SAPIENZA
UNIVERSITÀ DI ROMA

“Sapienza” University of Rome
Faculty of Information Engineering,
Informatics and Statistics
Department of Computer Science

Quantum Computing

Author
Alessio Bandiera

October 11, 2025

Contents

Information and Contacts

Personal notes and summaries collected as part of the *Quantum Computing* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link:
https://github.com/aflaag-notes. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: **alessio.bandiera02@gmail.com**
- LinkedIn: **Alessio Bandiera**

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

Suggested prerequisites:

TODO

Licence:

1

Introduction on Quantum Computation

1.1 The Qubit

Quantum computing is a rapidly developing discipline that explores how the laws of quantum mechanics can be used to *process information*. While classical computation is based on *bits* that take values of either 0 or 1, quantum computation relies on quantum bits, or **qubits**. A qubit can exist in a "superposition" of classical states, allowing it to encode richer information than a single bit. Furthermore, qubits can exhibit particular properties that enable forms of information processing with no classical counterpart. Such properties provide the foundation for algorithms that promise to solve certain problems more efficiently than their classical analogues.

The design of quantum algorithms requires a different perspective from that of classical computation. In classical computer science, the majority of widely studied algorithms are *deterministic*, meaning that for a given input they will always produce the *same output*. Some algorithms are *randomized*, making use of probability to achieve efficiency or simplicity, yet even in those cases the computation itself is ultimately classical in nature. In fact, to achieve such *randomness* classical algorithms employ **pseudo-random number generation**, which must ultimately produce finite sequences.

Quantum computation, by contrast, *incorporates probability* at its core. The act of measuring a quantum system does not reveal a single, predetermined result, but rather yields one outcome from a distribution of possible outcomes, with probabilities governed by the system's quantum state. This fundamental probabilistic characteristic distinguishes quantum algorithms from their classical counterparts.

In fact, in the context of quantum computing we are often interested in **probabilistic algorithms**: for such algorithms, a given input i can lead to a finite set of possible outputs $o_1, \ldots, o_N$, each occurring with an associated probability $p_1, \ldots, p_N$ — where $\sum_{i=1}^{n} p_i = 1$.

As previously mentioned, the quantum equivalent of the classical bits are the **qubit**, but define the qubits we first need to define some preliminary concepts. The following vectors are called **basis states**

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

and they represent the classical bits 0 and 1 respectively — the notation above is called "braket" notation and it will be explored in greater detail in later sections.

So what is a qubit? A qubit is the basic unit of information in quantum computing, which represents a **superposition** of states simultaneously — note that we will refer to qubits and their states interchangeably, since the only thing that we care about a qubit is its own state

In practice, the state of a qubit is a vector

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$ are called **probability amplitudes**. But why are we talking about probabilities in the first place? The "true" state of a qubit **cannot be observed**, and we say that the qubit is in a *superpotion* of $|0\rangle$ and $|1\rangle$ in the sense that α and β describe the probabilities of getting either states once the qubit is measured. This is because to know the value of a qubit we have to *measure it*, and the measurement operation itself will make the qubit *collapse* into either $|0\rangle$ or $|1\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively, i.e.

$$\Pr[\text{measured qubit is } |0\rangle] = |\alpha|^2 \qquad \Pr[\text{measured qubit is } |1\rangle] = |\beta|^2$$

To use a more compact notation, we will denote this property as follows:

$$\alpha\,|0\rangle + \beta\,|1\rangle \begin{cases} |0\rangle & @ \ |\alpha|^2 \\ |1\rangle & @ \ |\beta|^2 \end{cases}$$

where the @ notation (read as "at") denotes the probabilty of the corresponding outcome. Note that if we measure a collapsed qubit we will keep observing the same state indefinitely.

In reality, to be precise qubits actually collapse into any multiple $z\,|0\rangle$ or $z\,|1\rangle$, where $z \in \mathbb{C}$ is a complex number such that $|z| = 1$, but this is not relevant from a physical point of view. In fact, for any θ physicists treat $|\psi\rangle = |0\rangle$ and $|\psi'\rangle = e^{i\theta}\,|0\rangle$ as the *same physical state*, because probabilities depend on squared magnitudes and thus

$$\left|e^{i\theta}\alpha\right|^2 = |\alpha|^2$$

(and the same applies for β too) even though $|\psi\rangle$ and $|\psi'\rangle$ are different vectors mathematically. Therefore, in general we can actually drop the **global phases** from the qubits entirely.

1.2 Qubit operations

What can we do with qubits other then *measure them*? The operations that can be applied on qubits are restricted to **unitary transformations**.

Definition 1.1: Unitary transformation

A transformation U is said to be **unitary** if it preserves the norm of its input vector, i.e.

$$\forall v \quad ||Uv|| = ||v||$$

For instance, the identity matrix I is an example of trivial unitary transformation, but also the NOT matrix, which is the following

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

which has the effect of *swapping* the input basis state

$$\text{NOT}\,|0\rangle = |1\rangle \qquad \text{NOT}\,|1\rangle = |0\rangle$$

This matrix behaves as the classical NOT gate with the usual bits in classical computing, in fact will refer to *transformations* and *gates* interchangeably.

More in general, the NOT operation belongs to a family of operation represented by the so called **Pauli matrices**.

Definition 1.2: Pauli matrices

The **Pauli matrices** are the following four 2×2 matrices:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

In particular, we observe that the second matrix σ_x is exactly the matrix of the NOT operator. We will see the Z and Y operators — representing the other two matrices, respectively — as well in later sections.

Another very important transformation is represented by the **Hadamard gate**, which is the following matrix

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

This matrix has the effect of "mapping" classical states into superpositions:

$$H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \begin{cases} |0\rangle & @\ \frac{1}{2} \\ |1\rangle & @\ \frac{1}{2} \end{cases}$$

For instance, in this example given $|0\rangle$ which represents the classical bit 0, we get a qubit as output of the linear transformation. In general, the operation performed by the Hadamard gate can be represented as follows:

$$\forall a \in \{0, 1\} \quad \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a\,|1\rangle)$$

As a side note, as we mentioned at the beginning of the chapter quantum mechanics has randomness intrinsically, and since the operation $H|0\rangle$ returns a qubit that has 50% of probability of being either $|0\rangle$ or $|1\rangle$ once measured, this operation provides a true random number generator.

Lastly, can we *represent* qubits graphically? Well, we may be tempted to anwer negatively to this question, since a qubit is described by two complex numbers $\alpha, \beta \in \mathbb{C}$, which implies that we actually need 4 dimensions to correctly represent our vector. However, through polar coordinates we can actually define a graphical representation which allows us to "picture" qubits, through the so called **Bloch sphere**. First, consider a qubit

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

for some $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$, as usual. Now, recalling that any complex number $z \in \mathbb{C}$ can be actually written as follows

$$z = |z| e^{i\theta}$$

for some angle θ, we can actually rewrite our qubit as follows:

$$\begin{aligned}
|\psi\rangle &= |\alpha| e^{i\theta_\alpha}|0\rangle + |\beta| e^{i\theta_\beta}|1\rangle \\
&= e^{i\theta_\alpha}\left(|\alpha||0\rangle + |\beta| e^{i\left(\theta_\beta - \theta_\alpha\right)}|1\rangle\right) \\
&= |\alpha||0\rangle + |\beta| e^{i\left(\theta_\beta - \theta_\alpha\right)}|1\rangle && \left(e^{i\theta_\alpha} \text{ is a global phase}\right) \\
&= |\alpha||0\rangle + e^{i\varphi}|1\rangle && (\text{let } \varphi := \theta_\beta - \theta_\alpha \in [0, 2\pi))
\end{aligned}$$

and finally, since $|\alpha|^2 + |\beta|^2 = 1$, is precisely the equation of the circumference of radius 1, we usually rewrite the last equation as follows:

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

where $\theta \in [0, \pi], \varphi \in [0, 2\pi)$. This formulation of the qubit $|\psi\rangle$ allows us to represent it inside the Bloch sphere: in fact, in this formulation the qubit is normalized, which implies that it will lie on a 3 dimensional unit sphere, and it is described by the two phases θ and φ — in 2D polar coordinates there is only 1 angle, as in 3D polar coordinate there are two angles.

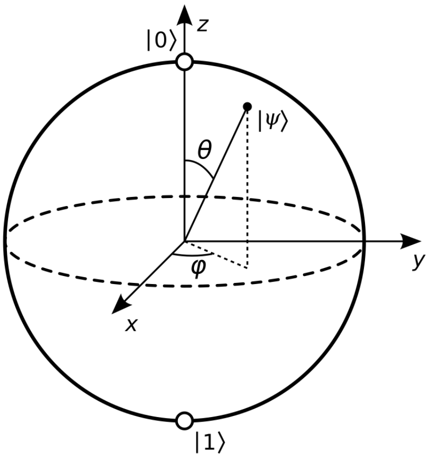

Figure 1.1: The Bloch sphere representing some qubit.

1.2.1 The tensor product

So far we have dealt with only one qubit at a time, but what if we have two qubits? First, let's look at the classical counterpart. If we take two bits $a, b \in \{0, 1\}$, we can represent 4 possible binary numbers, namely 00, 01, 10 and 11, which we can algebraically obtain by computing the usual cartesian product

$$\{0,1\}^2 = \{0,1\} \times \{0,1\} = \{(0,0),(0,1),(1,0),(1,1)\}$$

Note that in the cartesian products it holds that:

- the length of the tuples of the product is linear w.r.t. the number of factors of the cartesian products — in this case, 2
- each element of a tuple is *independent* from the other elements of the tuple

How can we evaluate all the possible states that two qubits can represent, instead? To answer this question, we need to introduce a new operator, which is called **tensor product**. Given two vectors $\begin{pmatrix} a \\ b \end{pmatrix}$ and $\begin{pmatrix} c \\ d \end{pmatrix}$, their tensor product is defined as follows

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

Hence, consider two qubits

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \qquad |\phi\rangle = \beta\, |0\rangle + \beta_1 |1\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$$

To obtain all the possible states of $|\psi\rangle$ and $|\phi\rangle$ we just have to compute the tensor product between them, which is

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \\ &= \alpha_0\beta_0 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_0\beta_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_1\beta_0 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_1\beta_1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned}$$

At the beginning of the chapter we defined $|0\rangle$ and $|1\rangle$ to be $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ without providing an explaination; now that we are dealing with more than 2 dimensions we can show why such names are used. In fact, we will use the following naming convention

$$|00\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

and in general it holds that
$$|\text{bin}(i)\rangle = e_i$$
where $\text{bin}(i)$ represents for the binary representation of i, and e_i is the i-th vector of the canonical basis. This implies that we can rewrite the previous tensor product as follows:

$$|\psi\rangle \otimes |\phi\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle = \sum_{i,j\in\{0,1\}} \alpha_i\beta_j |ij\rangle$$

As a final note, it can be easily proven that

$$\forall i, j \in \{0,1\} \quad |i\rangle \otimes |j\rangle = |ij\rangle$$

For example, given two qubits

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

we get that

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &\begin{cases} |0\rangle \text{ and } |0\rangle & @\ \frac{1}{4} \\ |0\rangle \text{ and } |1\rangle & @\ \frac{1}{4} \\ |1\rangle \text{ and } |0\rangle & @\ \frac{1}{4} \\ |1\rangle \text{ and } |1\rangle & @\ \frac{1}{4} \end{cases} \end{aligned}$$

where the probabilities at the end refer to the two individual qubits. To recap, in general the tensor product $|\psi\rangle \otimes |\phi\rangle$ of two qubits encodes the superposition of 4 basis states, namely $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.

Moreover, the following property can be proved easily.

Proposition 1.1: Distributive property of $\otimes$

Given three qubits $|\psi\rangle, |\phi\rangle$ and $|\chi\rangle$, it holds that

$$(|\psi\rangle + |\phi\rangle) \otimes |\chi\rangle = |\psi\rangle \otimes + |\phi\rangle \otimes |\chi\rangle$$

TODO

tensor product tra matrici? me va?

1.2.2 Controlled operations

Another familyh of very important gates in quantum computing is the *controlled operations*. The first controlled operation that we are going to discuss is the so called **Controlled NOT (CNOT)** gate, which is defined as follows:

a	b	$\text{CNOT}(a, b)$
0	0	0
0	1	1
1	0	1
1	1	0

In fact, the names comes from the fact that the first input a is called *control bit*, which if set to 1 will flip the *target bit* b — in fact, in its implementation what actually happens is that b's wire itself is flipped. Therefore, in general we will write that

$$\text{CNOT}(a, b) = (a, a \oplus b)$$

First, we observe that this function is clearly not invertible, since for instance if we know that the output is 0 we still need the input a to evaluate if b was 0 or 1. Hence, to solve this issue we usually pair the output of CNOT with a itself, so that we can actually invert the computation.

Moreover, so far we only dealt with transformation that only expected one qubit argument as input, but the CNOT gate would certainly need 2 inputs to perform any computation, so how do we provide two inputs to it? As we showed before, we konw that

$$\forall i, j \in \{0, 1\} \quad |i\rangle \otimes |j\rangle = |ij\rangle$$

which directly implies that the vector $|ij\rangle$ encapsulated two qubits at once without ambiguity. Hence, we can actually leverage the tensor product to provide the input to the CNOT matrix, such that the quantum CNOT will behave as follows

$$\text{CNOT}(|a\rangle \otimes |b\rangle) = |a\rangle \otimes |a \oplus b\rangle$$

Hence, the matrix that behaves as such is the following

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

which expects a 4×1 input vector, and outputs a 4×1 output vector as well.

Laslty, as for the CNOT operator, we can actually define controlled operators for both Y and Z, which are respectively called CY and CZ operators.

1.2.3 Quantum circuits

Now that we introduced a couple of quantum gates, we can show how computation is actually represented in quantum computing. For instance, consider the following picture:

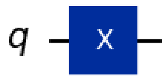

Figure 1.2: The NOT gate.

In this example, we have 1 single input qubit, namely q, and the box labeled with an X represents the NOT gate. We observe that, by convetion, all qubits in quantum circuits are assumed to be set to $|0\rangle$.

In the following example, instead, it is represented how the Hadamard gate looks like in quantum circuits.

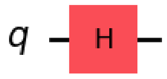

Figure 1.3: The Hadamard gate.

Moreover, if we consider two qubits as inputs q_0 and q_1, we can represent the CNOT operator as follows:

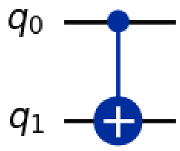

Figure 1.4: The CNOT gate.

We observe that q_1 then becomes the output of the CNOT operation, and q_0 remains unchanged. Lastly, the measurement operation is represented with the following picure:

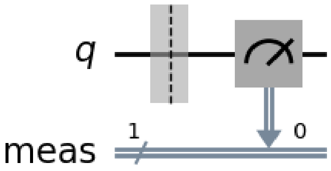

Figure 1.5: The measure operation.

In particular, in this cirtuit we see that:

- the vertical “double line” reprents *classical bits*
- the number 1 next to the label “meas” indicates the number of qubits that have been measured
- the number 0 is the index of the measured qubit

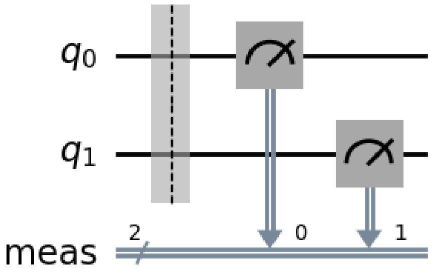

Figure 1.6: An exmaple of measurement of 2 qubits.

Lastly, another very important circuit is the following, which produces the so called **Greenberger-Horne-Zeilinger (GHZ)** state

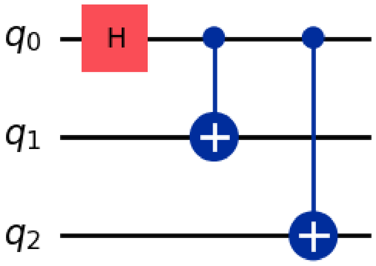

Figure 1.7: The GHZ quantum circuit.

which is represented as follows

$$|\mathrm{GHZ}\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

1.3 Peculiarities of quantum mechanics

1.3.1 Quantum entanglement

Consider the following quantum state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Can this state be rewritten as the tensor product of two distinct quantum states? We observe that for this to be possible we would require some complex values $\alpha_0, \alpha_1, \beta_0, \beta_1$ such that

$$\begin{cases} \alpha_0\beta_0 = \alpha_1\beta_1 = 0 \\ \alpha_0\beta_1 = \alpha_1\beta_0 = \frac{1}{\sqrt{2}} \end{cases}$$

but $\alpha_0\beta_0 = 0$ implies that at least one between α_0 and β_0 has to be 0, meaning that at least one between $\alpha_0\beta_1$ and $\alpha_1\beta_0$ has to be 0 as well. This proves that there is no such pair of quantum states which can describe $|\psi\rangle$ through the tensor product operation. In fact, we see that

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \begin{cases} |01\rangle & @\ \frac{1}{2} \\ |10\rangle & @\ \frac{1}{2} \end{cases}$$

Indeed, this particular state we chose is one of the so called **Bell states**.

Definition 1.3: Bell states

The following are the four **Bell states**:

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Whenever we have a state $|\psi\rangle$ that cannot be represented as the tensor product of two simpler quantum states, we say that the state is **entangled** — or that its possible outcomes are entangled. In particular, entangled states describe a very weird phenomenon first proposed as a thought experiment in a groundbreaking paper by **Einstein, Podolsky and Rosen (EPR)** [EPR35], the so called **EPR paradox**.

The thought experiment involves a pair of particles prepared in such *entangled state*. Einstein, Podolsky, and Rosen pointed out that, in this state, if the position of the first particle were measured, the result of measuring the position of the second particle *could be predicted*. If instead the momentum of the first particle were measured, then the result of measuring the momentum of the second particle could be predicted. They argued that no action taken on the first particle could instantaneously affect the other, since this would involve information being transmitted faster than light, which is impossible according to the theory of relativity. Einstein famously called this phenomenon "spooky action at a distance", and to the best of our knowledge the theory of quantum mechanics says that if we have two engangled states, and measure one of them — for instance, say that it collapses to $|0\rangle$ — the other state will **instantaneously** collapse to $|1\rangle$ (and viceversa). They are *perfectly anti-correlated*, even if the two states are phisically light-years away from each other.

To be precise, entanglement is *not* a way to tranfer information — collapsing happens instantaneously, which would violate the fact that nothing can travel faster than light, not even information. Instead, it is a way to share correlations nonlocally. In fact, it is a phenomenon that regards the *whole quantum system* considered: for instance, given three qubits q_0, q_1, q_2, such that q_1 and q_2 are entangled, we might want to only measure $q_0 \otimes q_1$, which in turn will make q_2 collapse into some quantum state that has to be mathematically computed in order to be predicted — this will be more clear when we will describe **quantum teleportation** in Section 1.3.3.

To finish off this section, we can actually generate entangled states, or **EPR pairs** for short, through quantum gates as such:

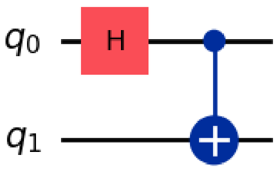

Figure 1.8: The quantum circuit for $|\Phi^+\rangle$.

In particular, we observe that the first Hadamard gate will transform $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and through the CNOT operation we obtain

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

1.3.2 No-cloning theorem

An operation that we take for granted in classical computation is the possibility to *copy* the value of a bit: if Alice has two bits $x, y \in \{0, 1\}$, and she wants to copy the value of x into y, she can do it without any issues. However, in quantum mechanics this is *not* possible, because it would quite literally violate the laws of physics — as far as we understand it.

In 1982 Wootters and Zurek [WZ82] proved the so called **no-cloning theorem**, which states that it is impossible to create an independent and identical copy of an arbitrary *unknown* quantum state.

Theorem 1.1: No-cloning theorem

There is no quantum transformation that copies an unknown quantum state.

Proof. by way of contradiction, suppose that there exists such a transformation CP that is able to copy an unknown quantum state — and in particular, we observe that such transformation would have to be linear. But clearly, in order to have a copy we need to actually *store* it somewhere, so we can assume that CP has to take two inputs, one being the state that we want to copy and the other one being the state that we want to replace with the copy of the first one. In other words, we are assuming that

$$\exists y \forall x \quad \mathrm{CP}(x \otimes y) = x \otimes x$$

Now, through some algebraic manipulation we get that

$$\begin{aligned}
&\exists y \forall x \quad \mathrm{CP}(x \otimes y) = x \times x \\
\equiv &\exists y \forall x, a \quad \mathrm{CP}((x + a) \otimes y) = (x + a) \otimes (x + a) \\
\equiv &\exists y \forall x, a \quad \mathrm{CP}(x \otimes y + a \otimes y) = (x + a) \otimes (x + a) && \text{(by distributivity of } \otimes\text{)} \\
\equiv &\exists y \forall x, a \quad \mathrm{CP}(x \otimes y) + \mathrm{CP}(a \otimes y) = (x + a) \otimes (x + a) && \text{(by linearity of CP)} \\
\equiv &\exists y \forall x, a \quad x \otimes x + a \otimes a = x \otimes x + x \otimes a + a \otimes x + a \otimes a && \text{(by definition of CP)} \\
\equiv &\exists y \forall x, a \quad \mathbf{0} = x \otimes a + a \times x
\end{aligned}$$

which should be true for every x and every a, however it does not hold for $x = |0\rangle$ and $a = |1\rangle$, thus raising a contradiction $\lightning$. □

The no-cloning theorem represents an inherent limitation of quantum computation, and has direct impacts on **quantum cryptography** and **quantum error correction**, but must importantly it directly impacts a phenomenon called **quantum teleportation**

1.3.3 Quantum teleportation

So far we saw that quantum states cannot be cloned, but can we at least *send* them? Suppose that Alice wants to send Bob $|\psi\rangle$, described by some α and β. Clearly, the only thing that Bob has to receive are indeed the probability amplitudes of $|\psi\rangle$, so even if Alice cannot clone her quantum state, nothing prevents her to build a quantum circuit which *destroys* her $|\psi\rangle$ but does allow Bob to receive α and β. This process is called **quantum teleportation**, and can be achieved through the following quantum circuit:

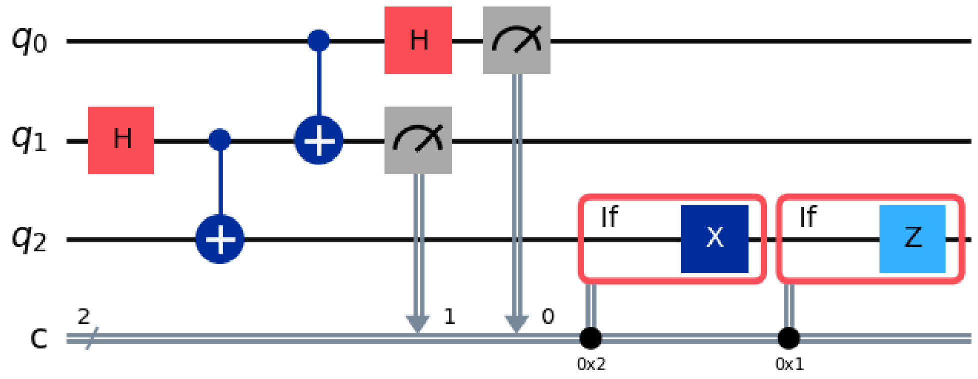

Figure 1.9: The Quantum Teleportation circuit.

There is quite a lot to unpack in this diagram. First, the quantum state that we want to teleport is q_0 in this diagram, and it will be teleported in q_2 at the end of the quantum computation.

In the first part of the circuit, we see that q_1 and q_2 are entangled (in an initial stage of the process, not performed by Alice nor Bob) in the Bell state $|\Phi^+\rangle$ thanks to the Hadamard and the CNOT gates — as we described in previous sections. In a real-world scenario, we will assume that q_1 and q_2 are given to Alice and Bob respectively (through some **quantum channel** such as optical fibers or free-space links in order to avoid *decoherence*), and quantum mechanics will guarantee that the teleportation will work even our two protagonists are thousands of kilometers away from each other.

After creating and entangling q_1 and q_2 (say for instance in a lab as preparation), we have the part of circuit that concerns Alice: in fact, she must apply a CNOT to her entangled qubit q_1, controlled by q_0, and then apply a Hadamard transformation to q_0. At this point, the circuit must apply a measurement to both q_0 and q_1 — and in particular, this operation will *destroy* the original state as previously anticipated.

Finally, it's Bob's turn: to obtain the original quantum state of q_0, the only thing he needs to do is first apply a CNOT to his entangled qubit q_2, controlled by q_1's outcome, followed by an application of a CZ, controlled by q_0's outcome instead — we observe that this part is indicated in the diagram through the `0x2` and `0x1` labels respectively. In fact, in the label `0xX` the number `X` represents the hexadecimal representation of the binary number obtained by joining the classical bits all together — for instance, in this circuit we have that 2 represents 10, meaning that only q_1 will be checked in the condition, and 1 represents 01, which means that only q_0 will be the control bit.

To show why the circuit actually works, we first need to discuss how computations with qubits and quantum gates is performed. In particular, we do not consider qubits *individually*, but instead we consider the whole **system** of qubits, i.e. $q_0 \otimes q_1 \otimes q_2$ simultaneously, and thus we will perform calculations as such. In fact, even if the drawing represents Alice's measurements of q_0 and q_1 independently, what happens in reality is that Alice is going to measure $q_0 \otimes q_1$ such that q_3 will collapse into its opposite.

Finally, we are ready to prove the correctness of the quantum teleportation circuit. First, we need to represent the initial quantum state, namely

$$\begin{aligned}
&q_0 \otimes q_1 \otimes q_2 \\
=&\left|\psi\right\rangle \otimes \left|\Phi^+\right\rangle \\
=&(\alpha\left|0\right\rangle_0 + \beta\left|1\right\rangle_0) \otimes \frac{1}{\sqrt{2}}(\left|00\right\rangle_{12} + \left|11\right\rangle_{12}) \\
=&\frac{1}{\sqrt{2}}[\alpha\left|0\right\rangle_0 \otimes (\left|00\right\rangle_{12} + \left|11\right\rangle_{12}) + \beta\left|1\right\rangle_0 \otimes (\left|00\right\rangle_{12} + \left|11\right\rangle_{12})]
\end{aligned}$$

where the notation $\left|00\right\rangle_{12}$ represents for example that we are considering q_1 and q_2's parts of states, respectively. From now on, we will omit the $\otimes$ symbol — as for the "normal" product. The next step is to apply the CNOT on q_0 and q_1, therefore the quantum state of the system becomes the following:

$$\frac{1}{\sqrt{2}}\left[\alpha\left|0\right\rangle_0 (\left|00\right\rangle_{12} + \left|11\right\rangle_{12}) + \beta\left|1\right\rangle_0 (\left|10\right\rangle_{12} + \left|01\right\rangle_{12})\right]$$

Next, we have to apply the Hadamard gate on q_0, which turns the quantum state into the following

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left[\alpha\frac{1}{\sqrt{2}}(\left|0\right\rangle_0 + \left|1\right\rangle_0)(\left|00\right\rangle_{12} + \left|11\right\rangle_{12}) + \beta\frac{1}{\sqrt{2}}(\left|0\right\rangle_0 - \left|1\right\rangle_0)(\left|10\right\rangle_{12} + \left|01\right\rangle_{12})\right] \\
=&\frac{1}{2}\left[\alpha(\left|000\right\rangle_{012} + \left|011\right\rangle_{012} + \left|100\right\rangle_{012} + \left|111\right\rangle_{012}) + \beta(\left|010\right\rangle_{012} + \left|001\right\rangle_{012} - \left|110\right\rangle_{012} - \left|101\right\rangle_{012})\right] \\
=&\frac{1}{2}\left[\left|00\right\rangle_{01}(\alpha\left|0\right\rangle_2 + \beta\left|1\right\rangle_2) + \left|01\right\rangle_{01}(\beta\left|0\right\rangle_2 + \alpha\left|1\right\rangle_2) + \left|10\right\rangle_{01}(\alpha\left|0\right\rangle_2 - \beta\left|1\right\rangle_2) + \left|11\right\rangle_{01}(\alpha\left|1\right\rangle_2 - \beta\left|0\right\rangle_2)\right] \\
=&\frac{1}{2}\left[\left|00\right\rangle_{01}\left|\psi\right\rangle_2 + \left|01\right\rangle_{01} X\left|\psi\right\rangle_2 + \left|10\right\rangle_{01} Z\left|\psi\right\rangle_2 + \left|11\right\rangle_{01} XZ\left|\psi\right\rangle_2\right]
\end{aligned}$$

Finally, Alice will perform the measurement on q_0 and q_1, and what will happen is that the *whole* quantum state of the quantum circuit will collapse as follows:

$$\begin{cases}
\left|00\right\rangle_{01} \otimes \left|\psi\right\rangle_2 & @\ \frac{1}{4} \\
\left|01\right\rangle_{01} \otimes X\left|\psi\right\rangle_2 & @\ \frac{1}{4} \\
\left|10\right\rangle_{01} \otimes Z\left|\psi\right\rangle_2 & @\ \frac{1}{4} \\
\left|11\right\rangle_{01} \otimes XZ\left|\psi\right\rangle_2 & @\ \frac{1}{4}
\end{cases}$$

Note that to perform the measurement operation on just q_0 and q_1 we would need some mathematical tools that are outside the scope of this course, therefore we will only show the probabilities of the outcomes as presented above. In fact, fom this table we can easily explain the last part of the quantum teleportation circuit, i.e. Bob's part, as shown below.

Alice's outcome	Bob's part	Bob's result
0 and 0	I	$\left\|\psi\right\rangle$
0 and 1	X	$XX\left\|\psi\right\rangle = \left\|\psi\right\rangle$
1 and 0	Z	$ZZ\left\|\psi\right\rangle = \left\|\psi\right\rangle$
1 and 1	XZ	$XZXZ\left\|\psi\right\rangle = \left\|\psi\right\rangle$

Lastly, note that even if the mathematical calculations don't highlight the fact that q_0 and q_1 are measured, these two bits are effectively *destroyed* as we already described. In fact, q_2 will be the only usable qubit after the whole process — for instance, nothing prevents us from applying more transformations on the state $|00\rangle_{01} \otimes |\psi\rangle_2$ *mathematically*, but in reality q_0 and q_1 are not usable anymore.

Bibliography

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Physical Review* 47.10 (May 1935), 777–780. ISSN: 0031-899X. DOI: 10.1103/physrev.47.777. URL: http://dx.doi.org/10.1103/PhysRev.47.777.

[WZ82] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (Oct. 1982), 802–803. ISSN: 1476-4687. DOI: 10.1038/299802a0. URL: http://dx.doi.org/10.1038/299802a0.