Quantum Computing
Notes of the course

Luca Leoni

Contents

1

Introduction to quantum computations

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 $< \cdot, \cdot >: \mathcal{H} \otimes \mathcal{H} \rightarrow \mathbb{C}$. 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

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

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 Λ be a measurable quantity with $\{\lambda_n\}_{n\in I}$ its possible values, I is a set of indices, a measurement of this quantity is defined by a set of operator $\{\hat{\Pi}_n\}_{n\in I}$ that respect the following relations:
>
> 1. If the state of the system is a generic $|\psi\rangle$ then the probability of measuring λ_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 λ_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 Π_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

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

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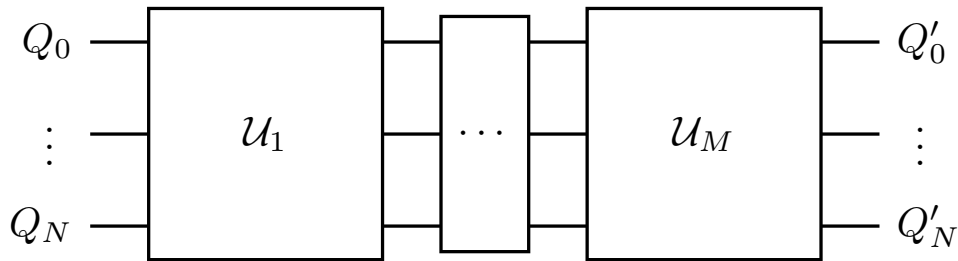
Figure 1.1: Sample image of a general quantum circuits where all the manipulations on the qubits are done using quantum gates, matrices, represented as blocks.

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 2×2 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 2×2 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
> $$\mathcal{U} = e^{i\lambda \mathbb{1}} \exp\left(i a \mathbf{n} \cdot \boldsymbol{\sigma}\right), \tag{1.15}$$
> 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 $\oplus$ 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
$|0\rangle$	$|+\rangle$
$|1\rangle$	$|-\rangle$

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

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

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

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

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

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

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

> **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*
>
> $$\sqrt{X} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \qquad (1.22)$$

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 4×4 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
$|00\rangle$	$|00\rangle$
$|01\rangle$	$|01\rangle$
$|10\rangle$	$|11\rangle$
$|11\rangle$	$|10\rangle$

$$\text{CNOT} = \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 0 & 0 \\ 0 & 0 & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \mathbb{1} & \mathbb{0} \\ \mathbb{0} & X \end{pmatrix}.$$
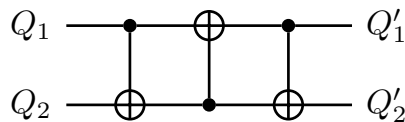
Where we can see how the total matrix is formed by the use of two known single qubit gates on the diagonal, creating the quantum version of the NOR opeartion in boolean logic. This form, with two gates on the diagonal, allow for a big flexibility inside this category of matrices, in particular it's easy to understand that one can create the C-version of every single qubit operator by simply defining it as

$$\mathrm{C}\mathcal{U} = \begin{pmatrix} \mathbb{1} & \mathbb{0} \\ \mathbb{0} & \mathcal{U} \end{pmatrix}. \qquad (1.23)$$

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


$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \qquad (1.24)$$

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

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

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
$|00\rangle$	ψ^{+}
$|01\rangle$	ϕ^{+}
$|10\rangle$	ψ^{-}
$|11\rangle$	ϕ^{-}
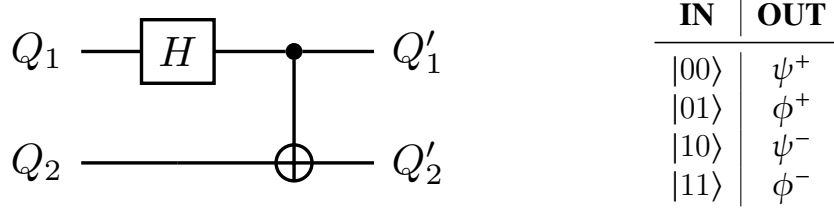
Basically, based on the initial state of the system we are able to generate one of the four Bell state and then study their behavior in specific circuits.

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

$$H\,|1\rangle\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle - |1\rangle\,|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right), \qquad (1.26)$$
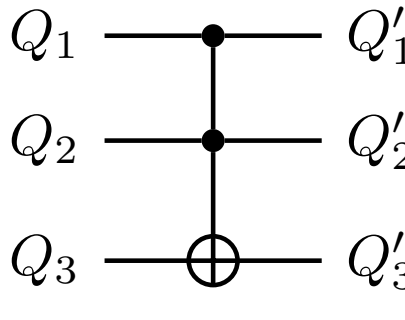
then the CNOT operation is applied using the first qubit as control, having the final result

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

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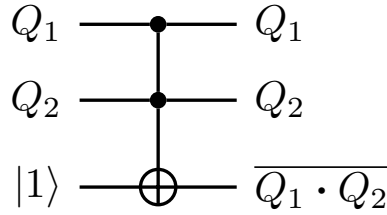
IN	OUT
$|001\rangle$	$|001\rangle$
$|011\rangle$	$|011\rangle$
$|101\rangle$	$|101\rangle$
$|111\rangle$	$|110\rangle$

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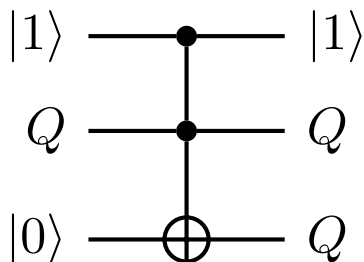
IN	OUT
$|100\rangle$	$|000\rangle$
$|110\rangle$	$|111\rangle$

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 λ_n for the measure of a physical quantity Λ. 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

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

basically we are aiming to create a set $\{\hat{P}_n\}$ so that $\mathcal{P}_n$ is the eigenspace of λ_n. Therefore, it's easy to understand that on a general ground we are searching for a specific type of measure constructed using projectors, that will take the following specific name and definition.

> **Definition 1.4.1: Projection valued measurement**
>
> We will call projection valued measurement, or PVM, a set of operators $\{\hat{P}_n\}_{n\in\mathcal{I}}$ so that $\hat{P}_n$ is a projector and the whole set is a measure.

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 Λ can take, the outcomes, are the eigenvalues of that operator λ_n. Nevertheless, for a general operator λ_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 1.4.2: Observables

An observable Λ 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 hermiticity, 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 Λ 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: Observable PVM

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.
☺

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

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

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

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

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

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

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

$$\hat{\Pi}_n^\dagger \hat{\Pi}_n = \hat{E}_n, \qquad\qquad (1.43)$$

are **positive valued operators**. In this way we are allowed to define as our operators the following objects

$$\hat{E}_1 = |1\rangle\langle 1|, \qquad\qquad \hat{E}_2 = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right), \qquad\qquad (1.44)$$

basically the projector on the states that are orthogonal to the ones that we were looking at. Nevertheless, the set composed by $\hat{E}_1$ and $\hat{E}_2$ is not sad to respect the relation Eq. (1.10) meaning that we are needed to add a third element in general that allow for the set to be a measure

$$\hat{E}_3 = \mathbb{1} - \hat{E}_2 - \hat{E}_1. \tag{1.45}$$

Then, using this new set we are able to obtain a more satisfying result since the now the possible outcomes of the measurement are three. In fact, we can imagine that doing a measure using $\{\hat{E}_n\}$ is experimentally equivalent to obtain three possible outcomes λ_n where the probabilities of the outcomes for the two states respectively are

$$\langle \psi_1 | \hat{E}_i | \psi_1 \rangle = \begin{cases} p_1 = 0 \\ p_2 \neq 0 \\ p_3 \neq 0 \end{cases}, \qquad\qquad \langle \psi_2 | \hat{E}_i | \psi_2 \rangle = \begin{cases} p_1 \neq 0 \\ p_2 = 0 \\ p_3 \neq 0 \end{cases}. \tag{1.46}$$

Therefore, now after a measure we are able to say that if the outcome is λ_1 or λ_2 the result is state $|\psi_1\rangle$ or $|\psi_2\rangle$ respectively, while λ_3 is telling us that the measure is not satisfying since we can't distinguish the two states. This may seem not so different respect to the PVM measure since still we have the case where the single measure can distinguish the two cases, but here we have also an outcome that tells us with certainty to have $|\psi_2\rangle$ that we didn't have before. Also, it is possible to demonstrate that the probability of an not satisfying measure is minimized by this set.

Therefore, with this simple case we have seen how the definition of measure in reality leaves large freedom in the choice of the operator set and not only projectors. In fact, we can now generaly define also the positive operator valued measurement as follows.

> **Definition 1.4.3: POVM**
>
> We will call positive operator valued measurement a set of operators $\{\hat{E}_n\}_{n \in \mathcal{I}}$ so that $\hat{E}_n$ is a positive valued operator and the whole set represent a measure.

This definition is much more general than PVM and can allow for better result in terms of computations as we have seen in the example shown beforehand. Nevertheless, the problem of these measures is that we actually don't know how to represent them in practice. In fact, for PVM the definition was made starting from a physical observable while here the physical representation is much more hidden. Still, doesn't mean that don't exist. Is possible to demonstrate that whatever measure, can be represented into a higher dimensional space through a unitary transformation composed a PVM, in this way everything can be physically interpreted. We can so state the following result in terms related to quantum computers applications as follows.

> **Theorem 1.4.2: Representation of measures**
>
> Any generalized measure on a system of N qubit $\mathcal{H}_Q$ can be realized as a PVM with the aid of auxiliary qubit and a unitary operator.

Proof: Imagine having a general measure $\{\hat{\Pi}_n\}_{n \in \mathcal{I}}$ acting on $\mathcal{H}_Q$, we can take an orthonormal set $\{|m\rangle\}_{m \in \mathcal{I}'}$, with $\#\mathcal{I} = \#\mathcal{I}'$, of states $|m\rangle \in \mathcal{H}_Q$ and construct an auxiliary space as

$$\mathcal{H}_{tot} = \mathcal{H}_Q \otimes \mathcal{H}_M, \qquad\qquad \mathcal{H}_M = \text{span}\{|m\rangle\}. \tag{1.47}$$

So, a general state inside the auxiliary space can be written as $|\psi\rangle |s\rangle$, with $|\psi\rangle \in \mathcal{H}_Q$ and $|s\rangle \in \mathcal{H}_M$. Now, we define the transformation $\mathcal{U}$ as follows

$$\mathcal{U} |\psi\rangle |s\rangle = \sum_n \left(\hat{\Pi}_n |\psi\rangle \right) |m\rangle , \tag{1.48}$$

which can be seen to be a unitary operator since the following relation can be obtained

$$\langle s| \langle\psi| \mathcal{U}^\dagger \mathcal{U} |\phi\rangle |s\rangle = \sum_{mm'} \langle\psi|\hat{\Pi}^\dagger_{m'}\hat{\Pi}_m|\phi\rangle \langle m'|m\rangle = \sum_m \langle\psi|\hat{\Pi}^\dagger_m\hat{\Pi}_m|\phi\rangle = \langle\psi|\phi\rangle . \tag{1.49}$$

Where the relation $\langle m|m'\rangle = \delta_{mm'}$ and $\sum_n \hat{\Pi}^\dagger_{m'}\hat{\Pi}_m = \mathbb{1}$ have been used during the process, demonstrating that $\mathcal{U}$ conserve the norm of the space being so unitary. Next we can define the projection operators to be given by the following

$$\hat{P}_m = \mathbb{1}_Q \otimes |m\rangle\langle m| , \tag{1.50}$$

creating a PVM set of measure. Then, we can see how the operator $\hat{P}_m\mathcal{U}$ act on a general state of the whole space as

$$\hat{P}_m\mathcal{U} |\psi\rangle |s\rangle = \sum_{m'} \left(\hat{\Pi}_n |\psi\rangle \right) \langle m|m'\rangle |m\rangle = \hat{\Pi}_m |\psi\rangle |m\rangle . \tag{1.51}$$

This is a powerful result since we can already see how this set of operations is able to reproduce the general measure in all of it's fascion. We can start by seeing how the probabilities that predicts are the same

$$p_m = \langle s| \langle\psi| \mathcal{U}^\dagger \hat{P}^\dagger_m \hat{P}_m \mathcal{U} |\psi\rangle |s\rangle = \langle\psi|\hat{\Pi}^\dagger_n\hat{\Pi}_n|\psi\rangle . \tag{1.52}$$

Thus, also the projection remains unchanged under the effect of this operator since

$$\frac{\hat{P}_m\mathcal{U} |\psi\rangle |s\rangle}{\sqrt{\langle s| \langle\psi| \mathcal{U}^\dagger \hat{P}^\dagger_m \hat{P}_m \mathcal{U} |\psi\rangle |s\rangle}} = \frac{\hat{\Pi}_m |\psi\rangle}{\sqrt{\langle\psi|\hat{\Pi}^\dagger_n\hat{\Pi}_n|\psi\rangle}} |m\rangle = |\psi_m\rangle |m\rangle . \tag{1.53}$$

Therefore, all the properties of the general measure are conserved, meaning that $\{\hat{P}_m\mathcal{U}\}$ successfully represent it. ☺

This result is telling is that doesn't matter with measure we are using we can always add a number of qubit so that the space becomes larger by a $\mathcal{H}_M$ with dimensions equal to the number of outcomes you want to measure and use a normal PVM along with a unitary transformation defined by the measure itself. In this way we can always use the same Z gate seen in the PVM example to measure the auxiliary qubit and based on the value of their state, which gives $|m\rangle$, we can know the outcomes of the others, since $|m\rangle$ correspond to a collapsed $|\psi_m\rangle$ and so λ_m as outcome.

> **Note**
>
> *This whole theory was though first by Von Neumann which tried to create it to describe the collapse on the wavefunction in a rigorous way. In particular He though that an experimental apparatus in general was the auxiliary system $\mathcal{H}_M$ that taking the measure made the system collapse in the way we have seen.*

Measuring is an important feature inside a quantum circuits since at the end of the manipulations we also need to know the result of the operations contained in the qubits states. In general, we are going to see how the measurement works inside a quantum circuit and their properties. First, we shall keep in mind that usually all the quantum computers are able to perform measurements mainly in the computational basis, meaning of the observable Z. This is due to a matter of experimental convenience, but lead us to try to reconduce every possible measure to that one. For example, we may work for a complex quantum circuit in a base like $|\pm\rangle$ so that a state is given by

$$|\psi\rangle = a\,|+\rangle + b\,|-\rangle, \tag{1.54}$$

but we can't use the measure given in that base since the QC only measure in computational base. The answer to this problem is in reality incredibly simple, and we can state it really quickly as

> **Theorem 1.4.3: Base change**
>
> Let's imagine having a circuit that prepare a qubit state $|\psi\rangle$ described on an orthonormal base $|e_1\rangle$ and $|e_2\rangle$. The measurement of the state can be performed still on the computational base without losing information by applying an appropriate rotation before the measure.

***Proof:*** Let $\mathcal{U}$ be the unitary transformation that acts as follows

$$\mathcal{U}\,|e_1\rangle = |0\rangle, \qquad\qquad \mathcal{U}\,|e_2\rangle = |1\rangle, \tag{1.55}$$

we can easily see how the state $|\psi\rangle$ can be written in a really simple way by using the following reasoning

$$|\psi\rangle = a\,|e_1\rangle + b\,|e_2\rangle = \mathcal{U}\,(a\,|0\rangle + b\,|1\rangle). \tag{1.56}$$

Meaning that the state $\mathcal{U}^\dagger\,|\psi\rangle$ will be a state written in the computational base with the same coefficients, therefore measuring it gives out the same probabilities of before we don't lose any informations. ☺

This little result is really helpful in practice, since basically means that we can perform a measurement using the same base in every possible situation by using circuit like in Fig. (1.2). Where we can see
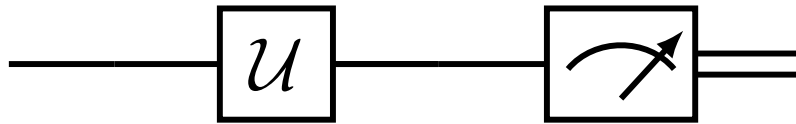
Figure 1.2: Simple quantum circuit for the measure of a qubit in a general base, composed by a rotation and the measure.
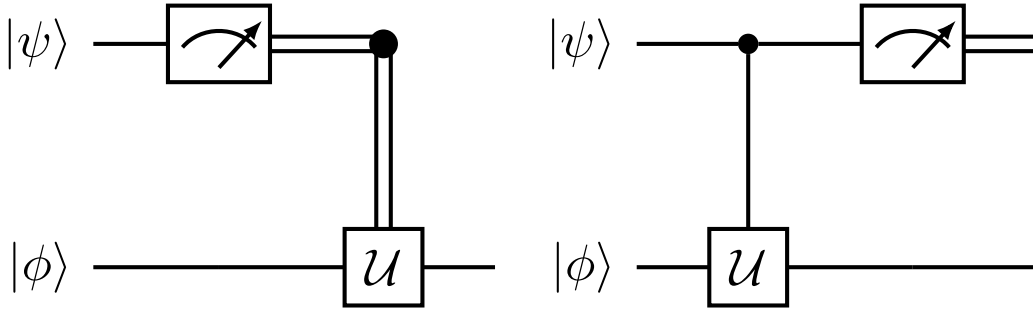
Figure 1.3: Representation of two equivalent circuits that uses classical and quantum control to apply an operation to the second qubit. In the first case the measurement on the first qubit is done before the control while in the other is done after, still the result will not change having that if the bit is 1 the operation is applied, while if is 0 will remain untouched.

how the measure is represented by the symbol with the arrow which take a quantum state and returns the outcome of the measure on a classical bit 1 or 0, seen as the double line.

The other important thing that we can say about measure inside circuits is that they can be applied in every point of the circuit and the final result of the computation will not change. To understand this we shall make an example using control gates as depicted in Fig. (1.3). We can see how the two circuits differ based on where the measurement is placed in the circuit. Nevertheless, if we analyze the system we can simply see how the outcome of the state $|\phi\rangle$ will be the same based on the value of the measurement. In fact, take the first circuit: the outcomes were

$$|\phi\rangle, \quad \text{if } c = 1; \qquad \mathcal{U}|\phi\rangle, \quad \text{if } c = 0, \tag{1.57}$$

where c represent the value of the bit. Now, if we take the second one, it's easy to see that if the measure gives 1 meant that the that $|\psi\rangle$ had a component along $|1\rangle$ passing through the control so that the rotation was applied to $|\phi\rangle$. Instead, if the value was 0 the opposite happens having so that the outcome at the end will be the exact same. This property of measurement takes the name of **principle of deferred measurement**, and allow us to place the measurement procedure always at the end of our circuits without the worries of modifying the outcome of the algorithm.

> **Attention**
>
> The deferred measurement principle it's not based on a mathematical result, since for it work in a general case we shall need that the measure operator $\hat{\Pi}_m$ commute with every possible gate $\mathcal{U}$. In this way we would have that
>
> $$\hat{\Pi}_m \mathcal{U}|\psi\rangle = \mathcal{U}\hat{\Pi}_m|\psi\rangle, \tag{1.58}$$
>
> which means that the final state at the end of the circuit remains the same. Nevertheless, it's easy to find a counter example by using $\mathcal{U} = X$ and $\hat{\Pi}_m = |1\rangle\langle 1|$, meaning that in general may exist a situation where the final outcome changes. Still, the principle could still hold since our aim is not really find out the exact value of the final state, but to understand it by using a single measure and the connection between the probabilities of certain outcomes and possible prepared states.

Therefore, even if mathematically the result can be different physically specking the result is the same.

> **Note**
>
> *It's possible to find that in several circuits the final measures are not explicitly written or are written only on certain qubit, that is because only the necessary measurements to understand the states of the qubits are shown, the non-necessary ones are skipped. This idea is also called **principle of implicit measurements** and will be more clear as we will talk about entanglement.*

1.5 Entanglement

The concept of entanglement comes from the need of describing the difference of certain type of states respect to others. In particular, we can understand it by first defining a really simple type of state called separable that has the following form.

> **Definition 1.5.1: Separable state**
>
> Taken a state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ it's called separable if $\exists |\phi_1\rangle \in \mathcal{H}_1, |\phi_2\rangle \in \mathcal{H}_2$ so that we can write
> $$|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle. \tag{1.59}$$

This type of states are really simple since we can decompose them into simpler once and work with them. To make an example we can see how the state $(|01\rangle + |00\rangle)/\sqrt{2}$ is a separable one since

$$\frac{|01\rangle + |00\rangle}{\sqrt{2}} = |0\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right), \tag{1.60}$$

holds true and so can be decomposed. Nevertheless, we shall not go much further to find out more complex states that cannot be decomposed for which we need to work in the higher dimensional space like the Bell's state $(|01\rangle + |10\rangle)/\sqrt{2}$. Those are entangled states, whose definition is therefore really simple as.

> **Definition 1.5.2: Entangled states**
>
> A state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ it's called entangled if it's not separable.

Therefore, the mathematical definition of entanglement seems really simple, but the physical consequences are not, and we shall see together why this is one of the main powers of QC.

> **Example 1.5.1**
>
> To make an example of how powerful the entanglement can be we can see how in theory we can transport the information of two bits, so 00, 01, 10 or 11, transmitting only one qubit. The idea is that two people, Alice and Bob, posses two qubit that are entangled in the following Bell state
>
> $$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{1.61}$$
>
> then Alice can perform one of four operations on it's qubit based on what wants to transmit to

Bob. In particular the following choices can be made

Operation	Final state
$\lvert 00 \rangle \rightarrow \mathbb{1}$	$\lvert \psi^+ \rangle$
$\lvert 01 \rangle \rightarrow Z$	$\lvert \psi^- \rangle$
$\lvert 10 \rangle \rightarrow X$	$\lvert \phi^+ \rangle$
$\lvert 11 \rangle \rightarrow iY$	$\lvert \phi^- \rangle$

So, based on the information that we want to send we have performed an operation of the Alice qubit to obtain a different Bell state. Then, Alice only need to send the qubit to Bob which need to perform a two qubit measure using the Bell's base and the state that will obtain will correspond to the selected two bit information obtained with the transport of only one qubit.


Note

This definition of Entanglement is not really the most general one that can be used. In fact, the Def. (1.5) it's a specific one called bi-entanglement since only two Hilbert spaces are counted, but the most general called n-entanglement count for $\lvert \psi \rangle \in \bigotimes_{i=1}^{n} \mathcal{H}_i$. Nevertheless, for QC application only the bi-entanglement plays an important role.

Quantum teleportation

The first real important application of entanglement that we will see it's the quantum protocol for the quantum teleportation of information. Basically we want to teleport a quantum state from one qubit to another, so that no matter is transported to one place to another but only the state of the qubits is changed transporting information. Also, at first site one can also think that the cloning theorem would be violated in a situation of this type, but that is not the case, and we will see why.

The circuit that is used in order to perform the teleportation protocol is reported in Fig. (1.4), and consist in the use of two qubit in order to transport a general state $\lvert \psi \rangle = a \lvert 0 \rangle + b \lvert 1 \rangle$ into one of those qubit. Thus, we want to understand how this is possible in general, and to do that let's pretend that the
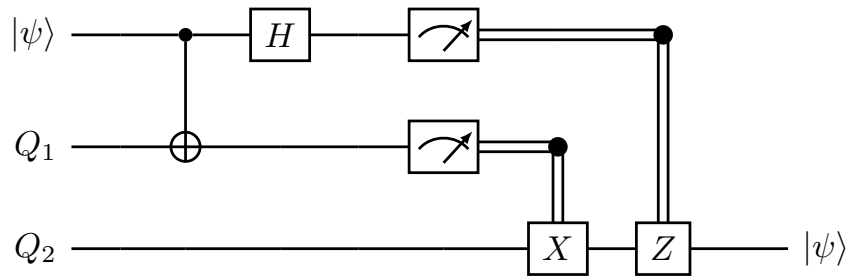
Figure 1.4: Quantum teleportation circuit for a quantum computer, see how it involves the measuring of two qubit to control two operations.

two qubit $|\psi\rangle$ and Q_1 are in possession of Alice, while Q_2 is with Bob. We will need that the two qubit Q_1, Q_2 are entangled in a $|\psi^+\rangle$ Bell state, then we can place them at whatever distance, so that Alice and Bob can be also on different planets. In this situation Alice will perform a series of operation on her qubit starting with a CNOT, to understand what this operation will do on the system we need first to look at the state of the hole three qubit, which will be

$$|\psi Q_1 Q_2\rangle = (a|0\rangle + b|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left[a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right]. \quad (1.62)$$

Then we can easily perform the CNOT on the first two qubit ending up in the following state

$$\frac{1}{\sqrt{2}}\left[a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle\right], \quad (1.63)$$

on which the Hadamart tranformation is applied on the first qubit, which we shall remember that transforms $|0\rangle$ in $|+\rangle$ and $|1\rangle$ in $|-\rangle$. Therefore, we will have the following form

$$\frac{1}{2}\left[a|000\rangle + a|100\rangle + a|011\rangle + a|111\rangle + b|010\rangle - b|110\rangle + b|001\rangle - b|101\rangle\right], \quad (1.64)$$

which can be rewritten by seeing how inside it four separable states can be found out, having

$$\frac{1}{2}\left[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)\right]. \quad (1.65)$$

At first sight this state may seem nothing special, but if the states inside parentheses are inspected one could find out different forms of $|\psi\rangle$ obtaining

$$\frac{1}{2}\left[|00\rangle(|\psi\rangle) + |01\rangle(X|\psi\rangle) + |10\rangle(Z|\psi\rangle) + |11\rangle(XZ|\psi\rangle)\right]. \quad (1.66)$$

We have so created a state where the two qubit state given by Alice's couple is entangled to the qubit of Bob, which will poses the $|\psi\rangle$ state up to two transformation based on the Alice's values. Therefore, if Alice measure it's two qubit and refers the outcomes to Bob, he can perform the right operations to obtain at the end the final state $|\psi\rangle$ on his qubit. An operation that inside the circuit is described by the two classical controls and can be seen gives the right result keeping in mind that $X^2 = Z^2 = \mathbb{1}$.

Thus, using this protocol a general state $|\psi\rangle$ can be transferred into another qubit at whatever distance without limitations. In fact, the circuit has been performed in several occasions starting from a teleportation distance of some centimeters to the experiment of Anton Zellinger that performed it at nearly one kilometer of distance inside Vienna. Today we are able to transfer states from hearth to satellite, but still this phenomenon result in being quite strange at first sight. Perhaps, as was told earlier, one can say that this **phenomenon contradicts Thm. (1.3.2)** with the coping of a general state into another one. This is a wrong affirmation, since the non-cloning theorem tells that the following operation doesn't exist

$$\mathcal{U}(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle, \quad (1.67)$$

while here the starting states have been measured by Alice, meaning that they have collapsed having a result more similar to

$$\mathcal{U}(|\psi\rangle \otimes |Q_1\rangle \otimes |Q_2\rangle) = |00\rangle \otimes |\psi\rangle. \quad (1.68)$$

Where $|00\rangle$ is only one of the four possible final result obtained. Another apparent contradiction that can be found out inside the teleportation protocol is the fact that **information seem to pass from one qubit to another faster than the speed of light**. That can't obviously be possible, since relativity forbid it, and in fact that is not the case. The two classical controls that are used inside the circuit solve the problem since in order to obtain the copied state inside Q_2 I first need Alice to transmit the result of the measurements to Bob and that classical exchange of information take times.

EPR paradox and Bell's inequality

Since in 2022, the year I'm writing these notes, the Nobel Prize in physics was awarded to Alain Specter, John Clauser and Anton Zeilinger for their experiments on entangled photons, a little part of the course was devoted to the description of the theory they allowed to uncover. To understand it we shall understand that in the first half of 1900 the idea of entanglement was difficult to accept. Especially Einstein was really skeptical about it since at first sight looked like a threat to its restricted relativity with information apparently traveling faster than light. Remained in history Einstein's definition of entanglement as "spooky action at a distance", showing how much he hated it. In this context, great work was putted by Einstein and others physicist in order to see if effectively QM was wrong or, better, not entirely right, meaning that we were still missing something to understand it at its fullest.

In 1935 Einstein, Podolsky and Rosen (EPR) delineated a theory trying to show that QM was indeed not complete, starting by defining what it means for a physical theory to be complete. The line of reasoning starts with the definition of the so-called elements of reality.

> **Definition 1.5.3: Elements of reality**
>
> A quantity is called element of reality if it has a value that can be predicted before experiment, basically it's already perfectly known already before taking the measure. A property of this type, for logic, must be owned by the system regardless of what you are making so that exist also before taking the measurement with a precise value.

This definition is purely based on logic, assuming that if I'm able to know the exact outcome of an experiment before taking the measure then the property that I'm measuring needs to have that value defined intrinsically inside it. Then, the next move is to use this definition to define when a theory is complete.

> **Definition 1.5.4: Complete theory**
>
> A physical theory is complete if it contains all elements of reality.

Using these two definitions, the three theoreticians demonstrated that QM is not complete if we assume the notion of locality. Where, locality was also defined by them as follows.

> **Definition 1.5.5: Locality**
>
> Measurements are independent if done in position and time that are not causally related.

With this they were able to create a thought experiment that demonstrated how some elements of reality were missing inside QM. The experiment that E. P. R. proposed is actually old, today the best way to understand this is by looking at the one proposed by David Bohm in 1951 which shows how spin is what is missing.

> **Theorem 1.5.1: Incompleteness of QM**
>
> Spin is an element of reality that is not contained entirely inside quantum mechanics.

Proof: We can imagine taking a singlet state of spin which is given by the following Bell state

$$|\phi^-\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}. \tag{1.69}$$

This state is a peculiar one, since it's possible to demonstrate that has the same form in every possible base. Meaning that if I change the base of representation to an orthonormal couple $\{|e_1\rangle, |e_2\rangle\}$ the state become

$$|\phi^-\rangle = \frac{|e_1 e_2\rangle - |e_2 e_1\rangle}{\sqrt{2}}. \tag{1.70}$$

Thus, if one measures the spin of the system in any direction, so using the right base, the same result will be found out meaning that the spin is an element of reality with a defined value. Nevertheless, in QM we know that the spin operators do not commute, meaning that we can't know both components of the spin at the same time. Basically, even if the whole spin vector is an element of reality quantum mechanics only allows for the partial knowledge of it, meaning that QM does not contain all elements of reality. ☺

This result showed, in the minds of Einstein and collegues, that the QM is not a complete theory needing still work to find out certain **hidden variables** whose treated statistically will recreate quanutm mechanics but used normaly will give deterministic results. Basically he was searching for the equivalent of classical mechanics starting from statistical mechanics, where now statistical mechanics is quantum mechanics itself.

This discussion was incredibly interesting at the time, but understanding what the hidden variables were remained more of a phylisofic question for a lot of times untill the idea of Bell. In 1964, he pusblished a paper showing how whatever deterministic real local theory using hidden variables is doomed to fail in reproducing the quantum mechanical result using the following reasoning. He focused his studies on a particuolar observable defined using four different ones Q, S, R and T, where all of them could only have two possible outcomes ± 1. The observable that we are interested in is the following

$$\mathcal{L} = QS + RS + RT - QT, \tag{1.71}$$

which posses some interesting properties such as it can have only two possible outcomes ± 2. Bell showed that inside a local real deterministic theory the following result must hold.

> **Theorem 1.5.2: Bell's inequality**
>
> Assuming locality and reality of the four observable composing $\mathcal{L}$ we have that the following relation hold
> $$\langle \mathcal{L} \rangle \leq 2. \tag{1.72}$$

Proof: We will assume that the four observables will be evaluated separetedly in four different measurements, having so that every draw forms the outcome (q, r, s, t) with a probability $P(q, r, s, t)$. We can so see how the following relation is true since we will have

$$\langle \mathcal{L} \rangle = \sum_{qsrt} (qs + rs + rt - qt) P(q, r, s, t) \leq 2 \sum_{qrst} P(q, r, s, t), \tag{1.73}$$

but the sum of the probability of all possible outcomes need to be normalized at 1 having so that the wanted relation holds. ☺

This result allowed to set a condition for the existence of the local hidden variables, the only thing remained to do is to show that quantum mechanics do not respect it. We can so take the following

example

$$Q = Z_1, \qquad\qquad S = -\frac{Z_2 + X_2}{\sqrt{2}}, \tag{1.74}$$

$$R = X_1, \qquad\qquad T = \frac{Z_2 - X_2}{\sqrt{2}}, \tag{1.75}$$

and evaluate the average of $\mathcal{L}$ in the singlet state. From locality, we can say that no correlation exist from the outcomes of the different measurements, so that their probability are independent of each other having

$$P(q, r, s, t) = P(q)P(r)P(s)P(t). \tag{1.76}$$

Meaning that the following is true

$$\langle \phi^-|\mathcal{L}|\phi^- \rangle = \langle QR \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2} > 2. \tag{1.77}$$

Meaning that QM doesn't respect Bell's inequality and so can't be reconstructed using local hidden variables. This line of reasoning was also proven experimentally by Cluaser first, and then also by Specter with a more refined experiment that reproduced accuratelly the $2\sqrt{2}$ result using photons and not spins. Therefore, local hidden variables will not be the answer to find out a deterministic quantum theory.

From that point on quantum information evolved a lot with the creation of quantum optics and entangled photons, in particualar the last part of the Nobel Prize was given to Zellinger sicne was the first to perform quantum teleportation in open air at a far distance in Vienna. He teleported a state using entangled photons from one part to the other of the Danube river.

1.6 Quantum algorithms

It's now to see some important quantum circuits that can be used in practice in order to obtain interesting results or behaviour inside a quantum computer. A lot of them will be not usefull per se, but are really important for the creation of larger and more powerful schemes.

Quantum Fourier Transform

The aim is to create an algorithm that bring the computational basis into the Fourier base, defined by the application of the Fourier transform on the vectors of the base itself. Therefore, we need first to recall the definition of discrete fourier transform which is given by.

Definition 1.6.1: Discrete Fourier transform

Taken a vector $(x_1, x_2, \ldots, x_N) \in \mathbb{C}^N$ it's Fourier transform is an application $\mathcal{U} : \mathbb{C}^N \to \mathbb{C}^N$ that actes in the following way

$$\mathcal{U}\mathbf{x} = \mathbf{y}, \qquad\qquad y_k = \frac{1}{\sqrt{N}}\sum_{j=1}^{N} e^{i2\pi\frac{jk}{N}} x_j. \tag{1.78}$$

We know that such an application posses a lot of properties, in particular we know how the following realtions are true

$$\mathcal{U}^{-1} = \mathcal{U}^*, \qquad\qquad \mathcal{U}^{-1} = \mathcal{U}^\dagger, \qquad\qquad (1.79)$$

meanging that it's a particular unitary transformation, and so we imagine that a circuit can represent it.

We basically want to create an algorithm that allows us to take the computational basis and perform Eq. (1.79) on it. In order to do that we will use a particular notation to describe the computational base of an N qubit system, using the binary representation.

Definition 1.6.2: Binary representation

Taken a system of N qubit, where the computational base has the form $\{|00\ldots0\rangle, |00\ldots1\rangle, \ldots\}$ we will write down the element s of the basis as $\{|j\rangle\}_{j=0}^{2^N-1}$ where the following relation is given

$$|j\rangle = |j_1 j_2 \ldots j_N\rangle, \qquad\qquad j = \sum_{i=1}^{N} j_i 2^{N-i}. \qquad\qquad (1.80)$$

basically j is the number described by the system state in binary base.

Using this notation it's really easy to write down the Fourier transform of the base having that

$$\mathcal{U}|j\rangle = \frac{1}{2^{N/2}} \sum_{k=0}^{2^N-1} e^{i2\pi \frac{jk}{2^N}} |k\rangle, \qquad\qquad (1.81)$$

having that the base is brought into another more complicated one. In fact, we can see how the states transform accordingly to the FT if the transformation is applied to the base. For example take a general state $|\psi\rangle$ we can see how

$$|\psi\rangle = \sum_j x_j |j\rangle, \qquad \mathcal{U}|\psi\rangle = \frac{1}{2^{N/2}} \sum_k \sum_j x_j e^{i2\pi \frac{jk}{2^N}} |k\rangle = \sum_k y_k |k\rangle, \qquad (1.82)$$

basically the coefficients defining the state in vector representation gets Fourier transformed. Still, this form of the Fourier tranform leaves not too much room for the creation of an algorithm that allow us to perform it in practice, so we need first to work a little on it and see how the following result holds.
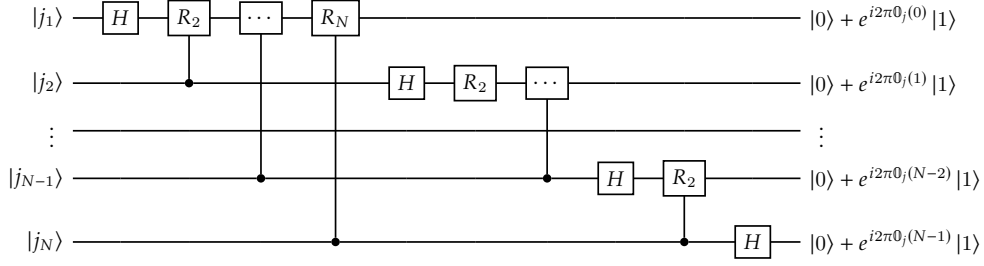

Theorem 1.6.1: Quantum Fourier Tranform

The Fourier transformation of the states in the computational basis can be rewritten as a sum of tensor product given by the following form using the binary representation for the base

$$\mathcal{U}|j\rangle = \frac{1}{2^{N/2}} \bigotimes_{l=1}^{N} \left[|0\rangle_l + e^{i2\pi\mathbb{0}_j(N-l)} |1\rangle_l \right]. \qquad (1.83)$$

Where the notation $\mathbb{0}_j(l)$ is defined as the following decimal number

$$\mathbb{0}_j(l) = \sum_{i=l+1}^{N} j_i 2^{l-i}. \qquad\qquad (1.84)$$

Figure 1.5: Circuits able to perform the quantum fourier tranform of the computational basis. It's important to notice how this algorithm is in reality not totally complete since the phases of the final states are inverted, so a series of swap gates needs to be inserted at the end to get the right form.

Proof: We can start to work around the expression of Eq. (1.81) by seing how we can rewrite $k/2^N$ in a more usefull form as

$$\frac{k}{2^N} = \sum_{l=1}^{N} k_l 2^{-l}. \tag{1.85}$$

We can then substitute it and see how, recalling that $|k\rangle = |k_1\rangle \otimes |k_2\rangle \cdots \otimes |k_N\rangle$, the following is true

$$\mathcal{U} |j\rangle = \frac{1}{2^{N/2}} \sum_{k=0}^{2^N-1} e^{i2\pi j \sum_{l=1}^{N} k_l 2^{-l}} |k\rangle = \frac{1}{2^{N/2}} \sum_{k=0}^{2^N-1} \bigotimes_{l=1}^{N} e^{i2\pi j k_l 2^{-l}} |k_l\rangle. \tag{1.86}$$

Now, the order of the operation can be inverted by taking some care anbd see how the expression become

$$\mathcal{U} |j\rangle = \frac{1}{2^{N/2}} \bigotimes_{l=1}^{N} \sum_{k_l=0,1} e^{i2\pi j k_l 2^{-l}} |k_l\rangle = \frac{1}{2^{N/2}} \bigotimes_{l=1}^{N} \left[|0\rangle_l + e^{i2\pi j 2^{-l}} |1\rangle_l \right]. \tag{1.87}$$

Now, we can see how the exponent can be simplified. In fact, if you use the definition of j we can see how

$$j2^{-l} = \sum_{i} j_i 2^{N-i-l} = \sum_{i \leq N-l} j_i 2^{N-i-l} + \sum_{i=N-l+1}^{N} j_i 2^{N-i-l} = \text{integer} + \mathbb{0}_j(N-l). \tag{1.88}$$

Obviously the integer part gives no contribution to the phase since multiply 2π at the exponent, so only the $\mathbb{0}_j(N-l)$ can be written obtaining the final result. ☺

Now, this form of the QFT is much more usefull on an algorithmic point of view since it's now easy per us to see the operations that needs to be done on the single qubits. In particular, to reproduce the result we will need two types of gates that are also easy to understand that are

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad\qquad R_k = \begin{pmatrix} 1 & 0 \\ 1 & e^{1\frac{2\pi}{2^k}} \end{pmatrix}, \tag{1.89}$$

28

basically the Hadamart and phase gates. The final form of the circuit is described in Fig. (1.5), where is possible to see how we can evaluate the QFT by the cimple use of controlled phase gates and swaps ones at teh end of the proces. This particular circuit is interesting since shows how quantum computers are able to perform fuorier transforms easily respect to classical algorithm. In fact, the number of gates required to perform such an operation scales as $O(n^2)$ while the number of logic gates needed to perform the computation of a fast fourier transform inside a classical computer scales as $O(n2^n)$. Quantum algorithm beats the classical one by an exponential factor. Nevertheless, the quantum algorithm has the big problem that the information are present in the phase of the states, and we are not able to evaluate them, basically meaning that the algorithm alone is useless. Still, we will see that QFT will still be used inside larger algorithm giving a lot of benefits.

Phase evaluation

The evaluation of phases inside quantum systems is always a troublesome problem, to the point that most of the time is thought as an impossible task. Nevertheless, is possible to see how the QFT algorithm is able to give us the possibility of experimentally evaluate a certain type of phase inside the system.

Let's imagine having a unitary operator $\mathcal{U}$ and wanting to evaluate the eigenvalues λ_n. We know from linear algebra that $\mathcal{U}\mathcal{U}^\dagger = \mathbb{1}$, so that from linear algebra we have the following information on the eigenvalues

$$\lambda_n \lambda_n^* = |\lambda_n|^2 = 1. \tag{1.90}$$

This relation tells us that the eigenvalues of such opeartors needs to be some kind of complex phases writable as

$$\lambda_n = e^{2\pi i \phi_n}, \qquad\qquad \phi_n \in [0, 1[. \tag{1.91}$$

Normally we would think that evaluating ϕ_n would be impossible since phases cannot be observed axperimentally. Still, we will show how using the eigenstate of the phases $|u_n\rangle$ and a simple operator $\mathcal{U}^{2^j}$ defined as follows

$$\mathcal{U}^{2^j} : |u_n\rangle \longmapsto e^{2\pi i \phi_n 2^j} |u_n\rangle, \tag{1.92}$$

we are able to approximate its value with a wanted precision. In particular, we are aiming to approximate ϕ_n using a decimal form like the one in Eq. (1.84), so that we want to find $(b_n^1, b_n^2, \ldots, b_n^t)$ so that

$$b_n = \frac{b_n^1}{2} + \frac{b_n^2}{4} + \cdots + \frac{b_n^t}{2^t}, \tag{1.93}$$

is the decimal number $b < \phi_n$ closer to it as possible. Therefore, we are going to demonstrate that the algorithm showed in Fig. (1.6) is able to do exactly that, find out the values of b_n^i approximating the phase up to a wanted accuracy.

> **Theorem 1.6.2: Phase evaluation**
>
> Taken a unitary operator $\mathcal{U}$ with eigenvalues defined by the phases ϕ_n, the circuit Fig. (1.6) is able to give as output its decimal approximation b_n with a wanted accuracy $\alpha > 0$, and precision
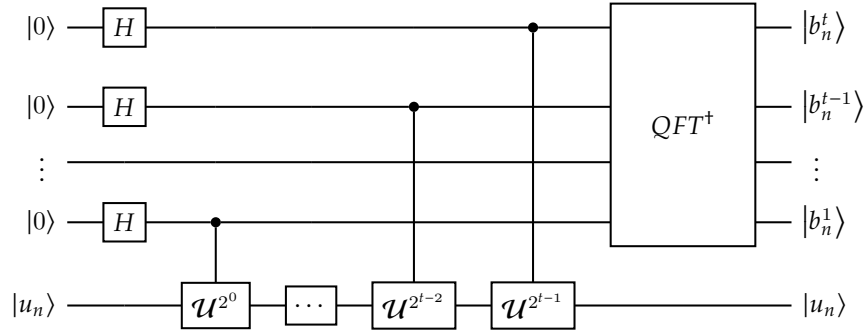
Figure 1.6: Quantum circuit for the approximation of the eigenvalues of a unitary operator up to a wanted accuracy based on the number of qubit used for the decimal approximation of the phase itself.

$\epsilon > 0$ if the number of qubit used for the operation is

$$t > \alpha + \ln\left(2 + \frac{1}{2\epsilon}\right). \tag{1.94}$$

Proof: First we need to look at what the circuit does effectivelly to the states, and it's easy to see that by looking at the case where $t = 1$ and see how the first part of the circuit works as follows

$$\left(C\mathcal{U}^{2^0}\right)(H \otimes \mathbb{1})\,|0\rangle \otimes |u_n\rangle = C\mathcal{U}^{2^0}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |u_n\rangle = \left(\frac{|0\rangle + e^{2\pi i\phi_n}\,|1\rangle}{\sqrt{2}}\right) \otimes |u_n\rangle. \tag{1.95}$$

Which can be easily generalized to all the applications on the geneanal t-dimensional circuit having a final form of the state given by

$$|\psi_f\rangle = \left[\bigotimes_{j=0}^{t-1}\left(\frac{|0\rangle + e^{2\pi i\phi_n 2^j}\,|1\rangle}{\sqrt{2}}\right)\right] \otimes |u_n\rangle \tag{1.96}$$

Now, we know how every real number can be written as a converging series of rational numbers such as Eq. (1.84) so that we are going to work with

$$\phi_n = \frac{\phi_n^1}{2} + \frac{\phi_n^2}{4} + \cdots = \sum_{i=1}^{\infty} \frac{\phi_i}{2^i} \approx \sum_{i=1}^{t} \frac{\phi_i}{2^i}. \tag{1.97}$$

Meaning that can be approximated using the decimal representation described before, having that the phases can be rewritten using the following form

$$\exp\left(2\pi i\phi_n 2^j\right) = \exp\left(2\pi i\left\{[\phi_n^1 2^{j-1} + \dots] + [\phi_n^{j+1} 2^{-1} + \dots]\right\}\right) = \exp\left(2\pi i\mathbb{0}_\phi(j)\right), \tag{1.98}$$

where the first part was an integer giving no contribution. In this way one can understand that in the first part of the $|\psi_f\rangle$ state we end up having the QFT of the initial states, allowing us to write it in binary representation as

$$|\psi_f\rangle \approx \left(\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi_n k} |k\rangle\right) \otimes |u_n\rangle. \tag{1.99}$$

In this way we can go and apply the inverse of the QFT and using the binary representation of the base to see what happens exactly in the transformation

$$QFT^\dagger |\psi_f\rangle = \frac{1}{2^t} \sum_{k=0}^{2^t-1} e^{2\pi i \phi_n k} \sum_{l=0}^{2^t-1} e^{-2\pi i k l/2^t} |l\rangle = \sum_l \left(\sum_{k=0}^{2^t-1} \frac{1}{2^t} e^{2\pi i(\phi_n - l/2^t)k}\right) |l\rangle = \sum_l c_l |l\rangle. \tag{1.100}$$

The state becomes a superposition of states in the binary computational base of the t qubits, and we know also the form of the coefficients. In fact, we can easily see how c_l are composed by a geometric series giving rise to the following result

$$c_l = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i(\phi_n - l/2^t)}\right)^k = \frac{1}{2^t} \frac{1 - e^{2\pi i(\phi_n - l/2^t)2^t}}{1 - e^{2\pi i(\phi_n - l/2^t)}}. \tag{1.101}$$

It's interesting to see how this result was obtained by truncating the real form of ϕ_n to a certain decimal order, but the procedure is general and works also in the case where the total series is retained.

Therefore, in Eq. (1.101) the value of ϕ_n can be a rational or irrational number, and we can see what happens to c_l in the two cases. In the case ϕ_n is rational we have that the approximation Eq. (1.97) is exact, and we can write how

$$(\phi_n - l/2^t)2^t = \sum_{i=1}^{t} \phi_n^i 2^{t-i} - l = int. \tag{1.102}$$

This means that the phase on the numerator of c_l is a multiple of 2π and therefore $c_l = 0$ for every value of l exept for $l = \phi_n 2^t$, where

$$c_{\phi_n 2^t} = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i(\phi_n - \phi_n)}\right)^k = \frac{2^t}{2^t} = 1. \tag{1.103}$$

This means that $c_l = \delta_{l\phi_n 2^t}$ which basically becomes a condition on the values of the single qubit that will take the following forms

$$\sum_{l=0}^{2^t-1} \delta_{l\phi_n 2^t} |l\rangle = |\phi_n 2^t\rangle = |\phi_n^1\rangle \otimes |\phi_n^2\rangle \otimes \cdots \otimes |\phi_n^t\rangle, \tag{1.104}$$

where the binary representation was used to write down the single qubits. Now, we can simply evaluate all the t qubits and have our approximation of the phase ϕ_n that is exact in this case, having that $b_n = \phi_n$.

In the case ϕ_n is irrational, the truncation in the series generate an error having also that $(\phi_n - l/2^t)2^t$ is not an integer anymore and c_l can be different from 0 for other l values. In this case we are going to approximate the value of ϕ_n using the values of b_n that we obtain from the evaluation, and we

want to know the error we are generating from such an approximation along with the accuracy of the result. Therefore, we select an error value ω and compute the probability of performing the measure

$$\tilde{P} = P(\bar{l} \in [-\omega - 1, \omega + 1]), \tag{1.105}$$

where $\bar{l} = l - \phi_n$ so that $\bar{l} = 0$ correspond to the real ϕ_n. This evaluation can be performed using as ω the value $2^{t-\alpha} - 1$, where α is called accuracy, obtaining the result of

$$1 - \tilde{P} \leq \frac{1}{2(2^{t-\alpha} - 2)}. \tag{1.106}$$

Which identify the probability of not obtaining the wanted result, that we are going to set below a certain precision ϵ having $1 - \tilde{P} < \epsilon$ so that the following relations is found

$$t > \alpha + \ln\left(2 + \frac{1}{2\epsilon}\right). \tag{1.107}$$

☺

Therefore, this algorithm is able to give us a really greate approximation for the phase that increase in accuracy as we scale up the number of qubit used in order to perform the operation. Also, it's possible to see how we from the inequality we can actually controll also the accuracy and precision of the prediction by setting them prior and then choose t in order to satisfy Eq. (1.94).

Grover algorithm

Search algorithm are one of the most important type of algorithm that exist, since the aim is to find out specific elements inside a set that satisfy some requirements defined by ceratin function $f(x)$. Normally this kind of algorithms are really expensive scaling up real quick with both dimensions of the set and complexity of the function to use, but inside a quantum computer we can try to create a really efficient version of them.

Let's imagine to work with n qubits, so that the computational base is composed by $N = 2^n$ elements that compose our set $\mathcal{N}$ in which only $1 \leq M \leq N$ elements are solutions of $f(x)$. Where, being solutions means that the state $|x\rangle$[1] that represent that element is so that

$$f(x) = \begin{cases} 1 & x \in \text{solution} \\ 0 & x \notin \text{solution} \end{cases}, \tag{1.108}$$

basically $f : \mathcal{S} \to \{0, 1\}$ is a boolean function that gives true if it's solution and false otherwise. Then, we are going to need two types of gates that will generate the building blocks of our algorithm.

Theorem 1.6.3: Oracle gate

The circuit shown in Fig. (1.7) is called oracle and is able to perform an inversion of the states that are not solution by using an ausiliary qubit in the $|1\rangle$ state.

$$O\,|x\rangle = (-1)^{f(x)}\,|x\rangle, \tag{1.109}$$

---

[1]We are using the binary representation for the state of the computational basis.
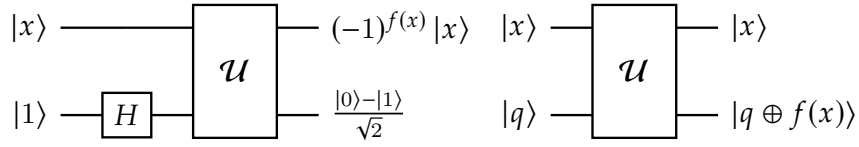
Figure 1.7: Quantum circuit for the oracle gate used inside the algorithm to perform an inversion of the state about the components that are not solution to the function that we are interested in.

so that if $|x\rangle$ is solution a -1 pops up, and remains equal otherwise.

Proof: We can simply go over the different steps of the circuit to see how the following happens to the state

$$\mathcal{U}\,(\mathbb{1} \otimes H)\,|x\rangle \otimes |1\rangle = \mathcal{U}\,|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle \otimes \frac{1}{\sqrt{2}} \begin{cases} |0\rangle - |1\rangle & x \in \mathcal{S}, \\ |1\rangle - |0\rangle & x \in \mathcal{E} \end{cases}. \tag{1.110}$$

Where $\mathcal{S}$ and $\mathcal{E}$ are the subset of $\mathcal{N}$ that contains the states that are solutions and not, respectivelly. Now, we can see how the difference between the two is simply a minus sign that we can imagine factorizing so that $|x\rangle$ takes it changing its phase as wanted. ☺

The next step is to define another type of gate that will be needed to perform another, more complex, type of reflection about the average state. Such gate is actually defined through also the use of a **conditional phase operator** defined as

$$\mathcal{U}_x = 2\,|x\rangle\langle x| - \mathbb{1}, \tag{1.111}$$

which has the effect of changing the phase to all state in the base that are not $|x\rangle$, and it's really easy to see since

$$\mathcal{U}_x\,|k\rangle = \begin{cases} |k\rangle & k = x, \\ -\,|k\rangle & k \neq x \end{cases}. \tag{1.112}$$

Using this idea we can define the wanted inversion operator in this particular way.

Theorem 1.6.4: Inversion about the average

We can define the inversion about the average operator inside the space $\mathcal{N}$ as $\tilde{\mathcal{U}} = H^{\otimes n}\mathcal{U}_0 H^{\otimes n}$ and see how it's effect on a general state is

$$|\phi\rangle = \sum_{k \in \mathcal{N}} \alpha_k\,|k\rangle\,, \qquad\qquad \tilde{\mathcal{U}}\,|\phi\rangle = \sum_{k \in \mathcal{N}} (2\,\langle \alpha\rangle - \alpha_k)\,|k\rangle\,. \tag{1.113}$$

Which defines an inversion about the average state $\langle \alpha\rangle$.

Proof: We can first have a look at the form of the operator itself, which can be rewritten in a compact way as follows

$$\tilde{\mathcal{U}} = 2H^{\otimes n}\,|0\rangle\!\langle 0|\,H^{\otimes n} - \mathbb{1} = 2\,|\psi\rangle\!\langle\psi| - \mathbb{1}, \qquad |\psi\rangle = \frac{1}{\sqrt{N}}\sum_{k\in\mathcal{N}}|k\rangle. \tag{1.114}$$

Then, we can apply it to a general state to see how we retain the wanted result. In particular, we are going to write that

$$\tilde{\mathcal{U}}\sum_{k\in\mathcal{N}}\alpha_k\,|k\rangle = 2\sum_{k\in\mathcal{N}}\alpha_k\,\langle\psi|k\rangle\,|\psi\rangle - \sum_{k\in\mathcal{N}}\alpha_k\,|k\rangle = 2\sum_{k\in\mathcal{N}}\sum_{l\in\mathcal{N}}\sum_{x\in\mathcal{N}}\frac{\alpha_k}{N}\,\langle l|k\rangle\,|x\rangle - \sum_{k\in\mathcal{N}}\alpha_k\,|k\rangle,$$
$$\tag{1.115}$$

where we can use the fact that $\langle l|k\rangle = \delta_{lk}$ to eliminate a summation and then see how $\sum_{k\in\mathcal{N}}\alpha_k/N = \langle\alpha\rangle$ so that the final result is obtained as

$$\tilde{\mathcal{U}}\sum_{k\in\mathcal{N}}\alpha_k\,|k\rangle = 2\sum_{x\in\mathcal{N}}\langle\alpha\rangle\,|x\rangle - \sum_{k\in\mathcal{N}}\alpha_k\,|k\rangle = \sum_{k\in\mathcal{N}}(2\,\langle\alpha\rangle - \alpha_k)\,|k\rangle. \tag{1.116}$$

☺

These two gates are the building blocks that will allow us to perform the quantum search and the idea to that is to actually define an operator that will allow us to transform the state into a linear combination of the ones that are solutions to our function. This can be done easily, since the following result holds, giving us the final form for the quantum search algorithm.

> **Theorem 1.6.5: Quantum search**
>
> A general state $H^{\otimes n}\,|0\rangle$ can be decomposed in two main parts inside $\mathcal{N}$ as
>
> $$|\psi\rangle = H^{\otimes n}\,|0\rangle = \sin\frac{\theta}{2}\,|\beta\rangle + \cos\frac{\theta}{2}\,|\alpha\rangle, \tag{1.117}$$
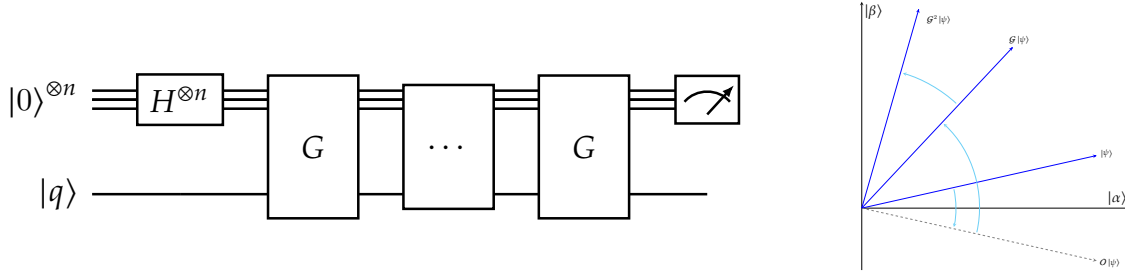>
> where $|\beta\rangle$ is a linear combination of all the solutions of $f(x)$, while $|\alpha\rangle$ a combination of all the non-solutions. The **Groover opeartor** $\mathcal{G} = \tilde{\mathcal{U}}O$ acts on this state by rotating the angle θ in the direction of $|\beta\rangle$, so that if applied R times we get
>
> $$\mathcal{G}^R\,|\psi\rangle = \sin\left(\frac{2R+1}{2}\theta\right)|\beta\rangle + \cos\left(\frac{2R+1}{2}\theta\right)|\alpha\rangle. \tag{1.118}$$
>
> Therefore, we can select the right number of $\mathcal{G}$ to perform in order to obtain the maximum likelihood to obtain as a result of the measurement the state $|\beta\rangle$ with the solutions of the function.

Proof: We can start by looking at the general state $|\psi\rangle$ and see how can be rewritten as linear combination of solution and non-solution as follows

$$|\psi\rangle = \frac{1}{\sqrt{N}}\left(\sum_{k\in\mathcal{S}}|k\rangle + \sum_{k\in\mathcal{E}}|k\rangle\right) = \sqrt{\frac{M}{N}}\left(\frac{1}{\sqrt{M}}\sum_{k\in\mathcal{S}}|k\rangle\right) + \sqrt{\frac{N-M}{N}}\left(\frac{1}{\sqrt{N-M}}\sum_{k\in\mathcal{E}}|k\rangle\right), \tag{1.119}$$

Figure 1.8: Graphical representation of the Groover's circuit, to the left, with transformations that happens to the state in the quantum search algorithm, to the right, in order to understand how the two reflection tranforms into a rotation.

now we can see how $\sqrt{M/N}$ and $\sqrt{N-M/N}$ can be setted as the sine and cosine, while the superpositions that are mulitpling are exactly the linear combinations of all solutions and non-solutions respectivelly. Therefore, we effectivelly have that the following is true

$$H^{\otimes n}\left|0\right\rangle = \sin\frac{\theta}{2}\left|\beta\right\rangle + \cos\frac{\theta}{2}\left|\alpha\right\rangle, \tag{1.120}$$

then we shall see what the operator $\mathcal{G}$ does on it, and that can be done by looking at O and $\tilde{\mathcal{U}}$ separatelly. First, it's easy to understand how the oracle gate simply changes the sign of the $\left|\beta\right\rangle$ coefficient, meaning that using it simply performs a reflection of the state respec to the $\left|\alpha\right\rangle$ one. Then, the inversion by the average operator instead perform another inversion in this case that is respect to the state $\left|\psi\right\rangle$, so that two inversions apply one after giving a final rotation of the state as

$$\mathcal{G}\left|\psi\right\rangle = \sin\left(\frac{3}{2}\theta\right)\left|\beta\right\rangle + \cos\left(\frac{3}{2}\theta\right)\left|\alpha\right\rangle, \tag{1.121}$$

which is also depicted in Fig. (1.8). Meaning that the rotation allowed for the state to become closer to the $\left|\beta\right\rangle$ state, and if we continue to perform it we will get as a state

$$\mathcal{G}^R\left|\psi\right\rangle = \sin\left(\frac{2R+1}{2}\theta\right)\left|\beta\right\rangle + \cos\left(\frac{2R+1}{2}\theta\right)\left|\alpha\right\rangle. \tag{1.122}$$

In this way we can see how the probabilities of having as result $\left|\beta\right\rangle$ scales up since the angle gets closer to $\pi/2$, which gives 1 as coefficient for that state. Still, it's possible to do too many rotations and ending up to go past the perfect value and increasing the coefficients for the $\left|\alpha\right\rangle$ state, still one can see how if R is choosen as

$$R = \left[\frac{\arccos\sqrt{M/N}}{\phi}\right], \qquad\qquad \phi \le 4, \tag{1.123}$$

where $[x]$ is the integer part function, we will have probabilities that looks like

$$P_\beta > 1/2, \qquad\qquad P_\alpha < 1/2. \tag{1.124}$$

Basically, we can select ϕ to obtain the most optimized result possible, and already we know that by default the probabilities are in favor of the right result that we are serching for. ☺

Therefore, this algorithm allows us to search inside a set of states of dimensions 2^n the ones that satisfy the condition imposed by a wanted function f. Also, all of this is done by using a minimal number of operations that scales linearly with the number of qubit that we are using, beating in an increadible way the classical search algorithm that scales exponentially.

35

Exercises

2.1 Gates

1: Double control gate

Verify the equivalence of the two following circuits:
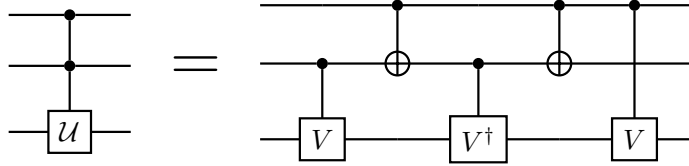
Where the unitary operation V is defined as $\sqrt{\mathcal{U}}$.

Solution: Two main ways of soliving this problem can be used, the first and simplest one is by constructing the thruth table of the two circuits and see that is the same. Something that is left to the reader since it's a really simple task. The other one is by going with a matrix multiplication and seing how the matrix form of the circuit on the right is the same as the general double control. To see that first we can write the following form of the matrix of the circuit

$$(CV_{13} \otimes \mathbb{1}_2)\,(CNOT_{12} \otimes \mathbb{1}_3)\left(\mathbb{1}_1 \otimes CV_{23}^{\dagger}\right)(CNOT_{12} \otimes \mathbb{1}_3)\,(\mathbb{1}_1 \otimes CV_{23})\,. \tag{2.1}$$

Now, we know how to write down the majority of those matrices but one. For example, we can easily write the following thing

$$\mathbb{1}_1 \otimes CV_{23}^{\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \mathbb{1} & 0 \\ 0 & V \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 & 0 & 0 \\ 0 & V & 0 & 0 \\ 0 & 0 & \mathbb{1} & 0 \\ 0 & 0 & 0 & V \end{pmatrix}, \tag{2.2}$$

where the tensor product rule has been used in the multiplication. Still, a problem is present in the evaluation of the first matrix, because the order matters in tensor product and in that case the control is applied to a qubit that is not directly attached to the one of the target. Therefore, the main way we have to evaluate that matrix is to swap the qubit and then use a normal control gate as we have seen right now

$$CV_{13} \otimes \mathbb{1}_2 = (S_{12} \otimes \mathbb{1}_3)(\mathbb{1}_1 \otimes CV_{23})(S_{12} \otimes \mathbb{1}_3). \tag{2.3}$$

By recalling the form of the swap operator matrix being Eq. (1.24) we can perform now all the computation to obtain

$$CV_{13} \otimes \mathbb{1}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & V & 0 \\ 0 & 0 & 0 & V \end{pmatrix}, \tag{2.4}$$

which then can be used to perform the matrix multiplication and obtain the final form of the gate that wuold be analogous to the one of a CCU gate. ☺

2.2 Measure

2: General one qubit measure

Take the general form of an observable acting on a qubit $A = \mathbf{n} \cdot \boldsymbol{\sigma}$, where $\boldsymbol{\sigma}$ is a vector containing the Pauli matrices and $\mathbf{n}$ is real versor. Find out the possible outcomes of a measure done on a general state $|\psi\rangle$ and their probability of happening.

At last, show how the measuring A on the computational basis is not totally equivalent to measuring it in the $|e_\pm\rangle$ orthonormal base of eigenstates since $|\psi\rangle$ collapse in different states, but the following circuit
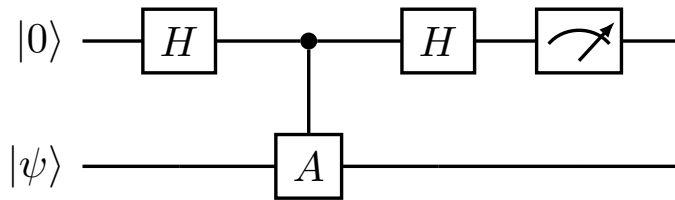
can instead reproduce the exact measure by evaluating the axiliary qubit, forming the POVM of the A PVM measure.

Solution: First we can easily find out the values of the eigenvalues by using the following trick. We can take the square of the matrix seeing how

$$(\mathbf{n} \cdot \boldsymbol{\sigma})^2 = n_x^2 X^2 + n_y^2 Y^2 + n_z^2 Z^2 + n_x n_y XY + n_x n_y YX + \dots, \tag{2.5}$$

by recalling that $XY = -YX$ for every couple of Pauli matrix and $X^2 = Y^2 = Z^2 = \mathbb{1}$ we can see how

$$(\mathbf{n} \cdot \sigma)^2 = |\mathbf{n}|\mathbb{1} = \mathbb{1}. \tag{2.6}$$

Therefore, we can say that the squares of the eigenvalues of A needs to give 1, but we can also say that the following is true

$$\operatorname{tr} A = n_x \operatorname{tr} X + n_y \operatorname{tr} Y + n_z \operatorname{tr} Z = 0. \tag{2.7}$$

Meaning that we can now find out the eigenvalues of the matrix $\lambda_\pm$ simply by knowing that $|\lambda_\pm|^2 = 1$ and that their sum needs to be zero $\lambda_+ + \lambda_- = 0$ having that the only possible solution is

$$\lambda_+ = +1, \qquad\qquad \lambda_- = -1. \tag{2.8}$$

Meaning that the only possible outcomes of the measure is still ±1 also for this observable.

Now, to measure the probability of one outcome to appear we need to write down the projector on the base of the observable. In particular, we can say that being A selfadjoint a base $|e_\pm\rangle$ of eigenvector exist whose projectors $P_\pm = |e_\pm\rangle\langle e_\pm|$ has the properties

$$\mathbf{n} \cdot \sigma = P_+ - P_-, \qquad\qquad \mathbb{1} = P_+ + P_-. \tag{2.9}$$

Meaning that we can invert those and find out in the end the following forms

$$P_\pm = \frac{\mathbb{1} \pm A}{2}. \tag{2.10}$$

From this we can easily write down the probabilities of measuring in a state like $|\psi\rangle = \alpha |e_+\rangle + \beta |e_2\rangle$ which are simply $p_+ = |\alpha|^2$ and $p_- = |\beta|^2$. Nevertheless, we are interested also in evaluating it in the computational base so that the state is written as $|\psi\rangle = a |0\rangle + b |1\rangle$ having that the probability becomes

$$\tilde{p}_\pm = \langle\psi|P_\pm|\psi\rangle = \frac{1}{2}\left[(1 \pm n_z) \pm 2n_x \operatorname{Re}\{a^*b\} \pm 2n_y \operatorname{Im}\{a^*b\}\right]. \tag{2.11}$$

Where one can see how the coefficients generate added terms to the probabilities in case of superpositioning, meaning that if one of the two a or b is zero the added terms vanishes. Also, those terms depends on the relative phase of the two coeffiecients meaning that **interference effects** can happen. Still, the values obtained are in reality equal to the one of α and β squared seen previusly if one does all the computations, meaning that the probabilities evaluated in the two bases are the same. What changes is the collapsing since in the normal base $|\psi\rangle$ collapse in one of the two $|e_\pm\rangle$ while in the computational will become either $|0\rangle$ or $|1\rangle$.

We can now see how the circuit we have seen that uses an auxiliary qubit to perform the computation is able to generate the exact measure we are searching for, also forming a POVM for that measure. To see that we can see how the state of the system evolves inside the circuit by starting from the application of the Hadamert gate and of the CA one having

$$|0\rangle |\psi\rangle = \frac{|0\rangle |\psi\rangle + |1\rangle A |\psi\rangle}{\sqrt{2}}. \tag{2.12}$$

Then, by using a second Hadamart gate we can easily see how the state can be written simply as

$$|0\rangle \left(\frac{\mathbb{1} + A}{2}\right) |\psi\rangle + |1\rangle \left(\frac{\mathbb{1} - A}{2}\right) |\psi\rangle = |0\rangle P_+ |\psi\rangle + |1\rangle P_- |\psi\rangle. \tag{2.13}$$

38

Meaning that we have an entangled state where, by measuring the first qubit in the computational base allow us to know the state of $|\psi\rangle$ that has collapsed in one of the two eigenstate of A. Also, we can see how the probability of measuring the outcome ± 1 in the computational base is given by

$$\langle 0|0\rangle \, \langle \psi|P_{\pm}^{\dagger}P_{\pm}|\psi\rangle = \tilde{p}_{\pm}. \tag{2.14}$$

Basically the probabilities remains the same but now the states collapse in the right way so that the full measure is obtained, we only need one extra qubit. ☺