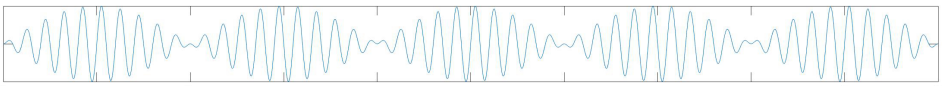
Étienne Bernard & Francesco Salvarani

Basic mathematics for quantum computing



Project IMEDiL
Inclusive Mathematics Education based on Digital Learning

Co-funded by the European Union

1. Introduction

Quantum mechanics represents a paradigm shift that overcame some important weaknesses of 19th century physics and led to the birth of modern physics. The basic ideas of quantum mechanics have also had many positive effects in other disciplines (such as computer science). In these notes, we develop the basic mathematical tools needed to describe some quantum problems, in particular quantum computation, which can be of educational value – inter alia – in understanding the fundamental principles of quantum mechanics.

We suppose that the reader has a basic knowledge of complex numbers and is familiar with some standard subjects of linear algebra, such as vector spaces on $\mathbb{C}$, Hermitian products and orthogonality, matrices in $\mathcal{M}_n(\mathbb{C})$, determinants, eigenvectors and eigenfunctions.

If not, the following text may be useful: Lang, Serge. Linear algebra. Third edition. Springer-Verlag, New York, 1987, ISBN 0-387-96412-6.

2. The postulates of Quantum Mechanics

There are several postulates of quantum mechanics, the first three of which are of direct interest to us:

First postulate: it is possible to associate, to any closed quantum system, a separable complex Hilbert space $\mathcal{H}$ such that

- Any pure state of the system can be represented by a vector $\Psi \in \mathcal{H}$ such that $\|\Psi\| = 1$;
- For any $a \in \mathbb{R}$, the vector Ψ and the vector $e^{ia}\Psi$ represent the same state;
- Any normalized vector $\Psi \in \mathcal{H}$ (i.e., a vector such that $\|\Psi\| = 1$) represents a pure and physically admissible state of the system.

Second postulate: to any observable A in classical mechanics corresponds a linear and self-adjoint operator $\hat{A}$ in $\mathcal{H}$.

Third postulate: in any measurement of the observable $\hat{A}$, the observed value is an eigenvalue of the spectrum of the operator $\hat{A}$, i.e. $\sigma(\hat{A})$.

In quantum computing, the corresponding physical systems are associated with finite-dimensional Hilbert spaces.

3. Qubits

Qubits are basic units of quantum information. They are dimensional objects. When it is important to underline the dimension, the

dimension is prefixed to the word "qubit". For example, a 1-qubit is a two-state system and can exist in any quantum superposition of two independent and distinguishable states and, according to the first postulate, the corresponding Hilbert space is $\mathbb{C}^2$.

3.1. **Definition of a qubit.** For some authors, the definition of a qubit includes its normalization (in a sense that will be specified later). Other authors do not impose a normalization condition to define the qubit, but treat qubits as equivalence classes and use the normalized qubit as the representative element of the class.

In these notes, the normalization condition in the definition of qubits will be included. For didactical purposes, these notes make the difference between (non-normalized) "states" and (normalized) "qubits". However, when a non-normalized quantum state will be manipulated, it will be meant that the considered quantity is equivalent to a qubit. The normalization procedure allows to deduce the corresponding normalized qubit.

Definition 1. *Consider two basic, independent quantum states* $|0\rangle$ *and* $|1\rangle$*. A* ***1-qubit*** *is a quantum state obtained as linear combination of the two basic quantum states* $|0\rangle$ *and* $|1\rangle$*,*

$$\alpha|0\rangle + \beta|1\rangle \quad \text{with } \alpha \in \mathbb{C} \quad \text{and} \quad \beta \in \mathbb{C},$$

under the normalization condition

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

Remark 1. *A 1-qubit is defined by two complex (ordered) numbers,* $\alpha = a_1 + ib_1$ *and* $\beta = a_2 + ib_2$ *(i.e., the vector* $(\alpha, \beta)^T \in \mathbb{C}^2$*) or, equivalently, by the vector* $(a_1, b_1, a_2, b_2)^T \in \mathbb{R}^4$*.*

Usually, qubits are represented by column vectors.

Two qubits can be merged together (by respecting a given order). The result is a quantum state, denoted as $|\psi\rangle$ and called 2-qubit when normalized, defined as follows.

Definition 2. *Consider four basic, independent quantum states* $|0.0\rangle$*,* $|0.1\rangle$*,* $|1.0\rangle$ *and* $|1.1\rangle$*. A* ***2-qubit*** *is a quantum state obtained by the superposition*

$$\alpha|0.0\rangle + \beta|0.1\rangle + \gamma|1.0\rangle + \delta|1.1\rangle \quad \text{with } \alpha, \beta, \gamma, \delta \in \mathbb{C}$$

under the normalization condition

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Hence, a 2-qubit can be defined as the vector $\alpha, \beta, \gamma, \delta)^T \in \mathbb{C}^4$ which is the Hilbert space associated to the closed system defined by the 2-qubits. Of course, these definitions can be generalized for defining d-qubits in higher dimension d.

Remark 2. *The notation $\langle \ | \ $ (which is the standard notation for vectors in quantum mechanics courses) reads "bra", whereas the notation $| \ \rangle$ reads "ket".*

3.2. **Operations.** The sum of two quantum states is done coefficient by coefficient (in the case of a sum, the normalization condition is not guaranteed). For example if

$$|\phi\rangle = (1-i)|0\rangle + 2i|1\rangle \quad \text{et} \quad |\psi\rangle = |0\rangle + (1-i)|1\rangle$$

then

$$|\phi\rangle + |\psi\rangle = (2-i)|0\rangle + (1+i)|1\rangle.$$

Note that the result is not a 1-qubit in general, but rather a quantum state.

Another example in the case of qubits in higher dimension is the following:

$$\frac{\sqrt{2}}{2}(|1.0\rangle - |0.1\rangle) + \frac{\sqrt{2}}{2}(|1.0\rangle + |0.1\rangle) \equiv \sqrt{2}|1.0\rangle.$$

Multiplication is the operation which allows to increase the dimension of qubits. For example, two 1-qubits can be multiplied, and the result is a 2-qubit. Note that the normalization is preserved by multiplication. The calculations are based on the basic rules for multiplying the basic quantum states:

$$|0\rangle \otimes |0\rangle = |0.0\rangle, \quad |0\rangle \otimes |1\rangle = |0.1\rangle,$$

$$|1\rangle \otimes |0\rangle = |1.0\rangle, \quad |1\rangle \otimes |1\rangle = |1.1\rangle.$$

For example, consider

$$|\phi\rangle = \frac{1}{\sqrt{14}}\left((1-3i)|0\rangle - 2i|1\rangle\right) \quad \text{et} \quad |\psi\rangle = \frac{1}{\sqrt{11}}\left(3|0\rangle - (1-i)|1\rangle\right).$$

By observing that

$$(1-3i)(1-i) = 1-i-3i+3i^2 = -2-4i \text{ and } 2i(1-i) = 2i-2i^2 = 2+2i,$$

we have

$$\begin{aligned}|\phi\rangle \otimes |\psi\rangle &= \frac{1}{\sqrt{154}}\Big[((1-3i)|0\rangle - 2i|1\rangle) \otimes (3|0\rangle - (1-i)|1\rangle)\Big] \\ &= \frac{1}{\sqrt{154}}\Big[3(1-3i)|0\rangle\otimes|0\rangle - (1-3i)(1-i)|0\rangle\otimes|1\rangle \\ &- 6i|1\rangle\otimes|0\rangle + 2i(1-i)|1\rangle\otimes|1\rangle\Big] \\ &= \frac{1}{\sqrt{154}}(3-9i)|0.0\rangle + \frac{1}{\sqrt{154}}(2+4i)|0.1\rangle \\ &- 6i|1.0\rangle + (2+2i)|1.1\rangle.\end{aligned}$$

Remark 3. *The same procedure can be applied for multiplying two non-normalized quantum states.*

The norm of a state is a real number. The norm is denoted by using the standard notation $\|\psi\|$. In particular, for a state described by

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

its norm is

$$\|\psi\| = \sqrt{|\alpha|^2 + |\beta|^2}.$$

On the other hand, the state

$$|\psi\rangle = \alpha|0.0\rangle + \beta|0.1\rangle + \gamma|1.0\rangle + \delta|1.1\rangle$$

has norm

$$\|\psi\| = \sqrt{|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2}.$$

The normalization of a state $|\psi\rangle$ is the qubit (of norm equal to one) given by

$$|\bar{\psi}\rangle = |\psi\rangle/\|\psi\|.$$

Example: Let $|\psi\rangle = (3+4i)|0\rangle + (2-i)|1\rangle$. Then

$$\|\psi\|^2 = |3+4i|^2 + |2-i|^2 = \left(3^2+4^2\right) + \left(2^2+(-1)^2\right) = 30.$$

Therefore $\|\psi\| = \sqrt{30}$.

Two quantum states are equivalent if there exists $z \in \mathbb{C}^*$ such that $|\phi\rangle = z|\psi\rangle$. Two equivalent quantum states cannot be distinguished by measurements.

Example: Consider

$$|0\rangle + |1\rangle \equiv \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

The 1-qubit in the r.h.s. is obtained by multiplying the quantum state in the l.h.s. by $k = 1/\sqrt{2}$.

Note that two equivalent states are not equal and therefore they must not be interchanged in the intermediate calculations. However, during the final measurement, one can replace a state by an equivalent state without changing the result, because the two elementary operations that define the equivalence do not change the probability calculation for the measurement.

3.3. **Product of qubits.** Let $|\phi\rangle$ be a m-qubit and $|\psi\rangle$ be a n-qubit. The tensor product of $|\phi\rangle$ by $|\psi\rangle$ is denoted $|\phi\rangle \otimes |\psi\rangle$ and is a $(m+n)$-qubit. The tensor product is computed with the same rules used for vectors. The result is a vector with $2^m \times 2^n = 2^{m+n}$ entries.

3.4. **Quantum entanglement.** In quantum mechanics, quantum entanglement is a phenomenon that occurs in a group of particles. The quantum state of a particle cannot be described independently of the state of the other particles of the group. The same phenomenon may occur in quantum computing. We specialize here the definition to the case of an entrangled 2-qubit, which is particularly important in the applications (see the Bell states described below).

Definition 3. *A 2-qubit $|\phi\rangle$ is said to be "not entangled" if there exist two 1-qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $|\phi\rangle$ can be written as tensor product, i.e.*

$$|\phi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,.$$

If there is no $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $|\phi\rangle$ can be written as tensor product, then the 2-qubit $|\phi\rangle$ is said to be "entangled'.

Example: Let

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Hence,

$$|\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}|0.0\rangle - \frac{1}{2}|0.1\rangle + \frac{1}{2}|1.0\rangle - \frac{1}{2}|1.1\rangle.$$

Hence, $|\phi\rangle$ defined as

$$|\phi\rangle = \frac{1}{2}|0.0\rangle - \frac{1}{2}|0.1\rangle + \frac{1}{2}|1.0\rangle - \frac{1}{2}|1.1\rangle$$

is not entrangled.

3.5. **The Bell states.** The Bell states are a set of 2-qubits that represent the most paradigmatical example of quantum entanglement. The four Bell states are listed below:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0.0\rangle + |1.1\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0.0\rangle - |1.1\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0.1\rangle + |1.0\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0.1\rangle - |1.0\rangle.$$

The following result hods.

Proposition 4. *The Bell states are entangled.*

4. Matrices

Matrices encode operations on qubits. In particular, according to the second postulate, the Hermitian matrices encode the observables. A quantum gate is described by a unitary matrix and allows one qubit to be transformed into another. Since these matrices are unitary, the transformation described by them is obviously invertible. It is an important difference with respect to classical computer ports, which may be not invertible. If the input vector is an n-qubit, then one needs to work with a unitary $n \times n$ matrices with complex entries . In such a situation, the output vector is a n-qubit.

Example: The Pauli matrices are a set of three 2×2 unitary complex matrices, whose explicit form is the following:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Remark 4. *Sometimes, the Pauli matrices are denoted with the indices x, y and z instead of 1, 2 and 3, i.e.*

$$\sigma_1 = \sigma_x \qquad \sigma_2 = \sigma_y \qquad \sigma_3 = \sigma_z.$$

Lemma 5. *The Pauli matrices, together with the identity matrix, form a basis for the real vector subspace of Hermitian matrices in $\mathcal{M}_2(\mathbb{C})$.*

Remark 5. *Let* $p = \begin{pmatrix} p_x \\ p_y \\ p_z \end{pmatrix} \in \mathbb{R}^3$. *The operator*

$$\hat{A}_p := p_x\sigma_x + p_y\sigma_y + p_z\sigma_z$$

is an observable which represents the polarization of the qubit along the vector p.

Each Pauli matrix has two eigenvalues: $\lambda_1 = +1$ and $\lambda_2 = -1$. Pairs of corresponding normalized eigenvectors are the following:

$$\psi_{x+} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad \psi_{x-} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix},$$
$$\psi_{y+} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad \psi_{y-} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix},$$
$$\psi_{z+} = \begin{pmatrix}1\\0\end{pmatrix}, \qquad \psi_{z-} = \begin{pmatrix}0\\1\end{pmatrix}.$$

Bibliography

For further study, please refer to the following texts, which are the sources of these notes.

- Hall, Brian. Quantum Theory for Mathematicians. Springer-Verlag, New York, 2013, ISBN 978-1-4614-7115-8
- Lang, Serge. Linear algebra. Third edition. Springer-Verlag, New York, 1987, ISBN 0-387-96412-6
- Rieffel, Eleanor & Polak, Wolfgang. Quantum computing. A gentle introduction, The MIT Press, Cambridge, Mass. 2011, ISBN 978-0-262-01506-6
- Bodin, Arnaud. Quantum. Un peu de mathématiques pour l'informatique quantique, Exo7, 2021
  `http://exo7.emath.fr/cours/livre-quantum.pdf`