UNIVERSIDAD
DE GRANADA

# DE NOVO GENOME ASSEMBLY USING QUANTUM ANNEALING

JOSÉ ANTONIO ÁLVAREZ OCETE

Trabajo Fin de Grado
Doble Grado en Ingeniería Informática y Matemáticas

**Tutores**
Carlos Cano
Antonio Lasanta

FACULTAD DE CIENCIAS
E.T.S. INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

*Granada, a 3 de julio de 2021*

# ÍNDICE GENERAL

# RESUMEN

TODO: resumen

TODO: que en el resumen en inglés no ponga en la cabecera Resumen.$^{en}$ español.

# 1

# QUANTUM MECHANICS MODEL

Quantum Mechanics are a mathematical framework in which quantum physics are developed. In this section, we will develop a quantum mechanics model in order to understand quantum computing. The Quantum Postulates will be our guidance. They provide a connection between the physical world and the mathematical formalization. We will provide context and formalization for each postulate, so both the mathematical precision and intuition notions are developed at the same time. This development is based on [1], [2] and [3].

## 1.1 POSTULATE 1: STATE SPACE

The first postulate sets the environment in which we will operate: The State Space. It will be a Hilbert space associated to a physicial system. Let us rigorously define the necessary concepts using the Bra-ket notation. We will start by revisiting the required linear algebra.

### 1.1.1 *Bra-ket notation*

Let $V$ be a complex vector space. That is, a vector space over $\mathbb{C}$. We will restrict our study to finite complex vector spaces. If $z$ is a vector in $V$, we will denote its coordinates either as $z = (z_1, z_2, \dots, z_n)$ or by column notation:

$$z = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}$$

Since $V$ is a vector space we have two basic operations: (vector) addition and scalar multiplication.

In quantum mechanics, the usual notation is the Dirac's, also known as *bra-ket* notation. In this context, vectors in a complex vector space are denoted as $|\varphi\rangle$ and are known as *kets*. The only exception to this is the zero vector, which will be denoted as $0 = (0, \dots, 0)$ instead of $|0\rangle$ since $|0\rangle$ will be used as something completely different. A *vector subspace* $W$ of $V$ is a subset of $W$ closed for addition and scalar multiplication.

A *base* of a vector space is a set of vectors $|v_1\rangle, \dots, |v_n\rangle$ such that they are linearly independent and any given vector $|v\rangle$ can be written as a linear combination of them: $|v\rangle = \sum_{i=1}^{n} \alpha_i |v_i\rangle$. The *dimension* of a vector space is the number of elements in any of its bases, which is independent from the chosen base.

**Definition 1.** Given two complex vector spaces $V$ and $W$, a *linear operator* is an application $M : V \to W$ that is linear in its inputs:

$$M\Big(\alpha|u\rangle + \beta|w\rangle\Big) = \alpha M(|u\rangle) + \beta M(|w\rangle)$$

If $V$ to $W$ have dimensions $n$ and $m$ respectively, there is a bijection between the operators from $V$ to $W$ and the $n$ by $m$ matrices. Given an operator $M$, the obtained matrix $M'$ is called the *matrix representation* of the linear operator. Furthermore, $M(|u\rangle) = M' \cdot |u\rangle$, so we usually denote the linear operator and its matrix representation by the same letter, and $M(|u\rangle)$ simply as $M|u\rangle$.

We will usually refer to linear operators simply as *operators*.

### 1.1.2 *Inner product and Hilbert Spaces*

Let us define another operation within the complex vector spaces.

**Definition 2.** Let $V$ be a complex vector space. An inner product $\langle \cdot | \cdot \rangle : V^2 \to \mathbb{C}$ is a function such that:

1) $\langle \cdot | \cdot \rangle$ is sesquilinear. That is,

  1.1) $\langle \cdot | \cdot \rangle$ is conjugate symmetric: for all $u, v$ in $V$, $\langle u|v\rangle = \overline{\langle v|u\rangle}$.

  1.2) $\langle \cdot | \cdot \rangle$ is linear on the second variable: for all $u, v, w$ in $V$ and $\alpha, \beta$ in $\mathbb{C}$:

$$\langle u|\alpha v + \beta w\rangle = \alpha\langle u|v\rangle + \beta\langle u|w\rangle$$

2) $\langle \cdot | \cdot \rangle$ is definite positive. That is, for all $u$ in $V$, $\langle u|u\rangle \geq 0$ and $\langle u|u\rangle = 0 \iff v = 0$.

Given this properties it can easily be proven that $\langle \cdot | \cdot \rangle$ is also conjugate linear on the first variable. That is, for all $u, v, w$ in $V$ and $\alpha, \beta$ in $\mathbb{C}$:

$$\langle \alpha u + \beta v|w\rangle = \overline{\alpha}\langle u|w\rangle + \overline{\beta}\langle v|w\rangle$$

We will sometimes denote the inner product $\langle \cdot | \cdot \rangle$ as $(\cdot, \cdot)$ to simplify notation.

Two vectors are said to be *orthonormal* if their inner product is zero. We define the norm of a vector $|v\rangle$ by:

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

A *unit vector* is a vector $|v\rangle$ such that $\| \, |v\rangle \quad \| = 1$. We also say that $|v\rangle$ is *normalized*, and we can normalize any vector except the zero vector by dividing it by its norm.

A base $|v_1\rangle, \ldots, |v_n\rangle$ is said to be *orthonormal* if every vector is a unit vector and they are pairwise orthogonal. That is, $\langle v_i | v_j \rangle = \delta_{ij}$ where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

**Definition 3.** An *inner product space* is a vector space with an associated inner product. A **Hilbert Space** is an inner product space that is also complete.

Hausdorff's Theorem states that every finite normed space is complete, therefore every finite inner product space over $\mathbb{C}$ is a Hilbert space [4]. Again, by Hausdorff's theorem, we know that every $n$ dimensional Hilbert space is isomorphic to $\mathbb{C}^n$. Thus, $\mathbb{C}^n$ is the canonical $n$ dimensional Hilbert space. Our study will be focused on these spaces.

Let $\alpha = a + i \cdot b \in \mathbb{C}$. We define the *conjugate*, $\bar{\alpha}$, as $\bar{\alpha} = a - i \cdot b$. The canonical inner product in $\mathbb{C}^n$ is:

$$\langle u | v \rangle \; = \sum_{i=1}^{n} \overline{u_i} v_j$$

where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$, for every $u, v$ in $\mathbb{C}^n$.

### 1.1.3 *Postulate 1 statement*

The reader should be familiar by now with the notation and the necessary linear algebra to formulate the first postulate.

> **Postulate 1.** Associated to any isolated physical system is a complex vector space with an inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

An important concern with this postulate is that it does not tell us which is the state space of a given system, nor its state vector. Although up to this point we cannot formally assure this, in quantum computing the state space will be fixed: $\mathbb{C}^{2^n}$ for an n-qubits system. Our evolving state vector will be a vector $2^n$-vector.

Let us start by modulating a simpler system: a single qubit system.

**Definition 4.** A state vector of the state space $\mathbb{C}^2$ is called a **qubit**. Thus, $\mathbb{C}^2$ may be called a single qubit state space.

Suppose $|0\rangle$, $|1\rangle$ form an orthonormal basis of a 2-dimensional Hilbert space. Then, any state vector in this state space may be described as:

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

where $\alpha, \beta$ are complex numbers called *amplitudes*. Thus, the condition that $|\varphi\rangle$ is a unit vector, $\langle\varphi|\varphi\rangle = 1$ is equivalent to $|\alpha|^2 + |\beta|^2 = 1$. This is known as the *normalization condition*.

We will always think of $|0\rangle$, $|1\rangle$ as a previously fixed orthonormal base. A linear combination of state vectors $\sum_i a_i|\varphi_i\rangle$ is called a *superposition* of the states $|\varphi_i\rangle$ with amplitudes $a_i$ respectively. For example, the state

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

is a superposition of the states $|0\rangle$ and $|1\rangle$ with amplitudes $1/\sqrt{2}$ and $-1/\sqrt{2}$ respectively.

### 1.1.4 *Quantum Computation Perspective: The Quantum Bit*

The bit is the minimum measure of information on classical computation and classical information theory. Everything in these fields is built from scratch based on bits. Likewise, quantum computing and quantum information theory are built upon the **qubit**.

We have reached the qubit definition from quantum physics and pure mathematics, describing the qubit as a mathematical object independent of its physical implementation. By describing them as mathematical entities we will be able to explore their properties mathematically without having to worry about the physics underneath. This allows us to construct the quantum computing and quantum information theories independently of the physical implementation.

So, intuitively, what is a qubit? Just like the classical bit, a qubit has a state. For the bit, the two only possible states are either 0 or 1. A qubit can take the states $|0\rangle$ and

$|1\rangle$ -corresponding to the classical states 0 and 1- or it can be in a *linear combination* of them:

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

Where $\alpha$ and $\beta$ are complex numbers. Thus, we can describe a qubit as a vector in a two-dimensional complex Hilbert space (the canonical $\mathbb{C}^2$), where $|0\rangle$ and $|1\rangle$ form an orthonormal basis called the *computational basis*. $|0\rangle$ and $|1\rangle$ will be called *computational basis states*.

At this point, the reader may ask themselves if a qubit may even physically exist, not just as a mathematical entity. After all, the first postulate states that given a *physical system*, there is an associated state space and vector states that describe the system. However, we define a qubit from state space ($\mathbb{C}^2$) without considering a physical system.

The answer is positive: there are numerous physical systems such that their associated state spaces are ($\mathbb{C}^2$). Thus, modeling a qubit. More intuitive examples are provided in section 1.2.4 and precise physical implementations are briefly discussed in section [TODOref].

## 1.2 POSTULATE 2: MEASUREMENT

The second postulate describes how states are 'measured', that is, how an outside observer may look inside the system. In classical physics, consider a simple system of a moving particle. 'Measuring' would be recording, for instance, the particle mass and speed at a given time. That is, someone **outside** the system would look **into** the system to record some information. Lastly, in the classical computation model measuring a bit is simply retrieving its content.

In quantum physics, measuring has some unexpected and sometimes counter-intuitive properties. Let us provide some linear algebra context before formulating the second postulate.

### 1.2.1 *Outer product*

**Definition 5.** Let $V, W$ be two vector spaces and $|v\rangle \in V, |w\rangle \in W$. We define the *outer product* between $|v\rangle$ and $|w\rangle$, $|w\rangle\langle v|$, as the only linear operator such that for any $|v'\rangle \in V$,

$$(|w\rangle\langle v|)\ |v'\rangle = |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

These identities provide a dual interpretation: the already known product of a complex value $\langle v|v'\rangle$ with a vector $|w\rangle$, and the application of the new operator, the outer product $|w\rangle\langle v|$ to the vector $|v'\rangle$. The outer product is defined so that this duality occurs.

Let us consider linear combinations of outer products. By definition, $\sum_i a_i|w_i\rangle\langle v_i|$ is the operator that transforms $|v'\rangle$ into $\sum_i a_i|w_i\rangle\langle v_i|v'\rangle = \sum_i a_i\langle v_i|v'\rangle|w_i\rangle$.

The most important result concerning outer products is the *completeness relation*:

**Proposition 1** (Completeness relation). *Let $|i\rangle$ be any orthonormal basis of a finite vector space $V$. Then:*

$$\sum_i |i\rangle\langle i| = I$$

**Proof.** Let $|v\rangle \in H$. $|v\rangle$ can be expressed as $\sum_i v_i|i\rangle$ for some complex numbers $v_i$. Notice that $\langle i|v\rangle = v_i$. Therefor:

$$|v\rangle = \sum_i v_i|i\rangle = \sum_i \langle i|v\rangle|i\rangle = \sum_i |i\rangle\langle i|v\rangle = \left(\sum_i |i\rangle\langle i|\right)|v\rangle$$

Since $|v\rangle$ was arbitrary, this proves that $\sum_i |i\rangle\langle i| = I$. □

**Corollary 1** (Cauchy-Schwarz inequality). *For any two vectors $|v\rangle, |w\rangle$ in a Hilbert space,*

$$|\langle v|w\rangle|^2 \leq \langle v|w\rangle\langle w|w\rangle$$

*where the equality occurs if and only if $|v\rangle$ and $|w\rangle$ are linearly dependant*

**Proof.** We provide a proof supposed that our Hilbert space is finite.

Let $|v\rangle, |w\rangle$ be two vectors of a finite Hilbert space $H$. Since $H$ is finite, using the Gram-Schmidt procedure we may obtain a basis $|i\rangle$ where the first vector is $|w\rangle/\sqrt{\langle w|w\rangle}$. Using the completeness relation $\sum_i |i\rangle\langle i| = I$:

$$\langle v|v\rangle\langle w|w\rangle = \langle v|I|v\rangle\langle w|w\rangle = \langle v|\sum_i(|i\rangle\langle i|)|v\rangle\langle w|w\rangle = \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle$$

The sum of a list of positive numbers is obviously greater than its first element, so:

$$\sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \geq \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle = \langle v|w\rangle\langle w|v\rangle = |\langle w|v\rangle|^2$$

Lastly, the equality occurs if and only if $\langle v|i\rangle = 0$ for every $|i\rangle \neq |w\rangle/\sqrt{\langle w|w\rangle}$. But since $|i\rangle$ is a base, this means $|v\rangle$ and $|w\rangle$ are linearly dependent. □

### 1.2.2 *Unitary and Hermitian operators*

Another way of looking at the inner product is the *adjoint*.

**Definition 6.** Let $A$ be an operator between $\mathbb{C}^n$ and $\mathbb{C}^m$, finite dimensional Hilbert spaces. That is, $A \in \mathcal{M}_{n\times m}(\mathbb{C})$. Then, its *adjoint* or *conjugate transpose* $A^\dagger$ is defined by:

$$(A^\dagger)_{ij} = \bar{A}_{ji}$$

If $|v\rangle$ is a vector, we can compute its adjoint by seeing it as a matrix. By convention, we will denote $|v\rangle^\dagger = \langle v|$. Adjoints of vector are usually called *bras*, making given sense to the *bra-ket* notation since $\langle v| \cdot |v\rangle = \langle v|v\rangle$, where $\cdot$ denotes the dot product.

Some useful algebraic identities associated to adjoints are:

- Given an operator $A \in \mathcal{M}_n(\mathbb{C})$, $A^\dagger$ is the only operator such that for any two vectors $|u\rangle, |v\rangle \in \mathbb{C}^n$: $(|u\rangle, A|v\rangle) = (A^\dagger|u\rangle, |v\rangle)$
- For any two operators $A, B$, $(AB)^\dagger = B^\dagger A^\dagger$.
- As a corollary, for any vector $|v\rangle$ and for any operator $A$, $(A|v\rangle)^\dagger = \langle v|A^\dagger$.

**Definition 7.** An operator $A$ is said to be *normal* if $AA^\dagger = A^\dagger A$.

Characterization of normal operators is provided in Theorem 1. There are two particular cases of normal operators that will be of special interest to us:

**Definition 8.** An operator $A$ is said to be *Hermitian* if its adjoint is itself: $A^\dagger = A$.

**Definition 9.** A matrix $U$ is said to be *unitary* if $UU^\dagger = I$. Similarly, an operator is said to be *unitary* if $UU^\dagger = I$. A unitary operator $U$ also fulfills that $U^\dagger U = I$.

Clearly, Hermitian and unitary operators are also normal. The importance of unitary matrices and operators in quantum computing lies in the following

**Proposition 2.** *Unitary operators preserve inner product between vectors. Thus, they also preserve the norm of a vector.*

**Proof.** Let $|u\rangle, |v\rangle \in \mathbb{C}^n$ and $U \in \mathcal{M}_n(\mathbb{C})$ be a unitary operator. Then:

$$(U|u\rangle, U|v\rangle) = \langle u|U^\dagger U|v\rangle = \langle u|I|v\rangle = \langle u|v\rangle = (|u\rangle, |v\rangle)$$

Which proves the proposition. □

An important type of Hermitian operators is the projectors.

**Definition 10.** Let $W$ be a $k$-dimensional subspace of the $d$-dimensional vector space $V$. Let $|1\rangle, \dots, |d\rangle$ be an orthonormal base of $V$ where $|1\rangle, \dots, |k\rangle$ is an orthonormal base of $W$. The *projector* onto the subspace $W$ is defined by:

$$P = \sum_{i=1}^{k} |i\rangle\langle i|$$

It can easily be shown that this definition is independent from the chosen base $|1\rangle, \ldots, |k\rangle$. Since $|v\rangle\langle v|$ is Hermitian for any vector $|v\rangle$, $P$ is also Hermitian: $P = P^{\dagger}$. We will often refer to the subspace onto which $P$ projects simply as $P$ for comodity. The *orthonormal completement* of $P$ is $Q \equiv I - P$. It can be verified the vector subspace $Q$ is spanned by the base $|k+1\rangle, \ldots, |d\rangle$.

As the reader may already imagine, n-qubits systems will be represented as vector states or *certain* state spaces. That is, as unitary vectors of certain Hilbert spaces. Thus, our definition of transformations on qubits must preserve their norm. These will be the qubits gates, which will be represented as unitary operators.

On the other hand, Hermitian operators will be key in order to study how a quantum system evolves with time using the Schrodinger equation in the third Postulate.

Finally, projectors will be used on as particular way of measurement and will be further discussed in section 1.4.3, once systems with multiple qubits have been introduced.

### 1.2.3 *Postulate 2 statement*

As previously discussed, the second postulate describes how a quantum system may be measured.

> **Postulate 2.** Quantum measurement are described by a collection $\{M_m\}$ of *measurement operators*. These act on the state space associated to the physical system being measured. The index $m$ refers to the measurement outcomes that may occur. That is, if $|\varphi\rangle$ is the vector state before measure, then the probability of the result $m$ occurring is:
>
> $$p(m) = \langle\varphi|M_m^{\dagger} M_m|\varphi\rangle$$
>
> and the state of the system after the measurement is:
>
> $$\frac{M_m|\varphi\rangle}{\sqrt{p(m)}}$$
>
> Finally, the measurement operator satisfy the *completeness equation*:
>
> $$\sum_m M_m^{\dagger} M_m = I$$

The completeness equation is equivalent to the fact that the probabilities of the different possible outcomes add up to one:

$$\sum_m p(m) = \sum_m \langle\varphi|M_m^\dagger M_m|\varphi\rangle = \langle\varphi|\sum_m (M_m^\dagger M_m)|\varphi\rangle = \langle\varphi|\varphi\rangle = 1$$

which holds for every state vector since they are unitary. Reciprocally, this equation occurring for every state vector $|\varphi\rangle$ implies the completeness equation.

The reader may have already noticed a huge difference between classic and quantum measurement: The measured state **changes** after the measurement. This means that we interfere with the system by merely looking into it! It will ultimately translate into huge differences between classical and quantum computing, such that we will generally not be able to clone a qubit (see theorem 3).

Let us look at an important example: *measurement of a qubit on the computational basis*. That is, measuring a qubit with two possible outcomes: $|0\rangle$ and $|1\rangle$. Although this is a particular case of projective measurement (further explained in section 1.4.3), it is worth introducing it now to deepen our understanding of qubits.

To obtain such results we use the operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. In order for $\{M_0, M_1\}$ to be a correct collection of measurement operators they must satisfy the completeness equation. Observe that each operator is Hemitian: $M_i^\dagger = (|i\rangle\langle i|)^\dagger = (\langle i|)^\dagger(|i\rangle)^\dagger = |i\rangle\langle i| = M_i$. Furthermore, $M_i^2 = |i\rangle\langle i|i\rangle\langle i| = |i\rangle\langle i| = M_i$.

Finally, the computational basis is an orthonormal basis and therefore the completeness relation tells us that:

$$\sum_i |i\rangle\langle i| = 1$$

We can see that the completeness equation holds:

$$\sum_i M_i^\dagger M_i = \sum_i M_i^2 = \sum_i M_i = \sum_i |i\rangle\langle i| = 1$$

Let's measure using this operators, also called *measure in the computational basis*, to better understand the measurement. Suppose the state being measured is $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then, the probability of obtaining the outcome 0 is:

$$p(0) = \langle\varphi|M_0^\dagger M_0|\varphi\rangle = \langle\varphi|M_0|\varphi\rangle = |a|^2$$

Similarly, the probability of obtaining the outcome 1 is $p(1) = |b|^2$. Naturally, $|a|^2 + |b|^2 = 1$. What happens after measuring? The post-measurement state will be, respectively if we measured 0 or 1:

$$\frac{M_0|\varphi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$$

$$\frac{M_1|\varphi\rangle}{|b|} = \frac{b}{|b|}|1\rangle$$

Factors like $a/|a|$ are known as *phases*. An importan result of quantum mechanics assures that multiplying by factors like these does not affect the state vector [1], so we virtually obtained $|0\rangle$ and $|1\rangle$. We may appreciate now how dividing by $\sqrt{p(m)}$ in the post-measurement state is only done so the resulting vector is a unit vector.

So if we measured a 0, the post-measurement vector will be $|0\rangle$ and vice-versa. Any measurements performed after the first one will yield exactly the same result. This behavior is called *qubit collapsing*.

We defined measurement to be independent of any basis so we may measure in the most convenient basis at each point. For example, we may use the following other basis:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

It can easily be proven that $\{|+\rangle, |-\rangle\}$ is a basis and therefore it satisfies the completeness equation. In fact, the operators $M_+ = |+\rangle\langle+|$ and $M_- = |-\rangle\langle-|$ satisfy the completeness equation. Using this operators, measuring the qubit $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ will output $+$ with probability:

$$p(+) = \langle\varphi|M_+^\dagger M_+|\varphi\rangle = \langle\varphi|M_+|\varphi\rangle = \langle\varphi|+\rangle\langle+|\varphi\rangle = \langle\varphi|+\rangle^2 =$$

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

$$p(-) = \frac{(\alpha-\beta)^2}{2}$$

And, naturally, $p(+) + p(-) = 1$. So $|\varphi\rangle$ will collapse to $|+\rangle$ with probability $(\alpha + \beta)^2/2$ when measured with this operators. Observe that the post-measurement state will never be $|0\rangle$ nor $|1\rangle$ in this case, we made the qubit collapse to the chosen state basis.

Finally, there is a technical fineness between the first and second postulates worth mentioning. The first postulate was stated for an *isolated* physical system, but by measuring the system we interfere with it. However, measuring devices are also quantum systems, so together the measured and the measuring system form a larger isolated system (it may be necessary to include more quantum systems, but this can be done).

### 1.2.4 *Real life qubit examples*

In classical computation, we may know the state of a bit by consulting it. That is, what can simply retrieve that information from the bit. The first difficulty we find in quantum computing is that once we *measure* a qubit it *collapses* to either $|0\rangle$ with probability $|\alpha|^2$, or to $|1\rangle$ with probability $|\beta|^2$. The obtained output reflects the qubit state *after* it has collapsed to either one of these states, so the outcome may only be either $|0\rangle$ or $|1\rangle$. This means that we may never retrieve directly the values $\alpha$ and $\beta$. Thus, being unable to clone a qubit. This is the main idea behind the no-cloning theorem 3.

We can, however, initialize qubits in a certain state and apply some operations to them in order to alter their coefficients, thus knowing their exact value. However, once a single measurement is done, the qubit collapses and the $\alpha$ and $\beta$ values are 'lost'.

Superposition and collapsing might be counter-intuitive concepts, so let us look at them with an analogy. We can think of a perfect coin being tossed as the following qubit:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

This does **not** represent a coin that has landed somehow on its side, but a spinning coin that has not landed yet. Upon measuring it, we 'make the coin land' and see the result: either heads or tails, and neither of the states in between. This example also describes the qubit collapse: once the coin has landed, we will see the same result every time we look at it -obviously-, just like every time a qubit is measured after the first measurement, the outcome will be the same since it has already collapsed. We will return to this state, also known as the Bell state, in section 1.4.2.

On the other hand, this was quite an inaccurate example since the system is not really isolated, although it was interesting intuition-wise. One of the first (accurate) qubit models ever proposed was the Schrodinger's Cat [5] [6]. In this hypothetical experiment, a cat would be locked in a room for an hour with a device that during that hour would *perhaps* trigger, killing the cat. On the other hand, with equal probability, it would not trigger at all. After the whole hour elapses, the cat would be alive and dead with equal probability, ending up in a halfway state. In this case, our computational bases would be the states alive and dead, and we achieve the state $|+\rangle$ after that hour. Once we open the room and check on the cat, our qubit collapses to either state and stays on it until further disturbance.

Although physical implementations are discussed in section [TODOref chapter], we cannot proceed any further without providing a more accurate and reproducible description of a qubit than 'a coin being tossed' and such a hypothetical cat experiment. A possible realization of a qubit is an electron in a single atom's orbit, as seen in Figure 1. An electron in an orbit may be in the so-called *ground* and *excited* states, $|0\rangle$ and $|1\rangle$ respectively, depending on its energy. By shining light to the electron with a certain energy and for a certain amount of time, one can make the electron move from the ground state to the excited state and vice versa. But most interestingly, one can apply the light to the electron during a smaller amount of time, moving the electron somehow 'halfway' between both states.

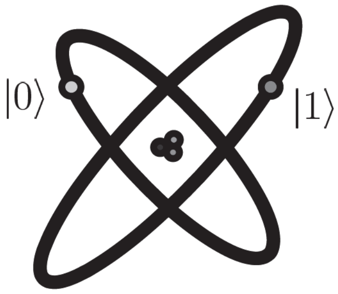

Figura 1: Qubit represented by two electron orbits in an atom, [1].

## 1.3 POSTULATE 3: EVOLUTION

The third postulate of quantum mechanics modulates the evolution of a quantum system. That is, the evolution of the state vector that describes the system. In order to properly formalize it, the concepts of eigenvectors, eigenvalues, and Hermitian operators are required.

### 1.3.1 *Eigenvalues and eigenvectors*

**Definition 11.** Let $V$ be a vector space and $A$ an operator on $V$. An *eigenvector* is a non zero vector $|v_\lambda\rangle$ such that $A|v_\lambda\rangle = \lambda|v_\lambda\rangle$ for a complex value $\lambda$ called the associated *eigenvalue*.

Eigenvalues and their associated eigenvectors will usually be denoted with the same letter for simplicity: $\lambda$ and $|\lambda\rangle$. We assume the reader is familiar with eigenvectors and values basic notions. For instance, that they may be calculated using the *characteristic equation*: $|I - \lambda A| = 0$.

**Definition 12.** A *diagonal representation* of an operator $A$ is a representation $\sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$ where the $|\lambda_i\rangle$ form an orthonormal set of A's eigenvectors and $\lambda_i$ are the respective eigenvalues. An operator is said to be *diagonalizable* if it allows a diagonal representation.

*Example* 1. As an example of this, let us consider the following matrix:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This matrix is called the *Z Pauli* matrix. It is relevant for quantum computing and it will be introduced later on along with the rest of the Pauli matrices. For now, Let's compute its diagonalizable representation. Since it is already diagonal we can infer that its eigenvalues are $\{1, -1\}$. Computing the diagonal representation we realize that a pair orthonormal eigenvectors are $\{|0\rangle, |1\rangle\}$ respectively. Therefore:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Normal operators have significant relevancy thanks to the following result:

**Theorem 1** (Spectral Decomposition Theorem)**.** *An operator $A$ is normal if and only if it is diagonalizable.*

**Proof.** TODO: To be copied, Box 2.2, page 72, Nielsenchen. □

Since Hermitian and unitary operators are normal, it follows the next

**Corollary 2.** *Any Hermitian operator is diagonalizable. Any unitary operator is diagonalizable.*

### 1.3.2 *Postulate 3 statement*

> **Postulate 3.** The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\varphi\rangle$ of the system at time $t_1$ is related to the state $|\varphi'\rangle$ of the system at time $t_2$ by a unitary operator $U$ which depends only on the times $t_1$ and $t_2$,
>
> $$|\varphi'\rangle = U|\varphi\rangle$$

Just like the first postulate does not provide the state space or state vector of the system, the third postulate does not provide the unitary transformation that concretes this evolution. For our quantum computing case, we will be the ones to define the unitary transformation to the system. That is, the quantum circuit that transforms our qubit.

*Example* 2. Let's consider the *X Pauli matrix*, also known as the *bit flip* matrix:

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

It is called the bit flip matrix because it takes $|0\rangle$ to $|1\rangle$ and vice-versa:

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

This product that we just computed is precisely what postulate 3 states: the evolution of our state vector following the unitary operator $X$: $X|0\rangle = |1\rangle$. Even though for an arbitrary system we do not know the specific unitary transformation the system follows, we can create systems that follow certain desired transformations. These are the basics of quantum gates and quantum circuits.

The description of the system evolution provided by Postulate 3 only bears information for those fixed times $t_1$ and $t_2$. A continuous time-description of this evolution is provided by the Schrodinger equation, which provides a redefinition of the second postulate.

> **Postulate 3'.** The time evolution of the state of a *closed* quantum system is described by the Schrodinger equation:
>
> $$i\hbar \frac{d|\varphi\rangle}{dt} = H|\varphi\rangle$$
>
> where $\hbar$ is *Planck's constant*, $i$ is the imaginary unit and $H$ is a fixed Hermitian operator known as the *Hamiltonian*.

There are several notes to make about this postulate. First, the Hamiltonian is fixed for the given system and it is not be confused with the *Hadamard quantum gate*, also represented by an $H$. Second, $\hbar$ is a physical constant that can be absorbed into the Hamiltonian for our purposes, simplifying the equation. Finally, this is a differential equation, so by knowing the initial state space of the system and the exact Hamiltonian we may know the exact evolution of the system.

Let us study the Hamiltonian in general. Since it is a Hermitian operator, it allows a spectral decomposition by theorem 1:

$$H = \sum_E E|E\rangle\langle E|$$

where $E$ are the eigenvalues and $|E\rangle$ the respective normalized eigenvectors. the states $|E\rangle$ are usually referred to as *energy eigenstates* or *stationary states*, and $E$ is the *energy* of the state $|E\rangle$. Furthermore, the lowest energy is called the *ground energy state* while the corresponding eigenstate is called the *ground state*.

*Example* 3. Suppose a single qubit system has a the following Hamiltonian:

$$H = \hbar\omega X = \hbar\omega \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Where $X$ is the first Pauli matrix, and $\omega$ is a positive parameter. H eigenenergy states are the same as $X$ eigenstates: $(|0\rangle + |1\rangle)/2$ and $(|0\rangle - |1\rangle)/2$ with respective energies $\hbar\omega$ and $-\hbar\omega$. Thus, the ground state is $(|0\rangle - |1\rangle)/2$ with ground state energy $-\hbar\omega$.

Let us deduce the connection between the Hamiltonian perpestive of dinamics, Postulate $3'$, and the unitary operator perspective, postulate 3. We can solve the Schrodinguer equation, which can be proven to be:

$$|\varphi(t_2)\rangle = \exp\left(\frac{-iH(t_2 - t_1)}{\hbar}\right)|\varphi(t_1)\rangle$$

We define:

$$U(t_1, t_2) \equiv \exp\left(\frac{-iH(t_2 - t_1)}{\hbar}\right)$$

Which is a unitary operator. In fact, any unitary operator $U$ may be expressed as $U = \exp(\text{iK})$ for some Hermitian operator $K$. Thus, we obtained:

$$|\varphi(t_2)\rangle = U(t_1, t_2)|\varphi(t_1)\rangle$$

Following this procedure, we have proven that there is a one to one correspondence between the continuous time-varying postulate $3'$ using the Hamiltonian and the more stationary discrete-time version using the unitary operator. Although the discrete-time vision is usually used in quantum computing, Quantum Annealing -the specific application of quantum mechanics used in this thesis- rests mostly on the Hamiltonian point of view. We will deepen in this architecture on section [TODOref].

It is worth mentioning that both versions of this postulate assume our physical system to be *closed*. That is, there is no interaction with the system coming from the exterior. In reality, the only real closed system is the universe as a whole. However, we may recreate sufficiently closed systems so that they can be described with approximations as being closed.

Furthermore, this severely interferes with postulate 2, where an outsider to the system may interfere with it by measuring it. The quantum system will evolve following postulate 3 until measurement is applied. Then they will evolve following the behavior described on postulate 2.

In practice, obtaining the Hamiltonian for a given quantum system is a really laborious work and usually needs experimental data [TODO: add evidence? stated as such in Niel.]. However, for our computational purposes, we will be the ones designing the Hamiltonian such that our system evolves as desired. In particular, chapter 3 [TODOref to QUBO chapter] describes in detail the construction of Hamiltonians for QUBO problems.

### 1.3.3 *Quantum Computing perspective: Quantum Gates*

Although quantum annealing does not make use of quantum gates, they are the basis of quantum computing and they fully rely on postulate 3. Because of their importance, a brief overview of quantum gates is provided o¡in this section. However, a profound understanding of them will not be necessary to understand the rest of the thesis.

Quantum computing is built upon the most simple operation we can compute on single qubits: quantum gates. Since state vectors are unit two-dimensional vectors, the operations we apply to them must preserve the norm. Thus, quantum gates will be represented by 2x2 unitary matrices. We have already introduce some of the most famous gates, the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Some of the others most important gates are the Hadamard gate (denoted as H), the phase gate (denoted as S), and the $\pi/8$ gate (denoted as T):

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

Although we have not described the fundamentals of multiple qubits systems (postulate 4 is required for this), it is worth mentioning a simple two-qubits gate for the purpose of this section. Just like in classical computing, conditional operations are essential for the construction of complex quantum algorithms. The most basic conditional operation is the *controlled-NOT* gate, also referred to as the CNOT gate. This gate takes two bits $|c\rangle|t\rangle$, a control qubit, and a target qubit. It flips the target qubit if the first qubit is set to $|1\rangle$, producing the operation $|c\rangle|t\rangle \to |c\rangle|c \oplus t\rangle$, where $\oplus$ denotes the exclusive-or operation. Therefore, if the control qubit is $|c\rangle = \alpha|0\rangle + \beta|1\rangle$, it will virtually flip the target qubit with probability $|\beta|^2$ and leave it how it is with probability $|\alpha|^2$.

One of the most important results of classical computation theory is that any boolean function may be constructed by only using AND, OR, and NOT gates, or by simply using NAND gates [7]. There is an equivalent result concerning quantum gates [3].

**Theorem 2.** *Any unitary matrix can be approximated by a combination of the Hadamard, CNOT, and $\pi/8$ gates.*

In this case, {H, CNOT, T} is called a *universal gate set*. In practice, is it efficient to build such any gate using only this gate set? The answer to the question is positive, as stated by the **Solovay-Kitaev theorem** [8]. However, this is out of the scope of this project. We provide a sketch proof of the previous theorem from [3].

**Proof.** TODO: copy proof from Bayens, Theorem 4.2 □

Further study of quantum circuits falls out of the scope of this thesis since we will use the D-Wave architecture, which relies on quantum annealing instead of quantum circuits.

## 1.4 postulate 4: composite systems

In this section, we introduce the last postulate, which lets us understand the state space associated with a physical system composed of other minor systems. This will allow us to study multiple-qubits systems and state some of the most important results in quantum mechanics and quantum computing: The *Heisenberg uncertainty principle* and the no-cloning theorem.

### 1.4.1 *Tensor product*

Let $V$ and $W$ be complex vector spaces with dimensions $m$ and $n$ respectively. Then, $V \otimes W$, read '$V$ tensor $W$', is a $mn$ complex vector space. Let $|v\rangle$ and $|w\rangle$ be vectors in $V$ and $W$ respectively. Then, $|v\rangle \otimes |w\rangle$ is in $V \otimes W$. Furthermore, any element of $V \otimes W$ may be expressed as a linear combinations of tensor products $|v\rangle \otimes |w\rangle$ of elements from $V$ and $W$. We may describe elements of $V \otimes W$ using the following equivalent notations: $|v\rangle \otimes |w\rangle$, $|v\rangle|w\rangle$, $|v, w\rangle$ and even $|vw\rangle$.

Let $|i\rangle$ and $|j\rangle$ be basis for $V$ and $W$ respectively. Then, $|i\rangle \otimes |j\rangle = |ij\rangle$ is a basis for $V \otimes W$. For example, consider the complex vector space $\mathbb{C}^2$. Then

$$|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle = |00\rangle + |11\rangle$$

is an element in $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ .

Although the tensor product is generally described as an abstract construct, we may provide a more visual perspective using the *Kronecker product*. This is a matrix representation for the tensor product of finite vector spaces. Suppose $A = \{a\}_{ij}$ is a $n \times m$ matrix and $B = \{b\}_{ij}$ is an $p \times q$ matrix. Then $A \otimes B$ is a $np \times mq$, matrix with the following representation:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nm}B \end{pmatrix}$$

For example:

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \otimes \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix} = \begin{pmatrix} 0 \times \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix} & 1 \times \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix} \\ 2 \times \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix} & 3 \times \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix} \end{pmatrix} =$$

$$\begin{pmatrix} 0 \times 10 & 0 \times 20 & 1 \times 10 & 1 \times 20 \\ 0 \times 30 & 0 \times 40 & 1 \times 30 & 1 \times 40 \\ 2 \times 10 & 2 \times 20 & 3 \times 10 & 3 \times 20 \\ 2 \times 30 & 2 \times 40 & 3 \times 30 & 3 \times 40 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 10 & 20 \\ 0 & 0 & 30 & 40 \\ 20 & 40 & 30 & 60 \\ 60 & 80 & 90 & 120 \end{pmatrix}$$

By definition, the tensor product satisfies:

- Let $\alpha$ be a complex number. For any $|v\rangle$ in $V$ and $|w\rangle$ in $W$,

$$\alpha(|v\rangle \otimes |w\rangle) = (\alpha|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle)$$

- For any $|v_1\rangle$, $|v_2\rangle$ in $V$ and $|w\rangle$ in $W$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

- For any $|v\rangle$ in $V$ and $|w_1\rangle$, $|w_2\rangle$ in $W$,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

The inner products of the spaces $V$ and $W$ may be use to extend and natural inner product the tensor space. Define:

$$\left( \sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right) \equiv \sum_{ij} \overline{a_i} b_j \langle v_i | v'_j \rangle \langle w_i | w'_j \rangle$$

With this product and the previous properties in mind, it can easily be proven that the tensor product of Hilbert spaces is a Hilbert space.

**Proposition 3.** *Let $H_1$ be and $H_2$ be two Hilbert spaces with respective orthonormal bases $B_1 = \{|v_i\rangle\}_{i=1,...,n}$ and $B_2 = \{|w_j\rangle\}_{j=1,...,m}$. Then, $H_1 \otimes H_2$ is a Hilbert space with inner product given by*

$$(|v\rangle \otimes |w\rangle, |v'\rangle \otimes |w'\rangle) = \langle vw|v'w'\rangle = \langle v|v'\rangle\langle w|w'\rangle$$

*For any $|v\rangle, |v'\rangle$ in $V$ and $|w\rangle, |w'\rangle$ in $W$. Furthermore, $B_1 \otimes B_2 = \{|v_i w_j\rangle\}_{i,j}$ is an orthonormal basis of $H_1 \otimes H_2$.*

**Proof.** By definition, $H_1 \otimes H_2$ is a complex vector space with $dim(H_1 \otimes H_2) = dim(H_1) \cdot dim(H_2)$. Furthermore, $B_1 \otimes B_2 = \{|v_i\rangle \otimes |w_j\rangle\}_{i,j} = \{|v_i w_j\rangle\}_{i,j}$ is a base of it. Let $|v_i w_j\rangle, |v_k w_l\rangle \in B_1 \otimes B_2$:

$$\langle v_i w_j|v_k w_l\rangle = \langle v_i|v_k\rangle\langle w_j|w_l\rangle = \delta_{ik}\delta_{jl}$$

which equals one if and only if $i = k$ and $j = l$, and zero otherwise. Thus, proving that $B_1 \otimes B_2$ is orthonormal.

Finally, for $H_1 \otimes H_2$ to be a Hilbert space the product defined above needs to be, in fact, an inner product. It suffies to prove that it is definite positive. Let $|v\rangle \in H_1 \otimes H_2$. Since $B_1 \otimes B_2$ is an orthonormal basis, there exist $\alpha_{ij} \in \mathbb{C}$ such that:

$$|v\rangle = \sum_{i,j} \alpha_{ij} |v_i w_j\rangle$$

By linearity:

$$\langle v|v\rangle = \sum_{i,j,k,l} \overline{\alpha_{ij}} \alpha_{kl} \langle v_i w_j|v_k w_l\rangle = \sum_{i,j,k,l} \overline{\alpha_{ij}} \alpha_{kl} \; \delta_{ik}\delta_{jl} = \sum_{i,j} |\alpha_{ij}|^2 \geq 0$$

where the equality holds if and only if $\alpha_{ij} = 0 \; \forall i, j$. □

From the inner product, the tensor space $H_1 \otimes H_2$ naturally inherits the notions of adjoint, unitary, normality and Hermicity. We will denote a vector $|\varphi\rangle$ tensored with itsel n times, $|\varphi\rangle \otimes \overset{n}{\ldots} \otimes |\varphi\rangle$, as $|\varphi\rangle^{\otimes n}$, and equivalently with Hilbert spaces: $H \otimes \overset{n}{\ldots} \otimes H$, as $H^{\otimes n}$. For our quantum computing purposes, the following case holds particular relevance.

**Corollary 3.** *The tensor product of $\mathbb{C}^2$ with itself n times, $\mathbb{C}^2 \otimes \overset{n}{\ldots} \otimes \mathbb{C}^2$, is isomorphic to $\mathbb{C}^{2^n}$.*

**Proof.** Let $H = \mathbb{C}^2 \otimes \overset{n}{\ldots} \otimes \mathbb{C}^2$. Since $dim(H) = dim(\mathbb{C}^2)^n = 2^n$, $H$ is a Hilbert space with dimension $2^n$. Thus, by Hausdorff's Theorem [4], it is isomorphic to the canonical complex vector space of dimension $2^n$, $\mathbb{C}^{2^n}$. □

In the same way that the inner product was naturally extended to the tensor space, we may extend operators ensuring linearity. Let $A : V \longrightarrow V'$ and $B : W \longrightarrow W'$ two operators between Hilbert spaces. Then, we define $A \otimes B : V \otimes W \longrightarrow V' \otimes W'$ using the following equation:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle$$

We extend this definition to every element of $V \otimes W$ ensuring linearity:

$$(A \otimes B)\left( \sum_i a_i |v_i\rangle \otimes |w_i\rangle \right) \equiv \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$$

It can be shown that $A \otimes B$ is a well-defined linear operator. In fact, any linear operator mapping $V \otimes W$ to $V' \otimes W'$ may be expressed as a linear combination of tensor product of linear operators mapping $V$ to $V'$ and $W$ to $W'$:

$$C = \sum_i a_i A_i \otimes B_i$$

where by definition:

$$\left( \sum_i a_i A_i \otimes B_i \right) |v\rangle \otimes |w\rangle = \sum_i a_i A_i |v\rangle \otimes B_i |w\rangle$$

### 1.4.2 *Postulate 4 statement*

Reaching the core of this section, suppose we consider two (or more) distinct physical systems. In order to describe the state of the composite system we need to make use of tensor product.

> **Postulate 4.** The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through $n$, and system number $i$ is prepared in the state $|\varphi_i\rangle$, then the joint state of the total system is $|\varphi_1\rangle \otimes \ldots \otimes |\varphi_n\rangle$.

Let us provide an intuitive notion of why is the tensor product used in order to describe composite systems. After all, we would expect that there exists a *somehow canonical way* os describing the product composition of systems, just like the cartesian product is used with vector spaces. Let us refer again to the so-called *superposition principle of quantum mechanics*. Let $|\varphi\rangle$ and $|\psi\rangle$ be two vector states of a system. Then, any superposition of the states, $\alpha|\varphi\rangle + \beta|\psi\rangle$, should also be another vector state, where $|\alpha|^2 + |\beta|^2 = 1$. Suppose we now have two systems $X$ and $Y$, with two vector states

$|\varphi_x\rangle$ and $|\varphi_y\rangle$. Then, we could describe the state of the composite system $XY$ as some state $|\varphi_x\rangle|\varphi_y\rangle$. Studying the superposition principle on composite systems leads us naturally to the notion of tensor product. It is important to note that this development is not thorough, since we are not taking the superposition principle as a fundamental component of our description of quantum mechanics. It does help up to build an intuitive notion on why this tensor product is used.

We now introduce the *Bell State* or *EPR pair:*

$$|+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Although it may seem harmless at first glance, this state has been responsible for many surprises during the development of quantum physics [9]. Let us have a first look into it, although we will come back to it later on.

The first thing to notice about this state is that it can be expressed as a single tensor product of state vector: $|+\rangle \neq |a\rangle|b\rangle$. This means that this state is not describing two independent physical systems put together with their respective vector states independently, it describes a **relation** between both systems too. It means that those systems are somehow interfering with each other. So we may affect one by disrupting the other.

This phenomenon is called *entaglement*. A state is called *entangled* when it cannot be expressed as the product of states of its component systems. This concept rests at the heart of the disparity between classic physics and quantum physics and it is key in quantum computing. It was deeply studied first by Einstein, Podolsky, and Rosen (EPR) [10] and second by John Bell [9].

### 1.4.3 *Projective measurement*

In this section, we explain an important particular case of measurement. In fact, this method of projective measurement is equivalent to Postulate 2, when they are combined with the capacity to perform unitary operations. It has huge relevancy in quantum computing and it is explained here because of its relation with composite systems. Let us state the alternative postulate:

> **Projective Measurement.** A projective measurement is described by an *observable*, $M$, a Hermitian operator on the state space of the system being described. The observable has a spectral decomposition:
>
> $$M = \sum_m m P_m$$

where $P_m$ is the projector onto the eigenspace with eigenvalue $m$. The possible outcomes of the measurement correspond to the eigenvalues, $m$, of the observable. Upon measuring the state $|\varphi\rangle$, the probability of the result $m$ ocurring is:

$$p(m) = \langle\varphi|P_m|\varphi\rangle$$

and the state of the system after the measurement, givent that outcome $m$ ocurred, is:

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

Projective measurements can be seen as a particular case of Postulate 2. Suppose the measurement operators from such postulate, in addition to satisying the completeness relation $\sum_m M_m M_m^\dagger = I$, also fulfill that $M_m$ are *orthogonal projectors*. That is, $M_m$ is Hermitian and $M_m M_{m'} = \delta_{mm'} M_m \ \forall m, m'$. With these aditional restricions it holds that $M_m M_m^\dagger = M_m M_m = M_m$. By choosing $P_m = M_m$ we see that projective measurements is a particular case of Postulate 2.

Thanks to the way projective measurements are expressed, they have nice and handy properties. Let us compute the average value of a projective measurement:

$$\begin{aligned} E(M) &= \sum_m m p(m) \\ &= \sum_m m\langle\varphi|P_m|\varphi\rangle \\ &= \langle\varphi|\left(\sum_m m P_m\right)|\varphi\rangle \\ &= \langle\varphi|M|\varphi\rangle \end{aligned} \tag{1}$$

The average value of an operator is usually written as $\langle M\rangle \equiv \langle\varphi|M|\varphi\rangle$. The standar deviation associated to observations of $M$ is then written as:

$$\begin{aligned} [\Delta(M)]^2 &= \left\langle (M - \langle M\rangle)^2 \right\rangle \\ &= \langle M^2\rangle - \langle M\rangle^2 \end{aligned} \tag{2}$$

This means that if we prepare our state $|\varphi\rangle$ multiple times and measure it, the measures will follow a normal distribution with expected value $\langle M\rangle$ and standard deviation $\Delta(M) = \sqrt{\langle M^2\rangle - \langle M\rangle^2}$. This formulation of standard deviation using observables provides us with an elegant proof of perhaps the most famous quantum mechanics result: The *Heisenberg uncertainty principle*. Such proof can be found in annex [TODOref anexo con la demostracion, copy from Box 2.4 in Niel.].

There are two additional notations worth mentioning regarding projective measurement. Instead of providing an observable $M$, we will sometimes provide a complete set of orthogonal projectors. That is, a set $P_m$ such that $\sum_i P_m = I$ and $P_m P_{m'} = \delta_{mm'} P_m$. The corresponding implicit observable used in this case is $M = \sum_m m P_m$. Finally, another widely used notation is to 'measure in a basis $|m\rangle$', where $|m\rangle$ form an orthonormal basis. This simply means that the chosen projectors are $P_m = |m\rangle\langle m|$ and the observable is $M = \sum_m m|m\rangle\langle m|$. This is the usual notation in quantum computing.

### 1.4.4 *Quantum Computing perspective: Multiple qubits*

Suppose we have a pair of qubits. In the classical case, two bits can be in four possible states: 00, 01, 10, and 11. Similarly, the two qubits computational basis states are $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. We arrive at this natural notation by knowing that each qubit has $\mathbb{C}^2$ as their associated state space and using the tensor product. Just like in the single qubit case, our two qubits system may be in a superposition of these four states:

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Correspondingly, the measurement of this system will result in either 00, 01, 10 or 11 since we are using the observable $\sum_{x\in\{0,1\}^2} x|x\rangle\langle x|$, where $\{0,1\}^2$ are the strings of length two where each character is either 0 or 1. In fact, it will yield state $x$ with probability $|\alpha_x|^2$, being $\alpha_x$ the coefficient associated with the state $|x\rangle$. The condition of the probabilities adding up to one is also called the *normalization condition* and can be expressed as $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$ for the two qubits case.

The fundamental differences with the single qubit case start on measurement. Of course, we can measure both qubits at the same time, but we could also measure only one of them. In order to achieve this we can use the projectors $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01|$ and $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11|$. Upon measuring, the system will collapse to $P_0|\varphi\rangle / \sqrt{p_0}$ with probability:

$$p_0 = \langle\varphi|P_0|\varphi\rangle = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

Since these are the coefficients associated with the first qubit being 0, this is the probability of first qubit being 0. Furthermore, our system will collapse to:

$$|\varphi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Note the normalization term $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$, which appears so the post-measurement state still satisfies the normalization condition. Naturally, after obtaining 0 in the first qubit we can still obtain either 0 or 1 in the second qubit, with probabilities

$$\frac{|\alpha_{00}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2} \text{ and } \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2 + |\alpha_{01}|^2}$$

respectively, adding up to 1. Correspondingly, the first qubit being measured will yield 1 with probability $p_1 = |\alpha_{10}|^2 + |\alpha_{11}|^2$.

Additionally, the first qubit independently should satisfy the normalization condition. That is, its probabilities of being 0 and 1 upon measurement must add up to 1. But those are $p_0$ and $p_1$, which add up to one because of the normalization condition for $|\varphi\rangle$, as expected.

Let us come back to the previously introduced *Bell State*:

$$|+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

When measuring using the previously defined projectors $P_0$ and $P_1$ we obtain that the first qubit will collapse to either 0 or 1 with equal probability $p_0 = p_1 = 1/2$. Most importantly, in the first case the qubit will collapse to the state:

$$\frac{|00\rangle / \sqrt{2}}{\sqrt{p_0}} = |00\rangle$$

Meaning that the second qubit also collapsed to 0. Note that we only affected the first qubit and the second one was disturbed. These are the consequences of entanglement, key in the appearance of impressive phenomenoms and discussions such as the EPR Paradox [10], [9].

Let us finally consider the more general case. In an n-qubits system our computational (orthonormal) basis would consist of the sates $|x_1 x_2 \ldots x_n\rangle$, where $x_i \in \{0, 1\}$. As we already know, in a single qubit system we have two amplitudes $\alpha_0$ and $\alpha_1$. We have four amplitudes for a 2-qubits system, eight for a 3-qubits system... And $2^n$ for an n-qubits system. This means that the number of amplitudes grows exponentially as we add qubits to the system. An immense increment compared to the classical case where the quantity of information that our system holds grows linearly with the numbers of bits. Of course, it is not that simple, since there are huge limitations on how we may access this information in the quantum realm such as how a qubit collapses upon measurement and the no-cloning theorem. However, we can already glimpse the power of quantum computing versus the classical one.

## 1.5 THE NO-CLONING THEOREM

A first exposure to the basis of quantum computing is fundamentally incomplete without the no-cloning theorem. It lets us understand one of the fundamental inconveniences of quantum computing: the impossibilty of cloning arbitrary states.

We proceed by formalizing the copying mechanism. Let $H$ be a state space and $|\varphi\rangle \in H$ the state to be copied. Given another state $|\varphi'\rangle \in H$, we would like to copy $|\varphi\rangle$ into $|\varphi'\rangle$. Since we can prepare $|\varphi'\rangle$ at will before the copying occurs, let $|\varphi'\rangle = |x_0\rangle$ be a fixed state. Then, our copying operation will take both states and produce the following result:

$$(|\varphi\rangle \otimes |x_0\rangle) \xrightarrow{U} |\varphi\rangle \otimes |\varphi\rangle$$

Operations between n-qubits (n-qubits gates) must preserve their norm, thus they must be unitary $n \times n$ matrices. In our case, $U$ is a $2dim(H) \times 2dim(H)$ unitary matrix. Let us now state and prove the theorem.

**Theorem 3** (No-cloning Theorem)**.** *There is no unitary operator $U : H^{\otimes 2} \longrightarrow H^{\otimes 2}$ and state $|x_0\rangle \in H$ such that for any arbitrary state $|\varphi\rangle \in H$ it holds*

$$U|\varphi\rangle|x_0\rangle = |\varphi\rangle|\varphi\rangle$$

**Proof.** Suppose there exists such unitary operator $U$ and such state $|x_0\rangle$. Let $|\varphi\rangle, |\psi\rangle \in H$. We may apply the copying operators to both of them:

$$\begin{aligned} U|\varphi\rangle|x_0\rangle &= |\varphi\rangle|\varphi\rangle \\ U|\psi\rangle|x_0\rangle &= |\psi\rangle|\psi\rangle \end{aligned}$$

Taking the inner product of both equations and using that $U$ is unitary results in:

$$\begin{gathered} \Big(U|\varphi\rangle|x_0\rangle, U|\psi\rangle|x_0\rangle\Big) = \Big(|\varphi\rangle|\varphi\rangle, |\psi\rangle|\psi\rangle\Big) \iff \\ \Big(|\varphi\rangle|x_0\rangle, |\psi\rangle|x_0\rangle\Big) = \langle\varphi|\psi\rangle\langle\varphi|\psi\rangle \iff \\ \langle\varphi|\psi\rangle\langle x_0|x_0\rangle = \langle\varphi|\psi\rangle^2 \end{gathered}$$

Since $|x_0\rangle$ is a normalized vector, $\langle x_0|x_0\rangle = 1$, and we obtain:

$$\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2$$

Which only holds if $\langle\varphi|\psi\rangle$ equals to either 0 or 1, which means $|\varphi\rangle$ and $|\psi\rangle$ are either equal or orthonormal. But those vectors were arbitrary, thus such a general cloning operator is impossible. □

TODO: Creo que me gustaría añadir aquí una sección sobre la EPR Paradox / teleportación cuántica.

# BIBLIOGRAPHY

[1] Michael A. Nielsen, Isaac Chuang, and Lov K. Grover. *Quantum Computation and Quantum Information*, volume 70. 2002. ISBN 9781107002173. doi: 10.1119/1.1463744.

[2] Daniel Manzano. A short introduction to the Lindblad master equation. *AIP Advances*, 10(2), feb 2020. ISSN 21583226. doi: 10.1063/1.5115323.

[3] Pablo Bayens. *Modelos de computación cuánticos*. PhD thesis, University of Granada, 2019. URL https://github.com/mx-psi/tfg/blob/master/tfg.pdf.

[4] Rafael Payá. Apuntes de Análisis Funcional. In Rafael Payá, editor, *Apuntes de Análisis Funcional*, chapter 5, pages 53–62. Granada, 2020. URL https://www.ugr.es/~rpaya/documentos/Funcional/2020-21/Apuntes_05.pdf.

[5] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Die Naturwissenschaften*, 23(48):807–812, nov 1935. ISSN 00281042. doi: 10.1007/BF01491891.

[6] John D. Trimmer. The Present Situation in Quantum Mechanics: A Translation of Schrödinger's Çat Paradox"Paper. *Proceedings of the American Philosophical Society*, 124(5):323–338, 1980. URL https://archive.is/20121204184041/http://www.tuhh.de/rzt/rzt/it/QM/cat.html#sect5.

[7] Dietlinde Lau. *Function Algebras on Finite Sets*. 2006. doi: 10.1007/3-540-36023-9.

[8] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1):081–095, jan 2006. ISSN 15337146. doi: 10.26421/qic6.1-6. URL https://arxiv.org/abs/quant-ph/0505030v2.

[9] J. S. BELL. on the Einstein Podolsky Rosen Paradox. Technical Report 3, 1995.

[10] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, may 1935. ISSN 0031899X. doi: 10.1103/PhysRev.47.777. URL https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777.