elaborated in Section 1.2.6, then given any initial state ρ, the final state, obtained by the limit $\Lambda = \lim_{N\to\infty}(\mathcal{T}_G)^N(\rho)$, is a fixed point of the quantum operation of the QGA. In particular, if the fixed point Λ is unique, i.e. is the only state with eigenvalue 1 of $\mathcal{T}_G(\Lambda) = \Lambda$, then any initial state ρ converges towards it. Additionally, the convergence towards this stationary state is provable exponential, according to the spectral subradius of the quantum channel [22]. The spectral subradius of a linear operator is its second larger eigenvalue in absolute value. This phenomenon leads to the analysis of the QGA in terms of quantum operations. In this section, we take the first steps towards this analysis obtaining the operator sum representation for the whole QGA, both employing BCQO and UQCM, and computing the fixed points for some restricted cases.

The single generation operation, $\mathcal{T}_G$, results from the composition of the operations of each subroutine. For instance, label the selection operation $\mathcal{T}_S$, the crossover operation $\mathcal{T}_C$ and the mutation operation $\mathcal{T}_M$, then $\mathcal{T}_G = \mathcal{T}_M \circ \mathcal{T}_C \circ \mathcal{T}_S$. Then the final state, after applying N generations of the algorithm, is

$$\rho_{\text{final\_1}} = (\mathcal{T}_G)^N(\rho_{\text{init}}). \tag{3.1}$$

If N is sufficiently large, the final state is exponentially close to a fixed point of $\mathcal{T}_G$. Moreover, if there is a unique fixed point, $\rho_{\text{final\_1}}$ is independent of the initial state. Additionally, the final states are potentially better if the algorithm is terminated right after a sorting operation,

$$\rho_{\text{final\_2}} = \big(\mathcal{T}_{\text{Sort}} \circ (\mathcal{T}_G)^N\big)(\rho_{\text{init}}), \tag{3.2}$$

but then $\rho_{\text{final\_2}}$ need not be a fixed point of $\mathcal{T}_G$. In order to analyse the asymptotic limit for $\rho_{\text{final\_2}}$, we split the selection operation into sorting and reset operations, $\mathcal{T}_S = \mathcal{T}_{\text{Reset}} \circ \mathcal{T}_{\text{Sort}}$. As a consequence,

$$\begin{aligned}
\rho_{\text{final_2}} &= \big(\mathcal{T}_{\text{Sort}} \circ (\mathcal{T}_M \circ \mathcal{T}_C \circ \mathcal{T}_{\text{Reset}} \circ \mathcal{T}_{\text{Sort}})^N\big)(\rho_{\text{init}}) && (3.3)\\
&= \big((\mathcal{T}_{\text{Sort}} \circ \mathcal{T}_M \circ \mathcal{T}_C \circ \mathcal{T}_{\text{Reset}})^N \circ \mathcal{T}_{\text{Sort}}\big)(\rho_{\text{init}}) && (3.4)\\
&= (\mathcal{T}'_G)^N(\mathcal{T}_{\text{Sort}}(\rho_{\text{init}})), && (3.5)
\end{aligned}$$

which clearly shows that $\rho_{\text{final\_2}}$ is nearly a fixed point of $\mathcal{T}'_G = \mathcal{T}_{\text{Sort}} \circ \mathcal{T}_M \circ \mathcal{T}_C \circ \mathcal{T}_{\text{Reset}}$ and that $\mathcal{T}_{\text{Sort}}(\rho_{\text{init}})$ behaves as the initial state. Therefore, we will focus on the analysis of the asymptotic limit for $\mathcal{T}'_G$, and redefine $\mathcal{T}_G = \mathcal{T}_{\text{Sort}} \circ \mathcal{T}_M \circ \mathcal{T}_C \circ \mathcal{T}_{\text{Reset}}$ instead.

In the following, we find the operator sum representation for each subroutine and the fixed points for the single generation step operation, employing the techniques described in Section 1.2.6.

3.1.1 Obtaining the operator sum representation

The aim of this section is to obtain the Kraus operators required for the operator sum representation of each subroutine. The general procedure is described in Section 1.2.6. In order to be more explicit, the selection and crossover subroutines have been divided into two sub-procedures.

Selection subroutine - sorting. As introduced in Section 2.5.2, the sorting subroutine can be simulated performing a unitary transformation in the joint system comprising population and ancillary qubits and, then, taking the reduced density matrix for the population state. Rewriting Eq. 2.12 ass

$$\mathcal{T}_{\text{Sort}}(\rho) = \text{tr}_a[U_{\text{SORT}}\rho \otimes |0\rangle\langle 0|\, U_{\text{SORT}}^\dagger], \tag{3.6}$$

$$\mathcal{T}_{\text{Sort}}(\rho) = \sum_{\sigma=0}^{2^a} \mathbb{I}^{\otimes nc} \otimes \langle\sigma|\left[U_{\text{SORT}}\rho \otimes |0\rangle\langle 0|\, U_{\text{SORT}}^\dagger\right]\mathbb{I}^{\otimes nc} \otimes |\sigma\rangle\,, \tag{3.7}$$

where σ represents each possible output state of the ancillary qubits, a is the number of ancillary qubits ($\frac{n}{2}(n-1)$ for Bubble Sort) and $\mathbb{I}$ is the identity operator on the space of each qubit. Then the Kraus operators for the sorting subroutine are $A_\sigma = (\mathbb{I}^{\otimes nc} \otimes \langle\sigma|)U_{\text{SORT}}(\mathbb{I}^{\otimes nc} \otimes |0\rangle)$, which satisfy $\mathcal{T}_{\text{Sort}}(\rho) = \sum_{\sigma=0}^{2^a} A_\sigma \rho A_\sigma^\dagger$. One should note that not all permutations σ are possible as an outcome of the sorting operation. For instance, if there was no permutation in the first and second sorting steps, which indicates an already sorted population, all the remaining sorting steps should take no action. Therefore, any permutation σ indicating no swap in the initial sorting steps must also indicate no swaps in the final ones. This reduces the number of non-zero Kraus operators.

Selection subroutine - reset. Denoting by tr_{low} the partial trace over the registers in the lower half of the population, the action of this procedure on an initial state ρ is

$$\mathcal{T}_{\text{Reset}}(\rho) = \text{tr}_{\text{low}}[\rho] \otimes |e_0\rangle\langle e_0|\,, \tag{3.8}$$

$$\mathcal{T}_{\text{Reset}}(\rho) = \sum_{r=0}^{2^{\frac{nc}{2}}} \left(\mathbb{I}^{\otimes \frac{nc}{2}} \otimes |e_0\rangle\langle r|\right)\rho\left(\mathbb{I}^{\otimes \frac{nc}{2}} \otimes |r\rangle\langle e_0|\right), \tag{3.9}$$

where $|e_0\rangle$ is the reference state for the lower registers. Then, $B_r = \mathbb{I}^{\otimes \frac{nc}{2}} \otimes |e_0\rangle\langle r|$ are the Kraus operators for $\mathcal{T}_{\text{Reset}}$.

Crossover subroutine - cloning. The operator sum representation of the cloning subroutine depends on the QCM employed to perform the pseudo-cloning of the individuals. For BCQO, one simply takes the appropriate unitary for the replication of the population, as described in Section 2.6.1. Therefore, there is a single Kraus operator in that case. In contrast, for UQCM one must obtain a set of Kraus operators to describe it. Recall that the UQCM's action on a system composed of two c-qubit registers is

$$\frac{2}{2^c+1} S_+\left(\text{tr}_2(\rho) \otimes \mathbb{I}^{\otimes c}\right) S_+, \tag{3.10}$$

where S_+ is the projection onto the space of states which are symmetric respect to register swap and tr_2 is the trace over the second register. As elaborated on Section 2.6, this operator can be extended to the whole population, n registers, employing tensor products and the reordering unitary, S_R,

$$\mathcal{T}_{\mathrm{Clone}}(\rho) = \left(\frac{2}{2^c+1}\right)^n S_R S_+^{\otimes n/2} S_R \left[\mathrm{tr}_{\mathrm{low}}(\rho) \otimes \mathbb{I}^{\otimes nc}\right] S_R S_+^{\otimes n/2} S_R. \tag{3.11}$$

This is equivalent to $\mathcal{T}_{\mathrm{Clone}}(\rho) = \sum_{j,k=1}^{2^{nc/2}} C_{j,k}\rho C_{j,k}^\dagger$, with the Kraus operators $C_{j,k} = S_R S_+^{n/2} S_R\big(\mathbb{I}^{\otimes nc/2} \otimes |j\rangle\langle k|\big)$, where both indices, j and k, run from 1 to $2^{nc/2}$. When composing the quantum channels of the subroutines, the action of the UQCM "overwrites" the action of the reset, so the reset can be omitted.

Crossover subroutine - swap. The swap operation is a unitary transformation combining qubit swap gates, as explained in Section 2.6. Therefore, there is a single Kraus operator, U_{Swap}.

Mutation subroutine. In the mutation subroutine one applies single-qubit unitaries with different probabilities. In general, consider applying on the state of the population mutation unitary U_μ with probability p_μ, for M different mutation possibilities. Then, the quantum operation for mutation can be described employing the ensemble of mutation unitaries with their associated probability, $\{(p_\mu, U_\mu)\}_{\mu=1}^M$, by

$$\mathcal{T}_M(\rho) = (1-p_m)\rho + \sum_{\mu=1}^{M} p_\mu U_\mu \rho U_\mu^\dagger, \tag{3.12}$$

defining p_m as the probability that at least one mutation occurs in the population, $p_m \equiv \sum_{\mu=1}^M p_\mu$. The Kraus operators can be identified as $C_\mu = \sqrt{p_\mu}U_\mu$ for $\mu = 1$ to M, and $C_0 = \sqrt{1-p_m}\mathbb{I}^{\otimes nc}$ for $\mu = 0$. For instance, consider the ensemble described in Section 2.7, where we propose to apply single qubit Pauli gates, X,Y and Z, with equal probability $p/3$ in every qubit. Therefore, the probability that at least one mutation occurs is $p_m = 1-(1-p)^{nc}$. The set of all possible mutation unitaries and the identity is $\{\mathbb{I}, X, Y, Z\}^{\otimes nc}$, which contains all possible Kronecker products of order nc that can be obtained combining the single qubit gates. The probability of each mutation unitary is $\left(\frac{p}{3}\right)^k (1-p)^{nc-k}$, where k is the number of non-identity single qubit unitaries involved. For example, with $nc = 4$ the probability of the mutation unitary $\mathbb{I}\otimes X\otimes \mathbb{I}\otimes Z$ is $\left(\frac{p}{3}\right)^2(1-p)^2$.

3.1.2 Remarks about the operator sum representation

Before obtaining the fixed points for $\mathcal{T}_G$ in the following section, let us advance some relevant results that can be concluded from its operator sum representation.

Regarding the stationary states of the sorting subroutine, one can verify that any linear combination of sorted populations is a fixed point of the sorting subroutine. In particular, this implies that any output state of the sorting subroutine is a fixed point, because it is a sorted state by definition. Therefore, the sorting subroutine is a projector onto the space of sorted states. To verify this,

consider the following pure state expressed as a superposition of two populations $|\psi\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle$, which is a particular case of Eq. 2.3. Applying the sorting unitary results in the following joint state for the population and ancillary system:

$$\alpha\,|\sigma_1(\psi_1)\rangle\,|\sigma_1\rangle + \beta\,|\sigma_2(\psi_2)\rangle\,|\sigma_2\rangle\,, \tag{3.13}$$

where σ_i denotes the permutation performed to sort $|\psi_i\rangle$, and $|\sigma_i(\psi_i)\rangle$ the state after this permutation. This state leads to two possible outcomes after taking the partial trace on the ancillary qubits,

$$\rho' = |\alpha|^2\,|\sigma_1(\psi_1)\rangle\langle\sigma_1(\psi_1)| + |\beta|^2\,|\sigma_2(\psi_2)\rangle\langle\sigma_2(\psi_2)|\,, \tag{3.14}$$

$$\rho'' = (\alpha\,|\sigma(\psi_1)\rangle + \beta\,|\sigma(\psi_2)\rangle)(\alpha^*\,\langle\sigma(\psi_1)| + \beta^*\,\langle\sigma(\psi_2)|). \tag{3.15}$$

The first outcome, which is a mixed state, is obtained if the initial populations undergo different permutations. The second outcome, in turn, is a pure state and it is obtained if $\sigma_1 = \sigma_2 = \sigma$. Moreover, if both initial states are already sorted, $|\psi_i\rangle = |\sigma_i(\psi_i)\rangle$ and $|\sigma\rangle = |0\rangle$, the state remains unchanged. In any case, the final state, either ρ' or ρ'', is a linear combination of sorted populations and it is unchanged if the sorting subroutine is applied to it. Therefore, $\mathcal{T}^2_{\text{Sort}}(\rho) = \mathcal{T}_{\text{Sort}}(\rho)$ for any state ρ, which shows that any outcome of the subroutine is a sorted state and that the quantum operation is in fact a projector onto its fixed point space.

Regarding the cloning subroutine, let us consider its action together with the reset of the lower registers. Indeed, as QCMs require a reference state in the registers that are overwritten, it is more reasonable to consider the preparation of this reference state as a part of the cloning process too. In the case of the BCQO, one can easily compute the transformation under the reset of the second register and the BCQO unitary of an arbitrary two-register mixed state, defined in the basis of perfectly cloned states as

$$\rho_{\text{init}} = \sum_{p,p',q,q'=1}^{2^c} \omega_{p,p',q,q'}\,|pp'\rangle\langle qq'| \quad \rightarrow \quad \rho_{\text{final}} = \sum_{p,q=1}^{2^c} \omega^{(1)}_{p,q}\,|pp\rangle\langle qq|\,, \tag{3.16}$$

where $\omega^{(1)}_{p,q} \equiv \sum_{k=1}^{n} \omega_{p,k,q,k}$. If we apply the same procedure to ρ_{final}, we obtain the state

$$\sum_{p=1}^{2^c} \omega^{(1)}_{p,p}\,|pp\rangle\langle pp|\,, \tag{3.17}$$

which is a fixed point. In fact, any state with the form $\rho = \sum_{j=1}^{2^c} \lambda_j\,|jj\rangle\langle jj|$ is a fixed point of the reset plus BCQO operation. Indeed, the set of fixed points is the set of density matrices commuting with the complete set of commuting operators used to define BCQO. In particular, these final states are symmetric with respect to register permutation. The fixed points for the whole population can be obtained by simple combination of the two-register fixed points. For example, for a population comprising four individuals (where the cloning is performed from register one to three and register two to four), the fixed points are $\rho = \sum_{j,i=1}^{2^c} \lambda_{ji}\,|jiji\rangle\langle jiji|$. The case with UQCM requires a more elaborated math which is out of the scope of this section, however, its fixed points must also be symmetric with respect to register permutation (due to the S_+ projection in the UQCM).

When it comes to obtaining the fixed points of the QGA, it would be tempting to focus on the states which are simultaneously fixed points of every subroutine. However, those states do not always exist and need not be the unique stationary states of the composite quantum channel. As far as we know, there are not proven necessary and sufficient conditions wich can be handled to obtain the fixed points of a composite quantum channel from the fixed points of its components. However, we can still derive insightful conclusions from their properties. Before reviewing these conclusions, let us define the following concept.

Definition 7 Computational Hamiltonian *or H_C refers to the c-qubit Hamiltonian whose eigenstates are the states of the computational basis, $|j\rangle$, with increasing energy, $\langle j|H|j\rangle > \langle j-1|H|j-1\rangle$ for all $j = 1, 2^c - 1$.*

The computational Hamiltonian is a reference for the performance of the QGA. Most importantly, its eigenstates are perfectly cloned by the BCQO by definition, hence, we should expect exceptional results for it. Additionally, the sorting subroutine for an arbitrary H_P is related to the one applied for H_C. In Section 2.5.2, we showed this relation through the change of basis unitary, U_P, $U_{\text{SORT}} = \left[U_P^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right] \tilde{U}_{\text{SORT}} \left[(U_P^\dagger)^{\otimes n} \otimes \mathbb{I}^{\otimes a}\right]$, where $\tilde{U}_{\text{SORT}}$ is the sorting subroutine for H_C. Similarly, let $\tilde{A}_\sigma$ be the Kraus operators for the sorting subroutine for H_C, then, the Kraus operators for H_P are $A_\sigma = U_P^{\otimes n} \tilde{A}_\sigma (U_P^\dagger)^{\otimes n}$. Therefore, the quantum operation for the sorting subroutine for H_P, $\mathcal{T}_{\text{Sort}}$, is related to the quantum operation for the sorting subroutine for H_C, $\tilde{\mathcal{T}}_{\text{Sort}}$,

$$\mathcal{T}_{\text{Sort}}(\rho) = U_P^{\otimes n} \tilde{\mathcal{T}}_{\text{Sort}} \left((U_P^\dagger)^{\otimes n} \rho U_P^{\otimes n} \right) (U_P^\dagger)^{\otimes n}. \tag{3.18}$$

This implies that the fixed points of $\tilde{\mathcal{T}}_{\text{Sort}}$, named $\tilde{\Lambda}$, are related with the fixed points of $\mathcal{T}_{\text{Sort}}$ by $\Lambda = U_P^{\otimes n} \tilde{\Lambda} (U_P^\dagger)^{\otimes n}$.

This property can also be proven for the quantum operation of UQCM (not for BCQO). Consider the state resulting from cloning two-register with initial state ρ,

$$\frac{1}{d+1} S_+ (\text{tr}_2(\rho) \otimes \mathbb{I}) S_+. \tag{3.19}$$

If we apply the same operation to $(U_P^\dagger)^{\otimes 2} \rho U_P^{\otimes 2}$, we obtain

$$(U_P^\dagger)^{\otimes 2} \left[\frac{1}{d+1} S_+ (\text{tr}_2(\rho) \otimes \mathbb{I}) S_+ \right] U_P^{\otimes 2}, \tag{3.20}$$

which shows that the cloning operation is completely independent of the basis of separable states it is represented in.

It is important to note that, for any $\mathcal{T}$ and arbitrary unitary U, one can always find $\tilde{\mathcal{T}}$ so that $\mathcal{T}(\rho) = U \tilde{\mathcal{T}}(U^\dagger \rho U) U^\dagger$. However, the important point here is that $\tilde{\mathcal{T}}_{\text{Sort}}$ is the quantum channel describing the sorting operation for H_C, and that the unitary performing the transformation is $(U_P)^{\otimes n}$. This shows that, when represented by the eigenbasis of H_P, the action of the sorting operation is identical to the action of the sorting operation for H_C, represented in the computational basis.

Unpleasantly, neither the swap subroutine in the crossover operator nor our mutation subroutine satisfy this property. Therefore, the fixed points for the QGA applied to any particular H_P cannot be obtained by a basis transformation of the fixed points of the QGA applied to H_C. The latter could support the idea of a performance of the QGA independent of the problem to be solved, i.e. independent of H_P. However, the swap and mutation (and BCQO, if used) subroutines forbid that feature. Instead, we should expect a performance varying with the problem solved, which is indeed observed in the numerical simulations presented in Section 3.2.

3.1.3 Finding the fixed points

In this section, we employ the method described in Section 1.2.6 to find the fixed points of the QGA. However, due to the computational cost and its small impact in the overall performance of the algorithm, we have omitted the mutation subroutine and only focused on the fixed points for the unmutated QGA. For the same reason, we obtained a larger amount of analytical results for the BCQO-based QGA than for the UQCM-based one. The former can be applied by a unitary transformation, which makes solving the eigenvalue equation for fixed points computationally easier.

We computed the fixed points for BCQO-based QGA applied to 600 different problem Hamiltonians. For all of the cases, except one, the fixed point was unique and was in complete agreement with the final states arising from the numerical simulations. The exceptional case whose fixed-point space is multi-dimensional is the BCQO-based QGA applied to the computational Hamiltonian. This stems from the fact that H_C is an observable which is perfectly cloned by the BCQO. For the sake of concreteness, we focus here in the analysis of the fixed points of that particular case.

Any fixed point of the BCQO-based QGA applied to H_C can be described as a mixture of four pure states,

$$\begin{aligned}\Lambda = \lambda_1 \left|00\ 00\ 00\ 00\right\rangle\!\left\langle 00\ 00\ 00\ 00\right| + \\ \lambda_2 \left|01\ 01\ 01\ 01\right\rangle\!\left\langle 01\ 01\ 01\ 01\right| + \\ \lambda_3 \left|10\ 10\ 10\ 10\right\rangle\!\left\langle 10\ 10\ 10\ 10\right| + \\ \lambda_4 \left|11\ 11\ 11\ 11\right\rangle\!\left\langle 11\ 11\ 11\ 11\right|,\end{aligned} \tag{3.21}$$

for some $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 1$ and $\lambda_i \geq 0$. Note that, for this particular case, the fixed point of the QGA is also a fixed point of every subroutine. However, it is not unique, therefore the coefficients depend on the initial state.

Let us show that the states of the computational basis always converge to $|\phi_{00}\rangle = |00\ 00\ 00\ 00\rangle$, $|\phi_{01}\rangle = |01\ 01\ 01\ 01\rangle$, $|\phi_{10}\rangle = |10\ 10\ 10\ 10\rangle$, or $|\phi_{11}\rangle = |11\ 11\ 11\ 11\rangle$, and then use this property to analyse an arbitrary case. We can classify the states of the computational basis in five categories which converge to $|\phi_{00}\rangle$, $|\phi_{01}\rangle$, $|\phi_{10}\rangle$ or $|\phi_{11}\rangle$:

A. If the initial state contains at least one register in the state $|00\rangle$, then it converges towards $|\phi_{00}\rangle$ with certainty. There are $4^4 - 3^4 = 175$ such states and we name P_A the projector onto the subspace they span.

B. If the initial state contains at least one register in the state $|01\rangle$ and other in the state $|10\rangle$, and none in $|00\rangle$, then it converges towards $|\phi_{00}\rangle$ with certainty. There are 48 such states and we name P_B the projector onto the subspace they span.

C. If the initial state contains at least one register in the state $|01\rangle$ and none in $|00\rangle$ nor $|10\rangle$, then it converges towards $|\phi_{01}\rangle$ with certainty. There are 16 such states and we name P_C the projector onto the subspace they span.

D. If the initial state contains at least one register in the state $|10\rangle$ and none in $|00\rangle$ nor $|01\rangle$, then it converges towards $|\phi_{10}\rangle$ with certainty. There are 16 such states and we name P_D the projector onto the subspace they span.

E. If the initial state contains only registers in state $|11\rangle$, i.e. it is the state $|\phi_{11}\rangle$, then it is a fixed point and it is invariant. We name P_E to the projector onto that state.

Therefore, if the initial state is the maximally mixed state then it converges towards the fixed point with the coefficients $\lambda_1 = \frac{223}{256}$, $\lambda_2 = \frac{16}{256}$, $\lambda_3 = \frac{16}{256}$, and $\lambda_4 = \frac{1}{256}$. This leads to a probability of 0.87 of measuring the ground state in any of the registers. For any other initial state, ρ, these coefficients can be calculated by means of the projectors defined above: $\lambda_1 = \mathrm{tr}((P_A + P_B)\rho)$, $\lambda_2 = \mathrm{tr}(P_C\rho)$, $\lambda_3 = \mathrm{tr}(P_D\rho)$, and $\lambda_4 = \mathrm{tr}(P_E\rho)$. The space spanned by vectors in category A and B being dimensionally larger than its complementary shows that, indeed, the λ_1 coefficient is prone to be higher than the others.

In Section 1.2.6, we explained that the spectral subradius of a quantum channel describes the convergence rate towards a fixed point, precisely, it is an upper bound for the terms that are linearly independent of the fixed point. Figure 3.1, shows a density plot describing the distribution of values obtained for the spectral subradius, denoted λ, for BCQO-based QGA without mutation applied to different problem Hamiltonians. The orange and green distributions for λ^2 and λ^5 represent the spectral subradius when the operation is applied two and five generations, respectively. These results show that a single generation of the algorithm halves the upper bound for the non-fixed point terms for about 20% of the cases, with two generations this proportion increases to about 60%, and with five generations it is up to 90%. With five generations for about 45% of the cases the upper bound for the non-fixed point terms is reduced below 10%. These results show a robust convergence towards the fixed points. Moreover, the spectral subradius for the BQCO-based QGA without mutation applied to H_C is zero, which is an exceptional value meaning that perfect convergence is achieved in one or two generations.

Regarding UQCM-based QGA, we only obtained its fixed point applied to H_C. That state is unique and we describe it by the following state ensemble

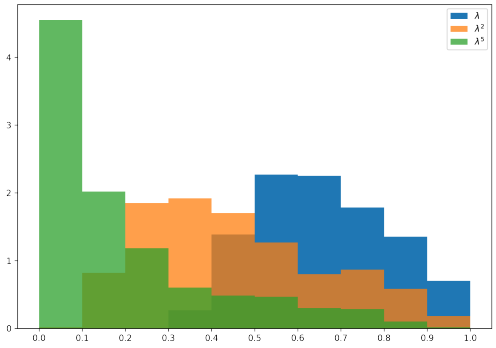


Figure 3.1: Distribution of the spectral subradius, λ, for BCQO-based QGA without mutation applied to different problem Hamiltonians.

(probabilities truncated to the third decimal):

State	*Probability*
$\|00\ 00\ 00\ 01\rangle$	0.151
$\|00\ 00\ 00\ 00\rangle$	0.143
$\|00\ 00\ 00\ 10\rangle$	0.143
$\|00\ 00\ 01\ 10\rangle$	0.136
$\|00\ 00\ 00\ 11\rangle$	0.090
$\|00\ 00\ 01\ 11\rangle$	0.059
$\|00\ 00\ 01\ 01\rangle$	0.056
$\|00\ 00\ 10\ 11\rangle$	0.055
$\|00\ 00\ 10\ 10\rangle$	0.036
$\|00\ 01\ 10\ 11\rangle$	0.024
$\|00\ 01\ 01\ 10\rangle$	0.023
$\|00\ 01\ 10\ 10\rangle$	0.021
$\|00\ 00\ 11\ 11\rangle$	0.019
$\frac{1}{\sqrt{2}}(\|00\ 00\ 01\ 11\rangle + \|00\ 01\ 01\ 10\rangle)$	0.014
$\|00\ 01\ 01\ 11\rangle$	0.011
$\|00\ 01\ 01\ 01\rangle$	0.009
$\|00\ 01\ 11\ 11\rangle$	0.003
$\frac{1}{\sqrt{2}}(\|00\ 01\ 01\ 11\rangle + \|01\ 01\ 01\ 10\rangle)$	0.001
$\|01\ 01\ 01\ 01\rangle$	0.001
$\|01\ 01\ 01\ 10\rangle$	0.001
$\|01\ 01\ 01\ 11\rangle$	0.001
$\|01\ 01\ 10\ 10\rangle$	0.001
$\|01\ 01\ 10\ 11\rangle$	0.001

(3.22)

Note that as all of the states of the ensemble are sorted states, the state is a fixed point of the sorting subroutine. However, the state is not a fixed point of the cloning subroutine (it is not symmetric with respect to register permutation) nor of the swap operation in the crossover subroutine. Remarkably, adding up the probability of each state in the ensemble containing a register in the state $|00\rangle$, we obtain a excellent probability of 0.994 for measuring the ground state in at least

one of the registers. This result agrees with numerical simulations. The spectral subradius for this case also guarantees a rapid convergence towards the fixed point, its value is 0.587, which reduces to 0.005 when applied 10 generations.

3.2 Numerical simulations of the QGA

In this section, we show the results obtained from several simulations performed to validate the results obtained via the quantum channel analysis, mainly the convergence of the algorithm and the characterization of the final state for different problem Hamiltonians. We generated several random problem Hamiltonians and employed different variants of the QGA to find low energy states, ideally the ground state. Let us note again that we are not focusing on comparing the QGA with the classical GA, but first we are validating its performance as an optimization method. Performing a fair comparison between the classical and quantum GA would require a more precise definition of the sorting oracle and the retrieval of information from the final state. Hereunder, we assume there is an efficient method to implement the sorting oracle and that we have unrestricted access to the final state.

In order to quantify the success of the algorithm we have measured the fidelity with the ground state in the state of the best register. In other words, take the population state ρ and compute the restricted density matrix for the first register ρ_{r_1}, afterwards, compute the fidelity with the ground state, $|u_0\rangle$, by $F = \langle u_0|\rho_{r_1}|u_0\rangle$. We refer to this magnitude as the *QGA fidelity* and it also indicates the probability to measure the ground state in ρ_{r_1}.

We performed calculations with four different variants of the QGA: BCQO-based with mutation, BCQO-based without mutation, UQCM-based with mutation, and UQCM-based without mutation. In the four cases, we employed $n = 4$ registers (individuals) and $c = 2$ qubits in each (chromosome length). The algorithm required typically 5 generations to converge fro BCQO-based without mutation and 10 generations for the other variants. With each variant of the QGA we solved numerous different problem Hamiltonians, above 500 for the variants without mutation and 200 for the variants including mutation. For each problem Hamiltonian we started with several different populations, and verified that similar results were obtained for all of them. Most of the problem Hamiltonians where generated randomly, employing a generator of pseudo-random real unitaries sampling from a Haar distribution. We performed this task making use of the Python library scipy, which provides a function based on a consolidated algorithm to perform the sampling [38].

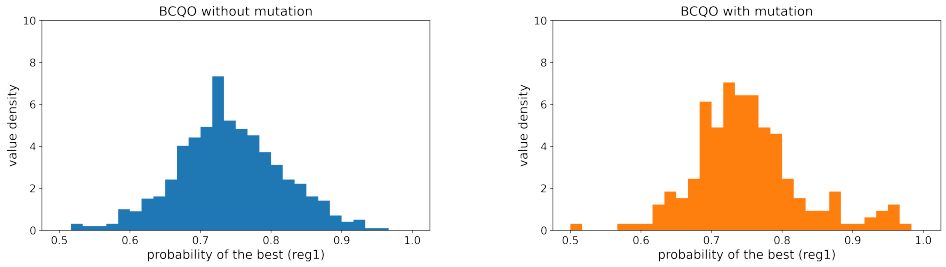
3.2.1 BCQO-based QGA

Firstly, the QGA was applied without mutation to solve 600 different problem Hamiltonians, and we obtained the QGA fidelity for each averaging over different initial states. Each Hamiltonian was solved with 50 different initial states, which resulted in similar final states and only required 5 generations to converge. The average fidelity was computed for each problem Hamiltonian and we constructed the density histogram shown in Fig. 3.2a. From the distribution of the fidelity,

which also represents the probability of measuring the ground state in the first register, it can be assured that at least in 80% of the cases the probability to measure the ground state is above 0.68. This QGA method obtains a fidelity in the range from 0.7 to 0.8 for half of the cases.

These problem Hamiltonians were also employed in the fixed point analysis (Section 3.1.3). The comparison between the fixed points obtained analytically and the states obtained via these simulations were in perfect agreement, thus showing that the fixed point analysis is a valid tool for analysing the performance of the QGA.

Figure 3.2b shows the density plot for the QGA fidelity obtained when the mutation subroutine was included. For this result, only 196 different problem Hamiltonians were employed, due to the computational cost of including mutation, and 50 different initial populations were used. In this case 10 generations were required to ensure the convergence of the population. The probability of mutation was 0.125, approximately one mutation per generation. As can be seen comparing Fig. 3.2a and Fig. 3.2b, both distributions are similar and, in general, a slight difference was observed between including mutation or not. Exceptionally, including mutation improved the QGA fidelity for some particular problem Hamiltonians, for example, the fidelity with the ground state of H_C increased from 0.786 to 0.958. Moreover, analysing the QGA fidelities obtained for different initial populations for this case, 80% of the final populations outstandingly achieved QGA fidelity 1. A deeper understanding of the reason for the improvement in those particular cases would guide further improvement of the mutation subroutine.

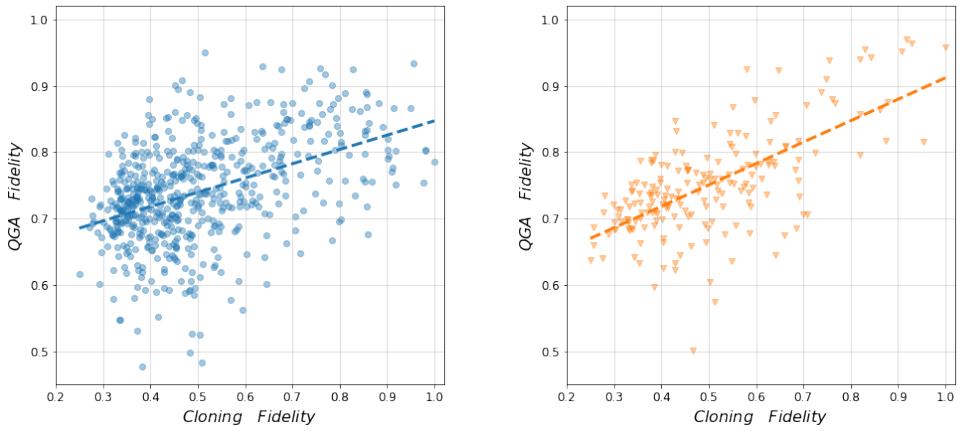


(a) (b)

Figure 3.2: Density plots for the fidelity of the final state of the first register with the ground state of each problem Hamiltonian solved with BCQO-based QGA, a) without mutation and b) with mutation.

Regarding the influence of the replication method, we found a consistent relationship between the cloning fidelity and the performance of the QGA. For each problem Hamiltonian, we computed the single copy fidelity of BCQO for the ground state, as described in Section 2.6.1; and compared its value with the QGA fidelity. Figure 3.3b, shows the scatter plot relating QGA fidelity and single copy fidelity with BCQO for the case without mutation, and Fig. 3.3a for the case with mutation. Both figures show that the QGA performs significantly better for problem Hamiltonians whose ground state have greater single copy fidelity with BCQO, which can be emphasised by the considerable correlation factor between the single copy fidelity and the QGA fidelity, 0.45 for the case without mutation and 0.66 for the case with mutation. The dashed lines depicted

in Fig. 3.3b and Fig. 3.3a, were obtained via linear regression and should be considered as a qualitative insight and not a formal result or expected linear relationship. In order to properly describe the relationship between the fidelity of the cloning method and the QGA fidelity, one should consider the influence of other subroutines. Moreover, the relationship found for BCQO may not hold for other cloning methods. However, the higher correlation factor found for the case with mutation suggests that mutation may be improving the performance of QGA applied to problem Hamiltonians whose ground state have a higher single copy fidelity with BCQO.



(a) (b)

Figure 3.3: Results for different problem Hamiltonians solved with BCQO-based QGA, a) without mutation and b) with mutation. The vertical axis represents the fidelity of the final state of the first register with the ground state of each problem Hamiltonian, and the horizontal axis represents the fidelity of the cloning of the ground state performed with BCQO.

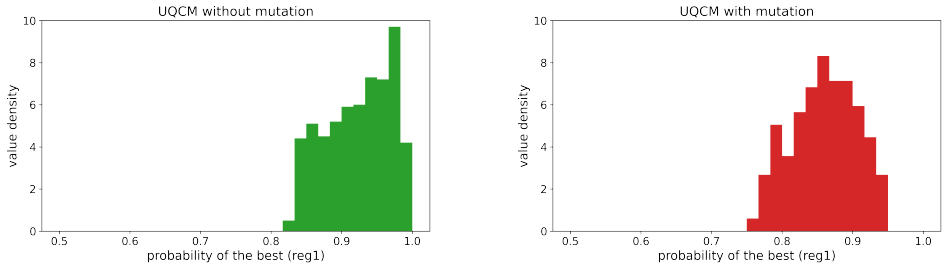
3.2.2 UQCM-based QGA

As performed for BCQO-based QGA, firstly we solved 600 different problem Hamiltonians with the QGA without mutation and obtained their QGA fidelity. Only 5 different initial populations were employed, achieving almost identical results for all of them, and 10 generations were applied to guarantee the convergence. The density plot for the average QGA fidelity for each problem Hamiltonian is shown in Fig. 3.4a. It can be assured that at least 90% of the cases achieve a QGA fidelity greater than 0.85.

In this case, because of the computational cost, we did not verify the agreement between the fixed point analysis and the simulations for every case. However, the results described in Section 3.1.3 sufficiently support the validity of the fixed point analysis in this case.

In Fig. 3.4b, we show the density plot for the QGA fidelity when the mutation subroutine was included. 200 different problem Hamiltonians were employed, each with 50 different initial populations, mutation was applied as in the BCQO

based case and only 10 generations were required for convergence. The noticeable difference between Fig. 3.4a and Fig. 3.4b suggests that mutation has an impact when UQCM is used in the crossover subroutine. More precisely, the distribution of the QGA fidelity is shifted to lower values by more than half a unit, the average QGA fidelity is 0.92 when mutation is omitted and 0.86 when it is included. Attending to H_C, for which the mutation improved the result in the BCQO-based QGA, the QGA fidelity is 0.99 for the case without mutation and 0.94 for the case with mutation, therefore, the improvement observed by including mutation in BCQO-based QGA cannot be extrapolated to UQCM-based QGA.



(a) (b)

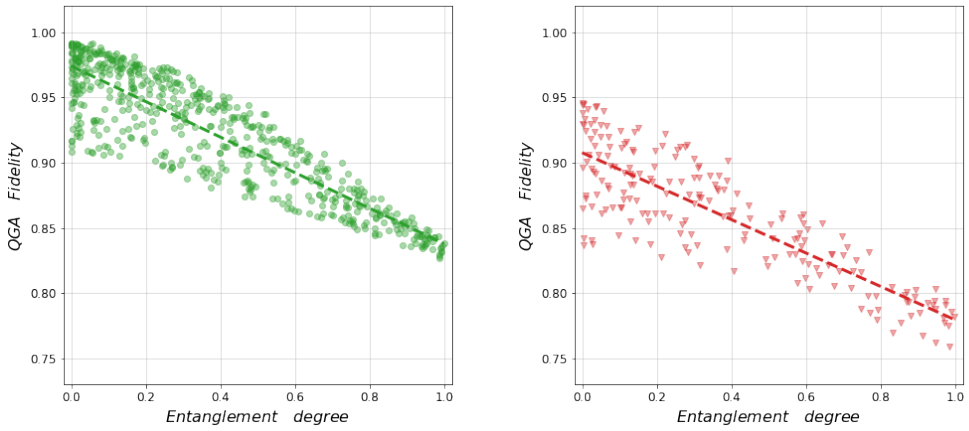
Figure 3.4: Density plots for the fidelity of the final state of the first register with the ground state of each problem Hamiltonian solved with UQCM-based QGA, a) without mutation and b) with mutation.

As described in Section 3.1.2, both the selection subroutine and the UQCM act equivalently on the eigenbasis of any problem Hamiltonian, therefore, the swap operation in the crossover subroutine must account for the variation observed in the QGA fidelity for the UQCM-based QGA. This operation swaps the second qubit of the last two registers, which should affect differently for distinct two-qubit states. This point suggests that entangled individuals are less prone to survive with our crossover subroutine.

In order to verify that idea, we analysed the relationship between the QGA fidelity and the degree of entanglement of the ground state of each problem Hamiltonian, measured as described in Section 1.2.4. Figures 3.5a and 3.5b show the scatter plot describing the relationship between the QGA fidelity and the entanglement degree of the ground state, for the QGA without mutation and with mutation respectively. Both figures show a considerable decrease in the QGA fidelity for problem Hamiltonians whose ground state is highly entangled. The correlation factor between the QGA fidelity and the entanglement degree is -0.89 for the case without mutation and -0.85 for the case with mutation. Again, the dashed lines were obtained with a linear fit, but must be interpreted qualitatively. The distribution of points is considerably similar in both cases, with the only difference of the vertical shift mentioned above.

3.3 Discussion of the results

To summarize, we have validated the performance of the QGA applied to different problem Hamiltonians, both via quantum channel analysis and numerical



(a) (b)

Figure 3.5: Results for different problem Hamiltonians solved with UQCM-based QGA, a) without mutation and b) with mutation. The vertical axis represents the fidelity of the final state of the first register with the ground state of each problem Hamiltonian, and the horizontal axis represents the degree of entanglement of the ground state.

simulations. Both approaches show high QGA fidelities, ranging above 0.5 for almost all of the cases and approaching 1 for many of them. The rapid convergence of the algorithm is supported by its dependence with the spectral subradius of the quantum channel, which have been shown to be small enough, and numerically by verifying the small difference between the states in subsequent generations, only requiring approximately 10 generations to go below the threshold of 10^{-3}.

The quantum channel analysis and the study of fixed points represents an innovative approach to the study of quantum genetic algorithms, which can be used to understand their asymptotic behaviour and convergence. Additionally, this approach can be used previous or complementary to simulations to estimate the performance of the algorithm with a less demanding computational cost, which particularly enables an efficient method for testing new variants of the subroutines composing the QGA. However, optimizing and improving this analytical approach is required in order to apply it efficiently to some subroutines, e.g. to the mutation subroutine.

We have performed a comparison of four different variants of the QGA, namely BCQO-based QGA and UQCM-based QGA both with and without mutation. Figure 3.6 shows a comparison of the distribution of the QGA fidelity for each variant. We have found that for virtually all the problem Hamiltonians studied here, the UQCM-based QGA without mutation consistently outperforms other variants in terms of average QGA fidelity. Unexpectedly, this advantage compared with BCQO is also observed for problem Hamiltonians whose ground state is cloned with better fidelity by BCQO than by UQCM. Moreover, it also suggest that our mutation method is harming the UQCM-based QGA's convergence towards better states. In contrast, the statistical variation resulting from including mutation in BCQO-based QGA is practically negligible, although we have observed a

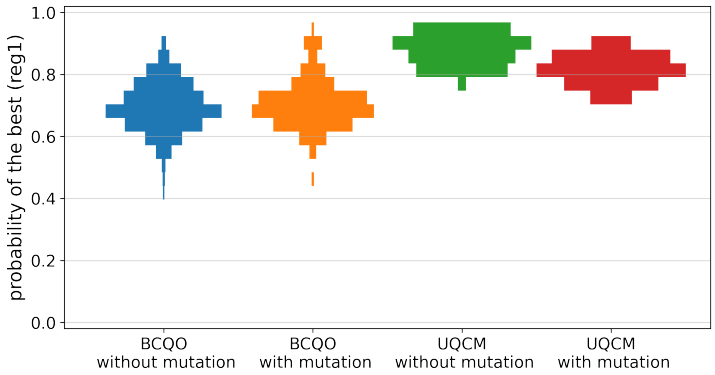


Figure 3.6: Comparison of the distribution of the QGA fidelity obtained by the QGA variats studied.

significant improvement associated to including mutation when the algorithm is applied to H_C. Moreover, the results suggest that further analysis of this phenomena may prove that BCQO-based QGA with mutation even outperforms UQCM-based QGA for solving problem Hamiltonians similar to the computational Hamiltonian.

With regard to limitations of these results, we must mention that further comprehension of the swap and mutation subroutines would provide deeper understanding of the variation of the performance of the algorithm. Maybe other implementations of sexual replication could lead to better state independent results. Similarly, variations in the mutation subroutine, such as adapting the set of mutation unitaries or tuning the mutation probability, should be considered as promising sources of improvement.

Conclusions

There is an obvious interest in merging evolutionary algorithms with quantum computation. Although several algorithms have been already developed, much is still unknown about the intersection between these two fields. For instance, it is still unclear whether the evolutionary principles inspiring heuristic optimization techniques can achieve a provable improvement. In this thesis, we deeply study the quantum genetic algorithm (QGA) originally proposed in Ref. [9]. This algorithm has the property to be completely implementable in quantum hardware, employing well known efficient quantum protocols as subroutines. Moreover, also exhibits similarities with the classical genetic algorithm (GA).

Besides, let us remark that due to the resemblance with classical GAs, in our algorithm every individual is stored in a different register. Therefore, this procedure is specially suitable for distributed quantum computing, as the registers representing different individuals could be stored in a network of quantum processors. This reduces significantly the technical requirements for these algorithms to be implemented in a physical quantum computer, although that realization is not in the near-term future.

In the first Chapter, we have introduced the fundamental principles of quantum mechanics, quantum computation and quantum information. These concepts are essential to understand the rest of the thesis.

In the second Chapter, we have shortly reviewed the classical GAs and the state of the art in the field of QGAs. Afterwards, we have described our proposal for a QGA, mainly focusing in the description of its building blocks. Particularly, we have provided a thorough description of each subroutine and some examples to illustrate their process.

Finally, in the third Chapter, we have shown the methodology employed to obtain the results. Indeed, we have discussed analytical techniques based on quantum channel analysis and numerical methods for classical simulations of the algorithms. We have analyzed four variants for the QGA verifying that all of them obtain successful results for most of the attempted problem cases. In particular, we have compared the performance of the QGA considering two different replication methods, namely, the biomimetic cloning of quantum observables (BCQO) and the universal quantum cloning machine (UQCM). As a result, we have concluded that the variant that the QGA employing UQCM for the replication and without mutation outperforms the other variants. Nevertheless, we note some aspects that could make BCQO-based QGA better suited for problem Hamiltonians whose ground state is cloned with high fidelity by BCQO, further work would be needed on that direction to verify that hint. This suggests that different variants of our algorithm in the definition of its subroutines could adapt better and lead to

improvements in the performance for particular problems. This feature resembles the ability of classical GAs to be adapted to a wide variety problem cases. In our opinion, the adaptability of the subroutines should be considered a relevant feature for any GA-based algorithm.

As mentioned above, our proposal of the QGA was already developed in the bachelor thesis of R. Ibarrondo [9]. In that work, the analysis was restricted to problems represented by Boolean functions, which can be represented by problem Hamiltonians that are diagonal in the computational basis. This framework was useful to verify the ability of the QGA to find the optimum for theese problems, but it did not provide any potential advantage against its classical counterpart. Instead, in this project, we have extended our analysis to generic problem Hamiltonians.We have been able to successfully verify its performance for small systems. This result is rather more encouraging, because Hamiltonians whose ground states do not lie in the computational basis are hard to represent and compute in a classical computer than they should be in a quantum computer.

Additionally, in this thesis, we have validated particular methods to quantify the performance of the QGA. For instance, we have introduced the QGA fidelity as an important success indicator and we have developed the first steps employing fixed points of quantum channels to prove the convergence of the algorithm. We envision a future work developing in detail the quantum channel analysis for the study of bioinspired algorithms.

Nevertheless, we have not proved yet any particular advantage for the QGA, because to do so we should also account for the information retrieval of the final population, which is indeed a complicated task. In fact, the information retrieval is exponentially hard (with respect to the number of qubits) if we want to obtain the whole state of the population. However, it could be efficient if we were only interested in partial information, such as the minimum energy related to the individuals or the expected value of an observable in the ground state. This illustrates that in order to prove any advantage, one should be able to find a relevant problem where 1) the problem Hamiltonian is easier to simulate in a quantum computer than in a classical computer, 2) the expected solution is not necessarily the computational basis, and 3) the required information retrieval can be efficiently performed. It is our belief that, in the area of molecular chemistry and quantum device engineering, there are problems meeting these requirements and, thus, they may take advantage of our algorithm. However, proving this statement is left for further work.

We have performed the calculations for the simulation of quantum algorithms of the third chapter with Python 3 programs, which are available in the repository of the University of the Basque Country (ADDI).

Bibliography

[1] D. A. Sofge. (2008) Prospective Algorithms for Quantum Evolutionary Computation. [Online]. Available: http://arxiv.org/abs/0804.1133

[2] U. Roy, S. Roy, and S. Nayek, "Optimization with Quantum Genetic Algorithm," *International Journal of Computer Applications*, vol. 102, no. 16, pp. 1–7, 2014.

[3] R. Lahoz-Beltra, "Quantum Genetic Algorithms for Computer Scientists," *Computers*, vol. 5, no. 4, p. 24, 2016.

[4] A. Narayanan and M. Moore, "Quantum-inspired genetic algorithms," in *Proceedings of IEEE International Conference on Evolutionary Computation*, 1996, pp. 61–66.

[5] B. Rylander, T. Soule, J. Foster, and J. Alves-Foss, "Quantum Evolutionary Programming," in *Proceedings of the 3rd Annual Conference on Genetic and Evolutionary Computation*, ser. GECCO'01, San Francisco, CA, USA, 2001, pp. 1005–1011.

[6] M. Udrescu, L. Prodan, and M. Vladutiu, "Implementing Quantum Genetic Algorithms: A Solution Based on Grover's Algorithm," in *Proceedings of the 3rd Conference on Computing Frontiers*, ser. CF '06. New York, NY, USA: Association for Computing Machinery, 2006, pp. 71–82.

[7] A. Malossini, E. Blanzieri, and T. Calarco, "Quantum genetic optimization," *IEEE Transactions on Evolutionary Computation*, vol. 12, no. 2, pp. 231–241, 2008.

[8] A. SaiToh, R. Rahimi, and M. Nakahara, "A quantum genetic algorithm with quantum crossover and mutation operations," *Quantum Information Processing*, vol. 13, no. 3, pp. 737–755, 2014.

[9] R. Ibarrondo. (2020) Quantum genetic algorithms: towards the design of evolutionary algorithms in a quantum computer. [Online]. Available: http://hdl.handle.net/10810/49102

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

[11] A. Galindo and P. Pascual, *Mecánica cuántica (I)*. Madrid: Eudema Universidad, 1989.

[12] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[13] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, pp. 1225–1256, 2005.

[14] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 54, no. 3, pp. 1844–1852, 1996.

[15] A. Ferraro, M. Galbiati, and M. Paris, "Cloning of observables," *Journal of Physics A: Mathematical and General*, vol. 39, no. 14, p. L219–L228, 2006.

[16] U. Alvarez-Rodriguez, M. Sanz, L. Lamata, and E. Solano, "Biomimetic cloning of quantum observables," *Scientific Reports*, vol. 4, pp. 4–7, 2014.

[17] N. Herbert, "FLASH-A superluminal communicator based upon a new kind of quantum measurement," *Foundations of Physics*, vol. 12, no. 12, pp. 1171–1179, 1982.

[18] K. A. Pati and S. L. Braunstein, "Impossibility of deleting an unknown quantum state," *Nature*, vol. 404, no. 6774, pp. 164–165, 2000.

[19] D. Bruß, "Characterizing entanglement," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4237–4251, 2002.

[20] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, "Matrix product state representations," *Quantum Information and Computation*, vol. 7, no. 5-6, pp. 401–430, 2007.

[21] M. Sanz, "Tensor Networks in Condensed Matter," Ph.D. dissertation, Technische Universität München, 2011.

[22] M. Sanz, D. Pérez-García, M. M. Wolf, and J. I. Cirac, "A quantum version of Wielandt's inequality," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4668–4673, 2010.

[23] M. Mitchell, *An introduction to genetic algorithms*. Cambridge, MA, USA: MIT Press, 1996.

[24] J. H. Holland, *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control and Artificial Intelligence*. Cambridge, MA, USA: MIT Press, 1992.

[25] K. H. Han and J. H. Kim, "Genetic quantum algorithm and its application to combinatorial optimization problem," *Proceedings of the IEEE Conference on Evolutionary Computation, ICEC*, vol. 2, pp. 1354–1360, 2000.

[26] K. H. Han, K. H. Park, C. H. Lee, and J. H. Kim, "Parallel quantum-inspired genetic algorithm for combinatorial optimization problem," *Proceedings of the IEEE Conference on Evolutionary Computation, ICEC*, vol. 2, no. 2, pp. 1422–1429, 2001.

[27] K. H. Han and J. H. Kim, "Quantum-Inspired Evolutionary Algorithm for a Class of Combinatorial Optimization," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 6, pp. 580–593, 2002.

[28] S. Yang, M. Wang, and L. Jiao, "A novel quantum evolutionary algorithm and its application," in *Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753)*, vol. 1, 2004, pp. 820–826.

[29] L. Wang, F. Tang, and H. Wu, "Hybrid genetic algorithm based on quantum computing for numerical optimization and parameter estimation," *Applied Mathematics and Computation*, vol. 171, no. 2, pp. 1141–1156, 2005.

[30] S. Yingchareonthawornchai, C. Aporntewan, and P. Chongstitvatana, "An implementation of compact genetic algorithm on a quantum computer," in *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*, 2012, pp. 131–135.

[31] J. Zhang, L. Liu, H. Li, and Z. Tang, "PID tuning based on improved quantum genetic algorithm," *Proceedings - 6th International Symposium on Computational Intelligence and Design, ISCID 2013*, vol. 2, pp. 44–47, 2013.

[32] L. Wang, H. Wu, and D. Zheng, "A Quantum-Inspired Genetic Algorithm for Scheduling Problems," in *Advances in Natural Computation*, L. Wang, K. Chen, and Y. S. Ong, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 417–423.

[33] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, New York, NY, USA, 1996, p. 212–219.

[34] C. Dürr and P. Høyer. (1996) A Quantum Algorithm for finding the minimum. [Online]. Available: arXiv:quant-ph/9607014

[35] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, 1998.

[36] D. W. Berry, M. Kieferová, A. Scherer, Y. R. Sanders, G. H. Low, N. Wiebe, C. Gidney, and R. Babbush, "Improved techniques for preparing eigenstates of fermionic Hamiltonians," *npj Quantum Information*, vol. 4, no. 1, pp. 1–7, 2018.

[37] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, "A new quantum ripple-carry addition circuit," pp. 1–9, 2008. [Online]. Available: http://arxiv.org/abs/quant-ph/0410184

[38] G. W. Stewart, "The efficient generation of random orthogonal matrices with an application to condition estimators," *SIAM Journal on Numerical Analysis*, vol. 17, no. 3, pp. 403–409, 1980.