UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Quantum key distribution and other related protocols

Autor: Joan Pau Condal Marco

Director: Dr. Luis Víctor Dieulefait
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 17 de gener de 2024

Contents

Abstract

The main goal of this work is to present an introduction to quantum computation and Quantum Key Distribution (QKD). The first chapter is dedicated to the basics of quantum mechanics needed to understand further concepts. Then the definition of quantum circuits is presented, along two examples: *Quantum teleportation* and the *Deutsch-Josza problem*.In the chapter about QKD, we will explain in detail the *BB84 algorithm* and some eavesdropping techniques, and we will take a look at the theory behind the *EPR Protocol*. Finally, we will explain the *CHSH Game*.

Resum

El propòsit d'aquest treball és presentar una introducció a la computació quàntica i a la distribució de claus quàntica (QKD). El primer capítol serà dedicat a explicar els conceptes bàsics de mecànica quàntica necessaris per entendre els conceptes posteriors. Després, es presentarà la definició de circuits quàntics, amb un parell d'exemples: la *teleportació quàntica* i el problema de *Deutsch-Josza*. En el capítol sobre QKD explorarem en detall l'algorisme *BB84*, i explorarem la teoria que hi ha darrere del *Protocol EPR*. Finalment, explicarem el *joc CHSH*.

2020 Mathematics Subject Classification. 81P48, 81P94

Acknowledgements

I would like to express my gratitude to my supervisor, Dr. Luis Víctor Dieulefait, who guided me through this journey, offered me lots of useful resources to start researching about the topic and was there to guide me at all times, always with his kindness.

To my friends, thanks for making this journey through college so full of beautiful moments. I had the most wonderful time thanks to you and I would not be here today if it weren't for all the encouragement I recieved during all these years.

To my family, my parents and siblings, thanks for all the love and support you have given me always.

Chapter 1

Introduction

Cryptography is the study of communication in the presence of adversaries [21], and can be traced all the way back to Ancient Egypt, when in the year 1900B.C. an inscription was carved using non-common hieroglyphics instead of the ordinary ones [18]. Since then, cryptography has evolved and played an important role in the history of communication. With the invention of computers in the first half of the 20th century, the *modern age of cryptography* began.

During the second half of the 20th century, modern age cryptography was dominated by *symmetric key* algorithms. In 1997, a symmetric-key algorithm named *Data Encryption Standard* (DES) became the standard to be used for Federal departments and agencies of the United States, to encrypt non-classified data [19]. These types of algorithms used the same key $\mathcal{K}$ to both encrypt and decrypt the data, and therefore the two parties communicating needed to have an exact copy of that key. That posed the problem of *key distribution*, i.e., how would the two parties obtain the copy of the key.

The problem of creating a secure private key was solved in November 1976, when Whitfield Diffie and Martin Hellman presented a new protocol named *Diffie-Hellman key exchange*, where a public key could be used in order for two parties to obtain an identical secret key. This started a new set of cryptographic algorithms named *asymmetric-key* cryptography. A notable example of an asymmetric-key algorithm was introduced the following year by Ron Rivest, Adi Shamir and Leonard Adleman, named *RSA*. The public key in the RSA algorithm is created with two numbers: the modulus and the exponent. The modulus is a number obtained by multiplying two - and only two - large prime numbers. The security of the RSA algorithm relies on the premise that given only the modulus, it is impossible to find the prime factors in a reasonable amount of time, but if an eavesdropper were to obtain its prime decomposition, then the communication using that particular public key would become unsecure.

The RSA algorithm is used worldwide to allow for two parties to secretly generate a secure key that can then be used in combination with a chosen symmetric-key protocol. For the RSA public key to be secure, the National Institute of Standards and Technology (NIST) recommends that the modulus of the key is at least 2048 bits long. This ensures that the key will be resilient against any attack done by classical computers.

Quantum computing was also developing during the second half of the 20th century, with new discoveries being made every decade. In the 1970s, the *no cloning theorem* was presented [5], a result that would become crucial when studying the security of cryptographic algorithms using quantum computing. In the 80s, the first key distribution algorithm that used quantum computation was presented by C. H. Bennett and G. Brassard [7], bringing the fields of cryptography and quantum computing together. And then, in the 1990s, Peter Shor discovered an algorithm that could solve the *factoring problem* and the *discrete log problem* with super polynomial speedup compared to any algorithm using classical computers.

The discovery of that algorithm posed a thread to asymmetric-key cryptography, like the RSA algorithm, that relied on prime decomposition, since a sufficiently powerful quantum computer could theoretically make any public key insecure. However, at that time Shor's algorithm was purely theoretical, and to this day the largest composite number that was decomposed using the algorithm was the number 21 in 2012.

With the fear that some day quantum computers will be able to break some asymmetric-key algorithms, two subjects that combine cryptography and quantum computation started to gain traction: *post-quantum cryptography* and *quantum key distribution*. The former studies classical cryptography algorithms that are theoretically resilient to attacks with quantum computers, but they are not our point of interest for this work. Here, we will study Quantum key distribution (QKD), a set of algorithms that use quantum computing to allow two parties to generate a secret private key. Instead of relying on computational complexity, the security of these algorithms are based on quantum mechanics, and as long as the eavesdropper is restricted to the laws of physics, it is provably impossible to obtain any information on the key without being detected.

In order to get to QKD algorithms, we will explore some basics about quantum computation and the notation used in the field, and how to represent quantum circuits. Then we will take a look at two examples of quantum algorithms that can be represented by quantum circuits: *quantum teleportation* and the *Deutsch-Jozsa algorithm*. Once we are familiarized with the language we need, two QKD protocols

will be presented: the *BB84 algorithm* and the *EPR Protocol*. Finally, we will take a look at the *CHSH Game*, where using an algorithm that takes advantage of quantum mechanics offers a considerable increase in probability of success compared to using classical strategies.

Chapter 2

Qubits

In this chapter, the notion of a quantum bit - qubit from now on - will be presented. Quantum algorithms work by manipulating them, just like classical computers work by manipulating classical bits. The main difference between classical bits and qubits is that, while the former can only have two states (0 and 1), qubits can have more than two states. Those states will be represented by vectors on a Hilbert space.
Here we will present the definition of Hilbert spaces, the various ways of representing qubits and the mathematical concepts behind their properties.

2.1 Dirac Notation

A qubit is a two-state quantum system, it can exist in any quantum superposition between two independent quantum states. To represent the state of a single qubit, we will use unitary vectors on a 2-dimensional complex Hilbert space.

Definition 2.1. *A* Hilbert space *is a real or complex inner product space that is also a complete metric space with respect to the distance function induced by the inner product.*

From now on, if not stated otherwise, $\mathcal{H}$ will denote the two-dimensional complex Hilbert space.

To correctly define the state of a qubit in $\mathcal{H}$, we will choose two linearly independent vectors to form a basis, and each of them will represent one of the two independent quantum states. If a qubit is in neither of those two states, rather in a superposition of those, a linear combination of the basis states will represent the superposition. Therefore, given the vectors

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

the state of a qubit can be described with the unitary vector

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \tag{2.2}$$

where $\alpha_0, \alpha_1 \in \mathbb{C}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$. These complex values that describe the state are called *amplitudes*. From now on, we will assume the condition of unitary for every vector representing a qubit.

However, using this notation for vectors in quantum mechanics can have some drawbacks, and for that reason another notation is used [1]. Since 1939 the Dirac Notation - sometimes called *Bra-Ket* notation - is used in quantum mechanics, and it is the notation that will be used here. Its goal is to represent vectors in a Hilbert space and linear applications corresponding to their dual counterparts in a similar way.

Definition 2.2. *Let $\psi \in \mathcal{H}$ be a vector in a Hilbert space. With the Dirac notation, we will write the vector inside of a **ket**, $|\,\psi\,\rangle$.*

The notation of the *ket* is particularly useful when given vectors with subscripts, for example, we could represent $\psi_a, \psi_b \in \mathcal{H}$ like $|\,a\,\rangle, |\,b\,\rangle$. From now on, the two basis vectors in 2.1 will be written in Dirac notation as follows:

$$|\,0\,\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |\,1\,\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.3}$$

The basis $\{|\,0\,\rangle, |\,1\,\rangle\}$ is called the *computational basis*, and the state of a qubit, like in 2.2, will be written as

$$|\,\psi\,\rangle = \alpha_0|\,0\,\rangle + \alpha_1|\,1\,\rangle \tag{2.4}$$

with the same constraint, $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Definition 2.3. *Given a vector on a Hilbert space $\psi \in \mathcal{H}$, we define the **bra** as the linear functional that maps any vector $\varphi \in \mathcal{H}$ to the inner product $\psi \cdot \varphi$*

$$\begin{aligned} \langle\,\psi\,| : \mathcal{H} &\to \mathbb{C} \\ \varphi &\mapsto \psi \cdot \varphi \end{aligned}$$

We represent the linear functional with $\langle\,\psi\,|$. Then, the inner product is written as $\psi \cdot \varphi \equiv \langle\,\psi\,||\,\varphi\,\rangle = \langle\,\psi\,|\,\varphi\,\rangle$

We can also represent the outer product of two vectors $|\,\psi\,\rangle, |\,\varphi\,\rangle \in \mathcal{H}$, defined as the linear function

$$\begin{aligned} |\,\psi\,\rangle\langle\,\varphi\,| :\ \mathcal{H} &\to \mathcal{H} \\ |\,\phi\,\rangle &\mapsto |\,\psi\,\rangle\langle\,\varphi\,|\,\phi\,\rangle \end{aligned}$$

An interpretation that will be quite useful is thinking about *bra*-vectors as complex-conjugated transposed *kets*, and both the *inner* and *outer* products as matrix multiplications.

$$\langle 0| = |0\rangle^\dagger = \begin{pmatrix} 1 & 0 \end{pmatrix}$$
$$\langle 0|1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$
$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

2.2 The Bloch Sphere

While the vector representation using Dirac's notation is the most common to represent the state of a single qubit, other representations also exist. The most used and also one that will help understand future concepts presented here, is the Bloch Sphere. Given a qubit in the state $|\psi\rangle \in \mathcal{H}$, we know that $\langle\psi|\psi\rangle = 1$, and this constraint allows us to write the vector in the form

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{2.5}$$

with θ, γ, $\varphi \in \mathbb{R}$. However, quantum mechanics tells us that we can actualy ignore the factor $e^{i\gamma}$ because it has no observable effect. Therefore we can rewrite the equation 2.5 and obtain:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{2.6}$$

with $0 \leq \theta \leq \pi$ and $0 \leq \varphi < 2\pi$. This representation is always unique, since given θ, φ the qubit state represented is unique. Reinterpreting the parameters θ, φ in spherical coordinates, we can specify a point in the unit sphere $\mathbf{S}^2 \subset \mathbb{R}^3$

$$\mathbf{p} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

And it is with this spherical coordinates that we define the Bloch Sphere, seen in figure 2.1. With this representation, the first and second vectors of the computational basis $\{|0\rangle, |1\rangle\}$ sit at the north and south pole respectively. In fact, any two antipodal points on the Bloch sphere will form an orthonormal basis of the 2-dimensional complex Hilbert space. The three pairs of antipodal points that lie on the three axis of the Bloch sphere are:

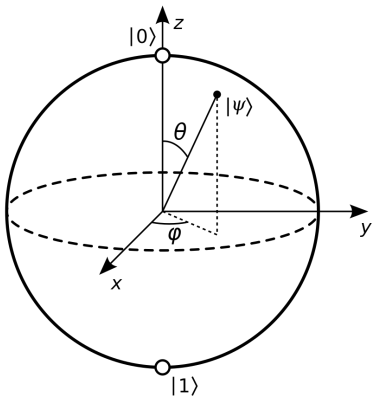


Figure 2.1: The Bloch Sphere

1. The $\mathbb{X}$-basis, called the *Hadamard basis*, formed by the two points that lie on the x-axis:

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.7}$$

2. The $\mathbb{Y}$-basis, formed by the two points that lie on the y-axis:

$$|+i\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \qquad |-i\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{2.8}$$

3. The $\mathbb{Z}$-basis, formed by the two points that lie on the z-axis, is the computational basis $\{|0\rangle, |1\rangle\}$.

2.3 Entanglement

One of the key concepts of quantum mechanics and also quantum computation is entanglement. This phenomenon occurs when the state of a particle cannot be described independently of the state of other particles. It is a key concept, since one can show that a classical computer can simulate a quantum computer that does not make use of entanglement [3]. In quantum mechanics, one can define entanglement of two or more particles using the tensor product.

2.3.1 The tensor product

Let $\mathcal{H}_m$, $\mathcal{H}_n$ be two complex Hilbert spaces of dimensions m and n respectively. Then the space $\mathcal{H}_m \otimes \mathcal{H}_n$ is the complex Hilbert space of dimension $m \cdot n$ that

contains all linear combinations of the tensor product $|\,v\,\rangle \otimes |\,w\,\rangle$, $|\,v\,\rangle \in \mathcal{H}_m$, $|\,w\,\rangle \in \mathcal{H}_n$. If $|\,v\,\rangle$ and $|\,w\,\rangle$ are defined as

$$|\,v\,\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \qquad\qquad |\,w\,\rangle = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \tag{2.9}$$

then the vector resulting of the tensor product is

$$|\,v\,\rangle \otimes |\,w\,\rangle = \begin{pmatrix} \alpha_1 \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \\ \vdots \\ \alpha_m \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1 \\ \vdots \\ \alpha_1\beta_n \\ \vdots \\ \alpha_m\beta_1 \\ \vdots \\ \alpha_m\beta_n \end{pmatrix} \tag{2.10}$$

Instead of writing $|\,v\,\rangle \otimes |\,w\,\rangle$, we will denote the tensor product of two vectors by $|\,v\,\rangle|\,w\,\rangle$, or even $|\,vw\,\rangle$. The tensor product satisfies the following properties:

1. For any $z \in \mathbb{C}$, $|\,v\,\rangle \in \mathcal{H}_m$, $|\,w\,\rangle \in \mathcal{H}_n$

$$z\,(|\,v\,\rangle \otimes |\,w\,\rangle) = z|\,v\,\rangle \otimes |\,w\,\rangle = |\,v\,\rangle \otimes z|\,w\,\rangle \tag{2.11}$$

2. For any $|\,v_1\,\rangle, |\,v_2\,\rangle \in \mathcal{H}_m$, and $|\,w\,\rangle \in \mathcal{H}_n$

$$(|\,v_1\,\rangle + |\,v_2\,\rangle) \otimes |\,w\,\rangle = |\,v_1\,\rangle \otimes |\,w\,\rangle + |\,v_2\,\rangle \otimes |\,w\,\rangle \tag{2.12}$$

3. For any $|\,v\,\rangle \in \mathcal{H}_m$ and any $|\,w_1\,\rangle, |\,w_2\,\rangle \in \mathcal{H}_n$

$$|\,v\,\rangle \otimes (|\,w_1\,\rangle + |\,w_2\,\rangle) = |\,v\,\rangle \otimes |\,w_1\,\rangle + |\,v\,\rangle \otimes |\,w_2\,\rangle \tag{2.13}$$

The definition of the tensor product is also extended to linear operators. Let A be a $m \times n$ matrix and B a $p \times q$ matrix. Then the result of $A \otimes B$ is a linear operator defined by the $mp \times nq$ matrix

$$A \otimes B \equiv \begin{pmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{pmatrix} \tag{2.14}$$

Finally, given any vector $|\,\psi\,\rangle \in \mathcal{H}$ or any linear operator $A : \mathcal{H} \mapsto \mathcal{H}'$, we define the notation $|\,\psi\,\rangle^{\otimes n}$, $A^{\otimes n}$ as follows

$$|\,\psi\,\rangle^{\otimes n} \equiv |\,\psi\,\rangle \otimes \cdots \otimes |\,\psi\,\rangle \tag{2.15}$$

$$A^{\otimes n} \equiv A \otimes \cdots \otimes A \tag{2.16}$$

2.3.2 Multiple qubits systems

In sections 2.1 and 2.2 we have seen the notation used when working with a single qubit. However, as we discussed earlier, when developing algorithms for quantum computers we are interested in using quantum entanglement, therefore we will be working with systems that use two or more qubits.

Firstly, we will describe the two-qubit systems, and the extrapolation to n-qubit systems will follow naturally. When working with a single qubit, we described its state with a unitary vector on a two-dimensional complex Hilbert space $\mathcal{H}$. With two qubits, the state of the system will be described by a unitary vector on the space $\mathcal{H}_1 \otimes \mathcal{H}_2$, where both $\mathcal{H}_1$ and $\mathcal{H}_2$ are two-dimensional complex Hilbert spaces. Furthermore, if the state of the first system is $|\,\psi_1\,\rangle \in \mathcal{H}_1$ and the state of the second system is $|\,\psi_2\,\rangle \in \mathcal{H}_2$, then the state of the composite system will be $|\,\psi_1\,\rangle \otimes |\,\psi_2\,\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$.

When working with multiple qubit systems, we can also define the computational basis. In the case of $\mathcal{H} \otimes \mathcal{H} = \mathcal{H}^{\otimes 2}$ we define the basis as

$$\{|\,0\,\rangle \otimes |\,0\,\rangle, |\,0\,\rangle \otimes |\,1\,\rangle, |\,1\,\rangle \otimes |\,0\,\rangle, |\,1\,\rangle \otimes |\,1\,\rangle\} = \{|\,00\,\rangle, |\,01\,\rangle, |\,10\,\rangle, |\,11\,\rangle\} \quad (2.17)$$

And we can extrapolate the idea to n-qubit systems defining the computational basis as

$$\{|\,\mathbf{x}\,\rangle | \; \mathbf{x} \in \{0,1\}^n\} \quad (2.18)$$

We have seen that given two states on each space $|\,\psi_1\,\rangle \in \mathcal{H}_1$ and $|\,\psi_2\,\rangle \in \mathcal{H}_2$ we can assign to it a state in the two-state space $\mathcal{H}_1 \otimes \mathcal{H}_2$. However, the reciprocal is not true. Given any state $|\,\phi\,\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, it is not guaranteed that there exist two vectors $|\,\psi_1\,\rangle \in \mathcal{H}_1$ and $|\,\psi_2\,\rangle \in \mathcal{H}_2$ such that $|\,\phi\,\rangle = |\,\psi_1\,\rangle \otimes |\,\psi_2\,\rangle$. If a state $|\,\phi\,\rangle$ satisfies that no such decomposition exists, we say that the state is *entangled*.

In the 4-dimensional space of two-state systems, there is a particular basis of entangled states that has proven to be particularly useful.

Definition 2.4. *The* Bell's states *or* EPR pairs *are four entangled pairs that form a basis in the four dimensional complex Hilbert space representing the state of a two-qubit system. The Bell's states are defined as*

1. $|\,\beta_{00}\,\rangle = \frac{1}{\sqrt{2}}\left(|\,00\,\rangle + |\,11\,\rangle\right)$
2. $|\,\beta_{10}\,\rangle = \frac{1}{\sqrt{2}}\left(|\,00\,\rangle - |\,11\,\rangle\right)$
3. $|\,\beta_{01}\,\rangle = \frac{1}{\sqrt{2}}\left(|\,01\,\rangle + |\,10\,\rangle\right)$
4. $|\,\beta_{11}\,\rangle = \frac{1}{\sqrt{2}}\left(|\,01\,\rangle - |\,10\,\rangle\right)$

It is easy to see that any Bell state is, in fact, an entangled state. Take for example the state $|\beta_{00}\rangle$. We know by definition that

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

and suppose that there exists two vectors $|a\rangle, |b\rangle \in \mathcal{H}$ such that

$$|a\rangle = \begin{pmatrix}a_1\\a_2\end{pmatrix} \qquad |b\rangle = \begin{pmatrix}b_1\\b_2\end{pmatrix}$$

and $|\beta_{00}\rangle = |a\rangle \otimes |b\rangle$, then it follows that

$$a_1b_1 = 1 \qquad a_1b_2 = 0$$
$$a_2b_1 = 0 \qquad a_2b_2 = 1$$

and this results in a contradiction.

The four Bell states form a base of $\mathcal{H} \otimes \mathcal{H}$ called the *Bell basis*.

2.4 Measurements

The final part of this chapter is dedicated to understanding qubit measurement. If we have a qubit $|\psi\rangle \in \mathcal{H}$ in an unknown state, and we choose two orthonormal states from $\mathcal{H}$ to form a basis, $\mathcal{B} = \{|a\rangle, |a^{\perp}\rangle\}$, then there exists two complex values $\alpha_0, \alpha_1 \in \mathbb{C}$ such that

$$|\psi\rangle = \alpha_0|a\rangle + \alpha_1|a^{\perp}\rangle \tag{2.19}$$

But having no prior information of the state of the qubit $|\psi\rangle$, means that there is no possible action that can give information about the values α_0, α_1. There is only one action one can perform to extract information from a qubit: *making a measurement*.

Once the basis $\mathcal{B}$ has been established, we can make a measurement to the qubit $|\psi\rangle$ with respect to the basis $\mathcal{B}$. The action of measuring $|\psi\rangle$ will *collapse* its state to either $|a\rangle$ or $|a^{\perp}\rangle$. By collapse, we mean that if, for example, the measurement results in the state $|a\rangle$ being observed, from that moment the qubit $|\psi\rangle$ will be in the state $|a\rangle$, and if it results in the state $|a^{\perp}\rangle$ being observed then $|\psi\rangle$ will be in the state $|a^{\perp}\rangle$.

If we are given a qubit in the state 2.19, and we know the values of $\alpha_0, \alpha_1 \in \mathbb{C}$, we can know the probabilities that the state collapses to either $|a\rangle$ or $|a^{\perp}\rangle$. The

probability that $|\psi\rangle$ collapses on the state $|a\rangle$ is $p(a) = |\alpha_0|^2$, and the probability that the qubit collapses on the state $|a^\perp\rangle$ is $p(a^\perp) = |\alpha_1|^2$. We can also calculate the probabilities using the inner product:

$$p(a) = |\langle a|\psi\rangle|^2 = |\alpha_0|^2 \qquad p(a^\perp) = |\langle a^\perp|\psi\rangle|^2 = |\alpha_1|^2 \tag{2.20}$$

It is important to note that the action of making a measurement is *destructive*, i.e. all the information that we had about the state before the measurement will be lost.

In the case of n qubit systems, given an orthonormal basis $\{|i\rangle\}_{0\leq i<n}$, $n \in \mathbb{N}$, and a unitary state

$$|\phi\rangle = \sum_{i=0}^{n-1} \alpha_i |i\rangle \tag{2.21}$$

with $\alpha_i \in \mathbb{C}, 0 \leq i < n$, after measuring each qubit individually, the probability that the resulting state is $|i\rangle$ is

$$p(i) = |\langle i|\phi\rangle|^2 = |\alpha_i|^2 \tag{2.22}$$

If the n-qubit system is not entangled, then one can measure each qubit independently and know that the results of the measurements are not correlated. However, this is not the case with entangled systems. If we have n entangled qubits, measuring a subset of them can give us information about the probabilities of the qubits that are not yet measured. This behavior is clear to see using the bell states defined in 2.4:

Example 2.5. Consider the first Bell state

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.23}$$

Given that the amplitude of $|00\rangle$ is $1/\sqrt{2}$, and the same applies to $|11\rangle$, we know that the Bell state will collapse to either of those states when measured with probability $1/2$ for each state.

Knowing this, if we measured the first qubit of the system and got a $|0\rangle$ as a result of the measurement with respect to the computational basis, we would know that the second qubit is also in the state $|0\rangle$, having collapsed without us measuring it directly.

In the same way, if the result obtained after measuring the first qubit with respect to the computational basis was $|1\rangle$, then the second qubit will also collapse to the state $|1\rangle$ even before we make the measurement.

This property of entanglement is extremely useful and the key to quantum algorithms. If used properly, one can find algorithms that exploit the entanglement of qubits in order to redesign classical algorithms, making them exponentially faster. In the next chapters, we will see some examples of this behavior.

Chapter 3

Quantum Circuits

With the necessary preliminaries to understand what qubits are and their most important properties, we can go a step further and begin to build algorithms using those properties. In this chapter we will present the notion of quantum gates, explain the most common ones, how they interact with each other and how they take advantage of both superposition and entanglement. At the end of the chapter, we will take a look at two algorithms: *quantum teleportation* and the *Deutsch-Jozsa algorithm*.

3.1 Reversible operations on qubits

In the previous chapter we talked about measurement and saw that it was an irreversible operation, i.e. once you measure a qubit with respect to a certain base, its state is changed and any previous information about amplitudes is lost. When building quantum algorithms, we want to be able to interact with qubits without losing said information. This is where reversible operations come into place.

Reversible operations on qubits are represented by *unitary linear operators*.

Definition 3.1. *A* linear operator *on a vector space V is a linear transformation $T : V \to V$ of the vector space to itself.*

As we saw in section 2.1, the outer product of any two vectors of a Hilbert space is a linear transformation.

Definition 3.2. *Given a vector field V, a linear operator U is called* unitary *if*

$$U^\dagger U = UU^\dagger = I \tag{3.1}$$

Where I denotes the identity matrix and $U^\dagger$ is the transposed and complex conjugated matrix U.

Given a unitary operator $U \in \mathcal{U}(\mathcal{H})$, where $\mathcal{U}(\mathcal{H})$ represents the set of unitary transformations of $\mathcal{H}$, and a qubit in the state $|\psi\rangle \in \mathcal{H}$, we can apply U to the state of the qubit and obtain a new state $U|\psi\rangle$. The condition of unitary on the linear operator guarantees that the state after the operator is applied is also represented by a unitary vector. Furthermore, we can apply the inverse operator $U^{-1} = U^\dagger$ if we desire to obtain the original state:

$$U^\dagger(U|\psi\rangle) = (U^\dagger U)|\psi\rangle = |\psi\rangle$$

A linear operator is not limited to one qubit states, and it can operate on n qubits simultaneously. Given n qubits in the state $|\varphi\rangle \in \mathcal{H}^{\otimes n}$, a unitary transformation acting on all n qubits at once is represented by a unitary matrix $U \in \mathcal{U}(\mathcal{H}^{\otimes n})$ of dimension 2^n.

3.2 Quantum logic gates

In quantum computing, logic gates are the building blocks of quantum algorithms. Quantum algorithms consist of an input - n qubits -, a set of gates (unitary transformations) and an output. We assume that, after running the circuit, the qubits on the output are measured using the computational basis, unless stated otherwise. In some particular cases, it might be necessary to measure a qubit *during* the algorithm, and in that case a measuring gate will be drawn and the basis in which we make the measurement will be stated.

To represent quantum circuits, we will make use of diagrams. The building blocks of the diagrams are wires and gates (unitary operators or measurement gates). Given that quantum circuits sometimes make use of classical bits of information sometimes, we will represent quantum wires and classical wires with different diagrams:

$$|\psi\rangle \text{ ——————} \tag{3.2}$$

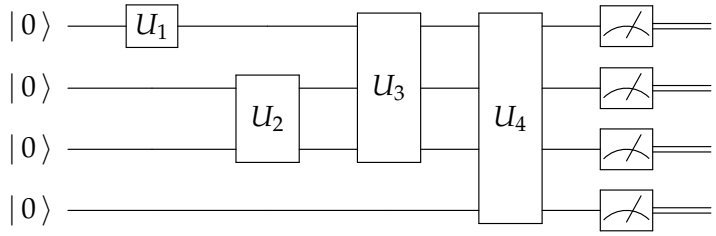
$$x \text{ ═══════} \tag{3.3}$$

where $\psi \in \mathcal{H}$ and $x \in \{0, 1\}$. In the previous diagram, 3.2 represents a quantum channel and 3.3 represents a classical channel. The diagrams are read from left to right, and multiple rows represent calculation happening at the same time. If we have a unitary operator U, we represent it in the circuit with a box:

$$|\psi\rangle \text{ ——} \boxed{U} \text{——} \tag{3.4}$$

and the result of the circuit 3.4 is $U|\psi\rangle$.

In the next circuit, 3.5, we give an example of an algorithm with multiple input qubits, and composed with multiple gates:



(3.5)

The qubits pass through a series of gates (U_1, U_2, U_3, U_4), with $U_i \in \mathcal{U}(\mathcal{H}^{\otimes i}), 1 \leq i \leq 4$, where each of the gates U_i acts on i qubits simultaneously. Finally, the four resulting qubits are measured, and a result is obtained. The output of the measurement gate, when measuring with respect to the computational basis, is the bit 0 if $|0\rangle$ is observed, and the bit 1 if $|1\rangle$ is observed.

To be able to understand and construct quantum circuits, the next sections will present the most used quantum gates that act on single qubits or sets of up to three qubits. Then, we will see how to extend any gate acting on m qubits to a gate acting on n qubits, with $m < n$.

3.2.1 Single qubit gates

Definition 3.3. *The* Pauli gates *are a set of three gates* $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ *represented by the three matrices* $(\sigma_x, \sigma_y, \sigma_z)$ *respectively. The matrices are defined by*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.6}$$

Each matrix represents a rotation of π rad around an axis of the Bloch Sphere. Each gate leaves one of the three basis $\{|0\rangle, |1\rangle\}, \{|+\rangle, |-\rangle\}, \{|+i\rangle, |-i\rangle\}$ unchanged. The Pauli **X** gate is also called the **NOT** gate, since it maps $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$, similar to how the binary NOT gate works. The three Pauli gates are represented in quantum circuits by the following diagrams:

$$\mathbf{X} \equiv \mathbf{NOT} \equiv \text{—}\boxed{\mathbf{X}}\text{—} \equiv \text{—}\oplus\text{—} \tag{3.7}$$

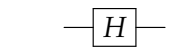
$$\mathbf{Y} \equiv \text{—}\boxed{\mathbf{Y}}\text{—} \tag{3.8}$$

$$\mathbf{Z} \equiv \text{—}\boxed{\mathbf{Z}}\text{—} \tag{3.9}$$

Definition 3.4. *The* Hadamard gate *is represented by the Hadamard matrix*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.10}$$

And in quantum circuits is represented by the following diagram:



(3.11)

The most important property about the Hadamard gate is that, in contrast to the Pauli gates, when applied to the computational basis the gate returns a state in superposition - assuming that the measurements are also made in the computational basis. This superposition comes from the fact that the gate maps the computational basis to the Hadamard basis:

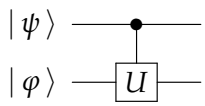
$$|0\rangle \mapsto H|0\rangle = |+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |1\rangle \mapsto H|1\rangle = |-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{3.12}$$

Therefore, measuring $H|0\rangle$ using the computational basis yields $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$.

3.2.2 Multiple qubit gates

Definition 3.5. Controlled gates *are operations performed on sets of $m+n$ qubits, with $m, n \in \mathbb{N}\backslash\{0\}$. The first group of m qubits are called the control bits, and when a condition over the state of the m bits is satisfied, an operation U is performed on the other n bits.*

A controlled operation with one control qubit and a gate U that acts on exactly one qubit is represented by the following diagram



(3.13)

In 3.13, the gate U is applied to $|\varphi\rangle$ if the qubit $|\psi\rangle$ is $|1\rangle$, and if $|\psi\rangle = |0\rangle$, then no operation will be performed. In the case that we have information about the gate U, we can represent the controlled operation over it in terms of matrices. Suppose that the gate is given by the matrix

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \tag{3.14}$$

Then, the matrix representing the circuit 3.13 will be of the form

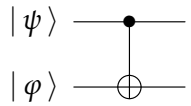
$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix} \tag{3.15}$$

where CU denotes Controlled-U.

It is true that no operation is applied to any qubit if the control qubits are all $|0\rangle$, and that the gate U is applied to the corresponding qubits if the control bits are all $|1\rangle$. However, unlike classical controlled gates, the control qubit can be in any state and is not limited to $|0\rangle$ or $|1\rangle$. If that is the case, where the control qubits are not in any of those two states, their states could also be modified when the gate is applied. In example 3.7 we will see an example of this behavior.

The most used controlled gate is the controlled Pauli **X** gate, with one or two qubits:

Definition 3.6. *The* controlled-not *gate or* ***CNOT*** *gate is the Pauli* **X** *gate with one control qubit, and is represented by the following diagram*



(3.16)

where $|\psi\rangle$ is the control qubit.

It is interesting to see how the gate behaves on the states of the computational basis compared to the states of the Hadamard basis:

Example 3.7. The following table shows the output to the controlled-not gate when certain inputs are applied:

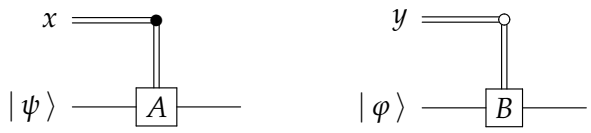
Input	**Output**	**Input**	**Output**
$\|00\rangle$	$\|00\rangle$	$\|++\rangle$	$\|++\rangle$
$\|01\rangle$	$\|01\rangle$	$\|+-\rangle$	$\|--\rangle$
$\|10\rangle$	$\|11\rangle$	$\|-+\rangle$	$\|-+\rangle$
$\|11\rangle$	$\|10\rangle$	$\|--\rangle$	$\|+-\rangle$

As we have seen before, if the computational basis is used on the **CNOT** gate, it flips the state of the second qubit if the first qubit is in the state $|1\rangle$. However, if the Hadamard basis is used, the roles of the qubits are inverted, meaning that is the second qubit that acts as the control. One can see in the table that if the second qubit is $|-\rangle$, then the state of the first qubit is changed.

Definition 3.8. *The* Toffoli gate*, also called the* ***CCNOT*** *(controlled-controlled-not) is a Pauli* **X** *gate with two control qubits. The matrix and circuit representation of the gate are the following:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{(3.17)}$$

Definition 3.9. Classically controlled *gates are unitary transformations that are applied to the corresponding qubit depending on the state of a classical bit. There are two types of classically controlled gates:*



(3.18)

where $x, y \in \{0, 1\}$*,* $\psi, \varphi \in \mathcal{H}$ *and* $A, B \in \mathcal{U}(\mathcal{H})$*. Then, in the first circuit, the gate* A *is applied to* $|\,\psi\,\rangle$ *if, and only if,* $x = 1$*. Inversely, in the second circuit, the gate* B *is applied to* $|\,\varphi\,\rangle$ *if, and only if,* $y = 0$*.*

3.3 Circuit composition

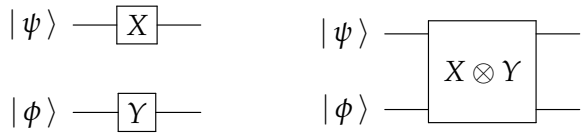
In order to build more complex quantum circuits, one has to work with multiple gates, wiring them together either serially or in parallel. Depending on how the gates are wired one would obtain a certain result or another, and in every algorithm a careful choice has to be made in order to select the gates used and their distribution in the circuit to obtain the desired result.

Serially wired gates are connected end to end in the circuit, and will be applied to the specific qubit. Given two unitary operators X, Y and a state $|\,\psi\,\rangle \in \mathcal{H}$, then the matrix $Y \cdot X$ has the same effect as serially connecting the gates X and Y in said order, i.e. the following circuits are equivalent:

(3.19)

Parallel gates are sets of independent gates, where every gate acts on a different set of qubits. If the gates are all applied at the same time, one can combine them

and obtain a single gate that acts on all the qubits at the same time, obtaining the same result. If we have two unitary vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ representing two states and two unitary transformations X, Y, the state after applying the gate X to $|\psi\rangle$ and Y to $|\phi\rangle$ will be $(X \otimes Y)|\psi \otimes \phi\rangle$. In terms of circuit diagrams, the following are equivalent:

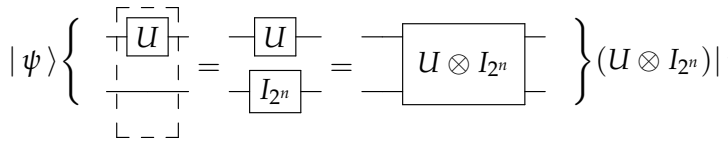


(3.20)

Combining parallel gates is essential when working with entangled states. If we have a state $|\psi\rangle \in \mathcal{H}^{\otimes(m+n)}$ and we want to apply a unitary transformation $U \in \mathcal{U}(\mathcal{H}^{\otimes m})$ to the first m qubits of the system, we have to be extra careful when writing the operation.

If the system is not entangled, we can represent $|\psi\rangle$ like $|\psi\rangle = |\psi_m\rangle \otimes |\psi_n\rangle \in \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n}$. With this representation, applying U to the first m qubits is equivalent to computing $(U|\psi_m\rangle) \otimes |\psi_n\rangle$.

However, if the system is in a entangled state, then there exists no decomposition such that $|\psi\rangle = |\psi_m\rangle \otimes |\psi_n\rangle \in \mathcal{H}^{\otimes m} \otimes \mathcal{H}^{\otimes n}$. Therefore, if we want to apply the transformation U to only the first m qubits, there is no easy way to make the calculation. Instead, we can combine the gate U with the unity matrix I_{2^n} using the tensor product. The resulting unitary transformation $U \otimes I_{2^n}$ will have the desired effect: the gate U will be applied to the first m qubits and the other n will remain in the same state.



(3.21)

To end the section, we will take a look at the Hadamard transform

Definition 3.10. *The* Hadamard transform *is the Hadamard gate H applied in parallel to n qubits. It is represented by the tensor product of n Hadamard gates:*

$$\bigotimes_{1}^{n} H = H^{\otimes n} = H_n \tag{3.22}$$

When applied to a system where n qubits are initialized to $|0\rangle$, the Hadamard transform will create a superposition, with equal probability of measuring any of the 2^n possible states. We can represent this superposition with

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \tag{3.23}$$

3.4 Circuit examples

To end the chapter about quantum circuits, two examples are presented: *Quantum Teleportation* and the *Deutsch-Jozsa Algorithm*. These algorithms will present circuits using the formerly introduced gates, and also quantum entanglement.

3.4.1 Quantum Teleportation

Preliminaries

The first algorithm presented is called *Quantum Teleportation*. Here we have two parties, A and B - we will call them Alice and Bob respectively - and Alice has a qubit in the unknown state represented by the unitary vector $|\psi\rangle_A \in \mathcal{H}$ with $|\psi\rangle_A = \alpha_0|0\rangle + \alpha_1|1\rangle$, $\alpha_0, \alpha_1 \in \mathbb{C}$. In the end, Alice wants Bob to have a qubit in the same state $|\psi\rangle$, but she has no information on the amplitudes α_0, α_1 and cannot send the qubit to Bob over a quantum channel.

Alice faces two more problems in order to send the qubit to Bob. The first problem is that the information that Alice can get to help Bob replicate the state of the qubit is almost null, as the state of a quantum system cannot fully be determined by making measurements. The second problem is that there is no way for Alice to clone the state of the qubit and obtain a second qubit in the same state as the one that Alice possesses without destroying the original, a limitation proven by the *no cloning theorem* [5].

In order to send the state $|\psi\rangle_A$ to Bob, the two parties will use a shared Bell state $|\beta_{00}\rangle$ defined in 2.4 as their initial state. Alice will have the first half of the Bell state, and Bob the second one. Therefore, the state at the start of the algorithm is

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)_A \otimes \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{3.24}$$

After the teleportation algorithm, any information from Alice's original qubit $|\psi\rangle_A$ will be lost due to measurement, and the second qubit from the Bell state that was in Bob's possession will be in the state $|\psi\rangle_B$.

The Algorithm

The algorithm starts with Alice in possession of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, the qubit that she wants to send to Bob. Furthermore, Alice and Bob each have one qubit of the entangled state β_{00} such that

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{3.25}$$

The state of the three qubits combined can be represented with:

$$|\psi\rangle_A|\beta_{00}\rangle_{AB} = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle) \tag{3.26}$$

And using the following identities:

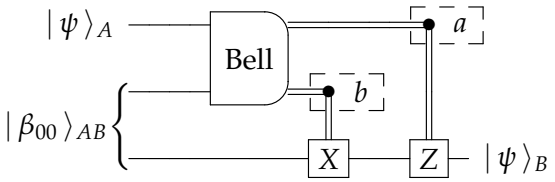
$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\beta_{00}\rangle + |\beta_{10}\rangle), \qquad |0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\beta_{01}\rangle + |\beta_{11}\rangle)$$
$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\beta_{01}\rangle - |\beta_{11}\rangle), \qquad |1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\beta_{00}\rangle - |\beta_{10}\rangle)$$

we can represent both qubits in Alice's possession using the Bell basis. By doing so, we obtain

$$\begin{aligned} |\psi\rangle_A|\beta_{00}\rangle_{AB} = &\frac{1}{2}|\beta_{00}\rangle_{AA} \otimes |\psi\rangle_B + \\ &\frac{1}{2}|\beta_{01}\rangle_{AA} \otimes \mathbf{X}|\psi\rangle_B + \\ &\frac{1}{2}|\beta_{10}\rangle_{AA} \otimes \mathbf{Z}|\psi\rangle_B + \\ &\frac{1}{2}|\beta_{11}\rangle_{AA} \otimes \mathbf{XZ}|\psi\rangle_B \end{aligned} \tag{3.27}$$

Therefore, if Alice measures the two qubits in her possession with the Bell basis, she will get one of the four Bell states, each with probability $1/4$. And after Alice makes the measurement, the qubit in Bob's possession will be in one of the following four states: $\{|\psi\rangle, \mathbf{X}|\psi\rangle, \mathbf{Z}|\psi\rangle, \mathbf{XZ}|\psi\rangle\}$. In order for Bob to be sure that he has the state $|\psi\rangle$ he applies the $\mathbf{X}$ and $\mathbf{Z}$ gates conditionally, depending on Alice's measurement. If the state of Alice's qubits after the measurement is $|\beta_{ab}\rangle$, with $a, b \in \{0, 1\}$, then b tells Bob if he needs to apply the $\mathbf{X}$ gate, and a if he has to apply the $\mathbf{Z}$ gate. After performing the required operations, the state of Bob's qubit will be $|\psi\rangle$.

The following diagram represents the algorithm of *Quantum teleportation*:



(3.28)

The main limitation of the algorithm is that Alice and Bob have to share a classical channel in order to communicate the values of a and b, and therefore the speed of the quantum teleportation algorithm is limited to the speed of the classical channel that connects the two parties.

3.4.2 The Deutsch-Jozsa Algorithm

The Deutsch-Jozsa Algorithm is a quantum algorithm that, even though it is of little use, is a good example of a solution to a problem that is exponentially faster if solved with a quantum algorithm compared to a classical algorithm. The problem that the algorithm solves is the following:

Definition 3.11. *In The* Deutsch-Jozsa Problem *we are given a reversible circuit for computing an unknown n-qubit function*

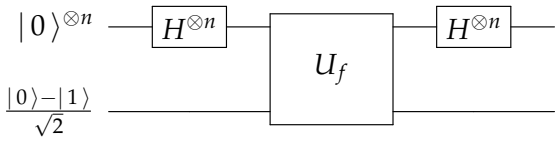
$$f : \{0,1\}^n \mapsto \{0,1\} \tag{3.29}$$

The circuit is treated as a black box*, so no information can be obtained about the function f, we can only evaluate any state $|\,\mathbf{x}\,\rangle$ with $\mathbf{x} \in \{0,1\}^n$ and obtain $f(\mathbf{x})$. We are given the promise that the function f is either balanced or constant, and our task is to determine which is true.*

To start we define the unitary operator U_f

$$U_f : |\,\mathbf{x}\,\rangle|\,y\,\rangle \mapsto |\,\mathbf{x}\,\rangle|\,y \oplus f(\mathbf{x})\,\rangle, \tag{3.30}$$

where $\mathbf{x}$ is a n-bit string and $\oplus$ denotes addition modulo 2. Then the circuit that solves the Deutsch-Jozsa Problem is the following:



(3.31)

Initially, the state of the circuit is

$$|\,0\,\rangle^{\otimes n} \otimes \left(\frac{|\,0\,\rangle - |\,1\,\rangle}{\sqrt{2}}\right). \tag{3.32}$$

The first step of the circuit is to apply the Hadamard transform to $|\,0\,\rangle^{\otimes n}$, and obtain the state

$$H^{\otimes n}|\,0\,\rangle^{\otimes n} \otimes \left(\frac{|\,0\,\rangle - |\,1\,\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\,\mathbf{x}\,\rangle \otimes \left(\frac{|\,0\,\rangle - |\,1\,\rangle}{\sqrt{2}}\right). \tag{3.33}$$

We then apply the formerly defined operator U_f to the combined state 3.33, and we obtain

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} \left(|\,\mathbf{x}\,\rangle \otimes \frac{|\,0 \oplus f(\mathbf{x})\,\rangle - |\,1 \oplus f(\mathbf{x})\,\rangle}{\sqrt{2}}\right) \tag{3.34}$$

Given that the result of the function f is either 0 or 1 we can evaluate both cases, and we see that the state of the last qubit is

$$f(\mathbf{x}) = 0 : \qquad \frac{1}{\sqrt{2}} \left(|\, 0 \,\rangle - |\, 1 \,\rangle \right) \tag{3.35}$$

$$f(\mathbf{x}) = 1 : \qquad \frac{1}{\sqrt{2}} \left(|\, 1 \,\rangle - |\, 0 \,\rangle \right). \tag{3.36}$$

And since both results only differ by a minus sign, we can rewrite 3.34 like

$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} \left(|\, \mathbf{x} \,\rangle \otimes (-1)^{f(\mathbf{x})} \frac{|\, 0 \,\rangle - |\, 1 \,\rangle}{\sqrt{2}} \right) \tag{3.37}$$

Before analyzing the last step of the algorithm, let us consider the effect of the Hadamard gate on $|\, x \,\rangle$, where $x \in \{0, 1\}$:

$$\begin{aligned} H|\, x \,\rangle &= \frac{1}{\sqrt{2}} \left(|\, 0 \,\rangle + (-1)^x |\, 1 \,\rangle \right) \\ &= \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{xz} |\, z \,\rangle. \end{aligned} \tag{3.38}$$

Therefore, if we have a n-qubit state $|\, \mathbf{x} \,\rangle$, where $\mathbf{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n$, the action of the Hadamard transform can be written as

$$\begin{aligned} H^{\otimes n} |\, \mathbf{x} \,\rangle &= H|\, x_1 \,\rangle \cdots H|\, x_n \,\rangle \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} |\, z_1 \,\rangle \right) \cdots \left(\sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} |\, z_n \,\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{z_1 \cdots z_n \in \{0,1\}^n} (-1)^{x_1 z_1 + \cdots + x_n z_n} |\, z_1 \,\rangle \cdots |\, z_n \,\rangle \end{aligned} \tag{3.39}$$

and it can be rewritten more succinctly as

$$H^{\otimes n} |\, \mathbf{x} \,\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{z} \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{z}} |\, \mathbf{z} \,\rangle \tag{3.40}$$

where $\mathbf{x} \cdot \mathbf{z}$ denotes the inner product of $\mathbf{x}$ and $\mathbf{z}$, reduced modulo 2.

Finally, in the last step of the algorithm, we apply $(H^{\otimes n} \otimes I)$ to the state 3.37, and

using 3.40, we can write the final state of the algorithm like

$$
\begin{aligned}
|\psi\rangle &= \left(H^{\otimes n} \otimes I\right) \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})} \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{z}} |\mathbf{z}\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \qquad (3.41) \\
&= \frac{1}{2^n} \sum_{\mathbf{z}\in\{0,1\}^n} \left(\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot\mathbf{z}} \right) |\mathbf{z}\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right).
\end{aligned}
$$

After the last step of the algorithm, the first n qubits of the state $|\psi\rangle$ are measured in the computational basis. To interpret the result of the measurements, we can consider the amplitude of $|\mathbf{z}\rangle = |0\rangle^{\otimes n}$ in $|\psi\rangle$, that is

$$
\frac{1}{2^n} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})}. \qquad (3.42)
$$

In the case that f were constant, the evaluations $f(\mathbf{x})$ would yield either all 0 or all 1, $\forall \mathbf{x} \in \{0,1\}^n$. In this case, 3.42 evaluates to either 1 or -1, and this means that the probability of measuring $|0\rangle^{\otimes n}$ is 1. In the case that f were balanced, the negative and positive amplitudes of 3.42 cancel out and the probability of measuring the state $|0\rangle^{\otimes n}$ is 0.

Therefore, we can conclude that if the measurement of the first n qubits of $|\psi\rangle$ is $|0\rangle^{\otimes n}$, then f is *constant*; and if the result of the measurement has *at least* one qubit in the state $|1\rangle$, then f is *balanced*.

If we wanted to solve the Deutsch-Jozsa problem with a classical algorithm, we would need to make $2^{n-1}+1$ queries to the function f in the worst case, in order to determine if said function in either *balanced* or *constant*. With the quantum algorithm presented in this chapter, we can determine that with just one query to the function f, a considerable improvement over the classical solution.

Chapter 4

Quantum Key Distribution

Quantum Key Distribution (QKD) is a secure communication method that takes advantage of the principles of quantum mechanics in order to generate a secure key that two parties, Alice and Bob, can use to establish a secure communication channel.

In this chapter, the notion of Quantum Key Distribution (QKD) is presented, along with two QKD protocols: *The BB84 Algorithm* and the *EPR Protocol*.

4.1 The basics of QKD

To better understand the QKD protocols, we need to understand the finality and prerequisites of the QKD scheme. As stated before, the scheme allows two parties to generate a secure key which can be used to securely establish a communication channel. In order to achieve this, the two parties need to be connected over two channels, a classical one and a quantum one. The limitations of both channels are explored later.

If the two parties already share a secure key $\mathcal{K}$, Alice can send a message M to Bob by using an encryption function and generating a *ciphertext*. When Bob receives the ciphertext, he can recover the original message M by means of a decryption function.

If an eavesdropper, named Eve, intercepts all the communications between Alice and Bob, but has no information on the key $\mathcal{K}$, then it is impossible for Eve to decipher the message M from the ciphertext C. Therefore, it is extremely important that Alice and Bob can generate a secure key.

In classical cryptography, the security of the communication relies on computational complexity. The most notable example of this is the RSA algorithm, which relies on the assumption that there is no known algorithm working in polynomial time to find the prime factors of an integer and is therefore impossible to find such

factors for large integers in a reasonable amount of time. However, using quantum computers, it is possible to find the factors of any integer N in polynomial time, using an algorithm discovered by *Peter Shor* in 1994.

In this context, the importance of QKD algorithms is clear, given that the key they produce is provably secure and does not rely on computational complexity in order to be secure. Algorithms like the BB84 allow Alice and Bob to generate a secure key that cannot be broken and in a way that both parties can be sure that the information an eavesdropper can possess is minimal. The generated key can then be used in combination with other classical algorithms, such as the *one-time pad* algorithm.

4.1.1 QKD Prerequisites

In order to generate a secure key, Alice and Bob need to have two communication channels: a classical channel and a quantum one.

The *classical channel* is a two-way communication channel, so Alice can send information to Bob and vice versa. In order for QKD to be effective, this channel needs to be authenticated, i.e. Eve can only read the communication happening on the channel, but cannot change the information in any way. This is crucial to generate a secure key, given that if Eve could read and write to the channel, she could impersonate Bob.

On the other hand, the *quantum channel* is less restricted. It is a one way communication channel from Alice to Bob, and Eve can have full control over it. She is able to perform any action to the qubits on the channel: measuring the qubits, intercepting them and sending qubits in any other state, or even performing unitary transformations on them - which includes entangling the qubits on the communication channel with ones in her possession.

There are some examples of QKD algorithms that do not require a quantum channel connecting the two parties, usually because those already share entangled states and can communicate using them. However, the classical channel is always required and the condition that it needs to be authenticated is always assumed.

4.2 The BB84 Algorithm

The BB84 Algorithm was the first QKD algorithm proposed, created by Charles Bennett and Gilles Brassard in 1984 - hence the name. This algorithm exploits the states in superposition, the fact that measuring either $|0\rangle$ or $|1\rangle$ with respect to the basis $\{|+\rangle, |-\rangle\}$ will yield any state from the basis with equal probability, but measuring them with respect to the basis $\{|0\rangle, |1\rangle\}$ will have no effect. In

this chapter, we will represent the computational basis with $H^0\{|0\rangle, |1\rangle\}$ or $\oplus$ and the Hadamard basis with $H^1\{|0\rangle, |1\rangle\}$ or $\otimes$, a notation that will be useful to describe the algorithm.

After describing the algorithm we will take a look at how an unauthorized listener can try to obtain information, but in the attempt also introduce errors that Alice and Bob can detect and decide, using a threshold, if the information that the eavesdropper has obtained is relevant enough to abort the communication, or not relevant enough and a secure key can still be extracted.

4.2.1 Steps of the algorithm

Suppose that Alice and Bob are already connected by a quantum channel and an authenticated classical channel, as previously described. Then, the BB84 Algorithm goes as follows:

Step 1: To start the algorithm, Alice prepares the *raw key*, a bit string of size N. We represent the raw key with $X \in \{0,1\}^N$. For each bit X_j, $0 \leq j < N$, she prepares a qubit in the state $|X_j\rangle \in \{|0\rangle, |1\rangle\}$.

With all the qubits prepared, Alice chooses another $\Theta \in \{0,1\}^N$ at random. This new bit string will dictate, for each qubit, if Alice applies the Hadamard gate before sending it. Therefore, she applies the gate H^{Θ_j} to the j-th qubit, where $H^0 = Id$ and $H^1 = H$. After this step, she obtains a string of qubits in the state $H^{\Theta_1}|X_1\rangle, \ldots, H^{\Theta_N}|X_N\rangle$.

Step 2: At this point, Alice sends the N qubits $H^{\Theta_1}|X_1\rangle, \ldots, H^{\Theta_N}|X_N\rangle$ one by one to Bob over the quantum channel. Since the quantum channel is public, if an eavesdropper were to interfere with the communication to obtain as much information as possible, it would be during this step. We will discuss the eavesdropping techniques in a later section.

Step 3: When Bob receives the qubits from Alice, he decides at random one basis to measure the corresponding qubit, choosing between the computational basis and the Hadamard basis. Again, we represent Bob's choice with $\Theta' \in \{0,1\}^N$. In this case, given $0 \leq j < N$, if $\Theta_j = 0$ then Bob will measure the j-th qubit Alice sent with respect to the basis $\{|0\rangle, |1\rangle\}$, and if $\Theta_j = 1$, he will measure the j-th qubit with respect to $\{|+\rangle, |-\rangle\}$.

After measuring all the N qubits and interpreting both states $|0\rangle, |+\rangle$ as a binary 0 and $|1\rangle, |-\rangle$ as a binary 1, Bob obtains an N bit string $Y \in \{0,1\}^N$.

Notice that if Alice sent to Bob the state $H|X_j\rangle \in \{|+\rangle, |-\rangle\}$, and Bob measures said state with respect to the Hadamard basis $H\{|0\rangle, |1\rangle\}$, the resulting

state obtained from the measurement will be the same state that Alice sent. However, if Bob had measured the state in the computational basis, the result from the measurement would have randomly collapsed to either $|0\rangle$ or $|1\rangle$. The same happens when Alice sends a qubit in the state $|X_j\rangle \in \{|0\rangle, |1\rangle\}$ and Bob measures with respect to the computational basis (obtaining the same state Alice sent) or with respect to the Hadamard gate (obtaining a random result).

Therefore, X, the bit string corresponding to Alice, and Y, the bit string corresponding to Bob, are identical at the positions j such that $\Theta_j = \Theta'_j$.

Step 4: In the last step of the algorithm, Alice and Bob share over the classical channel their choices of basis Θ, Θ'. They then consider the set of indices $J = \{j : \Theta_j = \Theta'_j\}$, of size $|J| \approx N/2$, and compute $\hat{X} = \left(X_j\right)_{j \in J}$ and $\hat{Y} = \left(Y_j\right)_{j \in J}$. Given the definition of J, the two computed bit strings should be equal and could be used as a key for communication. At this point, the key is called the *sifted key*. In table 4.1 we can see an example of the BB84 algorithm, depicting all the steps, where Alice sends to Bob 8 bits of information.

In reality, many errors can be introduced, due to either physical limitations or eavesdropping. In order to correct those errors, Alice and Bob will run an *error correction* algorithm in order to make sure that both $\hat{X}$ and $\hat{Y}$ are equal. And if there is evidence of eavesdropping, another algorithm called *privacy amplification* can be used to make sure that if Eve has gained some information, this information is minimal.

In the next section, we will discuss how can Alice and Bob detect errors by sharing some information over the public channel.

4.2.2 Eavesdropping and error detection

As we mentioned in the previous section, during the BB84 algorithm many errors can be introduced, and therefore it is essential to check for errors after the sifted key is generated, since if $\hat{X}$ and $\hat{Y}$ are not identical they cannot be used as a key.

When discussing errors in the QKD scheme, the *quantum bit error rate* (QBER), defined as the probability that a quantum bit experiences an error during the algorithm, is used. Before starting the algorithm, the two parties agree on a threshold for the QBER that, if it is reached, means that more errors occurred than what they are willing to assume. If that were the case, then they would abort the communication. In practice, it is only possible to calculate an approximation of the QBER without sharing too much information publicly.

To calculate an approximation of the QBER, Alice and Bob agree on a subset

Step 1:								
raw Key	0	1	1	1	0	1	0	0
Alice's sending basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
Alice sends	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$
Step 3:								
Bob's measuring basis	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Bob measures	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|+\rangle$
Bob's bit string	0	1	0	1	0	1	1	0
Step 4:								
sifted key		1		1		1		0

Table 4.1: An example of the four stages of the BB84 algorithm presented in this section, where Alice generates an 8 bit raw key.

of indexes $T \subset \{1, \ldots, |J|\}$ of size k, where $|J|$ is the size of the set of indexes of the sifted key. Then they share over the classical channel $X_T = \left(\hat{X}_i\right)_{i \in T}$ and $Y_T = \left(\hat{Y}_i\right)_{i \in T}$. An approximation of the QBER is then calculated as the number of disagreeing bits divided by k. Once the calculation has been made, if the QBER is below the threshold they agreed on, they discard all the bits they used for the calculation and use the other qubits indexed by J as the secret key.

To get a good approximation of the QBER it is important to agree on a large number of bits to share. But since those are sent through the classical channel, the chosen bits are made public and therefore cannot be used to generate the key. It is important to find an equilibrium between these two factors, and usually the length of bits to share is chosen such that $k \approx |J|/2$.

The size of qubits that Alice initially shares is determined by the desired length of the final key. To obtain a secret key of size n, Alice sends to Bob $(4+\delta)n$, $0 < \delta < 1$, qubits. After Bob measures all the qubits and they both share their respective choice of basis, they discard slightly less than $2n$ qubits that Bob measured in a different basis than Alice. From the remaining bits, they agree on exactly $2n$ to keep, and discard the others. To calculate an approximation of the QBER, they use n bits that are discarded afterward, leaving exactly n bits for the final key.

Intercept and resend

Let's consider now one of the most basic eavesdropping techniques, and see how an approximation of the QBER can warn of the presence of Eve. The eavesdropping technique presented here is called *intercept and resend* strategy.

In this attack, each time Alice sends a qubit to Bob, Eve intercepts it and measures the qubit with either the computational or the Hadamard basis, selected at random. For each qubit that Eve intercepts, she has a 50% chance of measuring it in the same basis that Alice chose. If that is the case, after measuring the qubit it will remain in the same state, and when Eve sends the qubit back to Bob over the quantum channel, it will still be in the same state that Alice had initially prepared, except that now Eve knows the value of the qubit.

However, if Eve selects a different basis than Alice for a certain qubit, after making the measurement the state of the qubit will not be the same that Alice had prepared. In this case, the presence of Eve can be detected when Alice and Bob run the error detection protocol.

When Bob receives the qubit over the quantum channel, he is not aware of Eve's interaction with the qubit. Following the algorithm, he randomly chooses between the computational or the Hadamard basis and makes a measurement on each qubit. Just like we saw in the previous section, in around 50% of the qubits, Bob will choose the same basis as Alice, and all the bits resulting from a measurement with a different basis than Alice's will be discarded.

From the remaining qubits, half of them were previously measured by Eve in a different basis that Alice had chosen, so when Bob makes the measurement, half of them will collapse onto the wrong bit, even though Bob measured the qubit in the same Basis that Alice used to send it. This concludes that, in the *intercept and resend* attack, the QBER is $0,25$.

In the error detection phase, Alice and Bob agree on a subset of n bits to share publicly and detect errors. If Eve has measured all the qubits sent by Alice, then Alice and Bob have a probability of $1 - (3/4)^n$ of detecting an error, and thus, the presence of Eve.

4.3 The EPR Protocol

In this section, we will present the *EPR Protocol*, proposed by Artur K. Ekert and inspired by the original BB84 algorithm. The original algorithm proposed in 1991 was similar to the BB84 algorithm, but it used three different basis to make the measurements, and entangled pairs of qubits. The entanglement allowed the two parties communicating to detect the presence of an eavesdropper by checking the *Bell inequality*.

However, in this section we will only explain a simplified scheme for the EPR Protocol, using entangled states and only two basis to make the measurements.

4.3.1 The simplified EPR Protocol

As we stated before, the EPR Protocol relies on Alice and Bob having entangled qubits in their possession. In particular, they need to share N qubits in the state $|\beta_{00}\rangle$, where Alice has the first qubit of the state and Bob the second. In order to obtain the qubits in their entangled state, it is possible that one of the parties prepared all the qubits, and sent the corresponding half of every bell state over a quantum channel. It is also possible that the two parties met at the same point in space, prepared the entangled states, and then they stored each their corresponding qubits for the next time they needed to communicate. However, we will not explore in more detail than that how the two parties manage to prepare the entangled states, and we will assume that this step is already completed.

For this protocol, Alice and Bob need to share a classical channel with the same condition as in the BB84 algorithm: it needs to be authenticated to make sure that an eavesdropper does not impersonate Bob. But unlike the BB84 protocol, if the two parties have all the Bell states already prepared, the quantum channel is not necessary.

For each Bell state, we will assume that Alice has the first qubit and Bob the second, and we will denote this by

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{4.1}$$

l Therefore, at the start of the algorithm, the state including all the entangled qubits is

$$\bigotimes_{i=1}^{N} |\beta_{00}\rangle_{AB} \tag{4.2}$$

With the Bell states prepared, Alice and Bob can start communicating following the steps described below.

Step 1: In the first step of the algorithm, Alice and Bob respectively choose $\Theta, \Theta' \in \{0,1\}^N$. Alice measures the i-th qubit with respect to the basis $H^{\Theta_i}\{|0\rangle, |1\rangle\}$. If $\Theta_i = 0$ she obtains either $|0\rangle$ or $|1\rangle$, and then saves the result of the measurement as a bit. However, if $\Theta_i = 1$, she will measure either $|+\rangle$ or $|-\rangle$. In this case, Alice will identify $|+\rangle$ with a binary 0 and $|-\rangle$ with a binary 1, and save the result as a bit. At the same time, Bob measures the i-th qubit with respect to the basis

$H^{\Theta'_i}\{|\,0\,\rangle, |\,1\,\rangle\}$, and identify the result of the measurement with either a binary 0 or a 1.

Notice that if we represent the state $|\,\beta_{00}\,\rangle$ in the Hadamard basis we obtain

$$\begin{aligned} |\,\beta_{00}\,\rangle &= \frac{1}{\sqrt{2}}(|\,00\,\rangle + |\,11\,\rangle) \\ &= \frac{1}{2\sqrt{2}}\left((|+\rangle + |-\rangle)(|+\rangle + |-\rangle) + (|+\rangle - |-\rangle)(|+\rangle - |-\rangle)\right) \\ &= \frac{1}{2\sqrt{2}}\left(|++\rangle + |--\rangle + |++\rangle + |--\rangle\right) \\ &= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \end{aligned} \tag{4.3}$$

With this equality we can be sure that, like in the BB84 algorithm, Alice and Bob will have the same results for the measurement for the i-th qubit when $\Theta_i = \Theta'_i$.

This is due to entanglement. Suppose that Alice measures the first qubit with respect to the Hadamard basis. Then, it will randomly collapse to either $|++\rangle$ or $|--\rangle$. If it collapses to $|++\rangle$, Alice will get a binary zero out of the measurement. If Bob then, by chance, also measures with respect to the Hadamard basis, since the qubit has already collapsed to $|++\rangle$ he will measure $|+\rangle$ with probability 1 and also get a binary zero out of the measurement.

In order to know at what positions Alice and Bob made the measurement with respect to the same basis, they need to exchange some information first. This is where the second step comes into place.

Step 2: This step consists of a public discussion. Now that all the qubits have been measured, Alice and Bob need to know at which indexes did they coincide making the measurements. For that reason, Alice shares her choice of Θ over the public channel, and so does Bob. After that, they discard all the qubits with indexes such that $\Theta_i \neq \Theta'_i$. Since Alice and Bob have a 50% chance of choosing the same basis for a given qubit, the length of the remaining qubits will be around $N/2$. The key obtained after discarding those positions is called the *raw key*.

Step 3: The last step of the algorithm is also dedicated to error detection, and there are two main reasons for this fact. The first and most important is eavesdropping. In the case that Alice sent to Bob the entangled qubits through a quantum channel, Eve could have intercepted the qubits in order to obtain information. If that were the case, a step of error detection should warn about the presence of Eve to the two parties establishing communication. The second reason to have this step of error correction is that entangled states can sometimes lose this property and become unentangled. Therefore, without correlation between Alice's and Bob's

qubits there could be errors in the raw key.

In order to check for errors, Alice and Bob agree on a subset of bits of the raw key, of size exactly one half the length of that key. They share through the public channel the value of the bits in those positions, and calculate an approximation of the QBER as the number of disagreeing bits divided by the number of bits shared.

If the approximation of the QBER calculated is below the threshold of errors that the two parties agreed on, then they use the remaining bits as the key. If not, they discard the remaining bits and abort the communication. Contrarily to what we did with the BB84 algorithm, we will not explore the eavesdropping techniques for the EPR Protocol.

Chapter 5

The CHSH Game

In this final chapter, we will analyze how a quantum strategy using entanglement can outperform any classical strategy in the *CHSH Game*.

5.1 Rules of the CHSH Game

In the CHSH Game, we have three parties, Alice and Bob, who are the *players*, and Charlie, the *referee*. To start the game, Charlie will choose $x, y \in \{0, 1\}$ at random, and send the bits to Alice and Bob respectively. When Alice receives x, she will reply $a \in \{0, 1\}$ to Charlie, and when Bob receives y, he will reply $b \in \{0, 1\}$ to Charlie. When the referee receives a, b checks whether $a \oplus b = x \wedge y$, where $\oplus$ denotes sum modulo two and $\wedge$ denotes multiplication modulo two. Alice and Bob win if the condition is satisfied.

It is important to note that Alice can have no information on y, and Bob no information on x. From the moment that both parties receive their corresponding bit, they are forbidden to communicate with one another. However, they can establish a strategy *before* the referee sends the bits, and then act according to said strategy to try and maximize their chances of winning.

We are going to study a classical strategy and a quantum one, to compare them and see if, in the case that Alice and Bob shared an entangled state, it would improve their chances of winning.

5.2 A Classical Approach

To study the classical version of the CHSH game, we will define what strategies can Alice and Bob agree on before starting the game, and then evaluate those against the referee's choice of $(x, y) \in \{0, 1\} \times \{0, 1\}$.

referee's choice	$(x,y)=(0,0)$	$(x,y)=(0,1)$	$(x,y)=(1,0)$	$(x,y)=(1,1)$
$\mathbf{a(x)\oplus b(y)}$	0	0	0	0
$\mathbf{x\wedge y}$	0	0	0	1
Result	Win	Win	Win	Fail

Table 5.1: Classical version of the CHSH game, where Alice and Bob always reply 0 to the referee.

Definition 5.1. *A* strategy *is a pair of functions*

$$\begin{aligned} a,b : \{0,1\} &\longrightarrow \{0,1\} \\ x &\mapsto a(x) \\ y &\mapsto b(y) \end{aligned}$$

Where $a(x)$ represents Alice's choice given a bit $x \in \{0,1\}$ and $b(y)$ represents Bob's choice given $y \in \{0,1\}$.

Given that there are only four applications that map $\{0,1\} \mapsto \{0,1\}$, Alice and Bob can only agree on 16 different strategies to play the game, and we can make use of this fact in order to calculate the probability of them winning. Let's consider for a case study the following strategy:

$$\begin{aligned} a(0) &\equiv 0 & b(0) &\equiv 0 \\ a(1) &\equiv 0 & b(1) &\equiv 0 \end{aligned}$$

With the strategy chosen, the referee elects one pair $(x,y) \in \{0,1\} \times \{0,1\}$ and sends each bit to Alice and Bob. Then they both respond with a bit corresponding to the chosen strategy. Considering the different four pairs $(x,y) \in \{0,1\} \times \{0,1\}$, the results of the game are described in table 5.1. Therefore, with the chosen strategy, Alice and Bob have a probability of $3/4$ of winning.

Checking all the other possibilities, we can see that for any strategy there is *at least* a pair $(x,y) \in \{0,1\} \times \{0,1\}$ in which the strategy will fail. Therefore, 75% is the best probability that Alice and Bob have of winning the game.

5.3 A Quantum Approach

Let's consider now that Alice and Bob prepared, before starting the game, a two qubit system in the state $|\,\beta_{00}\,\rangle_{AB} = \frac{1}{\sqrt{2}}(|\,0_A 0_B\,\rangle + |\,1_A 1_B\,\rangle)$. In this section, we

will present a strategy that Alice and Bob can follow in order to obtain a better winning probability than the 75% obtained by following the classical strategy. This will be possible thanks to the properties of the entangled states.

Consider the following qubit state:

$$|\psi_\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \qquad \theta \in [0, 2\pi) \tag{5.1}$$

And the matrix:

$$U_\theta = |0\rangle\langle\psi_\theta| + |1\rangle\langle\psi_{\theta+\pi/2}| \tag{5.2}$$

which is unitary by definition.

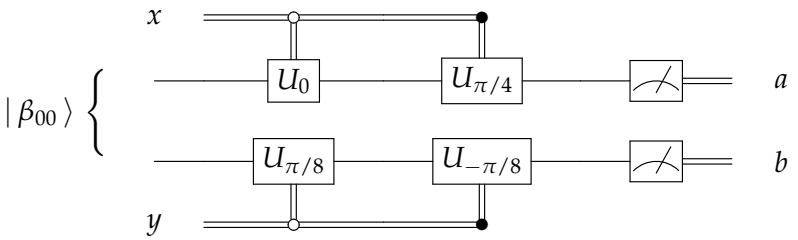
This state and the corresponding matrix will allow us to create a strategy that Alice and Bob can follow. Once the entangled state is prepared, the game starts and the referee chooses the corresponding pair $(x, y) \in \{0,1\} \times \{0,1\}$.

Alice receives her bit, x, and applies a unitary transformation to her qubit depending on the value of x. If the bit she has received is 0, she applies U_0 to her qubit, and if it is 1, she applies $U_{\pi/4}$.

Simultaneously, Bob receives y. If the bit is 0 he applies to his qubit the unitary transformation $U_{\pi/8}$, and if it is 1, he applies $U_{-\pi/8}$.

After applying the corresponding gates, Alice measures the qubit in her possession with respect to the computational basis $\{0,1\}$. If after the measurement the qubit has collapsed to the state $|0\rangle$, she replies a 0 to the referee. and if the qubit collapses on a $|1\rangle$, she replies a 1. Bob follows the same procedure, measuring his qubit in the computational basis and replying to the referee the outcome of the measurement. Finally, the referee computes $a \oplus b = x \wedge y$ and the game concludes with either a win or a fail.

We can represent both Alice's and Bob's choices depending on Charlie's x and y using the following quantum circuit:



(5.3)

In the circuit 5.3, the second row represents the qubit in Alice's possession, and the gates that she applies depending on the value of x. And the third row represents Bob's qubit and the gates that he applies depending on the value of y.

Let's explore how this strategy guarantees a better probability of winning for the two parties, compared to the 75% that guaranteed the classical strategy. We will explore in depth the case when the referee chooses the pair $(x, y) = (0, 0)$. Given this choice, the equation $a \oplus b = x \wedge y = 0$ will be satisfied in the case that $a = b = 0$ or $a = b = 1$.

To see what is the probability of both cases, we can explore the amplitudes of the two state qubit after the corresponding gates have been applied. Since we are looking at the case $(x, y) = (0, 0)$, Alice will have applied the gate U_0, and Bob the gate $U_{\frac{\pi}{8}}$. Hence, the state of the qubit *before* any measurement is made is given by

$$\left(U_0 \otimes U_{\frac{\pi}{8}}\right) | \beta_{00} \rangle \tag{5.4}$$

To calculate the probabilities of each measurement, it will be of great usefulness to be able to represent the state in 5.4 with the computational basis of $\mathcal{H}^{\otimes 2}$, $\{| 00 \rangle, | 01 \rangle, | 10 \rangle, | 11 \rangle\}$. With this representation, we can know the probabilities by looking at the corresponding amplitudes. There are two identities that are going to help us greatly, and those are presented below.

Identity 5.2. *The first identity comes easily by applying the properties of the tensor product to U_θ, obtaining:*

$$\begin{aligned} U_\alpha \otimes U_\beta = &\left(| 00 \rangle\langle \psi_\alpha \otimes \psi_\beta |\right) + \\ &\left(| 01 \rangle\langle \psi_\alpha \otimes \psi_{\beta+\pi/2} |\right) + \\ &\left(| 10 \rangle\langle \psi_{\alpha+\pi/2} \otimes \psi_\beta |\right) + \\ &\left(| 11 \rangle\langle \psi_{\alpha+\pi/2} \otimes \psi_{\beta+\pi/2} |\right). \end{aligned} \tag{5.5}$$

Identity 5.3. *The second identity that we will prove is*

$$\langle \psi_\alpha \otimes \psi_\beta | \beta_{00} \rangle = \frac{\cos(\alpha - \beta)}{\sqrt{2}} \tag{5.6}$$

To prove this identity, let's first expand the tensor product $\psi_\alpha \otimes \psi_\beta$ and represent it in the computational basis of $\mathcal{H}^{\otimes 2}$. Applying the linearity of the tensor product, we obtain

$$\begin{aligned} | \psi_\alpha \otimes \psi_\beta \rangle = &\cos\alpha \cos\beta | 00 \rangle + \\ &\cos\alpha \sin\beta | 01 \rangle + \\ &\cos\beta \sin\alpha | 10 \rangle + \\ &\sin\alpha \sin\beta | 11 \rangle \end{aligned} \tag{5.7}$$

Now, expanding the inner product in 5.6, we obtain

$$\begin{aligned}\langle \psi_\alpha \otimes \psi_\beta \,|\, \beta_{00} \rangle &= \langle \psi_\alpha \otimes \psi_\beta \,|\, \frac{1}{\sqrt{2}} \left(|\, 00 \rangle + |\, 11 \rangle \right) \rangle \\ &= \frac{1}{\sqrt{2}} \left(\langle \psi_\alpha \otimes \psi_\beta \,|\, 00 \rangle + \langle \psi_\alpha \otimes \psi_\beta \,|\, 11 \rangle \right) \\ &= \frac{1}{\sqrt{2}} \left(\cos\alpha \cos\beta + \sin\alpha \sin\beta \right) = \frac{\cos(\alpha - \beta)}{\sqrt{2}}\end{aligned} \tag{5.8}$$

Proving the equation in 5.6.

Given that Charlie sent the pair $(x, y) = (0, 0)$ to Alice and Bob respectively, Alice has applied the gate U_0 to her qubit, and Bob the gate $U_{\frac{\pi}{8}}$. Therefore, the entangled qubit is in the state

$$\left(U_0 \otimes U_{\frac{\pi}{8}} \right) |\, \beta_{00} \rangle \tag{5.9}$$

Using identities 5.2 and 5.3 we can represent the state in 5.9 using the computational basis:

$$\begin{aligned}\left(U_0 \otimes U_{\frac{\pi}{8}} \right) |\, \beta_{00} \rangle = \; & \frac{\cos(-\pi/8)}{\sqrt{2}} |\, 0_A 0_B \rangle \\ & + \frac{\cos(-5\pi/8)}{\sqrt{2}} |\, 0_A 1_B \rangle \\ & + \frac{\cos(3\pi/8)}{\sqrt{2}} |\, 1_A 0_B \rangle \\ & + \frac{\cos(-\pi/8)}{\sqrt{2}} |\, 1_A 1_B \rangle\end{aligned} \tag{5.10}$$

Since the referee chose the pair $(x, y) = (0, 0)$, Alice and Bob have to answer either $a = b = 0$ or $a = b = 1$ in order to win the game. This translates to them measuring the state $|\, 00 \rangle$ or the state $|\, 11 \rangle$, since both parties will answer the result of the measurement with respect to the computational basis.

With the amplitudes calculated in 5.10, we can see that the probability of winning the game is

$$\left(\frac{\cos(-\pi/8)}{\sqrt{2}} \right)^2 + \left(\frac{\cos(-\pi/8)}{\sqrt{2}} \right)^2 = \frac{2 + \sqrt{2}}{4} \approx 0.85 \tag{5.11}$$

and the probability of losing is

$$\left(\frac{\cos(-5\pi/8)}{\sqrt{2}} \right)^2 + \left(\frac{\cos(3\pi/8)}{\sqrt{2}} \right)^2 = \frac{2 - \sqrt{2}}{4} \approx 0.15 \tag{5.12}$$

It can be shown with similar arguments that for the remaining three cases of referee's choices, $\{(0,1),(1,0),(1,1)\}$, Alice and Bob win with the same probability of $(2+\sqrt{2})/4$.

It is clear then that the strategy using an entangled pair is more effective than any classical strategy.

Bibliography

[1] P. A. M. Dirac (1939). *A new notation for quantum mechanics*. Mathematical Proceedings of the Cambridge Philosophical Society, 35, pp 416-418 https://doi.org/10.1017/S0305004100021162

[2] Fehr, S. *Quantum Cryptography*. Found Phys 40, 494-531 2010. https://doi.org/10.1007/s10701-010-9408-4

[3] Vidal, G. *Efficient classical simulation of slightly entangled quantum computations*. https://doi.org/10.1103/PhysRevLett.91.147902

[4] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*. Nature 390, 575 (1997). https://doi.org/10.1038/37539

[5] Wootters, W., Zurek, W. A single quantum cannot be cloned. *Nature* **299**, 802-803 (1982). https://doi.org/10.1038/299802a0

[6] Deutsch David and Jozsa Richard 1992. Rapid solution of problems by quantum computation. Proc. R. Soc. Lond. A439553-558 http://doi.org/10.1098/rspa.1992.0167

[7] C. H. Bennett and G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984. https://doi.org/10.1016/j.tcs.2014.05.025.

[8] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). *The security of practical quantum key distribution*. Reviews of Modern Physics, 81(3), 1301-1350. https://doi.org/10.1103/revmodphys.81.1301

[9] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). *Quantum cryptography*. Reviews of Modern Physics, 74(1), 145-195.

https://doi.org/10.1103/revmodphys.74.145

[10] C. Lee, I. Sohn and W. Lee, *Eavesdropping Detection in BB84 Quantum Key Distribution Protocols*, in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2689-2701, Sept. 2022. https://doi.org/10.1109/TNSM.2022.3165202.

[11] Elboukhari, Mohamed, Azizi, Mostafa ans Azizi, Abdelmalek. (2010). Quantum Key Distribution Protocols: A Survey.

[12] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in quantum cryptography*. Adv. Opt. Photon. 12, 1012-1236 (2020). https://doi.org/10.1364/AOP.361502

[13] Nielsen, M. A., and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*: 10th Anniversary Edition. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511976667

[14] Yanofsky NS, Mannucci MA. Quantum Computing for Computer Scientists. Cambridge University Press; 2008. https://doi.org/10.1017/CBO9780511813887

[15] Ekert, A. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67(6), 661-663. https://doi.org/10.1103/physrevlett.67.661

[16] Hirvensalo, Mika. (2007). *EPR paradox and Bell inequalities*. Bulletin of the European Association for Theoretical Computer Science EATCS.

[17] KAYE, Phillip., LAFLAMME, R. y MOSCA, M., 2007. *An Introduction to quantum computing*. Oxford. ISBN 019857049X.

[18] David Kahn, *The Codebreakers*, Macmillan, 1967. ISBN-10: 0684831309

[19] FIPS PUB 46, 1977 Edition, January 15, 1977 - *DATA ENCRYPTION STANDARD*. U.S. Department of Commerce, National Bureau of Standards.

[20] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, Inc. ISBN: 0471128457

[21] Rivest, Ronald L. *Cryptology*. Handbook of Theoretical Computer Science Volume 1 (1990): 717-755.

[22] Morkel, Toni and Jhp Eloff. *Encryption Techniques: a Timeline Approach*. (2004).

[23] Julius O. Olwenyi, Aby Tino Thomas, Ayad Barsoum. *Cryptography in Modern World*. St. Mary's University, San Antonio, TX (USA)