# Quantum Computing
# Notes of the course

Luca Leoni

# Contents

# 1

# Introduction to quantum computations

## 1.1 Postulates of quantum mechanics

The course has the aim of introducing the follower to the working principles of quantum computing and how they work on a fundamental physical and mathematical level. Therefore, will come to the mind of the reader that all the theory ahead of us will rely on quantum mechanical principles that we will need to introduce first. This will be useful also to the experienced reader since a refresh can is always good, and also because we may want to restate the fundamental of quantum mechanics specifically for application to quantum calculators.

Quantum mechanics(QM) is the modern fundamental theory that describes reality and relies on a series of assumptions, or postulates, that allow us to describe the physical systems. There is not a standard version of the postulates, can vary in numbers, but we are going to use the description of QM that uses three postulates to define: states, evolution and mesuraments.

### Postulate 1

**Definition 1.1.1: States**

The set containing the possible states of the system is a Hilbert space $\mathcal{H}$ and of the vectors $|\psi\rangle \in \mathcal{H}$ only the normalized ones can describe the real state of the system.

This definition of the notion of state is really different from the simple coordinate couples of position and momenta $(\mathbf{r}, \mathbf{p})$ that we had in classical mechanics. In this situation the states are pure vectors inside a vector space that is the Hilbert space itself, meaning that all the properties known from linear algebra theory apply to them. In particular, we have the closure property of sum and multiplication with a scalar, or the presence of a scalar product $< \cdot, \cdot >: \mathcal{H} \otimes \mathcal{H} \to \mathbb{C}$. Those are all things that need to be present inside $\mathcal{H}$ to be an Hilbert space, and define those inside our restricted series of systems that describe quantum computer is simple. In fact, the main quantum computers rely on systems with a finite number of levels which posses a **finite dimensional** $\mathcal{H}$ which allow us to highly simplify all the computations thanks to the following

Theorem 1.1.1

If we have that $\dim \mathcal{H} = N$ then the space is holomorphic to $\mathbb{C}^N$.

That is a known fact indeed, but allow us to directly describe all the states of the system as complex vectors, along with the possible bases and the inner product. In fact, if we have a space with dimension $N$ we can write down directly an orthonormal base for the system as the canonical one and write whatever vector $|\psi\rangle$ as a superposition of those

$$|i\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \qquad\qquad |\psi\rangle = \sum_i \lambda_i |i\rangle .$$

The other part is that we can imagine the inner product inside this space to be exactly the one of the complex space, having so that we can simply define it by first define the raw vectors as follows

$$\langle\phi| = \left(|\phi\rangle\right)^\dagger = \begin{pmatrix} \alpha_0^* & \cdots & \alpha_i^* & \cdots & \alpha_N^* \end{pmatrix} .$$

Then, we can use the normal algebra to define the following inner product inside the space

$$\langle\phi|\psi\rangle = \alpha_0^*\lambda_0 + \cdots + \alpha_N^*\lambda_N = \sum_i \alpha_i^*\lambda_i .$$

Knowing it allow also to define to norm inside to space simply as $\|\psi\|^2 = \langle\psi|\psi\rangle$, which tells us that for a state to be normalized means that the following must be true, always

$$\langle\psi|\psi\rangle = \sum_i |\lambda_i|^2 = 1. \tag{1.1}$$

Which also show us how a state of a system doesn't care about the phase since even if I redefine it to be $|\phi\rangle = \exp(i\theta)\,|\psi\rangle$ will still be normalized, but one can also see how also observables are not touched.

We now have the full construction of the space we are going to use during our computations, and would be kind of interesting to use it to see how $\mathcal{H}$ will look like in some simple cases. In particular, we want to show how the states of a **qubit** are formed. The latter is non-other than a two level system, which so has $\dim \mathcal{H} = 2$, meaning that the base can be seen simply as

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

Which we will call as **computational base**, and all the state can be represented with them using a general linear combination that is normalized, so

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad\qquad |a|^2 + |b|^2 = 1.$$

This is effectively simple to use not only for its mathematical simplicity but also because a really simple geometric representation for those state can be used. In fact, one can see the following

Theorem 1.1.2

A state $|\psi\rangle$ in a qubit can be represented, instead of using the $a$ and $b$ couple, using two angles $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$ using the following form

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle . \tag{1.2}$$

***Proof:*** Devo pensare alla dimostrazione. 😄

This allows us to see a state of the system as a unitary vector on a circumference, referenced by the angles and so the direction in which is pointing. This is indeed remarkable as we will see, since this anticipate the fact that every possible modification of a state is non-other than a rotation, as we will see.

In this construction we can also easily create systems composed by a series of qubit together, since the Hilbert space generated will be the tensor product of the single qubit ones as

$$\mathcal{H}_N = \mathcal{H} \otimes \cdots \otimes \mathcal{H} = \mathbb{C}^{2N}.$$

Since we are working with a known operation, that is the tensor product, we can also readily create basis functions for the new states by simply make the tensor product of the ones of the older states. For example, calling $\{|0\rangle_1, |1\rangle_1\}$ the base of the first qubit and $\{|0\rangle_2, |1\rangle_2\}$ the base of the second one can easily see that the base for the combined system will be

$$\{|0\rangle_1 |0\rangle_2, |0\rangle_1 |1\rangle_2, |1\rangle_1 |0\rangle_2, |1\rangle_1 |1\rangle_2\}.$$

Most of the time the subscripts are omited, having so that $|0\rangle_1 |0\rangle_2 = |00\rangle$, but in this case the order in which you write the basis is important and needs to be remembered! The importance of order is also noticeable in the creation of a two-qubit state by using single qubit ones, if taken $|\psi\rangle = (a, b)$ and $|\phi\rangle = (cd)$ one can see how

$$|\psi\phi\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \neq (c|0\rangle + d|1\rangle) \otimes (a|0\rangle + b|1\rangle) = |\phi\psi\rangle .$$

In fact the coefficients on the bases $|01\rangle$ and $|10\rangle$ are different, and the order here is important, so the states are different.

**Note**

*It's interesting to note how the number of basis elements increase a lot as the number of qubits are inserted inside the system. In particular, the dimension of the space scales as $2^N$. This is in contrast with what happens for the phase space in classical dynamics, where to describe a particle I need 6 coordinates and as the particle increase the number rise as $6N$. Basically the quantum systems become more complex much quicker and that hints us why is difficult simulate quantum systems on classical computers.*

## Postulate 2

**Definition 1.1.2: Evolution**

The evolution of a closed system can be represented using a unitary operator $\mathcal{U}(t_1, t_2)$ that acts on the state making it evolve in time as follows

$$|\psi(t_2)\rangle = \mathcal{U}(t_1, t_2)\,|\psi(t_1)\rangle\,. \tag{1.3}$$

This is obviously a simplified version of the evolution postulate, which in reality should refer to the evolution of the state based on the Schrödinger equation(SE). In fact, we can also see how this principle can be derived directly from the latter. Therefore, let's start from the SE recalling its form

$$i\hbar\frac{\partial\,|\psi(t)\rangle}{\partial t} = \hat{\mathcal{H}}\,|\psi(t)\rangle\,, \tag{1.4}$$

where, being in a closed system, the Hamiltonian will be time independent. Under those conditions we can easily integrate the equation finding out the following general form for the evolution of the system

$$|\psi(t)\rangle = \exp\left(-i\frac{\hat{\mathcal{H}}}{\hbar}(t-t')\right)|\psi(t')\rangle = \mathcal{U}(t', t)\,|\psi(t')\rangle\,. \tag{1.5}$$

In this way we have found out an analytic form for the evolution operator that we were describing. Also, one can actually see how since $\hat{\mathcal{H}}$ is assumed to be selfadjoint, $\hat{\mathcal{H}}^\dagger = \hat{\mathcal{H}}$, then the following holds true

$$\mathcal{U}^\dagger(t', t) = \mathcal{U}(t, t') = \mathcal{U}^{-1}. \tag{1.6}$$

Which is telling us that $\mathcal{U}$ is effectively unitary as required by the postulate, but not only that. In fact inside this construction we will also have that the operator $\mathcal{U}$ will be also **linear** and **invertible**, giving always rise to reversible operations.

**Note**

*The properties of $\mathcal{U}$ of being linear and invertible are something that was not really present inside classical computers, in fact we will use that operator to manipulate qubits and every operation can be inverted. That didn't hold true for classical bits, where operations were often irreversible, or neither linear.*

## Postulate 3

So far all the description of QM relies on principles that are totally deterministic, solving the SE does not lead to probabilistic results. Nevertheless, the theory is renown to give a probabilistic interpretation of reality, and this comes from the definition of how we measure physical quantities. To understand it we shall write down the definition in the mathematical terms of linear algebra, where measuring means apply a linear operator to the state of the system and evaluate averages on them as follows.

**Definition 1.1.3: Measure**

Let $\Lambda$ be a measurable quantity with $\{\lambda_n\}_{n\in\mathcal{I}}$ its possible values, $\mathcal{I}$ is a set of indices, a measurement of this quantity is defined by a set of operator $\{\hat{\Pi}_n\}_{n\in\mathcal{I}}$ that respect the following relations:

1. If the state of the system is a generic $|\psi\rangle$ then the probability of measuring $\lambda_n$ is given by

$$p_n = \langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle\,. \tag{1.7}$$

2. After the measurement the state collapse into an eigenstate of $\lambda_n$ written as

$$|\psi_n\rangle = \frac{\hat{\Pi}_n\,|\psi\rangle}{\sqrt{\langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle}}. \tag{1.8}$$

Therefore, a measure is simply a set of operators that is able to describe the probability of having a certain outcome from an experiment. Therefore, in general we can have $\Pi_n$ to be whatever type of operator with restrictions only on how it acts onto the states. Nevertheless, it's easy to understand that from the definition of measure another restriction on their form needs to be done. In particular, we can use the properties of probability to see how the following needs to be true

$$\sum_n p_n = \sum_n \langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle = 1, \qquad \forall\,|\psi\rangle\in\mathcal{H}. \tag{1.9}$$

It's easy to understand that this condition can be translated to a condition on the set of operators per se, requiring that the following is true in order to have a proper measure

$$\sum_n \Pi_n^\dagger\Pi_n = \mathbb{1}. \tag{1.10}$$

A condition that we will need to keep in mind when we will need to create a measure further in the course.

Using this definition the reader can understand how in QM I really can't know which value $\lambda_n$ of a certain quantity the experiment will give in output, but only the probability of having it. This may arise the question to the reader of how we can predict something out of this theory if we can't know the final outcome. The answer is that, it's true, no single outcome can be predicted exactly, but the average quantity can be estimated without any problem. In fact, we can simply use the mathematical definition of average to see that

$$\langle\Lambda\rangle = \sum_n \lambda_n p_n = \sum_n \lambda_n\,\langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle\,. \tag{1.11}$$

Which shows how the average observable for a state $|\psi\rangle$ is a totally deterministic quantity. From this expression we can also see how different states can give also the same average, in fact it's easy to see how for $|\psi'\rangle = \exp(i\theta)\,|\psi\rangle$ with $\theta\in\mathbb{R}$ leads to

$$\langle\Lambda'\rangle = \left|e^{i\theta}\right|^2\sum_n \lambda_n\,\langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle = \sum_n \lambda_n\,\langle\psi|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi\rangle = \langle\Lambda\rangle\,. \tag{1.12}$$

This means that basically a system in state $|\psi\rangle$ or $|\psi'\rangle$ have same observable and, therefore, are indistinguishable giving us the reason why in the definition of the first postulate we have sad that no difference is present between states that differ only by a complex phase.

## 1.2 Quantum gates

After recalling the postulates of QM we want to focus a little on the second one and understanding how we can manipulate the states of qubits using it. In particular, the second postulate tells us that the evolution of a state in time is described by a unitary operator $\mathcal{U}$. Normally that operator should have infinite dimensions, nevertheless the qubits posses a finite dimensional Hilbert space meaning that also the operators inside it can be associated to finite matrices. To understand this we can take a system composed by $N$ qubits, so that $\dim \mathcal{H} = 2^N$, the operator could then be described as follows

$$\mathcal{U} : \mathbb{C}^{2N} \to \mathbb{C}^{2N}, \qquad \mathcal{U} = \begin{pmatrix} a_{11} & \cdots & a_{2^N 1} \\ \vdots & \ddots & \vdots \\ a_{12^N} & \cdots & a_{2^N 2^N} \end{pmatrix}. \tag{1.13}$$

This representation is incredibly useful on a mathematical level, in fact manipulating a simple qubit state will become as doing a matrix multiplication. In particular, we know that the state of a qubit can be written generally as $|\psi\rangle = a\,|0\rangle + b\,|1\rangle = (a, b)$, so applying a generic state manipulation $\mathcal{U}$ will simply mean doing the following

$$\mathcal{U}\,|\psi\rangle = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} Aa + Bb \\ Ca + Db \end{pmatrix} = |\psi'\rangle\,. \tag{1.14}$$

This matrix operations are called **quantum gates**, and we want to try to unveil some possible interesting forms that they can have starting to understand how effectively a so-called **quantum circuits** works. In fact, a quantum circuits is non-other than a series of quantum gates acting on the available qubits in order to obtain a specific state in the end, as depicted in Fig. (1.1).

Thus, what we want to do now is look deeper in the form that those gates can have, and try to identify some important operations that will follow us during the whole course. Therefore, I suggest to the reader (especially my future self) to look into them and try getting attune to their form and their actions on the qubits.

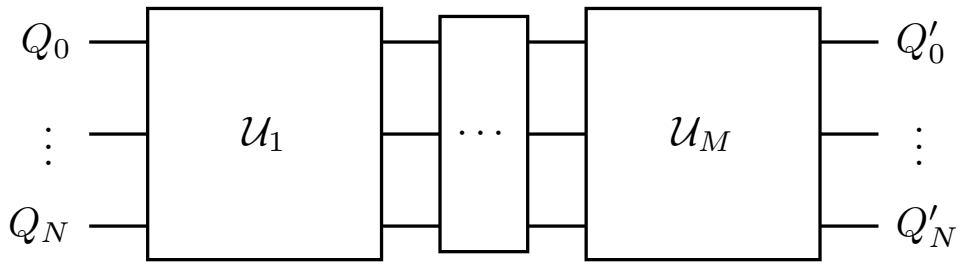



**Figure 1.1:** Sample image of a general quantum circuits where all the manipulations on the qubits are done using quantum gates, matrices, represented as blocks.

## Single qubit gates

The first type of gates that we want to analyze are the one that acts a single qubits, which are also the simplest ones. As we have pointed out previously an operation of this type can be written as a matrix like in Eq. (1.14). In particular, it's easy to understand that every $2 \times 2$ matrix that is unitary satisfy the second postulate being a valid quantum gate for the manipulation of a qubit state. That let us have an infinite amount of possibilities for the operations that we can do on a single unit of information, setting another difference with the classical bits. In fact, a normal bit could be manipulated through the application of the identity operation, leaving as it is, or the NOT one, changing its state. So, not only the qubits allow for an infinite number of possible states to be represented using superposition, but also allow for an infinite number of operations to be done on it showing a clear superiority.

This simple observation has already shown to us that we have a lot of room in which we can move in order to work with qubit, and what we need to do now is to point out the most significant and important operations that are present inside this really large space. The first, thing that is important to point out is that we know how to generate every $2 \times 2$ unitary matrix using four of them. Thus, mathematic has already given us a way to write down all the possible gates using a simple universal relation.

> Theorem 1.2.1: Universal single gate
>
> Every quantum gate $\mathcal{U}$ can be associated to a rotation of the state on the Bloch sphere, and therefore can be written as
>
> $$\mathcal{U} = e^{i\lambda \mathbb{1}} \exp\left(ia\mathbf{n} \cdot \boldsymbol{\sigma}\right), \tag{1.15}$$
>
> where $\lambda, \alpha \in \mathbb{R}$, $\mathbb{1}$ is the identity matrix, $\mathbf{n}$ is an appropriate unitary vector, and $\boldsymbol{\sigma}$ is a vector containing the three Pauli matrices.
>
> $$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.16}$$

This theorem tells us that only $4$ parameters are needed in order to define every possible gates, in fact the parameter $a$ is not really needed can be associated to the velocity of the rotation not really on the rotation itself. Therefore, we know how to write every possible operation, still the one that are interesting to us are limited, and so we will report them briefly discussing the form and the action of those specific gates.

**NOT.** The NOT operation is the equivalent of the one in the classical case, meaning that the effect is the one of negating the current state. That can be easily done by recalling that the $0$ and $1$ of our quantum logic are the state $|0\rangle$ and $|1\rangle$, leading us to the possibility of constructing the truth table and matrix associated to this operation.

| **IN** | **OUT** |
|---|---|
| $\|0\rangle$ | $\|1\rangle$ |
| $\|1\rangle$ | $\|0\rangle$ |

$$\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.17}$$

One can also notice that the final matrix obtained is exactly the $X$ Pauli matrix, with assure to us that is unitary since every one of them has the property $X^2 = Y^2 = Z^2 = \mathbb{1}$. This matrix is, in fact, drawn as $\bigoplus$ symbol inside circuits to recall that the $X$ matrix is getting used on a certain qubit.

**Hadamart.** This is the first real quantum gate that was thought of, the idea is the one of creating superpositions of the normal states. This can be done really easily since the gate that we are interested in, and it's truth table, is

| IN | OUT |
|---|---|
| $\|0\rangle$ | $\|+\rangle$ |
| $\|1\rangle$ | $\|-\rangle$ |

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.18}$$

.

Where we shall recall how $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are interesting states that forms the eigenvectors of the $X$ Pauli matrix, basically being the states in the $x$ direction on the Bloch sphere while the computational base is on the $z$ one. This gate has also really important properties that can be interesting such as

$$H^2 = \mathbb{1}, \qquad H^\dagger = H = H^{-1}, \qquad HZH = X. \tag{1.19}$$

**Phase.** This is another type of gate that wants to do a purely quantum operation, that is the one of adding a phase shift to the two components of the state. Basically we want a gate that starting from a state $|\psi\rangle = a|0\rangle + b|1\rangle$ is able to add a phase shift to the two bases that can be used to enhance interference effects. The idea is so the follwing

$$\Phi(\theta)|\psi\rangle = a|0\rangle + be^{i\theta}|1\rangle, \qquad \Phi(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}. \tag{1.20}$$

These types of gates can be used in a lot of situations since phase shift are really common inside quantum mechanical application, and some of them are most commonly used than the others and so a specific name was given to them

$$\Phi(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = S, \qquad \Phi(\pi/4) = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix} = T, \qquad T^2 = S. \tag{1.21}$$

**Note**

*I want to stress out how the idea of the qubit is basically creating a new type of logic. In the classical computers the boolean logic was the only possible thing with the bits that could be only 0 and 1 along with two possible operations: identity or NOT. Now, the qubit can have infinite states and infinite operations can be done on it having so an incredible much richer logic that allow things obviously impossible before. An example of it is the $\sqrt{NOT}$ operation which was demonstrated impossible to define since no operation applied to times could bring to the NOT one, even inside the context of fuzzy logic. In quantum logic we can do it simply by taking the square root of the Pauli matrix*

$$\sqrt{X} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \tag{1.22}$$

## Two qubits gates

The next step is adding a second qubit to our system and see how the possible gates changes. On a mathematical level the answer is really simple since we are simply modifying $\mathcal{H}$ to have two more dimensions, having so that now $\mathcal{U} : \mathbb{C}^4 \to \mathbb{C}^4$ being represented by a $4 \times 4$ unitary matrix. Thus, the

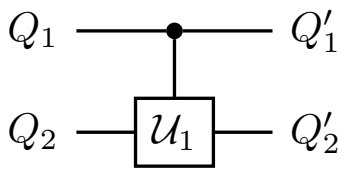
possibilities for the usable gates have increased respect to the single qubit once. Nevertheless, also in this case we want to make some order and explicitly write down the ones that are used the most and that we will see more frequently.

**Control.** The control gates, in reality, are a class of two qubits gates that one of the two as the control one, not being modified, and perform operations on the other. To understand the concept we can have a look at the most important control gate that is the **CNOT**. The latter is a gate that takes two qubits and: when the control one is $|0\rangle$ then nothing is done, if the control is $|1\rangle$ then the NOT is performed on the other qubit. At first this gate may seem complicated to realize, but that would be a wrong assumption since both the truth table and matrix are simple as

| IN | OUT |
|---|---|
| $\|00\rangle$ | $\|00\rangle$ |
| $\|01\rangle$ | $\|01\rangle$ |
| $\|10\rangle$ | $\|11\rangle$ |
| $\|11\rangle$ | $\|10\rangle$ |

$$\text{CNOT} = \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & \mathbb{0} \\ \mathbb{0} & X \end{pmatrix}.$$

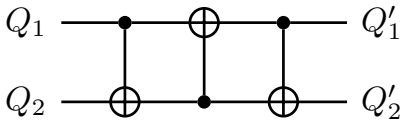
Where we can see how the total matrix is formed by the use of two known single qubit gates on the diagonal, creating the quantum version of the NOR opeartion in boolean logic. This form, with two gates on the diagonal, allow for a big flexibility inside this category of matrices, in particular it's easy to understand that one can create the C-version of every single qubit operator by simply defining it as




$$\text{C}\mathcal{U} = \begin{pmatrix} \mathbb{1} & \mathbb{0} \\ \mathbb{0} & \mathcal{U} \end{pmatrix}. \tag{1.23}$$

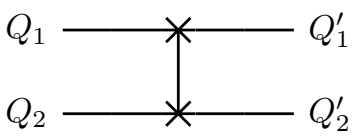
Where, in the graphical representation the dot describe the control qubit.

**Swap.** This gate is in reality a simple circuits constructed using three CNOT gates in order, and the reason of the name can be easily seen by the truth table.




| IN | OUT |
|---|---|
| $\|00\rangle$ | $\|00\rangle$ |
| $\|01\rangle$ | $\|10\rangle$ |
| $\|10\rangle$ | $\|01\rangle$ |
| $\|11\rangle$ | $\|11\rangle$ |

Thus, one can see that the effect is literally the one of swapping the states of the qubit. This is a simple and clever operation that can be written in a simple matrix form thanks to the fact that we know the matrix describing the gate of the circuit of which is formed. Therefore, we can write down the final gate by simply matrix multiplying the gates of which is composed in the right order and then having the following one described by its own simbol

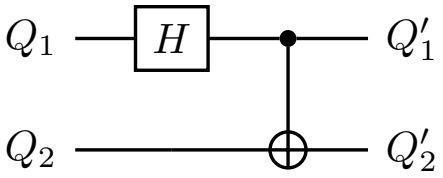



$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1.24}$$

**Bell.** This is a simple circuit that nevertheless is really important since allow for the creation of particular states of major interest in physics, the Bell's states. The latter are four quantum mechanical states defined as follows

$$\psi^{\pm} = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \qquad \phi^{\pm} = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{1.25}$$

They are mostly important in the theoretical study of spin states, but they appear also in other areas of QM. Thus, we want to describe a circuit that is able to prepare the system in those states and the way in which this can be done is the following




| IN | OUT |
|---|---|
| $\|00\rangle$ | $\psi^+$ |
| $\|01\rangle$ | $\phi^+$ |
| $\|10\rangle$ | $\psi^-$ |
| $\|11\rangle$ | $\phi^-$ |

Basically, based on the initial state of the system we are able to generate one of the four Bell state and then study their behavior in specific circuits.

**Example 1.2.1** (Circuit solving)

As a scrupulous, I want to see the computation of the Bell's gate output for the case $|10\rangle$ just to show the reader how effectively solve the circuit. At first the Hadamart gate is used on the first qubit

$$H|1\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle - |1\rangle|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right), \tag{1.26}$$

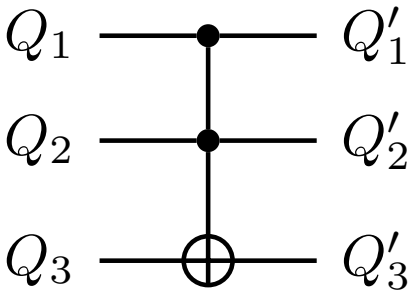
then the CNOT operation is applied using the first qubit as control, having the final result

$$\psi^+ = \frac{1}{\sqrt{2}} = \left(|00\rangle - |11\rangle\right) \tag{1.27}$$

## N qubits gates

We can now step into assuming to have a general number of qubits to work with and see how some general gates can effectively be created also in this case, in particular two main types of gates play a huge role in the whole theory of quantum computers.

**Toffoli.** This is a specific 3-qubit gate that has the aim of making a control NOT gate using two different controls. Basically, having two controls the idea is to apply the NOT to the target if and only if both the two controls are in state $|1\rangle$. For this reason the gate is also called CCNOT and has the following matrix and circuit representation




$$\text{CCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The task of writing down the truth table from the matrix representation is left to the reader to effectively see how the aim of applying a NOT to the last qubit only if the first two are in $|1\rangle$ is accomplished.

**N control.** These gates are a generalization of the Toffoli one to an N number of control and an M number of targets. In general the idea is to apply a general M-qubit gate $\mathcal{U}$ to the targets qubits if the N controls are in the state $|1\rangle$, the general form of the matrix is analogous to the one already seen for the CU gates and the circuit is also totally analogous to the Toffoli and CU one.

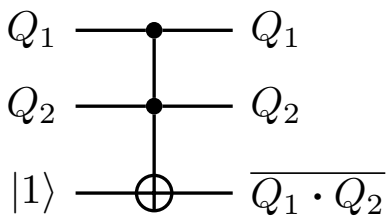
## 1.3 Performing classical computations

The quantum computer seems to have all the potential of performing computations that normal computers can't do, but it's not obvious that they can still perform the task of a normal one. That is a problem, in fact creating computers that are not able to perform simple tasks would be useless for us, and so we want to demonstrate that this isn't the case.

The question "can quantum computers do classical computations?" comes from the doubt that in the possible operations that can be done on the qubits may not be able to simulate the two general operations that give rise to all the classical logic. These operations are the NAND gate and the COPY one, which together forms the building block of all the other possible operations. The first one is the **universal operation** of classical logic meaning that every circuit can be constructed using only NAND opeartions, while the latter constitute a problem due to some properties of QM that makes coping a non-trivial matter. Here we want to take the two properties one at a time and demonstrate that QC can perform both using the **Toffoli gate**.

### NAND operation

The possibility of a QC to perform the NAND operation is not obvious, and the reason for that is the fact that all the quantum operations that we can perform on a qubit are invertible which the NAND is not. Basically it's not sure that a non-invertible operation can be constructed using invertible ones, or better if we can represent it using an invertible operation on a qubit. Fortunately turns out that performing the NAND on qubit is not only possible, but simple. The idea is using a Toffoli gate and setting one of the three qubits to $|1\rangle$, obtaining as output the NAND of the other two as we can see in the following circuit.




| IN | OUT |
|---|---|
| $\|001\rangle$ | $\|001\rangle$ |
| $\|011\rangle$ | $\|011\rangle$ |
| $\|101\rangle$ | $\|101\rangle$ |
| $\|111\rangle$ | $\|110\rangle$ |

Which clearly reconstruct the NAND as wanted, meaning that using QC we are able to recreate every possible classical circuit.

## Coping information

First, we shall clarify why this operation represent a problem inside quantum circuits, and the reason is intrinsic inside QM and in the known result called **non-cloning theorem**, which states the following.

> Theorem 1.3.1: Non-cloning
>
> Taken a state $|\psi\rangle$ of a system of qubit, it does not exist a unitary operation $\mathcal{U}$ with the following property
>
> $$\mathcal{U}\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle\,, \tag{1.28}$$
>
> where $|s\rangle$ is another arbitrary state.

***Proof:*** Let's imagine that such operation exist, and take three arbitrary states $|\psi\rangle$, $|\phi\rangle$ and $|s\rangle$. Since $\mathcal{U}$ is unitary the following relation must hold true

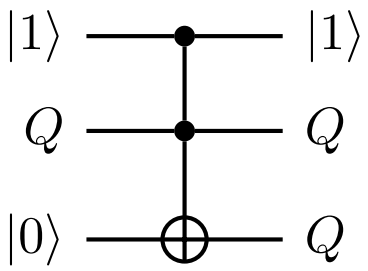
$$\langle s\phi|\psi s\rangle = \langle s|s\rangle \langle \phi|\psi\rangle = \langle s\phi|\mathcal{U}^\dagger\mathcal{U}|\psi s\rangle\,, \tag{1.29}$$

but using relation Eq. (1.28) and the normalization of the states it's possible to see that the latter equation becomes

$$\langle \phi|\psi\rangle = \langle \phi|\psi\rangle^2\,. \tag{1.30}$$

This is not true in general, but only if we select carefully the two states in order for them to respect this relation. Otherwise, the operation $\mathcal{U}$ cannot be unitary and therefore is not a viable quantum gate. 😄

This result may seem a problem by all means, but already in the proof is hidden the answer to overcome it. In fact, we have said that a cloning operation can exist if the starting states are selected carefully so that the norm of the states is conserved. In practice this means that we can use a Toffoli gate with two entries selected in a specific way to obtain the following copy gate.




| IN | OUT |
|---|---|
| $\|100\rangle$ | $\|000\rangle$ |
| $\|110\rangle$ | $\|111\rangle$ |

In this way also coping information to one qubit to another can be done always using the Toffoli gate, making it probably the most important of all, and demonstrating that QC can perform all classical computations along with the unexplored quantum ones.

## 1.4 Measurements

During the first section we have introduced the concept of measure as a set $\{\hat{\Pi}_n\}_{n\in\mathcal{I}}$ of operators that allow us to evaluate the probability of having a certain outcome $\lambda_n$ for the measure of a physical quantity $\Lambda$. Nevertheless, even if we have listed the main properties that such operators should have we didn't specify the forms that they can possess. It is now time to introduce the main way in which such set of operators can present themselves and how they will work inside quantum circuits.

### Projection valued measurement

If we take a look back to the different properties stated in Def. (1.1.3) an idea should arise, especially by looking at the collapse condition. The latter, in fact, can be thought as the state of the system gets projected into a certain state that posses a definite value of the physical quantity we are interested in measuring. In fact, it's easy to see how the following is true

$$\hat{\Pi}_n |\psi_n\rangle = |\psi_n\rangle\,, \qquad\qquad p_n = \langle\psi_n|\hat{\Pi}_n^\dagger\hat{\Pi}_n|\psi_n\rangle = 1. \tag{1.31}$$

Operators that posses this effect of taking a general state $|\psi\rangle$ and taking it into another are really known in mathematics and are called **projector operators**, represented as $\hat{P}$. This type of operator is defined, in particular, by two main conditions

$$\hat{P}^\dagger = \hat{P}, \qquad\qquad \hat{P}^2 = \hat{P}, \tag{1.32}$$

these two properties are enough to give $\hat{P}$ a lot of power allowing it to define alone a subspace of the vector space in which is working. In our case this means

$$\mathcal{P} = \left\{ |\psi\rangle \middle| \exists \left|\phi\right\rangle \in \mathcal{H} : |\psi\rangle = \hat{P}\left|\phi\right\rangle \right\}, \tag{1.33}$$

basically we are aiming to create a set $\{\hat{P}_n\}$ so that $\mathcal{P}_n$ is the eigenspace of $\lambda_n$.

To find out the right projectors to create the complete set we can simply use the properties of the observable in QM. An observable quantity is represented in QM using an operator $\hat{\Lambda}$ and the possible values that $\Lambda$ can take, the outcomes, are the eigenvalues of that operator $\lambda_n$. Nevertheless, for a general operator $\lambda_n$ can be complex, or worst they can not exist, that is a problem since is absurd to mesure a complex number in an experiment, therefore we will make a further assumption giving out the following definition.

**Definition 1.4.1: Observables**

An observable $\Lambda$ in QM is represented by a hermitian operator $\hat{\Lambda}$, so that

$$\hat{\Lambda}\dagger = \hat{\Lambda}. \tag{1.34}$$

A really important theorem of linear algebra called **spectral theorem** allow us to say that, with this further assumption of hermiticy, the operator can be diagonalyzed and the eigenvalues are all real. Along

with that, the spectral theorem also allow us to say that a set of eigenstates $\{|\psi_n\rangle\}$ with the following properties exist

$$\hat{\Lambda}\,|\psi_n\rangle = \lambda_n\,|\psi_n\rangle\,, \qquad \langle\psi_n|\psi_m\rangle = \delta_{nm}, \qquad \sum_n |\psi_n\rangle\langle\psi_n| = \mathbb{1}, \tag{1.35}$$

forming an orthonormal base for $\mathcal{H}$. These properties should hint us that the set of projectors that we want to create to measure $\Lambda$ may be the ones that project onto the eigenspace generated by $|\psi_n\rangle$, and we can easily see how that is the case.

> **Theorem 1.4.1: PVM measure**
> Taken $\hat{\Lambda}$ an observable the set of projectors $\{\hat{P}_n\}_{n\in\mathcal{I}}$ onto the orthonormal base of eigenstate $\{|\psi_n\rangle\}_{n\in\mathcal{I}}$ of $\hat{\Lambda}$ forms a measure for the observable itself called **Projection valued measurement**.

***Proof:*** We are going to define the projector $\hat{P}_n$ as follows

$$\hat{P}_n = |\psi_n\rangle\langle\psi_n|\,, \tag{1.36}$$

which can be easily seen it's a projector, the demonstration is left to the reader. We want to see how all the requirement in Def. (1.1.3) are verified, we can start from the probability by taking a general state $|\psi\rangle$ and writing

$$|\psi\rangle = \sum_n c_n\,|\psi_n\rangle\,, \qquad p_n = \langle\psi|\hat{P}_n^\dagger\hat{P}_n|\psi\rangle = \langle\psi|\hat{P}_n|\psi\rangle = |c_n|^2. \tag{1.37}$$

Where I have first written the expansion of $|\psi\rangle$ on the orthonormal base and then used the properties in Eq. (1.32) and Eq. (1.35) to obtain the probability. It's possible to see how the values of $|c_n|^2$ effectively represents probabilities since also the condition Eq. (1.10) is respected by the set of operators defined thanks to the completeness condition of the orthonormal base

$$\sum_n \hat{P}_n^\dagger\hat{P}_n = \sum_n \hat{P}_n = \sum_n |\psi_n\rangle\langle\psi_n| = \mathbb{1}. \tag{1.38}$$

Therefore, the first condition for having a measure is respected. We can now see how also the second one is obtained as we want since we can write

$$|\psi_n\rangle = \frac{\hat{P}\,|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n^\dagger\hat{P}_n|\psi\rangle}} = \frac{c_n}{\sqrt{|c_n|^2}}\,|\psi_n\rangle = e^{i\theta}\,|\psi_n\rangle\,, \tag{1.39}$$

and since a complex phase doesn't change the physical state of the system the wanted result is achieved. 😄

> **Example 1.4.1** (Qubit PVM)
> To make an example we can use a qubit, where we can imagine measuring the state as $|1\rangle$ or $|0\rangle$, so a computational base measurament. We can also easily imagine what is the form of the

operator, the observable, that has them as eigenstates

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Z\,|i\rangle = \lambda_i\,|i\rangle\,, \tag{1.40}$$

where it's easy to see, by using the $\mathbb{C}^2$ representation of the states, how $\lambda_0 = 1$ and $\lambda_1 = -1$. This means that for every state $|\psi\rangle$ we can measure the probability of a certain outcome, state $|1\rangle$ or $|0\rangle$, to appear by using the set of operators defined by $\hat{P}_i = |i\rangle\langle i|$ given as matrix by

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.41}$$

Applied to a general vector they will give in general the first or second component, respectively.

## Positive operator valued measurement

In the PVM description of measure that we have given just now we use projector operators to predict the probabilities, which posses a series of properties that makes them really well suited for the task. Nevertheless, they are not the only possible choice, in particular such projectors posses the property of being hermitian that general measures can totally not have. We want so to see a case where another type of measure respect to the PVM can be a better choice to study the system.

Let's imagine having a qubit and a quantum circuit that is able to prepare it in two states given by

$$|\psi_1\rangle = |0\rangle\,, \qquad |\psi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{1.42}$$

We want to see if we are able to understand which state after a measure. Using the PVM measure of a qubit using $Z$ as an observable we can easily see how $|\psi_1\rangle$ posses a probability equal to $1$ of being in state $|0\rangle$, while $|\psi_2\rangle$ has $p_i = 1/2$ for both states. This means that if I take a measure and the outcome is $\lambda = -1$ I know that the only state that can have that outcome is $|\psi_2\rangle$ since has a non-zero probability of being in state $|1\rangle$. Instead, if the result is $\lambda = 1$ I can't say which one of the two state is the right one. We can also understand why we are not able to decide, since the two states that we are working with are not orthogonal respect to the computational base and so $|\psi_2\rangle$ has non-zero probability of being in both states. Therefore, we would like to use a set of operators that instead are able to give us this property, and a possible way of obtaining them is by taking $\{\hat{\Pi}_n\}$ so that

$$\hat{\Pi}_n^\dagger \hat{\Pi}_n = \hat{E}_n, \tag{1.43}$$

are **positive valued operators**.