QCCS reduction semantics

Gabriele Tedeschi

July 18, 2022

Contents

1 Introduction **2**

2 Background **3**
2.1 Quantum Computing 3
2.1.1 State space 3
2.1.2 Unitary Transformations 5
2.1.3 Measurement 6
2.1.4 Composite quantum systems 7
2.1.5 Density matrix formalism 9
2.2 Process Calculi 9

3 chapter 3 **10**

4 chapter 4 **11**

5 Conclusions **12**

Bibliography **13**

Chapter 1

Introduction

Chapter 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 nature and evolution of quantum systems. Since quantum computing is just the technique of manipulating quantum systems to perform some computation, it will necessarily follows the same postulates. 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 space

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 transpose* 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.

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

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 electron 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 , 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 $|1\rangle$, 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 $\mathcal{H}^2$. As we will see, $|+\rangle$ and $|-\rangle$ are both an equal superposition of $|0\rangle$ and $|1\rangle$. What differs in the two is the *relative phase*, i.e. the phase between the $|0\rangle$ and $|1\rangle$ component. The states $|0\rangle + |1\rangle$, $-|0\rangle - |1\rangle$, $i|0\rangle + i|1\rangle$ are all equal to $|+\rangle$ times a certain global phase, and are considered the same state. The states $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$, $|0\rangle + i|1\rangle$, instead, all differs for a relative phase factor, and have a different behaviors when applied to the same computation.

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 postulate makes 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:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

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:

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

2.1.3 Measurement

The second postulate describes only the evolution of isolated systems. Such system do not exchange energy nor information with the environment, and all their computations are always reversible (and are in fact formalized with invertible, unitary matrices). To extract classical information from the system, to *measure* the output of a quantum computation, it is needed an interaction between the quantum system and the environment. As we will see, this measurement operation is first of all non-invertible, as different state could produce the same outcome when measured, but is also fundamentally probabilistic: a generic state $|\psi\rangle$ could produce different measurement outcomes $m_1, m_2, \ldots$, each with a certain probability that depends on $|\psi\rangle$.

From a physical point of view, if a system is in a superposition of states, measuring it can cause the wavefunction to collapse to a single state, in a purely probabilistic way. This means that, even if we compute a state that contains the desired information, this information is often difficult to recover, because directly measuring it can destroy the information and produce a trivial outcome.

> **Postulate III**: Quantum measurements are described by a set $\{M_m\}$ of measurement operators, where the index m refers to the measurement outcomes that may occur in the experiment. The set of measurement operators must be *complete*, i.e.:
>
> $$\sum_m M_m^\dagger M_m = I$$
>
> If the state of the quantum system is $|\psi\rangle$ before the measurement, then the probability that result m occurs is
>
> $$p_m = \langle\psi| M_m^\dagger M_m |\psi\rangle$$
>
> and the state after the measurement will be
>
> $$\frac{1}{\sqrt{p_m}} M_m |\psi\rangle$$

The most common class of quantum measurements is composed of *projective measurements*. Such measurements are described by a set of *orthogonal projectors*, i.e. Hermitian operators such that

$$M_m M_{m'} = \begin{cases} \mathbf{0} & \text{if } m \neq m' \\ M_m & \text{if } m = m' \end{cases}$$

The simplest example of (projective) measurement is simply measuring a state in the computational basis, i.e. projecting it in its 0-1 component. The measurement in the computational basis is defined as

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

And it's effect of the state $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ is:

$$\frac{1}{\sqrt{p_0}} M_0 |\psi\rangle = \frac{1}{|\alpha|} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_0 |\psi\rangle = |\alpha^2|$$

$$\frac{1}{\sqrt{p_1}} M_1 |\psi\rangle = \frac{1}{|\beta|} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_1 |\psi\rangle = |\beta^2|$$

Notice that, when measuring the $|0\rangle$ state in the computational basis, the outcome will always be $|0\rangle$ with probability $|\alpha|^2 = 1$, in a completely deterministic behavior. When instead measuring the $|+\rangle$ or the $|-\rangle$ state, we get either $|0\rangle$ or $|1\rangle$, with equal probability $|\alpha|^2 = |\beta|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

2.1.4 Composite quantum systems

In the previous sections we characterized 1-qubit systems and how they evolve, describing a computation as a series of unitaries and measurements acting on a 2-dimensional Hilbert space. What said before applies easily to larger quantum systems and higher dimensional Hilbert spaces, once again thanks to an elegant mathematical formulation.

If we have two photons, each described by a (2-dimensional) Hilbert space $\mathcal{H}$, the most natural way to describe the system composed of both photons is as the *tensor product* of Hilbert spaces.

If $\mathcal{H}_n$ is a n-dimensional Hilbert space, and $\mathcal{H}_m$ is a m dimensional Hilbert space, their tensor product $\mathcal{H}_n \otimes \mathcal{H}_m$ is a nm Hilbert space. If $\{|\psi_1\rangle, \dots |\psi_n\rangle\}$ is a basis of $\mathcal{H}_n$, and $\{|\phi_1\rangle, \dots |\phi_m\rangle\}$ is a base of $\mathcal{H}_m$, then a basis of $\mathcal{H}_n \otimes \mathcal{H}_m$ is

$$\left\{ |\psi_i\rangle \otimes |\phi_j\rangle \mid i \in [1, \dots n], j \in [1, \dots m] \right\}$$

where $|\psi\rangle \otimes |\phi\rangle$ denotes the Kronecker product. We will often omit the tensor symbol, writing $|\psi\rangle |\phi\rangle$ or also $|\psi\phi\rangle$ instead of $|\psi\rangle \otimes |\phi\rangle$. We can now state the last postulate we need:

> **Postulate IV**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

If a single qubit is described by a 2-dimensional space $\mathcal{H}$, we will write $\mathcal{H}^{\otimes n}$ to intend the tensor product n copies of $\mathcal{H}$, of dimension 2^n. So, a compound system composed of two qubits has a state space $\mathcal{H}^{\otimes 2}$, its canonical basis is

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

and all its vector can be expressed as a linear combination:

$$|\psi\rangle \in \mathcal{H}^{\otimes 2} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

A quantum state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said *separable* when can be expressed as the product of two vectors, one in $\mathcal{H}_1$ and the other in $\mathcal{H}_2$. From the definition of the Kronecker product, all separable states of $\mathcal{H}^{\otimes 2}$ are of the form:

$$|\psi\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

One of the defining characteristics of quantum systems is that not all states in $\mathcal{H}^{\otimes 2}$ are separable. The existence of such states, called *entangled* states, implies that a composite system can not always be described as simply the juxtaposition of two smaller states. When a qubit q_1 is entangled with an other qubit q_2, its evolution depends not only on the transformations applied to q_1, but also on the transformations applied on q_2, that could be even light-years away. This surprising result does not allow faster then light communication, as we will see in the next section.

The classical example of an entangled state is the so called $|\Phi^+\rangle$ *Bell state*:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The fourth postulate tells us that the state space of a composite system is simply the tensor product of the state spaces of the smaller systems. The tensor product of Hilbert spaces is still an Hilbert space, the composition of unit vector is still a unit vector, and the composition of unitary transformation is still unitary. For example, the (Kronecker) composition of H and I matrices is defined as a block matrix:

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

And when applied to a two-qubit system, it applies H on the first qubit, and leav the second one unaltered:

$$(H \otimes I)\,|00\rangle = H\,|0\rangle \otimes I\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |+\rangle \otimes |0\rangle$$

One of the most common two-qubit unitary that is not just the composition of one-qubit transformations is the CNOT matrix:

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

This matrix applies a X transformation on the second qubit only if the first one is $|1\rangle$. This means that if the first bit is in a superposition of $|0\rangle$ and $|1\rangle$, after applying

this transformation the whole system will be in a superposition: or the two bits are left equal, or the second one has been flipped. As an example, we can show how the CNOT transformation is used to create entanglement.

$$\mathrm{CNOT}\,|00\rangle = |00\rangle \qquad \mathrm{CNOT}\,|10\rangle = |11\rangle$$
$$\mathrm{CNOT}\,|{+}0\rangle = \frac{1}{\sqrt{2}}\big(\mathrm{CNOT}\,|00\rangle + \mathrm{CNOT}\,|10\rangle\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) = |\Phi^+\rangle$$
$$\mathrm{CNOT}\,|{-}0\rangle = \frac{1}{\sqrt{2}}\big(\mathrm{CNOT}\,|00\rangle - \mathrm{CNOT}\,|10\rangle\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big) = |\Phi^-\rangle$$

2.1.5 Density matrix formalism

outer product
positive semidefinite operators

2.2 Process Calculi

Chapter 3

chapter 3

Chapter 4

chapter 4

Chapter 5

Conclusions

Bibliography

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