QCCS reduction semantics

Gabriele Tedeschi

20 giugno 2022

Indice

Capitolo 1

Introduction

Capitolo 2

Background

In this chapter, we review some fundamentals concepts in quantum computing and formal methods.

2.1 Quantum Computing

The laws on Quantum Mechanics, as we understand them, are elegantly formalized in a mathematical framework, built upon simple linear algebra. This framework is based on a few *postulates* that describe the behaviour of quantum systems. Since quantum computing is just the technique of manipulating quantum systems to perform some computation, it must follow the same rules. Before presenting each postulate, we will recall the necessary basic definition from linear algebra, formulated in the Dirac's "bra-ket" notation. For further reading, the standard textbook on the subject is [1].

2.1.1 State vector

A *column vector* in a complex vector space is written $|\psi\rangle$, and it's called a "ket",

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Its *conjugate transposed* is written $\langle\psi|$, and its called a "bra".

$$\langle\psi| = |\psi\rangle^\dagger = (\alpha_1^* \ldots \alpha_n^*)$$

A (finite-dimensional) *Hilbert space*, often denoted as $\mathcal{H}$, is a complex inner product space, i.e. a complex vector space equipped with a binary operator $\langle \_ | \_ \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ called *inner product*, dot product, or simply "braket".

$$\langle\psi|\phi\rangle = \begin{pmatrix} \alpha_1^* \ldots \alpha_n^* \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \sum_i \alpha_i^* \beta_i$$

The inner product satisfies the following properties:

Conjugate symmetry	$\langle\psi\|\phi\rangle = \langle\phi\|\psi\rangle^*$
Linearity	$\langle\psi\| (\alpha \|\phi\rangle + \beta \|\varphi\rangle) = \alpha \langle\psi\|\phi\rangle + \beta \langle\psi\|\varphi\rangle$
Positive definiteness	$\langle\psi\|\psi\rangle \geq 0$

Notice that $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle$ is the $\mathbf{0}$ vector. Besides, thanks to conjugate symmetry, we have $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle^*$, so $\langle\psi|\psi\rangle$ it's always a real, non-negative number, when $|\psi\rangle \neq \mathbf{0}$.

Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if

$$\langle\psi|\phi\rangle = 0$$

The *norm* of $|\psi\rangle$ is defined as:

$$\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$$

A *unit vector* is a vector $|\psi\rangle$ such that

$$\| |\psi\rangle \| = 1$$

.

A set of vectors $\{|\psi\rangle_i\}_i$ is an *orthonormal basis* of $\mathcal{H}$ if

- each vector $|\phi\rangle \in \mathcal{H}$ can be expressed as a *linear combination* of the vector in the basis, $|\phi\rangle = \sum_i \alpha_i |\psi\rangle_i$.
- All the vector in the basis are orthogonal
- All the vector in the basis are unit vector

We're now ready to present the postulates of Quantum Mechanics, in the form more convenient for quantum computing.

> **Postulate I**: The state of an isolated physical system is represented, at a fixed time t, by a unit vector $|\psi\rangle$, called the *state vector*, belonging to a Hilbert space $\mathcal{H}$, called the *state space*.

When describing the state oh a quantum system, we ignore the *global phase factor*[1], i.e.

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = -\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \lambda\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \text{ for each } \lambda \text{ such that } |\lambda| = 1$$

The simplest, prototypical example of a quantum physical system is a *qubit*: a qubit is a physical system with associated a two-dimensional Hilbert Space $\mathcal{H}^2$. Such systems comprehend an elector in the ground or excited state, a vertically or horizontally polarized photon, or a spin up or spin down particle.

Taken for example a photon, we could say that the photon is in state $|0\rangle$ when vertically polarized, and in state $|1\rangle$ when is horizontally polarized, where $|0\rangle$ and $|1\rangle$ are the two unit vector of the Hilbert space defined as

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

The vectors $\{|0\rangle, |1\rangle\}$ form an orthonormal basis of $\mathcal{H}^2$, called the *computational basis*. Since they form a basis, each vector $|\psi\rangle \in \mathcal{H}^2$ can be expressed as

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

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

[1] An equivalent formulation, in fact, says that a quantum system is described not by a vector but by a *ray*, a one-dimensional subspace of $\mathcal{H}$

So, the state of any qubit can mathematically be described as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, a linear combination of $|0\rangle$ and $|1\rangle$. From the physical point of view, this means that the qubit is in a *quantum superposition* of state $|0\rangle$ and *ko*, like a photon being diagonally-polarized, or an electron being at the same time in the excited and in the ground state.

Other important vectors in the $\mathcal{H}^2$ state space are $|+\rangle$ and $|-\rangle$,

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

that form the so called *hadamard basis* of $\mathcal{H}^2$.

2.1.2 Unitary Transformations

For each linear operator A acting on a Hilbert space $\mathcal{H}$, we denote as $A^\dagger$ the *adjoint* of A, i.e. the unique linear operator such that

$$\langle\psi|A\phi\rangle = \langle A^\dagger\psi|\phi\rangle$$

A linear operator A acting on a n-dimensional Hilbert space $\mathcal{H}^n$ can be represented as a $n \times n$ matrix, and its adjoint is calculated as

$$A^\dagger = (A^*)^T$$

the conjugate transpose of the matrix A.

If it holds that $A = A^\dagger$, we say that A is self-adjoint, or *Hermitian*.

A linear operator U is said to be *unitary* when $U^\dagger = U^{-1}$, which implies

$$UU^\dagger = U^\dagger U = I$$

Unitary matrices enjoy many useful properties, first of all that they have a spectral decomposition. An other defining characteristic is that they preserve the inner product, $\langle\psi|\phi\rangle = \langle U\psi|U\phi\rangle$

$$\langle U\psi|U\phi\rangle = \langle\psi|\,U^\dagger U\,|\psi\rangle = \langle\psi|\,I\,|\psi\rangle = \langle\psi|\phi\rangle$$

A corollary of this property is that applying a unitary operator to a unit vector gives a unit vector

$$\langle U\psi|U\psi\rangle = \langle\psi|\psi\rangle = 1$$

The following postulates make obvious why we are interested in unitary transformation.

> **Postulate II**: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_0 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_0 and t_1.
>
> $$|\psi'\rangle = U\,|\psi\rangle$$

According to what we said before, if a physical system starts in a unit state, it will always remain in a unit state.

In quantum computing, the the programmer can manipulate the state of a qubit, applying unitary transformations to it. Some of the most frequent transformation, implemented in every quantum computer, are:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

For example, the H operator, called the Hadamard operator, or Hadamard gate, is used to *create superposition*, as it transforms a vector from the computational basis to the Hadamard basis:

$$H|0\rangle = |+\rangle \qquad H|1\rangle = |-\rangle$$
$$H|+\rangle = |0\rangle \qquad H|-\rangle = |1\rangle$$

2.1.3 Measurement

2.1.4 Composite quantum systems

tensor product

2.1.5 Density matrix formalism

outer product

positive semidefinite operators

2.2 Process Calculi

Capitolo 3

chapter 3

Capitolo 4

chapter 4

Capitolo 5

Conclusions

Bibliography

[1] Michael A. Nielsen e Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.