Università degli Studi di Milano Bicocca

Teoria della informazione e della computazione quantistica

Raccolta di appunti, dispense e libri

Anno accademico 2021/2022

Marco Gobbo

https://github.com/marcogobbo/tecnologie-quantistiche

October 10, 2021

Contents

Chapter 1

Introduction

1.1 Qubits

The **bit** is the fundamental concept of classical computation and information. Quantum computation and information are built upon an analogous concept: the **quantum bit**, or **qubit**. What is a qubit? Quantum mechanically, a qubit is any two-level system. For example, we can use the two different polarizations of a photon, the alignment of a nuclear spin in a uniform magnetic field, or the two states of an electron orbiting a single atom or molecule (ammonia-based quantum computer[i]). Just as a classical bit has a **state** - either 0 or 1 - a qubit also has a **state**. Two possible states for a qubit are the state $|0\rangle$ and $|1\rangle$ (we use *Dirac notation*[ii]). The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form *linear combinations* of states, often called *superpositions*:

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

The numbers α and β are complex numbers. See in another way, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are know as computational basis states and form an orthonormal basis for this vector space. We can examine a bit to determine whether it is in the state 0 or 1. For example, computers do this all-time when they retrieve the contents of their memory. Instead, quantum mechanics tells us that we can only acquire much more restricted information about the quantum state. When we measure a qubit, we get either 0 with probability α or 1 with probability β. Naturally, they must satisfy the following condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

Like in a QM system, the phase is irrelevant, it's a degree of freedom. For this reason, qubits could store infinite information. However, this conclusion turn out to be misleading, because of the behavior of a qubit when observed. Remind that the

---

[i]Ferguson, A., Cain, P., Williams, D., & Briggs, G. (2002). Ammonia-based quantum computer. Phys. Rev. A, 65, 034303.

[ii]Also known as bra-ket notation, it is a formalism introduced by Paul Dirac to describe one quantum state. The name derives from the fact that the scalar product of two states ϕ and ψ is denoted with a bracket $\langle\phi|\psi\rangle$ consisting of two parts: $\langle\phi|$ the *bra* and $|\psi\rangle$ the *ket*.

measurement of a qubit will give only either 0 or 1. Furthermore, measurement changes the state of a qubit, collapsing it from its superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the measurement result. From a single measurement one obtains only a single bit of information about the state of the qubit, thus resolving the apparent paradox. It turns out that only if infinitely many identically prepared qubits were measured would one be able to determine α and β for a qubit in the state $|\psi\rangle$.

1.1.1   Summary for general principles on QM

- **Postulate I**: What is a state? We use Dirac notation to represents a vector in an Hilbert-space (finite dimension) $|\psi\rangle \in \mathcal{H}$, where the states lives. The states is given by a vector also named as *ray* and it should have a unit norm (conservation of probability) $|||\psi\rangle|| = 1$. All phases are irrelevant $|\psi\rangle \approx e^{i\alpha}|\psi\rangle$ $\alpha \in \mathbb{R}$, if two states differs from a phase, they have the same physical effect.

If we have two states $|\psi_1\rangle$ and $|\psi_2\rangle$, and we consider their linear combination: $|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$, then $|\psi\rangle$ is also a state in $\mathcal{H}$. But we need to pay attention for $|\psi\rangle$, we need to normalize it for the conservation of probability.

Definition 1.1 (**Scalar product**). *We define **scalar product** the following quantity: $\langle\phi|\psi\rangle$ (**bra-ket** notation), where $\langle\phi|$ is the dual vector of $|\phi\rangle$.*

Qubit systems work in $\mathcal{H} = \mathbb{C}^2$. Where a vector $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ has $z_1, z_2 \in \mathbb{C}$. We can also say that $|0\rangle$ and $|1\rangle$ are an orthogonal bases:

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

where their scalar products are:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \qquad \langle 0|1\rangle = \langle 1|0\rangle = 0$$

So our general state it can be written as:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = z_1|0\rangle + z_2|1\rangle$$

The scalar product between $|\phi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ and $|\psi\rangle = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$ is defined as:

$$\langle\psi|\phi\rangle = w_1^* z_1 + w_2^* z_2$$

If we have $|\phi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ (ket), we transpose and conjugate $\langle\phi| = (z_1^*, z_2^*)$ (bra). Then we can rewrite the scalar product as:

$$\langle\psi|\phi\rangle = (w_1^*, w_2^*) \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = w_1^* z_1 + w_2^* z_2$$

Summing up, we can write a generic state as:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1|0\rangle + z_2|1\rangle$$

with these two constraints:

- **Conservation of probability**: $|z_1|^2 + |z_2|^2 = 1$

- **Phase invariance**: $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = e^{i\alpha} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \Rightarrow \begin{matrix} z_1 \approx e^{i\alpha} z_1 \\ z_2 \approx e^{i\alpha} z_2 \end{matrix}$

Obtaining

$$|\psi\rangle = z_1|0\rangle + z_2|1\rangle$$

Using the **conservation of probability**:

$$|\psi\rangle = \cos\frac{\theta}{2}e^{i\phi_1}|0\rangle + \sin\frac{\theta}{2}e^{i\phi_2}|1\rangle$$

Using the **phase invariance**, so long as ϕ_1 and ϕ_2 still arbitrary, we have a freedom by multplying for a phase $e^{i\alpha}$[iii]:

$$|\psi\rangle = \left(\cos\frac{\theta}{2}e^{i\phi_1}|0\rangle + \sin\frac{\theta}{2}e^{i\phi_2}|1\rangle \right)e^{i\alpha}$$

Redefining $\phi_1 = -\alpha$ and $\phi = \phi_2 + \alpha$ we get the general parametrization of a general qubit:

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

1.1.2 Bloch sphere

We can visualize the generic state of a qubit using the spherical coordinates and with the introduction of a unit vector $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, we get the **Bloch sphere** (note also as S^2 unit sphere).
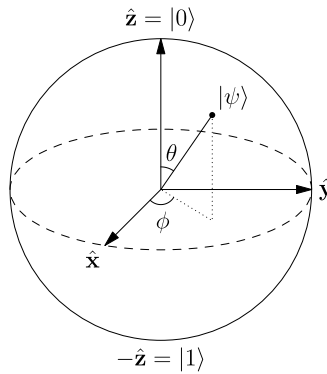

Figure 1.1: General rappresentation of a qubit state $|\psi\rangle$ on the Bloch sphere

Each state coincides with each point present on the surface of the sphere, there is a one-to-one correspondence between a point on the surface and a state $|\psi\rangle$. We must underline the fact that the scalar product which we define in $\mathbb{C}^2$ is different from the scalar product in S^2, because, in the last one, $|0\rangle$ and $|1\rangle$ are in the same direction but opposite verse, so their scalar product is equal to -1 while in $\mathbb{C}^2$ is equal to 0. The Bloch sphere is a useful technique to visualize the qubit states.

[iii]The global phase is physically irrelevant, while the relative phase is physically important for certain phenomena like interference.

- **Postulate II**: What can we measure? In QM we measure observables and they are described from a self-adjoint operator:

$$\hat{A} : \mathcal{H} \to \mathcal{H}$$

where $\hat{A}^\dagger = \hat{A}$, more specifically $\hat{A}^\dagger = (A^\intercal)^* \Rightarrow (A^\dagger)_{ij} = A_{ji}^*$

According to what we saw in the braket notation $(\langle\phi| = |\phi\rangle^\dagger)$, we will therefore have:

$$|\psi\rangle = B |\phi\rangle \Rightarrow \langle\psi| = \langle\phi| B^\dagger$$

Focusing on self-adjoint operators, we recall an important theorem of linear algebra:

Theorem 1.1 (Spectral Theorem). *Suppose $\hat{A}$ is a self-adjoint operator on a (real or complex) Hilbert space $\mathcal{H}$. Then there is an orthonormal basis of $\mathcal{H}$ consisting of eigenvectors of $\hat{A}$, which we denote as $|n\rangle$. Each eigenvalue a_n is real.*

$$\hat{A} |n\rangle = a_n |n\rangle \ \ where \ \ \langle n|m\rangle = \delta_{ij}$$

An important consequence to underline is that the number of orthonormal eigenvectors $|n\rangle$ is equal to the dimension of the Hilbert space that contains them, and being *linearly independent* and *orthonormal* (therefore orthogonal) they are a *basis* for the Hilbert space under consideration. Being a basis, we can expand any state $|\psi\rangle$ as a linear combination of eigenvectors $|n\rangle$:

$$|\psi\rangle = \sum_{n=1}^{N} \alpha_n |n\rangle$$

where $\alpha_n \in \mathbb{C}$, $N = \dim \mathcal{H}$.

Returning to our case of a two-level system, the Hilbert space we consider is $\mathbb{C}^2$ and we have taken the states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ as *canonical basis* (also know as *computational basis*). In this vector space, our operators are represented by a 2×2 matrices. In order to satisfy the self-adjoint condition, the matrix representation of a generic operator $\hat{A}$ must be expressed as:

$$\hat{A} = \begin{pmatrix} a + b & c - id \\ c + id & a - b \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$. As we have decomposed a generic state vector $|\psi\rangle$ through a linear combination of eigenvectors $|n\rangle$, we can decompose a generic operator $\hat{A}$ as:

$$\hat{A} = a\mathbb{I} + b\sigma_1 + c\sigma_2 + d\sigma_3$$

where $\mathbb{I}$ is the **identity** and $\sigma_1, \sigma_2, \sigma_3$ are the **Pauli matrices**:

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

They are used in the spin description as $\hat{\vec{S}} = \frac{\hbar}{2}\hat{\vec{\sigma}}$.

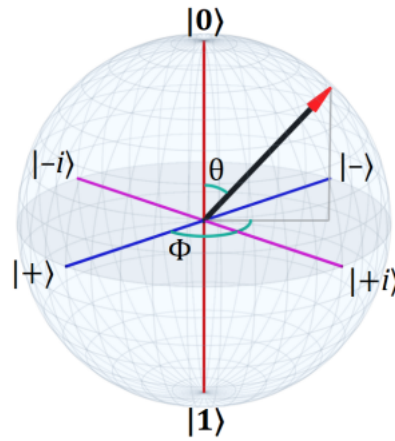Now let's look at the eigenvalues and eigenvectors of Pauli matrices:

Pauli matrices	Eigenvectors		Eigenvalues
$\hat{\sigma}_1$	$\lvert +\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},$	$\lvert -\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	{1,-1}
$\hat{\sigma}_2$	$\lvert i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix},$	$\lvert -i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	{1,-1}
$\hat{\sigma}_3$	$\lvert 0\rangle = \begin{pmatrix}1\\0\end{pmatrix},$	$\lvert 1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$	{1,-1}

We observe, for example, that

$$\lvert +\rangle = \frac{\lvert 0\rangle + \lvert 1\rangle}{\sqrt{2}} \qquad \lvert -\rangle = \frac{\lvert 0\rangle - \lvert 1\rangle}{\sqrt{2}}$$

We can see these new bases on the Bloch sphere.

If we define the spin along a generic direction $\vec{n} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$, then along $\vec{n}$ we will have:

$$\hat{\vec{\sigma}} \cdot \vec{n} = \cos\phi\sin\theta\sigma_1 + \sin\phi\sin\theta\sigma_2 + \cos\theta\sigma_3$$

- **Postulate III**:

  1. **Measurement**: Let's take the operator self-adjoint $\hat{A}$, with his base $\lvert n\rangle$ where we have $\hat{A}\lvert n\rangle = a_n\lvert n\rangle$, and $a_i \neq a_j \; \forall i \neq j$. We can expand $\lvert \psi\rangle$ on $\lvert n\rangle$ base, such that $\lvert \psi\rangle = \sum_n \alpha_n\lvert n\rangle$. By measuring the quantity A, we obtain the value a_n with probability equals to $\lvert \alpha_n\rvert^2$. (We already assumed that $\lvert \psi\rvert^2 = 1$).

  2. **Collapse of the wave function**: After the measure what happens to the ψ state? When we do a measure, instantly $\lvert \psi\rangle$ collapse to the state $\lvert n\rangle$ which gave us the a_n value: $\lvert \psi\rangle \rightarrow \lvert n\rangle$. If we do another measure on $\lvert \psi\rangle$, we get again $\lvert n\rangle$ with a probability of 1 (**Born's rule**).

Let's consider for a qubit $\lvert \psi\rangle$ (dim = 2) the most general state:

$$\lvert \psi\rangle = \cos\frac{\theta}{2}\lvert 0\rangle + \sin\frac{\theta}{2}e^{i\phi}\lvert 1\rangle$$

If we perform an experiment to measure a spin, in the z-basis ($\sigma_3 : \{|0\rangle, |1\rangle\}$) the probabilities will be:

$$P(|0\rangle) = \left|\cos^2\frac{\theta}{2}\right| \qquad P(|1\rangle) = \left|\sin^2\frac{\theta}{2}\right|$$

we must note that: $P(|0\rangle) + P(|1\rangle) = 1$

Instead, if we consider the x-basis ($\sigma_1 : \{|+\rangle, |-\rangle\}$) our $|\psi\rangle$ state will be:

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

the new probabilities will be:

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

$$P(|-\rangle) = \frac{1}{2}\left|\cos\frac{\theta}{2} - e^{i\phi}\sin\frac{\theta}{2}\right|^2$$

Let us now analyze the following situation, suppose we have a psi state written as a linear combination of $|+\rangle$ and $|-\rangle$. If during the measurement of the x-component of $|\psi\rangle$ we obtain $|+\rangle$, a subsequent measurement, always of the same component, will produce the same result with a probability of 100%. Now we know that we are in the $|+\rangle$ state, let's measure the component along x. By the Heisenberg uncertainty principle we will have:

$$P(|+\rangle) = \frac{1}{2} \qquad P(|-\rangle) = \frac{1}{2}$$

The same goes for all directions as:

$$[\hat{S}_i, \hat{S}_j] = i\hbar\varepsilon_{ijk}\hat{S}_k$$

Suppose we have **degeneration** on $|\psi\rangle$, this means that some eigenvalues are equal to each other, associated with different eigenstates:

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle + \alpha_4|4\rangle + \alpha_5|5\rangle\,\alpha_6|6\rangle$$

where we suppose the degeneracy on $a_1 = a_2$ and $a_4 = a_5 = a_6$.

$$|\psi\rangle = \underbrace{\alpha_1|1\rangle + \alpha_2|2\rangle}_{\hat{P}_{a_1}|\psi\rangle} + \underbrace{\alpha_3|3\rangle}_{\hat{P}_{a_3}|\psi\rangle} + \underbrace{\alpha_4|4\rangle + \alpha_5|5\rangle\,\alpha_6|6\rangle}_{\hat{P}_{a_4}|\psi\rangle}$$

To describe this situation we introduce **projectors** $\hat{P}_{ai}$ with their following properties:

1. $\hat{P}_a^\dagger = \hat{P}_a$

2. $\hat{P}_a^2 = \hat{P}_a$

3. $\sum_i \hat{P}_{a_i} = \mathbb{I}$

These are useful for treating Born rule, in the previous case we have 3 possible outcomes. And the probability to get these outcomes is:

$$P(a_n) = ||P_{a_n}|\psi\rangle||^2$$

After the measurement, our wave function will collapse to the normalized state:

$$|\psi\rangle \rightarrow \frac{P_{a_n} |\psi\rangle}{||P_{a_n} |\psi\rangle ||}$$

For example, if we look at the probability of getting $a_1 = a_2$, we'll get:

$$P(a_1) = ||\alpha_1 |1\rangle + \alpha_2 |2\rangle ||^2 = |\alpha_1|^2 + |\alpha_2|^2 \quad \text{Parseval Identity}$$

What happens to the state $|\psi\rangle$? It will collapse in the state (properly normalized):

$$|\psi\rangle = \frac{1}{\sqrt{|\alpha_1|^2 + |\alpha_2|^2}} \left(\alpha_1 |1\rangle + \alpha_2 |2\rangle \right)$$

Now I have an uncertainty about $|\psi\rangle$ for $|1\rangle$ or $|2\rangle$, but if I can realize an experiment that allows me to solve the degeneration, I will have a well-defined state (think about H atom).

- **Postulate IV**: The last postulate states that time evolution is described by the Schrödinger equation:

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

  where $\hat{H}$ is the hamiltonian operator and it is self-adjoint.

An important thing to note is the fact that the probability is conserved:

$$\langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|\psi(0)\rangle = 1$$

When we solve Schrödinger equation, we get, by introducing the so call **time operator** $\hat{U}(t)$:

$$|\psi(t)\rangle = \hat{U}(t) |\psi(0)\rangle$$

if $\hat{H}$ is time-indipendent:

$$\hat{U}(t) = e^{-\frac{i}{\hbar}\hat{H}t}$$

if $\hat{H} = \hat{H}(t)$, we have to distinguish the case of commutating and non-commutating hamiltonians at different times.
The fact that in time evolution, the probability is preserved, is due to the fact that $\hat{U}(t)$ is a unitary operator:

- $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger U = \mathbb{I}$

- $\left\langle \hat{U}\phi \Big| \hat{U}\psi \right\rangle = \left\langle \phi \Big| \hat{U}^\dagger\hat{U}\psi \right\rangle = \langle\phi|\mathbb{I}\psi\rangle = \langle\phi|\psi\rangle$
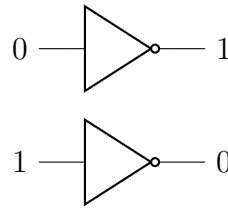
Since it is a unitary operator:

$$\hat{U}^\dagger\hat{U} = \left(e^{-\frac{i}{\hbar}\hat{H}t}\right)^\dagger e^{-\frac{i}{\hbar}\hat{H}t} = e^{\frac{i}{\hbar}\hat{H}t}e^{-\frac{i}{\hbar}\hat{H}t} = \mathbb{I}$$

1.2   Gates

Definition 1.2 (**Quantum Circuit**). *A **quantum circuit** is a model of quantum computing where there is an ordered sequence of **quantum gates** that are applied to the **qubits**.*

Definition 1.3 (**Quantum Gates**). *The quantum analogue of the classical logic gates are the **quantum gates**. The main difference from the classic case lies in the fact that we cannot directly implement all the ports classics like and, or, xor, . . .*

If in classical circuits, the use of logic gates is trivial, think of the `NOT` gate:

In a **qubit** we can do more things and these will be described from an hamiltonian:

$$|\psi\rangle \ -\boxed{\hat{U}}- \ \hat{U}\,|\psi\rangle$$

$\hat{U}$ can be any unitary operator like $\hat{U} = e^{-\frac{i}{\hbar}\hat{H}t}$ where $\hat{H}$ describes a given phenomena. Since **Pauli matrices** are unitary: $\sigma_i^\dagger = \sigma_i$, $\sigma_i^2 = \mathbb{I}$, if we want to study, for example, the spin of a particle inside a magnetic field, then: $\hat{H} = \vec{\sigma} \cdot \vec{B}$.