Black-box Testing of Quantum Systems

Trabajo de Fin de Grado
Curso 2020–2021

Autor
Pablo Vázquez Gomis

Director
Alfredo Ibias
Manuel Núñez

Grado en Ingeniería Informática
Facultad de Informática
Universidad Complutense de Madrid

Black-box Testing of Quantum Systems

Trabajo de Fin de Grado en Ingeniería Informática
Departamento de Sistemas Informáticos y Computación

Autor
Pablo Vázquez Gomis

Director
Alfredo Ibias
Manuel Núñez

Convocatoria: *Junio 2021*

Grado en Ingeniería Informática
Facultad de Informática
Universidad Complutense de Madrid

10 de junio de 2021

Dedicatoria

A mi abuelo, Juan Gomis, por enseñarme a ver el mundo de forma crítica y objetiva e inspirarme siempre a ser la mejor versión de mí mismo.

A mis padres Elena y Alfonso y a mis hermanos Elena, Juan y Gonzalo, por todo su apoyo durante los años buenos y los difíciles. Por darme las herramientas y la libertad para decidir mi camino.

A mi novia y a mis amigos por todos los buenos momentos a lo largo de estos años y por todas las historias que hemos vivido y las que aún están por descubrir.

Agradecimientos

Me gustaría agradecer a mis directores Manuel Nuñez y Alfredo Ibias por su inestimable ayuda en este proyecto y, junto a Miguel Benito, darme a conocer el mundo de la investigación y ayudarme a dar mis primeros pasos en él.

Me gustaría también agradecer a mis profesores, en especial a Gonzalo Méndez y Félix del Teso, su apoyo durante mi etapa universitaria.

Por último, agradecer las oportunidades que me ha dado la Facultad de Informática de la UCM así como a todas las personas que me han hecho crecer durante estos años.

Resumen

La Computación Cuántica es un área en expansión en campos como Informática, Física y Matemáticas debido a sus increíbles resultados resolviendo problemas complejos mucho más rápido que cualquier ordenador clásico. Sin embargo, las dificultades físicas que presenta la Mecánica Cuántica, añadido a la complejidad que conlleva el desarrollo de algoritmos, ha hecho que la Computación Cuántica sea muy susceptible a errores. Por tanto, asegurar la calidad de los aparatos y algoritmos va a ser de vital importancia en el futuro del campo.

En este trabajo presentamos una breve introducción a la Mecánica Cuántica, seguido de un posible nuevo marco de referencia basado en un formalismo al que llamamos *Maquinas de Turing Híbridas*. Este formalismo permite especificar sistemas complejos juntando máquinas de Turing cuánticas y clásicas. Por último, presentamos un estudio en una de las pocas técnicas existentes en el testeo de caja negra de sistemas cuánticos, el llamado *Self Testing*, junto con un experimento practico.

Palabras clave

Computación Cuántica, Máquinas de Turing cuánticas, desigualdades de Bell, Self Testing

Abstract

Quantum Computing is a growing field in Computer Science, Physics and Mathematics because it presents stunning results in solving very complex problems faster that any classical computer. However, the physical difficulties that Quantum Mechanics presents, added to the complex development of quantum algorithms, made the field to be very prone to errors. Thus, ensuring the quality of the devices and algorithms will take a very important role in the future of the field.

In this Thesis we present a brief introduction to Quantum Mechanics, followed by a new possible testing framework based on a formalism that we call *Hybrid Turing Machines*. This formalism allows to design complex systems by joining quantum and classical Turing Machines. Finally, we present a study of one of the very few techniques in Quantum Testing for black boxes, called *Self Testing*, along with a practical experiment.

Keywords

Quantum Computing, quantum Turing machines, Bell's inequalities, Self Testing

Contents

Chapter 1

Introduction

1.1. Background

When an electric charged particle is oscillating, that is, moving with a periodic movement, it generates an electromagnetic wave, which we call *light*. As a result, the particle looses energy. This phenomenon led to various problems with the well-known Rutherford Model of an atom (see Figure 1.1), because orbiting electrons would collapse into the nucleus as a result of the energy losses.

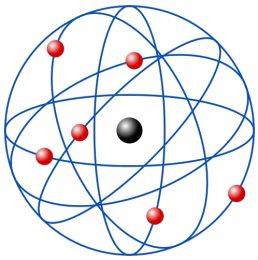


Figure 1.1: Rutherford atomic model[1]

In 1900, Max Planck introduced the idea that energy emissions came in discrete packages of size proportionally to the frequency rather than with continuous emissions [Planck (1901)]. This fact, together with the results of the photoelectric effect presented by Albert Einstein [Einstein (1905)], which described that light could also be thought as a stream of particles called a *photon*, gave birth to Borh's atomic model [Bohr (1913)]. In this model, electrons stay in stable orbits and can only jump to other stable orbits by emitting or absorbing discrete packages of energy. This is known as the old quantum theory. Jumping back to 1803, the *double-slit experiment* proved that matter had both wave and particle like properties. Schrödinger, in 1926, proposed that electrons could be seen as waves, rather than particles orbiting a nucleus and gave a very complete mathematical description of this idea [Schrödinger (1926)]. In particular, a particle, such as an electron is de-

[1] Cburnett, CC BY-SA 3.0 `http://creativecommons.org/licenses/by-sa/3.0/`, via Wikimedia Commons.

scribed by a wave function Ψ that evolves according to his famous equation

$$i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = \hat{H}\Psi(\mathbf{r},t) \tag{1.1}$$

In addition, Heisenberg and Born had already gave a description based on matrices which Schrödinger proved to be equivalent to his interpretation of continuous waves.

The Stern-Gerlach Experiment These mathematical descriptions were key to interpret the results of the Stern-Gerlach experiment. Particles, such as atoms and electrons, behave as if they had angular momentum and as such they presented magnetic properties. In 1922, they discovered that when particles with a spin in a given direction were deflected by a non-homogeneous magnetic field and measured afterwards, rather than showing a continuous spectrum (shown as 4 in Figure 1.2) as were classically expected it showed only two discrete values (shown as 5 in Figure 1.2). This results showed that spin is a quantum property and, as such, measurement of that property has a discrete distribution.

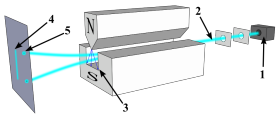


Figure 1.2: The Stern-Gerlach Experiment[2]

In 1926, Max Born proposed that the wave function could be interpreted as the probability distribution of finding the particle $\Psi(\vec{r})$ at some point x in space [Born (1926)]. This probability is given by $|\Psi(x)|^2$. Einstein was very concerned with the probabilistic nature of quantum mechanics and in 1935 along with Boris Podolsky and Nathan Rosen proposed a thought experiment arguing that quantum mechanics was *incomplete* [Einstein et al. (1935)]. This led to the *hidden variable interpretation*, which we will see in detail in Section 4.2. Another very interesting interpretation is the *many world interpretation* in which there is no distinction between classical and quantum and a measurement generates two simultaneous universes for which we only perceive one.

1.2. Objectives and work plan

The main goal of the work behind this Thesis is to review the current state of the black-box testing of quantum system and propose some new ideas in this scenario. Given that the field of Quantum Computing is still growing, there has not been many approaches dealing with testing. Although

[2]By Tatoute - Own work, CC BY-SA 4.0, `https://commons.wikimedia.org/w/index.php?curid=34095239`.

it will definitely be of crucial importance in a future, most of the efforts now focus on the physical realizations of quantum computers or in the mathematical specification and proofs of work of new algorithms. However, there have been some exceptional advances in the field. Here we present one of the most relevant results of such investigations called *Self Testing*. In this black-box device-independent scenario we can, for certain states, certify that a source is in fact generating quantum states and what quantum state is generating. These results are of vital importance in order to certify devices such as random quantum generators but most importantly, they are used in protocols of key distribution using quantum devices and channels such as [Bennett and Brassard (1984)]. Such systems are mostly compiled of a mixture of quantum and classical systems, delegating hard computing task to the quantum part and allowing the classical system to do every other task. In order to appropriately represent these systems, we introduce a formalism based on what we call *Hybrid Turing Machines*.

The work plan of the Thesis is as follows. Chapter 2 gives an introduction to the basic mathematical notions behind Quantum Mechanics, by following the historical process, emphasising in the current state. Then, Chapter 3 gives a background on Turing Machines, both classical and quantum, and how they work in order to later present the mixed Hybrid Turing Machine. Chapter 4 presents the ideas and the mathematical formalism of Self Testing along with an experimental example simulated with qiskit [Gambetta et al. (2021)]. Finally, in Chapter 5 we review our results, present our conclusions and sketch possible lines for future work.

Chapter 2

Quantum Computing: Fundamentals

2.1. Mathematical Foundations

In 1955, John von Neumann presented his book entitled "Mathematical Foundations of Quantum Mechanics" [Von Neumann (1955)] in which he introduced a new mathematical formulation of Quantum Mechanics. At the time, there were two formulations for Quantum Mechanics presented by Schrödinger as "Wave Mechanics" and Heisenberg-Born-Jordan as "Matrix Mechanics". As we said before, Schrödinger already had proven the equivalence of the two and later on Dirac and Jordan developed the "Transformation Theory", which joined both theories.[1] Von Neumann presented a new mathematical framework, based on Hilbert Spaces, that was equivalent but much simpler that the previously stated methods. This mathematical foundation is currently the most commonly used in the field of Quantum Computation and it will be used throughout this document. This mathematical notation also provides a level of abstraction to the fundamental physics underlying it. So, the same mathematical machinery can represent the spin of a particle or the angle of an electromagnetic field or any other physical object with quantum properties.

Von Neumann stated that both representation of quantum mechanics could be unified into an infinite Hilbert Space. Rieffel and Polak [Rieffel and Polak (2011)] explained that since the Schrödinger equation 1.1 is linear, the set of solutions expands to a complex vector space that also has an inner product. Von Neumman realize that with infinite dimensions, the set of solutions describes a complex Hilbert Space[2]. We call such space the *state*

[1] It is worth to mention that although this theory was correct, it lead to many errors when used.

[2] Usually, an infinite dimensional space is not needed in the field of Quantum Compu-

space.

Definition 2.1.1 *A complex Hilbert Space $\mathcal{H}$ is a complete complex vector space with an inner product*

$$\langle \cdot, \cdot \rangle \colon \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

that satisfies the following conditions:

- Positive*:* $\langle v, v \rangle \geq 0$.
- Nondegenerate*:* $\langle v, v \rangle = 0 \iff v = 0$.
- Linear*:* $\langle ax_1 + bx_2, y \rangle = a\langle x_1, y \rangle + b\langle x_2, y \rangle$.
- Symetric*:* $\langle x, y \rangle = \overline{\langle y, x \rangle}$.

Given the fact that a *state space* S is an inner product space, it is also a norm space with norm

$$\|v\| = \sqrt{\langle v, v \rangle}$$

In addition, since it is a norm space we have that it is also a metric space with a metric given by

$$d(v, w) = \|v - w\|$$

where $v, w \in S$. The proof to these statements can be found in [Klipfel and Bons (2009)].

When working in the field of Quantum Mechanics, it is common to use the Dirac Notation to represent vectors and other mathematical operations. This notation was introduced by Paul Dirac in 1939 [Dirac (1939)] as a way to simplify and unify the notation used at that time. We present the equivalence to vectors and matrices as they are the most common representation but this notation is used when working with wave mechanics. In particular, Dirac presented the following ideas. A column vector $\vec{v}$ is represented as a *ket* $|v\rangle$ where v is just an arbitrary label. Its transpose conjugate is called a *bra* $\langle v|$. In the matrix representation, they represent row and column vectors, respectively.

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \qquad\qquad \langle v| = \begin{pmatrix} \overline{v_1}, \cdots, \overline{v_n} \end{pmatrix}$$

Given two vectors $|a\rangle$ and $|b\rangle$, their *inner product* is represented as $\langle a|b\rangle$ and formally defined as follows:

$$\langle a|b\rangle = \begin{pmatrix} \overline{a_1}, \cdots, \overline{a_n} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} \overline{a_i} b_i$$

tation.

Similarly, given two vectors $|a\rangle$ and $|b\rangle$, the *outer product* is represented as $|a\rangle\langle b|$ and formally defined as follows:

$$|a\rangle\langle b| = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1, \cdots, b_n \end{pmatrix} = \begin{bmatrix} a_1 b_1 & \cdots & a_n b_1 \\ \vdots & \ddots & \vdots \\ a_n b_1 & \cdots & a_n b_n \end{bmatrix}$$

Let us note that the outer product will be useful in order to represent transformations.

Given two Hilbert spaces V and W, the *tensor product* $\otimes\colon V \times W \to V \otimes W$ is defined for each par of kets $|\psi\rangle \in V$ and $|\phi\rangle \in W$ as follows:

$$|\psi\rangle \otimes |\phi\rangle \equiv |\psi\rangle\,|\phi\rangle \equiv |\psi\phi\rangle$$

Let us note that if V has dimension n and W has dimension m then $V \otimes W$ will have dimension $n \cdot m$. For example, we have

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \times 1 \\ 1 \times 0 \\ 0 \times 1 \\ 0 \times 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2.2. Quantum States

Just as the *state space* is the space of the set of solutions of the Schrödinger equation 1.1, a *quantum state* is the representation of a single solution within the Hilbert space of solutions. Formally, a quantum state is a *ray* in a Projective Hilbert Space $\mathcal{H}$, that is, a set of equivalence classes such that given two vectors $v, w \in \mathcal{H}$, we have

$$v \sim w \iff v = \lambda w$$

where the $\sim$ operator represents the equivalence between v and w and $\lambda \in \mathbb{C}$. Because there is no physical difference between vectors in the same equivalence class, it is common to add the constrain that a *quantum state* is a *unitary* vector in the Hilbert Space. In this case, there is no need to normalize later on when dealing with probabilities. A quantum state is usually represented by a ket $|\psi\rangle$ for some label ψ.

The usual representation of Euclidean Spaces considers a set of orthonormal vectors of the space. This set is called the *basis* of the space. In the case of Quantum Computation, it is common to use the *computational basis states* whose basic set of basis in matrix representation is:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

So, for any arbitrary state of the system $|\psi\rangle$ we have

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

with $a, b \in \mathbb{C}$. If $a, b \neq 0$ then we say that $|\psi\rangle$ is in a superposition of states $|0\rangle$ and $|1\rangle$.

Although we have mentioned the computational basis, it is worth to point out that this is not the only basis that it is used in Quantum Computation. In fact, we can always express any arbitrary state with respect to some orthonormal basis set $\{b_1, b_2, \cdots, b_n\}$ in the following way:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i\,|b_i\rangle$$

where $\alpha_i \in \mathbb{C}$.

There is an important property concerning the physical indistinguishability of apparently different states. Specifically, there is no distinction between the states $|\psi\rangle$ and $e^{i\phi}\,|\psi\rangle$. Therefore, we have

$$|\psi\rangle \sim e^{i\phi}\,|\psi\rangle$$

In this case, the term $e^{i\phi}$ is called a *global phase*. On the contrary, if we consider the states $|\psi\rangle$ and $a\,|0\rangle + e^{i\phi}b\,|1\rangle$ the we can distinguish them, that is, we have

$$|\psi\rangle \nsim a\,|0\rangle + e^{i\phi}b\,|1\rangle$$

In this case, the term $e^{i\phi}$ is called a *relative phase*.

We will use the notation explained in Section 2.1 to refer to the inner product of two states. Since any arbitrary state $|\psi\rangle$ must be a unit vector then we have

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} = \langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$$

We can expand the space by using the tensor product described in Section 2.1. As an example, if we have two independent systems $\mathcal{H}_1$ and $\mathcal{H}_2$, with n and m dimensions respectively, and their respective state vectors are $|\psi_1\rangle$ and $|\psi_2\rangle$, then we can represent both systems as $\mathcal{H}_1 \otimes \mathcal{H}_2$ with state vectors $|\psi_1\rangle \otimes |\psi_2\rangle$. Let us note that such union will extend its dimension up to $n \cdot m$.

In the literature, it is common to denominate state vectors as *qubits*. A qubit is a state of dimension 2 since it is the most basic unit of information possible in a quantum system.

2.2.1. Transformations

Transformations are a fundamental key part of Quantum Computing because they describe a way to manipulate quantum states and as such make

use of the computational advantages it brings us. This idea is very well described by the second postulate on Nielsen and Chuang's book [Nielsen and Chuang (2010)]:

> The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,
>
> $$\left|\psi'\right\rangle = U\left|\psi\right\rangle$$

A *close* quantum system is a system that does not interact with any other system. Although this is not really physically possible, there are very good approximations that make such a postulate still valid. Another thing to keep in mind is the fact that this evolution only describes changes of the system in discrete times. If we would like to consider a continuous representation, we must, once again, turn our attention to the Schrödinger Equation 1.1. In practice, in particular for the scope of this work, a discrete transformation is sufficient for the purposes of computation. The final key piece of information is the fact that transformations must be unitary.

Definition 2.2.1 *A* unitary tranformation U *is a mapping from a Hilbert space* $\mathcal{H}$ *onto itself* $U\colon \mathcal{H} \to \mathcal{H}$ *such that*

$$UU^\dagger = U^\dagger U = I$$

where $U^\dagger$ is the Hermitian adjoint. U must also be linear such that if we apply it to an arbitrary state we get $U\left|\psi\right\rangle = aU\left|0\right\rangle + bU\left|1\right\rangle$. More generally, for any orthonormal basis $\{b_1, ..., b_n\}$ we have

$$U(\sum_{i=1}^{n} \alpha_i \left|b_i\right\rangle) = \sum_{i=1}^{n} \alpha_i U\left|b_i\right\rangle$$

There are many transformations that are widely used in the literature. For example, we can mention the *Pauli operators*, which rotate the quantum system in one of the three possible dimensions for a 2-state system by π degrees. Their matrix representation is:

$$\sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.1}$$

Let us note that since these matrixes are unitary and Hermitian, they can be also used as measurements (see next section).

2.2.2. Measurements

Measurement in Quantum Mechanics (and other areas of Physics) are directly related to properties that we can observe, such as position and spin. This is what is known as an *observable*. In this field, an observable is represented by an Hermitian Operator M whose spectral decomposition is the following

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. Before any measurement is done, the probability of getting the result m for some state $|\psi\rangle$ is given by the following expression:

$$p(m) = \langle\psi| P_m |\psi\rangle \tag{2.2}$$

and the resulting state of such measurement ends up being:

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

This mathematical notation is trying to express the results of the Stern-Gerlach experiment and the variations of it. For example, we can define the two discrete bands shown in the experiment as $+1$ and -1 with respect to a center 0 on the z axis. Then, in order to describe the measurement, we have $M_Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, whose eigenvalues are $+1$ (with eigenvector $|0\rangle$) and -1 (with eigenvector $|1\rangle$). Actually, the solution to M_Z gives out eigenspaces $\lambda_0 |0\rangle$ and $\lambda_1 |1\rangle$ but they are equivalent to $|0\rangle$ and $|1\rangle$. It can be seen that there is a direct correlation between the possible results of the experiment and the eigenvalues corresponding to the observer M_Z. When measured, the probability of finding, for example, $+1$ on some state $|\psi\rangle = a|0\rangle + b|1\rangle$ is equal to

$$\begin{aligned} p(+1) &= \langle\psi|0\rangle\langle 0|\psi\rangle \\ &= (\overline{a}\langle 0| + \overline{b}\langle 1|)|0\rangle\langle 0|(a|0\rangle + b|1\rangle) \\ &= (\overline{a}\langle 0|0\rangle + \overline{b}\langle 1|0\rangle)(a\langle 0|0\rangle + b\langle 1|1\rangle) \\ &= |a|^2 \end{aligned}$$

In addition, the state reached after we get the result $+1$ is

$$\frac{|0\rangle\langle 0|(a|0\rangle + b|1\rangle)}{\sqrt{a^2}} = \frac{a|0\rangle}{a} = |0\rangle$$

Let us note that after the measurement, there is no information about the previous state and there is no possible way of restoring it, other than

executing the same transformations once again. Given an observable M, let a_i be all the possible result measurements, that is, all the eigenvalues of M. We denote the average value of M by

$$\langle M \rangle = \sum_i a_i p(a_i)$$

where $p(a_i)$ is the corresponding probability with regard to some state $|\psi\rangle$.

2.2.3. Pure and Mixed States

Section 2.1 describes the usual mathematical representation of a *pure* system, that is, a system such that we have all the information. This might seem contradictory since some of the most crucial ideas of Quantum Mechanics say that the measurement of the system is probabilistic and, as such, we cannot know the complete information of such system. However, what the concept of purity tries to describe is the certainty that the state vector describes the whole system in $\mathcal{H}$. However, we might have, as a result of noise or whatever external factor, a *mixture* of states such that we might have a state $|\psi_1\rangle$ with probability p_1 and a state $|\psi_2\rangle$ with probability p_2. Keep in mind that such probabilities only describe our lack of information about the complete system and are not a result of quantum mechanical measurements. The set $\{p_i, |\psi_i\rangle\}$ of all the possible states is called an *ensemble of states*. We describe such systems by using a mathematical tool called *density matrices*.

Definition 2.2.2 *Given an ensemble of states* $\{p_i, |\psi_i\rangle\}$, *where* $\sum_i p_i = 1$, *we define a* density matrix ρ *as*

$$\rho = \sum_i p_i \, |\psi_i\rangle \, \langle\psi_i|$$

Next, we enumerate some simple properties of this type of states. The evolution of the state described by ρ by some unitary operator U is given by

$$\rho' = U \rho U^\dagger$$

The probability of a measurement of the state described by ρ is given by the trace of the projection of such measurement

$$p(m) = tr(M_m M_m^\dagger \rho)$$

Where the trace of a matrix is the sum of the elements of its diagonal $tr(\rho) = \sum_i \rho_{ii}$. In addition, the state resulting after a measurement is

$$\frac{M_m \rho M_m^\dagger}{p(m)}$$

A simple way to distinguish pure from mixed states consists in taking the trace of ρ^2 such that $tr(\rho^2) = 1$ for pure spaces and $tr(\rho^2) < 1$ for mixed. The trace is *invariant* to a change of basis characterized by P. So, given a density matrix ρ we have

$$tr(\rho) = tr(P\rho P^\dagger)$$

Such density matrix also admits a decomposition over an orthonormal basis $\{|x_i\rangle\}$ for the eigenvectors and eigenvalues of ρ, that is,

$$\rho = \sum_i \lambda_i |x_i\rangle \langle x_i|$$

Finally, note that we can *purify* a density matrix to a pure state in a higher Hilbert space $H = H_\rho \otimes H_P$, where H_P is the purification space. Then $|\psi\rangle_{AP}$ is given by

$$|\psi\rangle_{AP} = \sum_i \lambda_i |x_i\rangle \otimes |P_i\rangle$$

where $|P_i\rangle$ conform an orthonormal basis for the space H_P.

Chapter 3

Formal Definition of Quantum Systems

Quantum systems, even simple ones, are very prone to errors. Not just by the implicit difficulty that comes from noise and external influences but also from the complexity that involves the development of quantum algorithms. In order to ensure the quality and the correct working of such quantum systems and algorithms Quantum Tl;esting acquires a very important role. It is common in classical testing to differentiate between black-box and white-box scenarios. In a white-box scenario the internal structure of the machine, algorithm or device generally called system under test (SUT), that we are testing is visible. For example, we might have access to the code of a software system. Quantum systems add even more constrains in this scenario, even if we can know the transformations that occur inside the machine we cannot check the result of each one since any measurement will irremediably destroy the state of the system. Black-box scenarios, quantum or classical, do not allow the tester to see inside the SUT and the only possible interaction with the machine are through its inputs and outputs. In our case, we distinguish between black and white box scenarios by taking into account whether we know the transformations and measurements done to the system, even though we cannot see how the state is transformed. In order to describe systems, we will introduce a formalism that we call *N-Hybrid Turing Machine* where we combine classical and quantum versions of the usual Turing machine formalism.

3.1. Preliminaries

Quantum computation can be seen as the ability to transform quantum systems in order to solve a problem. In that sense, we can take advantage

of the laws of quantum mechanics to craft algorithms such as superposition and entanglement. However, the only way to interact with such systems must be purely classical. For example, we can find the exposition time we need to change a particle in one state to another using a concrete type of microwave. However, the exposure of the particle to such wave is a classical iteration, regardless of its final quantum effect on the particle. With this in mind, any machine that transforms a quantum system must in fact be driven by a classical setting. The most common tool we have to describe classical computers is the well-known Turing Machine [Turing (1936)] formalism.

It consist in an infinite tape divided by cells. Each cell can contain a symbol from a set Σ or a blank symbol b. The machine also contains a head that points to a cell and can read and write the symbol in the cell. It can also move right or left, denoted by $\{R, L\}$. The machine also has a set of internal states Q, with one initial state q_0 and a set of final states Q_F. Initially, all the cells are blank but the ones that contains the input string $x \in \Sigma^*$. The head also points to the cell with the first symbol of the string. There also exists a transition function (the program) that takes a state and a symbol and returns a state, a symbol, and the direction the head is going to move next. Extracted from the book of Hopcroft and Ulllman [Hopcroft and Ullman (1979)], we can formally define a Turing Machine as follows.

Definition 3.1.1 *A* Turing Machine (TM) *is a tuple*

$$\langle Q, \Gamma, b, \Sigma, \delta, q_0, Q_F \rangle$$

where

- Q *is the set of states*
- Γ *is the set of tape symbols*
- $b \in \Gamma$ *is the symbol representing an empty cell*
- $\Sigma \subseteq \Gamma \setminus \{b\}$ *is the set of input symbols*
- δ *is a partial function* $\delta \colon Q \times \Gamma \to Q \times \Gamma \times \{R, L\}$ *called the transition function*
- $q_0 \in Q$ *is the initial state*
- $Q_F \subseteq Q$ *is the set of finals states.*

Intuitively, the head of the machine will read the first symbol of the string $\alpha \in \Sigma$ and will pass it to the function $\delta(q_0, \alpha)$, which will give out the next state q, some symbol $\beta \in \Sigma$ and some direction $X \in \{R, L\}$. The head will write β in the current cell and will move in the direction X and read the next cell. Eventually, we might arrive to a state q_c while processing a symbol for

which δ might not be defined. In this case, the machine halts. If the current state is a final state $q_c \in Q_F$, then the input string is said to be accepted. Otherwise it is rejected. After all the changes, there is a finite string left in the tape. We will consider it to be the output string.

In his paper, Alan Turing shows the existence of what is known as a *Universal Turing Machine*. Such machine should be able to simulate every other Turing Machine. However, with the arrival of Quantum Mechanics physical systems of such nature could not be simulated due to it's exponential growth and other laws such as entanglement. In 1985, David Deutsch published a paper presenting an alternative, more powerful, model of computation that could simulate such system [Deutsch and Penrose (1985)]. This model is now called a *Quantum Turing Machine*.

3.2. Quantum Turing Machines

The motivation for building a Quantum Turing Machine (QTM) is to be able to simulate physical phenomena that otherwise cannot be efficiently computed, for example, quantum systems. Quantum Turing Machines use the properties of quantum systems to compute a function f. As such, the machine is represented as an element of some Hilbert Space. The formal definition for a Quantum Turing Machine [Ozawa (2002)] is the following.

Definition 3.2.1 *A* Quantum Turing Machine (QTM) *is a tuple*

$$\langle \xi, Q, T, \Sigma, q_0, Q_f, U \rangle$$

Where

- $\xi \in \mathbf{Z}$ *represents the head of the machine and* $\mathcal{H}_\xi$ *is the operating space for the head of sufficient dimension.*
- Q *is the set of states of the machine and* $\mathcal{H}_Q$ *is the operating space for the processor of dimension* $\log_2(|Q|)$.
- $T \in \Sigma$ *is the infinite string from the finite set* Σ *and* $\mathcal{H}_T$ *is the operating space for the memory of infinite dimension of which only a finite amount is used.*
- *The initial state* q_0.
- *The final set of states* Q_F.
- *The transition operator* U *that acts on* $\mathcal{H}_\xi \otimes \mathcal{H}_Q \otimes \mathcal{H}_T$.

And the system is represented by the state

$$|\xi\rangle \otimes |q\rangle \otimes |T\rangle$$

The system changes according to some unitary operator U that can only change $|\xi\rangle$ by one unit. Initially, all the states of the system are set to 0 (or the ground state) with the exception of some finite section of the memory, which will hold the program or function and its arguments. We will represent the codification of the program that calculates the function f as $\pi(f) \in \Sigma^*$. Then, the initial state of the system is:

$$|0\rangle |q_0\rangle |\pi(f), i, \mathbf{0}\rangle$$

where $\mathbf{0}$, for simplification purposes, represents a string of qubits in the ground state. The idea is that the memory holds the program and arguments and the processor is used to hold the state of the machine. By applying U until the machine halts we compute the function. One of the main problems is to identify when the machine has finished. As usual when dealing with quantum systems, if we would perform a measure then we would destroy the computations if there were not finished. To solve this problem, we set aside a qubit in the processor to indicate whether the machine has halted or not. This qubit would always be in the ground state until it has finished. Therefore, we can measure it repeatedly without effecting other qubits. The system would then be

$$|0\rangle |0, q_0\rangle |\pi(f), i, \mathbf{0}\rangle$$

Another important notion is the fact that U must be unitary according to the laws of quantum mechanics (Def. 2.2.1) and as such it must be reversible. That means that operations cannot destroy information of the machine. Following these rules, and executing the machine until it halts, the final state would be

$$|\xi'\rangle |1, q_f\rangle |\pi(f), i, f(i) \oplus \mathbf{0}, \mathbf{0}\rangle$$

Where $q_f \in Q_f$. Once we know that the machine has finished, we can make a measurement on the state in order to get the final result. Such result would be classical and bound to some labels in Σ. This result is also probabilistic, since measurement in quantum mechanics can give a random result from a set of superposed states (Def. 2.2).

An equivalent, but significantly easier, model of computation for quantum mechanics is the *Quantum Circuit* (QC). Just as in the classical counterpart each qubit of the system is expressed as a line or cable and for each transformation we use a box with the label in it (in this setting, they are called gates). Next we briefly introduce this formalism.

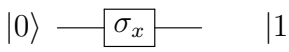
Definition 3.2.2 *A* Quantum Circuit *is a sequence* $[U_1, \ldots, U_n]$ *of Quantum transformations* U_i *(called gates) applied to an initial quantum state* $|\psi\rangle$ *such that the final state* $|\psi'\rangle$ *is*

$$|\psi'\rangle = U_n \cdot \ldots \cdot U_1 |\psi\rangle$$

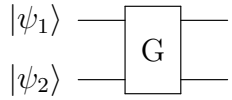
Quantum circuits have a graphical representation that makes its use easier than a QTM. For example, let us suppose that we have a system in the state $|0\rangle$ and we apply the transformation expressed as the Pauli operator σ_x (see Equation 2.1). In this case, the final result would be:

$$\sigma_x |0\rangle = |1\rangle$$

The equivalent quantum circuit would be the following:



where time goes from left to right. If a gate G is executed over two qubits, then we represent it as



The previous system allows us to program a quantum computer in a similar fashion as we would construct a classical circuit. In this scenario, the input state is always bound, usually to the ground state $|0\rangle$, and the input string $x \in \Sigma^*$ codifies the gates applied to the system . In addition, for each symbol $\alpha \in \Sigma$ there exists a unique gate U_α. This formalism has the same computational power as a QTM [Chi-Chih Yao (1993)].

3.3. N-Hybrid Turing Machines

In theory, all we would need to simulate any system, quantum or classical, would be a QTM. However, due to the difficulty of the development of quantum physical systems and quantum algorithms, the current approach to quantum computing is an hybrid model, where part of the calculations are done in a classical computer and only the heavy tasks are delegated to the quantum system. An effort made in this direction was to allow QTMs to observe each computational step [Perdrix (2011)]. Here, we present a weaker but simpler hybrid model of computation that closes the gap between the theoretical approach of QTMs and the physical realizations. In addition, we think that this formalism can be taken as initial step to introduce, in future work, a complete testing framework.

Definition 3.3.1 *An* N-Quantum Classical Hybrid Turing Machine ($QC - HTM_N$) *is a tuple*

$$\langle T_1, Q_1, \cdots, T_N, Q_N \rangle$$

where each T_i is a classical Turing machine, each Q_i is a quantum Turing machine and we have the following conditions:

- *For every output string $y \in \Sigma^*_{T_i}$,there exists a one to one label transformation $f : \Sigma^*_{T_i} \to \Sigma^*_{Q_i}$ such that $f(y) \in \Sigma^*_{Q_i}$ is the input string of Q_i*

- *For every measured output string $w \in \Sigma^*_{Q_i}$ there exists a one to one label transformation $g : \Sigma^*_{Q_i} \to \Sigma^*_{T_{i+1}}$ such that $g(w) \in \Sigma^*_{T_{i+1}}$ is the input string of T_{i+1}*

- *An input string $x \in \Sigma^*_{T_1}$ is accepted iff each input string (transformed under some labels) of T_i and Q_i are accepted.*

For the sake of simplicity, we will assume that the labels in the outputs and input machines are the same. So, for all $\alpha \in \Sigma_{T_i}$ we have $f(\alpha) = \alpha$ and for all $\alpha \in \Sigma_{Q_i}$ we have $g(\alpha) = \alpha$. The idea is to connect machines using its inputs and outputs. Informally, this model describes a system in which we do $2N$ steps of computation alternating classical and quantum. This resembles closely to how quantum computers are thought of work. Heavy intensive tasks that can not be done classically must be done in quantum computers but everything else, although possible to do in a quantum system is easier (and cheaper) to do in a classical one. The idea is, at some time of the computation, a computer receives some classical input that drives the computation or describes the program to be computed then, after the machine halts, the result of the computation is passed as the input of the next machine thus connecting one another. This approach allows the creation of complex machines that can closely resemble the new paradigm of computation. The model presented in Definition 3.3.1 is a specific case of such type of interconnected machines. One could imagine the same framework to be applied to any kind of Turing Machine that has an input and a output such that the latter could be used as input of the next machine. Next, we formally introduce a formalism according to this idea.

Definition 3.3.2 *An* Abstract IO Machine *(AIOM) is an element from the set of classes of Turing Machines that satisfy the following criteria*

- *It has an input alphabet Σ_I and an output alphabet Σ_O.*

- *It can accept or reject every input string $x \in \Sigma^*_I$ and generate some output string $y \in \Sigma^*_O$.*

An AIOM can be any kind of machine that has an input and a output, such as classical normal Turing Machines, Quantum Turing Machines, Probabilistic Turing Machines, etc. This allows us to generalize the notion of QC-HTM for all these types of machines.

Definition 3.3.3 *An* N-Hybrid Turing Machine (HTM_N) *is a tuple of N AIOMs*

$$\langle M_1, \ldots, M_N \rangle$$

such that

- *For every output string* $y \in \Sigma^*_{O_i}$ *there exists a one to one label transformation* $\delta : \Sigma_{O_i} \to \Sigma_{I_{i+1}}$ *such that* $\delta(y) \in \Sigma_{I_{i+1}}$ *is the input string of* M_{i+1}.
- *An input string* $x \in \Sigma_{I_1}$ *is accepted iff each input string (transformed under some labels) of* M_i *is accepted.*

This definition also allows to change the order of the QC-HTM and start and end on the same machine. Note that in a QC-HTM we could simply assume that the last machine or the first one does not modify the output at all but this scenario is better handle by an HTM.

Chapter 4

Self Testing

The growth of Quantum Computing brings some of the most interesting promises and theoretical results in our era. As a consequence, the fields of cryptography and securing information had to find a way to work within the quantum framework. In 1984, Bennett and Brassard presented the first protocol for a secure public key distribution protocol in a quantum setting [Bennett and Brassard (1984)]. In that protocol, Alice sends qubits to Bob in one of two possible measuring basis (e.g. the computational basis $\{|0\rangle, |1\rangle\}$ and the Fourier basis $\{|+\rangle, |-\rangle\}$). When received, Bob measures those qubits with a random choice of the two posible basis. Alice and Bob share in a public manner the basis that they use and discard all the results where the basis do not match. A subset of the results with the same basis is then made public. With very high probability, if some results are not equal to each other we can know that a third party has been eavesdropping. Otherwise, the set of results that reminds private would be the key shared by Alice and Bob. It should be noted that such protocol, as many others, heavily rely on the fact that the measurement devices can be trusted. Challenging such assumption, Mayers and Yao proposed and coined the procedure known as *Self testing* [Mayers and Yao (2004)].

4.1. The Self Testing Scenario

Let us suppose that we have some device that is said to produce an entangled state $|\psi\rangle$ in a system with two particles. One of these particles is send to Alice and the other one to Bob. Both of them are really far away from each other and they both have some measuring apparatus with some classical settings x for Alice and y for Bob. Due to the distance they cannot communicate their choice of settings but they can share, after a while, the results that they have found. Each of these results is a classical value, denoted by a for Alice and b for Bob. With all this information they can

generate a probability distribution for each possible combination of settings. Informally, *Self Testing* refers to the procedure in which we can determine which state the source is producing only from each probability distribution with respect to the settings.

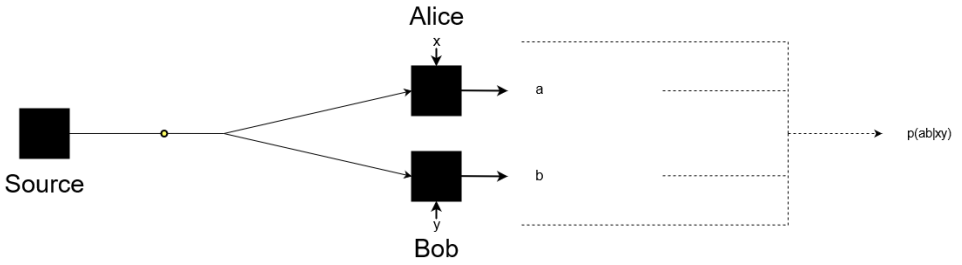


Figure 4.1: Diagram of the Self testing Scenario

It should be noted that not all the states can be uniquely determined by their probability distribution. Thus, only certain sources (those who generate those special states) can be self tested. One important class of states (and measurements) that can be self tested are those that violate *Bell's inequality*. Due to their practical uses, such states are the most commonly found in the self testing literature.

4.2. Bell's Locality

When the theory of Quantum Mechanics started to gain popularity, scientist like Albert Einstein [Einstein et al. (1935)] did not like some of its implications, in particular, the concept of *entanglement*. Let us consider the state

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

on some Hilbert Space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Let us suppose that each Hilbert space belongs to Alice and Bob respectively such that

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$$

where $|x\rangle_A$ represent the qubit of the system belonging to Alice and $|x\rangle_B$ the qubit belonging to Bob. If Alice were to measure her local system with some set of measurements $M_z = \{M_0, M_1\}$ and got the result 0 then, at the same moment, Bob's system would collapse into the state 1 and viceversa. The idea that the collapse of Bob's system would happen faster than light could travel to that system was shocking at the time (in fact, it still is) and Albert Einstein, Boris Podolsky and Nathan Rosen proposed a new way to interpret such result [Einstein et al. (1935)]. They argued that the wave

function did not collapse into one or another state when measured but instead there existed a set of *hidden variables* λ such that when those particles were generated, they already had a deterministic, but unknown to us, result and measurement was just a way of discovering such result. The key idea is that in both interpretations there appeared to be no way of knowing what is happening when a particle is measured and both could predict the correct results after measurement.

In 1964, John Bell proposed a way to physically test whether the hidden variable interpretation was correct [Bell (1964)]. Let us imagine that a source emits a pair of particles and each particle is given to Alice and Bob, respectively. Alice can now measure her particle in one of these settings x and Bob can do the same with his particle y. The possible outcomes of each measurement are denoted by a, in the case of Alice, and by b, in the case of Bob. By making some measurements and assuming that the source always emits the same particle, experimental results have found that

$$p(ab \mid xy) \neq p(a \mid x)p(b \mid y)$$

This result implies that the particles seem to not be independent from each other. The idea of *locality* can be expressed in the following way.

Definition 4.2.1 *The set of correlations $p(ab \mid xy)$ is said to be* local *if there exists a* hidden variable λ*, with probability distribution $q(\lambda)$, such that*

$$p(ab \mid xy) = \int_\Lambda q(\lambda)p(a \mid x, \lambda)p(b \mid y, \lambda)d\lambda \tag{4.1}$$

The notion of $q(\lambda)$ is included to take into account physical properties that are not fully controllable. Let $\langle a_x b_y \rangle$ denote the average value of ab for some xy, that is, the value $\sum_{a,b} ab \cdot p(ab \mid xy)$. Then, let us consider the *CHSH inequality* [Clauser et al. (1969)]:

$$\langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2$$

This inequality holds when a set of correlations is local but there are some states that are not and the result is known as a violation of Bell's inequality. The proof of this result can be found in [Brunner et al. (2014)]. For example, let us consider the state $|\phi^-\rangle$ and the measurements $A_0 = \sigma_z \otimes I$ and $A_1 = \sigma_x \otimes I$ for Alice and the measurements $B_0 = I \otimes \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$ and $B_1 = I \otimes \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$ for Bob. The average value of $\langle a_z b_z \rangle$ is equal to $\frac{1}{\sqrt{2}}$. In this case, the CHSH inequality can be rewritten as

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

If we compute the average value for each term we get

$$\langle A_0 B_0 \rangle = \langle A_0 B_1 \rangle = \langle A_1 B_0 \rangle = \frac{1}{\sqrt{2}} \qquad \langle A_1 B_1 \rangle = -\frac{1}{\sqrt{2}} \tag{4.2}$$

Then, the CHSH inequality ends up being

$$\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = 2\sqrt{2} \not\leq 2$$

that clearly violates the CHSH inequality, proving the non locality of the correlations found. This result is one of the most amazing results in Quantum Mechanics because it does not only provides a method for practical testing of non-locality but it also certifies the quantum properties of entanglement, one of the most useful tools in Quantum Computing. This results also give us a simple method to check, only using a set of correlations and measurements as the device-independent scenario, the problems found in Section 4.1. Since entanglement is a unique quantum property that can violate Bell's inequality, any non-local system must be a quantum system and as such we can test other properties of it.

One key point of finding the violation of a Bell's inequality is the choice of measurements. In fact, only local *anticommuting observables* can lead to the maximal violation of Bell's inequalities. The proof of this statement can be found in [Šupić and Bowles (2020)].

4.3. Formal Definition of Self Testing

The main result found by Mayers and Yao was that for specific states, such as those that violate Bell's inequalities, we can certify that a source is in fact generating quantum states in such state. More importantly, it does it in a black-box device independent scenario with nothing but the correlations between the settings and the results. Given an ideal setting, that is, a state $|\phi\rangle$ and some projective measurements for Alice and Bob $P_{a|x}$ and $P_{b|y}$, the actual probability distribution found by running the experiment multiple times with all the possible settings $\tilde{p}(ab|xy)$ is said to *self test* the machine if we have

$$\tilde{p}(ab|xy) = p(ab|xy) \tag{4.3}$$

up to a local change of basis. The probability distribution $p(ab|xy)$ represents the ideal probability distribution that is found with the ideal state $|\phi\rangle$ and the local projective measurements. There are a couple of constraints that must be taken into account and complicate Expression 4.3. Since we are working in a device independent scenario, we cannot rule out different degrees of freedom happening inside the machine. Another constraint is the fact that the ideal measurements are defined with respect to some basis [McKague et al. (2012)]. In order to solve these difficulties, we need to ensure that there exists an *isometry* that can extract the ideal state from the physical one. The next two definitions are taken from [Šupić and Bowles (2020)] and were presented in the context of self testing in [Mayers and Yao (2004)].

Definition 4.3.1 *Given two Hilbert spaces $\mathcal{H}_{S_1}$ and $\mathcal{H}_{S_2}$, an* isometry *is any linear transformation from $\mathcal{H}_{S_1}$ to $\mathcal{H}_{S_2}$ that preserves the inner product.*

If we work in the self testing scenario presented in Section 4.1, we need the concept of local isometry.

Definition 4.3.2 *Given two Hilbert spaces $\mathcal{H}_{S_1}$ and $\mathcal{H}_{S_2}$, a* local isometry *is a tensor product of isometries acting locally, that is,*

$$\Phi_A \otimes \Phi_B : \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} \to \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$$

Let us remind that, in order to take into account different degrees of freedom, the spaces $\mathcal{H}_{S_1}$ and $\mathcal{H}_{S_2}$ can have different dimensions. Once we have the concept of isometry, we are ready to give a complete description of self testing.

We have seen in Section 4.2 that given some probability distribution we can test whether the devices act in a non local way and thus share an entangled state. What self testing attempts to do is to find the actual entangled state and its measurements from the correlations alone. The key to self testing is to find the isometry that can extract from the physical state $|\psi\rangle$ embedded in a higher space the reference state $|\phi\rangle$ tensor with some junk state. The formal definition is as follows.

Definition 4.3.3 *The correlations $p(ab|xy)$* self test *the state $|\phi\rangle$ if for any state $|\psi\rangle$ and measurements $\{M_{a|x}\}$ and $\{N_{b|y}\}$, compatible with the correlations $p(ab|xy)$, there exist local isometries Φ_A and Φ_B such that*

$$\Phi_A \otimes \Phi_B(|\psi\rangle) = |\phi\rangle \otimes |\xi\rangle$$

for some junk state $|\xi\rangle$.

The main idea of self testing is to prove the existence of such isometry. By revealing the maximal violation of some Bell's inequality, we can ensure the anticommutativity of the local measurements and build the isometry. Given some unknown measurement operators M_x and N_y, for Alice and Bob respectively, that lead to the maximal violation of some Bell's Inequality, we can build the Unitary controlled operators Z_A, Z_B and X_A, X_B as follows

$$Z_A = \frac{1}{\sqrt{2}}(M_0 + M_1) \qquad Z_B = \frac{1}{\sqrt{2}}(M_0 - M_1)$$
$$Z_B = N_0 \qquad X_B = N_1$$

Using these gates, we can build the so-called *partial swap gate* isometry (see Figure 4.2).

The input of the isometry would be the state compatible with the correlations (the state generated by the source) embedded to a higher space

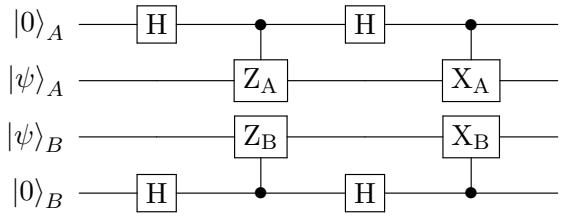


Figure 4.2: Circuit of the partial swap gate isometry

which is represented as two states in the ground state. The output of the gate would be the state we wanted to self test $|\phi\rangle$ and some other junk state $|\xi\rangle$. It is important to notice that the output states are separable and as such we can ignore the junk state. The proof of this statement can be found in [McKague et al. (2012)] and a more explicit explanation can be found in [Šupić and Bowles (2020)]. Let us emphasize that there is no need to actually execute the isometry in order to self test the state: it is enough to prove its existence. This means, in particular, that by knowing the correlations and the fact that a violation of a Bell's inequality exists, one can know whether a certain state is being generated by the source by means of the partial swap gate.

4.4. Experimental Results

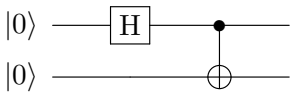
In order to show the advantages of self testing, next we present some real experiments and a step by step. These experiments are developed using qiskit, a python library developed by IBM [Gambetta et al. (2021)] and executed locally in an MSI-Modern 14, running an Intel Core i7 processor and 16 GB of RAM.

We will be working in the scenario where Alice and Bob has settings $x = 0, 1$ and $y = 0, 1$. The output for both of them, in all settings, will be $a, b = \pm 1$. The first part will follow the same example as the one presented in Section 4.2. Because we are working in a device independent scenario, and as such it is a black box scenario, when simulating the scene we must break such assumption and give a formal description of the inner workings of the source. However, we can later ensure that the calculations made by Alice and Bob have no knowledge of the source.

In our case, the *source* is described as a quantum circuit that can be embedded in other circuits. The formal specification in this example would be the entangled state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4.4}$$

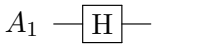
This can be presented, using the computational basis, as the following circuit:



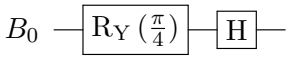
Now, given some setting x and y, the *measurement* operators for Alice and Bob are the following:

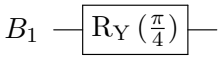
$$A_0 = \sigma_z \qquad A_1 = \sigma_x$$
$$B_0 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \qquad B_1 \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z)$$

However, qiskit only allows to measure in the computational basis σ_z. Thus, if we need to measure in a different basis, we need to transform the state to that basis and then measure in the computational basis. In this running example, the circuit transformations are the following:



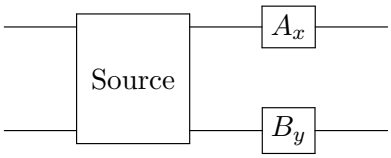
(4.5)





(4.6)

Finally, considering the *self testing scenario*, the final circuit represented in a black box scenario would be:



Let us note that Alice and Bob only act on their share of the state and as such they are working independently from each other.

Once we have a practical way of representing and executing the scenario, we can run the experiments multiple times (executing the circuit), with all possible combinations of x and y with the goal of computing the correlations $p(ab|xy)$. Specifically, for each setting we transform the circuit given in Equation 4.5 and execute it 1.000.000 times to get a set of correlations the most accurate possible. The loop is executed with the seed 1 by qiskit so that the results can be replicated. An interesting result is that the correlations end up being equal to each other due to how qiskit executes the circuit with a seed rather than a more pseudo-random run. The results of our experiments are described in table 4.1.

These correlations allow us to compute the averages for $\langle A_x B_y \rangle$. We can use these values to check whether they maximally violate some Bell's Inequality.

$$\langle A_0 B_0 \rangle = 0.706462 \qquad \langle A_0 B_1 \rangle = 0.706462$$
$$\langle A_1 B_0 \rangle = 0.706462 \qquad \langle A_1 B_1 \rangle = -0.707162$$

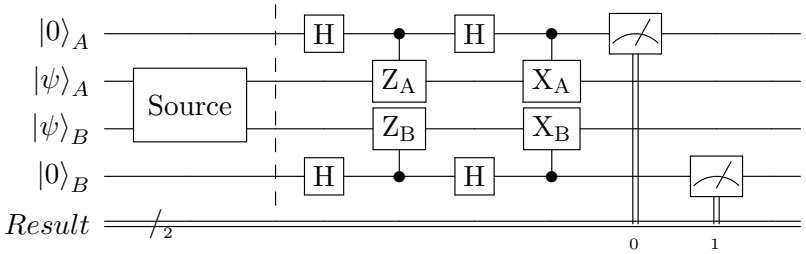
$(x,y)/(a,b)$	$(+1,+1)$	$(+1,-1)$	$(-1,+1)$	$(-1,-1)$
$(0,0)$	0.426035	0.07341	0.073359	0.427196
$(0,1)$	0.426035	0.07341	0.073359	0.427196
$(1,0)$	0.426035	0.07341	0.073359	0.427196
$(1,1)$	0.07313	0.426315	0.427266	0.073289

Table 4.1: Correlations $p(ab|xy)$

We can see that the averages get really close to the theoretical averages given in Equation 4.2. So, unsurprisingly when calculating the CHSH inequality, we get

$$\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle = 2.826548 \approx 2\sqrt{2} \not\leq 2$$

From this we can deduce that the particles generated by the source violate Bell's locality and as such they must be entangled. In order to self test that the source generates states in the form of Equation 4.4, we need to find an isometry that can extract the state $|\phi\rangle$ from any state compatible with the correlations of table 4.1. In this case, since we have observed the maximal violation of the CHSH inequality, we can use the isometry corresponding to the circuit given in Figure 4.2. The state generated by the source is by definition compatible with $p(ab|xy)$. Since we do not have access to the measurements A_x and B_y, there is no practical way, nor necessity, to actually build this isometry. However, for the sake of clarity, we will show that it actually works as expected. The corresponding circuit is



In addition, computing the probability distribution in the computational basis we get:

$$p(|00\rangle) = 0.499445 \quad p(|01\rangle) = 0 \quad p(|10\rangle) = 0 \quad p(|11\rangle) = 0.500555$$

which very closely approximates the state

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

just as we wanted to prove.

Chapter 5

Conclusions and Future Work

Quantum Computing opens the door for new and exciting approaches to testing, while black-box scenarios gain even more importance given how the laws of quantum mechanics and, more specifically measurements, work. In this project, we first reviewed these laws and gave an introduction to the mathematical framework currently used in the field. Next, we introduced a new non-trivial model of computation that, although equivalent to a Quantum Turing Machine, allows a more detailed specification of systems. The future of quantum computers seems to be guided towards the use of classical computers for simple tasks along with the execution of computational expensive tasks in quantum computers and, as such, we hope that *Hybrid Turing Machines* can help to develop more specific testing methods in this framework.

The latter part of the project focused on an already developed testing framework for quantum systems in a black-box device-independent scenario called *Self Testing*. By analyzing the theoretical definitions, along with a practical experiment, we have concluded the effectiveness of this testing method and, more importantly, its applicability regardless the device and with very little information of the system. It is also a unique testing method for quantum systems and in the case of Bell states also acquires added robustness based on pure physical properties.

Quantum Computing is still constructing its foundations and most of the current research focuses on developing physical realizations of quantum computers and making them available for practical use. Testing of quantum system has a wide range of potential research lines. Self Testing sets the first stone in this path but there is still room for development of more testing methods. In this setting, Hybrid Turing Machines can facilitate the development of testing methods in a more structured and detailed way. Specifically, we think that they can be used to introduce a notion of *quantum conformance* where we can establish the conformance of a black-box with respect

to a certain specification given as a Hybrid Turing Machine. Additionally, it would be desirable to provide an alternative characterization of the conformance relation as a testing framework. In this case, it would be necessary to give a precise definition of concepts such as test, test application and successful/failed application of a test.

Bibliography

Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, Vol. 1, 195–200, 1964.

Bennett, C. H. and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175. India, 1984.

Bohr, N. On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, Vol. 26(151), 1–25, 1913.

Born, M. Quantenmechanik der stoßvorgänge. *Zeitschrift für Physik*, Vol. 38(11), 803–827, 1926. ISSN 0044-3328.

Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. and Wehner, S. Bell nonlocality. *Reviews of Modern Physics*, Vol. 86(2), 419–478, 2014. ISSN 1539-0756.

Chi-Chih Yao, A. Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, 352–361. 1993.

Clauser, J. F., Horne, M. A., Shimony, A. and Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, Vol. 23, 880–884, 1969.

Deutsch, D. and Penrose, R. Quantum theory, the church and turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, Vol. 400(1818), 97–117, 1985.

Dirac, P. A. M. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, Vol. 35(3), 416–418, 1939.

Einstein, A. Concerning an heuristic point of view toward the emission and transformation of light. *Annalen Phys.*, Vol. 17, 132–148, 1905.

Einstein, A., Podolsky, B. and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, Vol. 47, 777–780, 1935.

Gambetta, J., Treinish, M., Nation, P., Kassebaum, P., Rodríguez, D. M., qiskit bot, de la Puente González, S., Hu, S., Krsulich, K., Zdanski, L., Yu, J., McKay, D., Gomez, J., Capelluto, L., Travis-S-IBM, Gacon, J., Panigrahi, A., lerongil, Rahman, R. I., Wood, S., Bello, L., Drew, Schwarm, J., GEORGE, M., Marques, M., Hamido, O. C., RohitMidha23, Dague, S., Garion, S. and tigerjack. Qiskit/qiskit: Qiskit 0.25.2. Available at `https://doi.org/10.5281/zenodo.4707982`, 2021.

Hopcroft, J. E. and Ullman, J. D. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley Publishing Company, 1979.

Klipfel, J. and Bons, B. A brief introduction to Hilbert space and quantum logic. Available at `https://www.whitman.edu/Documents/Academics/Mathematics/klipfel.pdf`, 2009.

Mayers, D. and Yao, A. Self testing quantum apparatus. *Quantum Info. Comput.*, Vol. 4(4), 273–286, 2004. ISSN 1533-7146.

McKague, M., Yang, T. H. and Scarani, V. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, Vol. 45(45), 455304, 2012.

Nielsen, M. A. and Chuang, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

Ozawa, M. *Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting*, 241–248. Springer US, Boston, MA, 2002. ISBN 978-0-306-47097-4.

Perdrix, S. Partial observation of quantum turing machines and a weaker well-formedness condition. *Electronic Notes in Theoretical Computer Science*, Vol. 270(1), 99–111, 2011. ISSN 1571-0661. Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008).

Planck, M. On the Law of Distribution of Energy in the Normal Spectrum. *Annalen Phys.*, Vol. 4, 553, 1901.

Rieffel, E. and Polak, W. *Quantum Computing: A Gentle Introduction*. The MIT Press, 1st edn., 2011. ISBN 9780262015066.

Schrödinger, E. Quantisierung als Eigenwertproblem. *Annalen Phys.*, Vol. 384(6), 489–527, 1926.

Šupić, I. and Bowles, J. Self-testing of quantum systems: a review. *Quantum*, Vol. 4, 337, 2020. ISSN 2521-327X.

Turing, A. M. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, Vol. s2-42(1), 230–265, 1936. ISSN 0024-6115.

Von Neumann, J. *Mathematical foundations of quantum mechanics; 1st ed.*. Investigations in physics. Princeton Univ. Press, Princeton, NJ, 1955. Trans. of : Mathematische Grundlagen der Quantenmechanik.