Quantum Information Theory

Lecture Notes by Angela Capel and Paul Gondolf,[1]

Institute of Mathematics
University of Tübingen

April 19, 2023

[1] In case you find mistakes or typos, let us know: angela.capel@uni-tuebingen.de, paul.gondolf@uni-tuebingen.de

Contents

Chapter 1

Basic Notions in Quantum Information

1.1 Scope of the course and Bibliography

This course is primarily designed for students enrolled at the University of Tübingen in various programs such as the M.Sc. in Mathematical Physics and the M.Sc. in Advanced Quantum Physics, although students from other degrees like the B.Sc. in Physics, B.Sc. in Mathematics, and related topics, are welcome to attend it as well. In general, it is also accessible to individuals with foundational knowledge in mathematical analysis, linear algebra, probability theory, and an eagerness to explore the captivating realm of quantum information theory.

1.1.1 Bibliography

A wealth of literature exists on the topics we will explore in this course, including Quantum Information Theory, Quantum Computing, Fault Tolerance, Error Correction, and more. To assist students in their studies, we have compiled a concise list of the primary texts frequently utilized in similar courses within the community. Additionally, we offer our Lecture Notes as a valuable reference tool that summarizes course content and provides supplementary material and references in certain areas. It is important to note that our Lecture Notes are not meant to substitute any of the other texts authored by leading quantum information experts. We strongly encourage students to consult these works to augment their understanding of the subject.

The short selection of manuscripts has been done accordingly to the contents intended for this course. The lectures, and therefore these notes, have been prepared consulting these texts, as well as some others, and they are properly referenced in this respect. The main references in which our notes are based are the following:

1. Lectures Notes
2. Nielsen-Chuang, “Quantum Computation and Quantum Information” [2]
3. de Wolf, “Quantum Computing: Lecture Notes”, [8]
4. Preskill, “Quantum Computation. Lecture Notes”, [4]

Some other books/notes used for the construction of these notes will be properly referenced in the main text.

1.2 What is Quantum Information?

The scientific field of Quantum Information has a lot of different facets and encompasses the fields of Mathematics, Physics and Computer Science. Its main questions concern the control of quantum systems. I.e. *can we construct and manipulate complex quantum systems? And if so, what are the scientific and technological applications?* It is important to remark that the field of Quantum Information Science does not study the frontier of short (subnuclear) distances or long (cosmological) distances, but rather the frontier of highly complex quantum systems, what is usually known as *the entanglement frontier.*

Compared to the classical world that we know, as it is the world we experience every day, the quantum world exhibits behaviours that are counter-intuitive to our classical understanding of the world. These additional properties, which will be discussed in detail throughout the course, provide quantum systems with, in a sense, more complex and richer behaviour, meaning that we can expect to simulate a classical system using a quantum system, and it is generally believed that this is not possible the other way around (although it still remains an unproven conjecture in full generality). However, quantum systems present the phenomenon of *decoherence*, as opposed to classical systems, and this effect tends to destroy information very fast and, thus, quantum systems end up losing their special properties after some time and behaving like classical ones. It is a major problem to determine how hard solving the problem arising from decoherence is and whether we will be able to overcome it with the current techniques of science. Nevertheless, the special properties of quantum systems torched a large research effort whose main goal is to control the quantum behaviour of scalable quantum systems and achieve the “quantum advantage”, which will allow us to prepare and control complex quantum systems that behave in ways that cannot be predicted using digital computers. For that, we will need to find what quantum tasks are feasible and which quantum problems are hard to simulate classically.

1.2.1 Example: Shor’s factoring algorithm

To give an example of the theoretically expected improvement in behaviour of a quantum computer with respect to a classical one, let us present some basic calculations on the required time to factorize a certain number with both devices. For that, we make use of one of the first breakthroughs in the first steps of the field of Quantum Computing in the past century, namely the algorithm devised by Shor to factor numbers in their prime components. We will discuss such an algorithm in detail in a future chapter of the current notes (see [5] as well as the references [8, 6]).

Assume that we want to factor a number into its two prime factors $n = p_1 \cdot p_2$. Some theoretical computations show that we have the following comparison of computational time using Shor’s algorithm on a quantum computer and a classical algorithm on a classical computer:

Numbers	Classical computer	Quantum computer
193 digits	30 CPU years	0.1 seconds
500 digits	10^{12} CPU years	2 seconds

Moreover, as a hint of the meaning of the previous table in an impactful case, the energy consumption to crack RSA-encryption would demand 10^6 terawatt hours for the classical and 10 megawatt hours for a quantum computer.[1]

[1] This estimate stems from about 10 years ago.

1.2.2 Emergence of Quantum Information Science

There were several coetaneous facts that could be considered as the seed for the creation of the new field of Quantum Information Science. Some of the most remarkable facts which gave rise to this field are:

- A genuine concern regarding the true value of Moore's law in the coming years. This concern was based on the physical limit of computer chips, i.e. the space per bit cannot be shrunk indefinitely but is limited by the physical properties of the chip material (diameter of atoms, etc.).
- At a similar time, it was the first moment in history in which researchers in labs managed to control ”single quantum systems”, isolating them from systems with many quantum systems.
- Moreover, there was also an increase in the recognition of the computational power generated by quantum mechanics, which might allow for the design of computational devices based on the laws of such a field.
- Finally, another motivating aspect was the relevance of certain implications of quantum mechanics in practical aspects for society, such as to the security of public key cryptography.

1.2.3 Quantum Information vs. Classical Information

To conclude this short introduction to Quantum Information Theory, let us briefly mention the main differences with respect to the realm of Classical Information Theory. The three key properties of a quantum system compared to a classical system are the following ones:

- **(True) randomness.** Note that, even though we sometimes discuss some processes in classical mechanics as random ones, they are frequently just ”pseudo-random”, in the sense that their outcome might be predetermined, even if we do not know it in advance (and that is why we take it to be random). However, clicks in a Geiger counter, for instance, are intrinsically random, not pseudo-random, as, at every instant of time, there is always a certain probability of having more clicks in the next second or not having them, but the outcome is not predetermined in any way.
- **Uncertainty.** If we consider two operators A and B which do not commute, this means that measuring A influences the outcome of a subsequent measurement of B and vice versa.
- **Entanglement.** This property can be summarized as “the whole is more definite than the parts”. This means that even knowing a joint system AB (pure), the (mixed) state of A may be highly uncertain.

All these terms will be further defined and formalized as we proceed with the course.

1.2.4 Notation

In the next sections, we are going to provide a brief introduction to quantum mechanics and its formalism, from a mathematical perspective. The concepts that we will introduce below are essential for the postulates that we will present subsequently.

Beforehand, we need to introduce some notation. From now on, we will be working with n-dimensional (complex) Hilbert spaces $\mathcal{H}$, which can be identified with $\mathbb{C}^n$. If the dimension is irrelevant or clear from the context we will just write $\mathcal{H}$.

Notation. We further introduce the following (*bra-ket*) notation originally used by Paul Dirac (1904 - 1984). He set

$$\begin{aligned} |\psi\rangle &\in \mathbb{C}^n \qquad \text{to be a vector,} \\ \langle\psi| &\in (\mathbb{C}^n)^* \qquad \text{to be a dual vector.} \end{aligned} \tag{1.2.1}$$

This notation originated from the notation for the inner product on $\mathcal{H}$:

$$\langle\psi|\psi\rangle \in \mathbb{R}\,. \tag{1.2.2}$$

In this notation one can write the rank one operators onto the space spanned by $|\psi\rangle$ as a ket-bra

$$|\psi\rangle\langle\psi| : \mathbb{C}^n \to \mathbb{C}^n \tag{1.2.3}$$

allowing for the convenient use of these objects, for every $|\xi\rangle \in \mathbb{C}^n$,

$$|\psi\rangle\langle\psi|\xi\rangle = \langle\psi|\xi\rangle\,|\psi\rangle \in \mathbb{C}^n\,. \tag{1.2.4}$$

The content of the following subsections has been inspired by some basic texts of quantum information theory, such as the courses [3], [8] and [6], as well as the books [7], although one of the most fundamental texts in this field is [2]. We refer the reader to any of those texts for further knowledge on the topic.

1.3 Qubits and basic operations

Arguably, the most essential concept for quantum information theory is the one of a qubit. A *qubit* is the simplest quantum mechanical system and plays the same role in quantum information theory as the *bit* in classical information theory, which can be 0 or 1. Hence, it is the basic unit of information and extends the concept of a classical bit, which is just 0 or 1 to a *superposition* of those two. Formally, it is the system described by a two-dimensional Hilbert space. We will denote the canonical basis of this vector space $\mathbb{C}^2$ as $\{|0\rangle\,, |1\rangle\}$, i.e.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.3.1}$$

This basis is usually called the *computational basis*. Then, while a classical bit can be in the state 0 or in the state 1, an arbitrary state for a qubit is a vector

$$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle \in \mathbb{C}^2 \tag{1.3.2}$$

with $a_0, a_1 \in \mathbb{C}$ and $|a_0|^2 + |a_1|^2 = 1$. If $a_0 \neq 0, a_1 \neq 0$, we say that the state is in superposition of the situations $|0\rangle$ and $|1\rangle$. Notice that this fact leads to the essential difference between the possible states of a bit, which are just two, 0 or 1, and the possible states of a qubit, which, in principle, are infinite. This new situation allows us to perform new protocols for quantum information processing. Indeed, this principle constitutes the basis of the theoretical quantum computer, for which we can briefly mention the main idea behind it in a nutshell:

- If we consider one bit, we can perform 1 operation at a time, whereas we can perform 2 operations simultaneously with one qubit. This is due to the superposition phenomenon mentioned above, since now an arbitrary state is of the form

  $$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle \in \mathbb{C}^2\,,$$

  where one can see two basic bits (thus, operations) being performed at the same time.

- If we now have two bits, we can perform 2 operations at a time, while, if we consider two qubits, 4 operations can be performed at the same time (we will see that when we consider a superposition of the four elements of the Bell basis).
- In general, with n qubits, one can perform n operations simultaneously (one per each bit), whereas with n qubits one can perform 2^n operations at the same time.

Hence, theoretically, a quantum computer should be able give an exponential improvement to the amount of operations performed in parallel compared to a classical computer (i.e. an exponential speed-up).

Let us go back now to the definition and basic properties of qubits. It is important to remark that, even though a given qubit can be in any superposition state $a_0 |0\rangle + a_1 |1\rangle$, if we *measure* the state of such a qubit, we will obtain either the value $|0\rangle$ or $|1\rangle$ for the state of the qubit (these states can be seen as classical ones), with certain probabilities. Hence, we cannot "observe" the superposition phenomenon, although we are able to use it, as we will see below.

In the following, another basis will be also rather important and we want to introduce it here. It is given as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.3.3}$$

To extract classical information from a quantum system one performs a measurement. Performing such a measurement on such an arbitrary state the systems turns out to be in the state $|0\rangle$ with probability $|a_0|^2$ and in the state $|1\rangle$ with $|a_1|^2$.

A single qubit lives in $\mathbb{C}^2$. However, one can consider systems of more qubit to have richer spaces. For example, if we consider 2 qubits, the 2-qubit system that we get has four elements in a possible basis:

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\},$$

where, in each case, the qubit in the left part denotes the first qubit (and associated to the first system), and the right one denotes the second qubit. If one considers $|0\rangle \otimes |1\rangle$, for instance, this element can be also expressed by $|0\rangle |1\rangle$ or $|01\rangle$, and the structure of tensor product implies that in $\mathbb{C}^4$ can be written as:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

More generally, as mentioned previously, if one considers a system of n qubits, a basis of such system has 2^n elements (it is equivalent to saying that, with n qubits, one can perform 2^n operations simultaneously). In particular, one can always consider for such elements of the basis the elements $|a_1\rangle \otimes |a_2\rangle \otimes \ldots \otimes |a_n\rangle$, with $a_i \in \{0, 1\}$ for all $i = 1, \ldots, n$. Since there are 2^n elements in this basis, we can change this previous notation to $|0\rangle, |1\rangle, \ldots |2^{n-1}\rangle$, to simplify it.

Therefore, a quantum state on n qubits, because of superposition, is given by

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} |2^n - 1\rangle, \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Moreover, as in the case of a single qubit, if one measures this in the computational basis, one just gets a "classical" n-bit state, $|i\rangle$, with probability $|\alpha_i|^2$.

In a more general setting, consider a physical system that can be in N different, mutually exclusive classical states (in the case of the qubit, $N = 2$, and for n qubits, $N = 2^n$). A *mixed quantum state* $|\varphi\rangle$ is a superposition of *pure quantum state* in the following form:

$$|\varphi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \ldots + \alpha_N |N\rangle.$$

The elements α_i in the previous expression are complex numbers that are called *amplitudes*, and, in this expression, it is easy to read the superposition phenomenon as the possibility of a quantum system to be in N classical states states at the same time (or perform N operations simultaneously, as mentioned above).

1.3.1 Measurement

In general, given a quantum state, we can consider two different scenarios: Either we measure it, or we let it evolve under a unitary without measuring it. In this subsection, we explain the first case.

Let us recall some basic notions about Hilbert spaces and their scalar products. Let $\mathcal{H}$ be a Hilbert space (in general, we will just consider finite-dimensional spaces) and let $T : \mathcal{H} \to \mathcal{H}$ be a linear operator on it. Since $\mathcal{H}$ is a Hilbert space, in particular it is a normed space with an associated norm $\|\cdot\|_{\mathcal{H}}$ induced by a scalar product $\langle \cdot \mid \cdot \rangle$.

We say that T is a bounded operator if

$$\|T\|_{\mathcal{H}\to\mathcal{H}} := \sup_{x\in\mathcal{H}} \frac{\|T(x)\|_{\mathcal{H}}}{\|x\|_{\mathcal{H}}} < \infty,$$

and denote by $\mathcal{B}(\mathcal{H})$ the space of bounded linear operators on $\mathcal{H}$. Moreover, if $T : \mathcal{H} \to \mathcal{H}$, we can define its dual operator, and denote it by T^*, as the operator that satisfies

$$\langle y \mid T(x)\rangle = \langle T^*(y) \mid x\rangle \qquad \text{for every } x, y \in \mathcal{H}.$$

Now we are in position to formally define a measurement in the following form:

Definition. 1.3.1 (Measurement)
Let $\{M_n\}_n \subset \mathcal{B}(\mathcal{H})$ be a collection of operators verifying

$$\sum_n M_n^* M_n = \mathbb{1} \tag{1.3.4}$$

where $\mathbb{1}$ denotes the identity operator (we drop the subindex with the dimension when there is no possible confusion) and M_n^* denotes the dual of the operator M_n. This collection of operators is called **quantum measurements** when the following holds: Given a state of a quantum system $|\varphi\rangle$ before performing this operation to measure it, the probability that result $|n\rangle$ occurs is given by

$$p(n) = \langle \varphi \mid M_n^* M_n \varphi\rangle \tag{1.3.5}$$

and the state of the system after this operation is given by

$$\frac{M_n |\varphi\rangle}{\sqrt{p(n)}}.$$

Consider again the state

$$|\varphi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \ldots + \alpha_N |N\rangle.$$

and assume that we measure it. As we have already mentioned, we will obtain the classical state $|i\rangle$, with probability $|\alpha_i|^2$, thus we cannot "see" the superposition itself. Among some other things, this means that the probability to get specifically the state $|i\rangle$ when we measure, and not another one, is $|\alpha_i|^2$. Hence, since the quantum state induces a probability distribution on the classical states, this implies

$$\sum_{i=1}^{N} |\alpha_i|^2 = 1.$$

Notice that when we measure $|\varphi\rangle$ and get a classical state, $|\varphi\rangle$ disappears, and all that is left is the classical state itself. We say then that $|\varphi\rangle$ has *collapsed* to the classical state that we got, and the information encoded in the amplitudes α_i is now gone.

In general, we will measure in the computational basis. However, there are several ways to perform these measurements, that we will present throughout this section. Let us begin with the easiest one, the measurement of a qubit in its computational basis. It is defined by the measurement operators:

$$M_0 = |0\rangle\langle 0| \qquad \text{and} \qquad M_1 = |1\rangle\langle 1|.$$

Notice that both operators are *selfadjoint*, i.e., they coincide with their dual operators (actually, they are projections), and they verify $M_i^* M_i = M_i^2 = M_i$, for $i = 1, 2$, where M_i^* denotes the dual of the operator M_i, and $M_0 + M_1 = \mathbb{1}$. Also, when we measure

$$|\varphi\rangle = \alpha_0 \, |0\rangle + \alpha_1 \, |1\rangle,$$

the probability to obtain the outcome $|i\rangle$ is $|\alpha_i|^2$, and the state after measurement in that case is $\frac{\alpha_i}{|\alpha_i|} \, |i\rangle$. Actually, we can see that this state is equivalent to $|i\rangle$ (since it is just a rotation of the latter).

Indeed, consider $|\varphi\rangle$ and $e^{i\theta} \, |\varphi\rangle$ (which is a more general expression for the element mentioned above) and assume that we measure both states with a measurement $\{M_n\}_n$. Then, the probability of getting outcome n for the second element is

$$\left\langle \varphi e^{-i\theta} | M_n^* M_n | e^{i\theta} \varphi \right\rangle = \langle \varphi | M_n^* M_n | \varphi \rangle,$$

the same that for the first element. Hence, both states are operationally identical.

1.3.2 Projective Measurements

In this subsubsection, we are going to introduce *projective measurements*, which play an special role in Postulate III of quantum mechanics (as we will see in the following section). They can be defined in the following form.

Definition. 1.3.2 (Projective measurement)
Consider a collection $\{M_n\}_n \subset \mathcal{B}(\mathcal{H})$ of measurements, as described in Definition 1.3.1. Assume that they have the additional property that the M_n are orthogonal projections, i.e., they are self-adjoint and verify

$$M_n M_m = \delta_{mn} M_n,$$

where $\delta_{mn} = 1$ iff $m = n$ and 0 otherwise. These measurements are called **projective measurements**.

It is clear that each one of these operators M_n projects on a subspace $\mathcal{H}_n \subset \mathcal{H}$ of the global Hilbert space. Hence, an *observable* M can be defined as the Hermitian operator

$$M = \sum_n \lambda_n M_n,$$

where the term in the right hand-side is, in fact, the spectral decomposition of M. Moreover, the possible outcomes of the measurement correspond to the eigenvalues λ_n of the observable, and when we measure the state $|\varphi\rangle$, the probability of getting state $|n\rangle$ is:

$$p(n) = \langle\varphi|M_n|\varphi\rangle.$$

With this notation, the average value of the measurement, with respect to the state $|\varphi\rangle$, is

$$\sum_n np(n) = \sum_n n \langle\varphi|M_n|\varphi\rangle = \langle\varphi|M|\varphi\rangle.$$

1.3.3 POVM Measurements

In many situations, we will not be as interested in the post measurement state of our particle itself as in the probabilities of the different possible measurement outcomes. In this case, we can reduce to the formalism of the so called *Positive Operator Valued Measurements (POVM's)*.

Let us recall that an operator $T \in \mathcal{B}(\mathcal{H})$ is said to be *positive* (shortened form of *positive semidefinite*) if

$$\langle x, T(x)\rangle \geq 0 \qquad \forall x \in \mathcal{H}.$$

As we will see below, the operators mentioned in the definition of POVM are clearly positive, since

$$\langle x, E_n(x)\rangle = \langle M_n(x), M_n(x)\rangle = \|M_n(x)\| \geq 0 \qquad \forall x \in \mathcal{H}.$$

Definition. 1.3.3 (Positive operator valued measure)
Consider a measurement $\{M_n\}_n \in \mathcal{B}(\mathcal{H})$ as in the Definition 1.3.1. Then, we can define the *positive* operators

$$E_n = M_n^* M_n.$$

This family of operators $\{E_n\}_n$ is called a **POVM**.

The operators presented in the definition of POVM clearly satisfy

$$\sum_n E_n = \mathbb{1}$$

and their probability of obtaining outcome m is

$$p(m) = \langle\varphi|E_m|\varphi\rangle.$$

Conversely, if we have a collection of positive operators $\{E_n\}_n$ verifying $\sum_n E_n = \mathbb{1}$, we can define a measurement $\{M_n\}_n$ from them just by considering $M_n = \sqrt{E_n}$.

1.3.4 Unitary Evolution

As opposed to the previous subsection, now we let our quantum state evolve without measuring it. Assume we have a system of the form

$$|\varphi\rangle = \alpha_1 |1\rangle + \ldots + \alpha_N |N\rangle \tag{1.3.6}$$

and want to transform this to the system

$$|\psi\rangle = \beta_1 |1\rangle + \ldots + \beta_N |N\rangle . \tag{1.3.7}$$

Quantum mechanics only allows linear operations to be applied to quantum states. This means that, after a change of notation (identifying $|\varphi\rangle$ with an n-dimensional vector), applying an operation that changes $|\varphi\rangle$ to $|\psi\rangle$ corresponds just to a multiplication by an $N \times N$ complex-valued matrix. With the previous expressions for $|\varphi\rangle$ and $|\psi\rangle$, one has

$$U \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_N \end{pmatrix} \tag{1.3.8}$$

and adding the condition that

$$\sum_{i=1}^{N} |\beta_i|^2 = 1, \tag{1.3.9}$$

we immediately get that U has to be a unitary. This means

$$UU^* = U^*U = \mathbb{1} \tag{1.3.10}$$

Since it is unitary, then, in particular, $U^{-1} = U^*$, and this inverse always exists, what can be translated in the quantum setting to the fact that every non-measuring operation on a quantum state must be reversible (in contrast with measurements, which were clearly non-reversible).

We present now a prominent example of unitaries, the *Pauli matrices.*

Example.

$$\begin{aligned} \sigma_0 = \mathbb{1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \sigma_x = X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y = Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \sigma_z = Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{1.3.11}$$

From a quantum computational point of view we can think of unitary matrices as quantum logical gates. We will deepen in this connection in the first section of the following chapter.

1.3.5 Density operators

In this subsection, we introduce the density operators formalism that will be necessary to present the Postulates of the Quantum Mechanics in the Schrödinger picture. Before moving to the definition of density operators, let us start by recalling some basic concepts. We start by recalling the notion of trace of an operator.

Definition. 1.3.4 (Trace)
Let $T : \mathcal{H} \to \mathcal{H}$ a linear map represented by a matrix M in a certain basis. We then define

$$\text{Tr}[T] = \text{Tr}[M] = \sum_i M_{ii} \in \mathbb{C} \tag{1.3.12}$$

as the sum of the diagonal elements of the matrix M. The trace of T is well defined as it is cyclic and linear. This means it it is invariant under basis change.

It is easy to see that the trace is linear and cyclic, i.e., for A and B matrices,

$$\text{Tr}(AB) = \text{Tr}(BA).$$

From this last property, one also gets unitary invariance: For every unitary operator U,

$$\text{Tr}(UAU^*) = \text{Tr}(U^*UA) = \text{Tr}(A).$$

Finally, another useful and interesting property concerning the trace is the following. Let $|\varphi\rangle \in \mathcal{H}$ be a state (or unit vector), and consider the rank-one operator $|\varphi\rangle\langle\varphi| : \mathcal{H} \to \mathcal{H}$, which projects in the direction of $|\varphi\rangle$. Consider now an arbitrary operator $T \in \mathcal{B}(\mathcal{H})$ and suppose that we want to compute $\text{Tr}(A|\varphi\rangle\langle\varphi|)$. To do that, before we express $|\varphi\rangle$ in a basis $\{|i\rangle\}$ of $\mathcal{H}$ where the first element is exactly $|\varphi\rangle$, i.e., $|\varphi\rangle = |1\rangle$. Then, we get:

$$\text{Tr}(A|\varphi\rangle\langle\varphi|) = \sum_i \langle i|A|\varphi\rangle\langle\varphi|i\rangle = \langle\varphi|A|\varphi\rangle$$

Now, let us move to the formalism of density operators. In the previous subsections, we have described the state of a physical system identifying it with a unit vector in the Hilbert space $\mathcal{H}$. However, there is an equivalent description with trace-class operators on the Hilbert space. One of the main advantages of this description with respect to certain problems appears, for example, when dealing with real experimental systems where noise is present.

A motivation for this formalism comes from the following situation: Sometimes, we do not know whether our system is in a specific state $|\varphi\rangle$, but rather that it is in each one of the states $|\varphi_i\rangle$ with probability p_i, respectively. Hence, we would like to be able to consider the element

$$\sum_i p_i |\varphi_i\rangle,$$

with the constants p_i verifying

$$\sum_i p_i = 1,$$

and work with it as a state. However, it is not a state anymore, since it is not a unit vector. To avoid this difficulty, one can associate each state $|\varphi_i\rangle$ to the rank-one projector $|\varphi_i\rangle\langle\varphi_i|$. Hence, the state in the previous scenario can be described, instead, in the following form

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|,$$

where ρ is a Hermitian, positive semidefinite, and trace one operator. Indeed, it is clear from its description that ρ is Hermitian and has trace one (because of the linearity of the trace and the fact that $\mathrm{Tr}(|\varphi_i\rangle\langle\varphi_i|) = 1$). To see that it is positive semidefinite, notice that for any $|\phi\rangle \in \mathcal{H}$,

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\varphi_i\rangle\langle\varphi_i|\phi\rangle = \sum_i p_i |\langle\phi|\varphi_i\rangle|^2 \geq 0.$$

These operators are called *density operators* or *density matrices* and the set of such elements is usually denoted by $\mathcal{S}(\mathcal{H})$.

Definition. 1.3.5 (Quantum state/Density operators)
A quantum state or density operator is an linear continues operator $\rho \in \mathcal{B}(\mathcal{H})$, which is positive semi-definite, i.e.

$$\langle\psi|\rho|\psi\rangle \geq 0 \qquad \forall\, |\psi\rangle \in \mathcal{H}, \tag{1.3.13}$$

and has trace one, i.e. $\mathrm{Tr}[\rho] = 1$.

1.4 Postulates of quantum mechanics

The postulates of quantum mechanics were derived after a long process of trial and error, which involved a considerable amount of guessing and fumbling by the originators of the theory. The motivation for them is not always clear; even to experts the basic postulates of quantum mechanics appear surprising.

In this section, we mostly focus on the mathematical formulation for the postulates of quantum mechanics in two different (and dual) settings, Heisenberg and Schrödinger picture. These two descriptions will help us to understand the topics presented above.

1.4.1 Heisenberg picture

The postulates in the Heisenberg picture can be stated as follows.

Postulate. 1
Given an isolated physical system, there is a complex Hilbert space $\mathcal{H}$ associated to it, called **state space**. Moreover, the physical system is described by a **state vector**, a normalised vector in this space.

In general, the state space $\mathcal{H}$ of the system under study will depend on the specific physical system, but we know that it is a *separable* Hilbert space. Frequently, one restricts to finite-dimensional Hilbert spaces for simplicity.

Postulate. 2
Given an isolated physical system, its evolution is described by a **unitary**. If the system is in the state $|\varphi_1\rangle$ at time $t = t_1$ and in the state $|\varphi_2\rangle$ at time $t = t_2$, then there exists a unitary $U(t_1, t_2) = U_{t_1,t_2}$ such that

$$|\varphi_2\rangle = U_{t_1,t_2} |\varphi_1\rangle . \tag{1.4.1}$$

This can be generalised using the Schrödinger equation: Given a closed quantum system (with no interaction with an environment), the time evolution of a state on such system is described by

$$i\hbar \frac{d}{dt} |\varphi_t\rangle = H |\varphi_t\rangle . \tag{1.4.2}$$

where $\hbar$ is the Planck's constant. The linear self-adjoint operator H (generally time dependent) is called *Hamiltonian* and describes the dynamics of the system. Let us consider the spectral decomposition of the Hamiltonian (since it is a Hermitian operator):

$$H = \sum_{E_i} E_i |E_i\rangle\langle E_i|,$$

where we denote by E_i the eigenvalues and by $|E_i\rangle$ the corresponding normalized eigenvectors, to emphasize the fact that these eigenvalues represent some energies of the physical system. Indeed, the states $|E_i\rangle$ are usually called *energy eigenstates* or *stationary states*, with associated energy E_i.

The lowest energy is known as *ground state energy*, and its associated eigenstate is known as the *ground state*, a fundamental element in the theory of quantum systems. Moreover, when the difference between the two smallest eigenvalues is strictly positive, this difference is called *spectral gap*, and we say in that case that the system is *gapped.* Determining whether a physical system has or not a spectral gap is a really important problem in Quantum Physics.

The states $|E_i\rangle$ mentioned above are called stationary because their only change in time is of the form

$$|E_i\rangle \mapsto \exp(-iE_i t/\hbar)\, |E_i\rangle.$$

Let us see now the connection between the two formulations for this postulate. If we consider the Schrödinger equation, we can see:

$$|\varphi(t_2)\rangle\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] |\varphi(t_1)\rangle\rangle = U(t_1, t_2)\, |\varphi(t_1)\rangle\rangle,$$

where we are defining:

$$U(t_1, t_2) := \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right].$$

This operation is easily seen to be unitary, and, furthermore, one can see that any unitary operator U can be written in the form

$$U = \exp(iK),$$

for some Hermitian operator K.

Postulate. 3
Given a physical system, with associated Hilbert space $\mathcal{H}$, the quantum measurements over such system are described by a collection $\{M_n\}_n \subset \mathcal{B}(\mathcal{H})$ of measurements as defined in Definition 1.3.1.

More specificaly, the index n refers to the measurement outcomes that may occur in the experiment, and given a state of a quantum system $|\varphi\rangle$ before a measurement, the probability that result $|n\rangle$ occurs is given by

$$p(n) = \langle\varphi|M_n^* M_n|\varphi\rangle$$

and the state of the system after the measurement is given by

$$\frac{M_n\,|\varphi\rangle}{\sqrt{p(n)}}.$$

Finally, measurement operators satisfy:

$$\sum_n M_n^* M_n = \mathbb{1}.$$

Finally, the fourth postulate can be stated as follows.

Postulate. 4
Given a composite physical system, its state space is also composite, and corresponds to the tensor product of the state spaces of the component physical systems. Moreover, if each system i is prepared in the state $|\varphi_i\rangle$, then the composite system is in the state $|\varphi_1\rangle \otimes \ldots \otimes |\varphi_n\rangle$.

After introducing the fourth postulate, it is necessary to make the following remark, which leads to introducing the concept of *entanglement.* Consider two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. Since these two Hilbert spaces have inner products (resp. $\langle\cdot \mid \cdot\rangle_1$ and $\langle\cdot \mid \cdot\rangle_2$), it is a natural question whether one can introduce an inner product, and therefore a topology, on the tensor product that arise naturally from those of the factors. This can be done by defining the inner product as:

$$\langle\varphi_1 \otimes \varphi_2 \mid \psi_1 \otimes \psi_2\rangle = \langle\varphi_1 \mid \psi_1\rangle_1 \langle\varphi_2 \mid \psi_2\rangle_2$$

for every $\varphi_1, \psi_1 \in \mathcal{H}_1$ and $\varphi_2, \psi_2 \in \mathcal{H}_2$, and extending by linearity. Finally, we take the completion under this inner product, and we get as the resulting Hilbert space the tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$. This can be generalized to the tensor product of n Hilbert spaces.

Now, a composite Hilbert space, i.e., a Hilbert space of the form $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, contains elements which are not tensor products of elements of each one of the components. In other words, if $|\varphi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, there do not exist, in general, $|\varphi_i\rangle \in \mathcal{H}_i$ for all i so that

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \ldots \otimes |\varphi_n\rangle.$$

A standard example of a non trivial two qubit state is the *EPR pair*[1], or *Bell state* is the following state:

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

This structure of tensor products leads to the definition of *quantum entanglement*, a behaviour that seems to be at the root of many of the most surprising phenomena in quantum mechanics.

Definition. 1.4.1 (Entanglement)
Given a state $|\varphi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, we say that $|\varphi\rangle$ is **entangled** if it cannot be written as an elementary tensor product of the form

$$|\varphi_i\rangle \otimes \ldots \otimes |\varphi_n\rangle \tag{1.4.3}$$

Notice that, in particular, one needs to have more than one system to talk about entangled states.

1.4.2 Schrödinger Picture

In the Schrödinger picture, we consider density matrices instead of states.

Postulate. 1
Given an isolated physical system, there is a complex Hilbert space $\mathcal{H}$ which is known as the state space of the system. This system is completely described by its **density operator**, which is a Hermitian, positive semidefinite and trace one operator $\rho \in \mathcal{S}(\mathcal{H})$.

Moreover, if we know the probability of the system in every state (for each state ρ_i, the probability that the system is in that state is p_i), then the state ρ can be written as

$$\sum_i p_i \rho_i.$$

Since the Heisenberg and Schrödinger picture are duals, there is an identification between observables in the Heisenberg picture and density matrices in the Schrödinger one. This leads to directly calling by *states* the density matrices, in a slight abuse of notation. With this notation, we denote by *pure states* the density matrices of the form

$$\rho = |\varphi\rangle \langle\varphi|$$

and by *mixed states* the ones of the form

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|.$$

For the second postulate, concerning evolution of systems, we have the following formulation.

Postulate. 2
Given an isolated physical system, with associated Hilbert space $\mathcal{H}$, its evolution is described by a **unitary transformation**. More specifically, if the state of the system t_1 is described by the density matrix ρ_1 and the state of the system at instant $t_2 > t_1$ is described by ρ_2, then there exist a unitary operator U, which depends only on t_1 and t_2, such that

$$\rho_2 = U\rho_1 U^*.$$

As in the Heisenberg picture, the evolution of a density matrix is given by a unitary. To explain the form of the statement of the second postulate, consider

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|.$$

Notice that, since the system initially is in the state $|\varphi_i\rangle$ with probability p_i, then after the evolution given by a unitary U it will be in state $U|\varphi_i\rangle$ with probability p_i. Therefore, the associated density operator will be given by

$$\sum_i p_i U|\varphi_i\rangle\langle\varphi_i|U^* = U\left(\sum_i p_i |\varphi_i\rangle\langle\varphi_i|\right)U^* = U\rho U^*.$$

Moving to the third postulate and the relation with quantum measurements, we have the following formulation for it.

Postulate. 3
Given an isolated physical system, with associated Hilbert space $\mathcal{H}$, any quantum measurements on it are described by a collection of measurement operators $\{M_n\}_n$ as the ones described in Definition 1.3.1. As in the case of the Heisenberg picture, each index n refers to the different outcomes that may occur when measuring. Indeed, if the state of the quantum system is ρ before the measurement, the probability that we get result n is given by

$$p(n) = \mathrm{Tr}(M_n^* M_n \rho),$$

and the state that we get after the measurement is given by:

$$\frac{M_n \rho M_n^*}{p(n)}.$$

Moreover, since probabilities need to sum one, these operators have to satisfy

$$\sum_n M_n^* M_n = \mathbb{1}.$$

Suppose that we measure with the measurement $\{M_n\}_n$ a mixed state of the form

$$\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|.$$

Then, if the initial state is $|\varphi_i\rangle$, for instance, the probability of having outcome n is

$$p(n|i) = \langle\varphi_i|M_n^* M_n|\varphi_i\rangle = \mathrm{Tr}(M_n^* M_n |\varphi_i\rangle\langle\varphi_i|).$$

Hence, the total probability of this outcome is

$$p(n) = \sum_i p(n|i) p_i = \sum_i p_i \,\mathrm{Tr}(M_n^* M_n |\varphi_i\rangle\langle\varphi_i|) = \mathrm{Tr}(\rho M_n^* M_n),$$

because of the definition of ρ. And analogously, one can see that the post-measurement state is given by:

$$\frac{M_n \rho M_n^*}{p(n)}.$$

Finally, concerning the state space of a composite physical system, we get the following postulate, due to the linearity of tensor products.

Postulate. 4
Given a composite physical system, its state space is the tensor product of the state spaces of the component physical systems.

Moreover, if each system i is initially prepared in state ρ_i, then the state in which the composite system is prepared is given as the tensor product of the ρ_i, i.e., $\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$.

These reformulations of the postulates of quantum mechanics in terms of the density operator are, clearly, mathematically equivalent to the description in terms of the state vector. However, as a way of thinking about quantum mechanics, the density operator approach has advantages with respect to two main facts: the description of quantum systems whose state is not known, and the description of subsystems of a composite quantum system.

1.5 Quantum circuits

In this subsection, first, we present a brief survey on classical Boolean circuits, and, then, we introduce some notions of quantum circuits, by outlining the difference with respect to the latter ones.

1.5.1 Classical circuits

A classical circuit is used to represent functions from $\{0,1\}^n$ to $\{0,1\}$. It is a computational model that consists of decomposing each function in some elemental operations, so that this procedure allows us to represent all the possible functions in the domain. This model has good properties in general and is fundamental in computational theory.

In classical complexity theory, we can define a Boolean circuit more formally as follows.

Definition. 1.5.1 (Boolean circuit)
A Boolean circuit is a finite directed acyclic graph composed of AND, OR an NOT gates (see Figure 1.1).

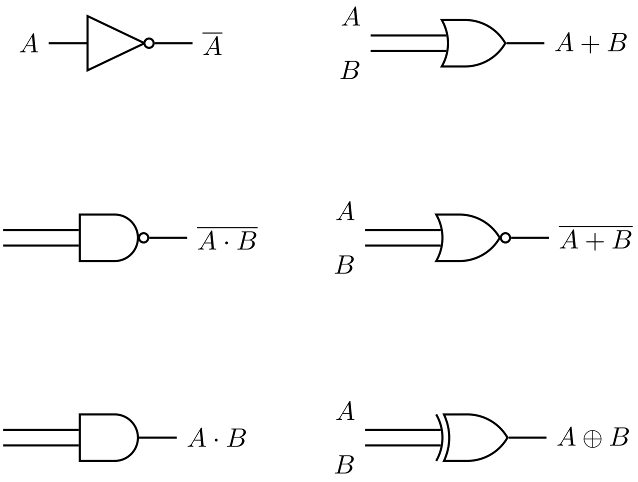

fig. 1.1: Some classical gates for two qubits. AND, OR and NOT are used to construct the rest.

An important theoretical result is that any function on bits can be computed from the composition of NAND gates alone, which is thus known as a *universal gate*. By contrast, the XOR alone or even with NOT is not universal (one can notice that just by taking a look at the parity).

The idea of classical circuits lays on the following facts:

- Every circuit has n input nodes, which contain n input bits.
- The circuit is made of those three gates (AND, OR and NOT), and combinations of then, as well as some output nodes.
- The initial input bits are fed into combinations of the previous gates, so that eventually the output nodes assume some value.

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a Boolean function. Then, we say that a circuit *computes* it if the output nodes get the right value $f(x)$ for every $x \in \{0,1\}^n$.

Now we can introduce some concepts related to the complexity of some circuits. Let us denote a *circuit family* by a set $\mathcal{C} = \{C_n\}$, each one of them of *input size* n (which means that the number of input nodes, and hence bits, is exactly n). We assume that each one of these circuits has one output bit. Then, we say that this family *recognizes* a certain *language* $L \subseteq \bigcup_{n\geq 0} \{0,1\}^n$ (which we denote hereafter by $\{0,1\}^*$) if, for every $x \in \{0,1\}^n$, the circuit C_n outputs:

- 1 if $x \in L$.
- 0 if $x \notin L$.

1.5.2 Quantum gates

Let us move now to quantum circuits, which generalize the idea of classical circuit families. In this case, we replace the AND, OR and NOT gates by elementary *quantum gates.* We define a quantum gate as a unitary transformation in a small number of qubits, usually 1, 2 or 3. The following are the most important gates 1-qubit gates:

1. **Bitflip gate**: It negates the bit, i.e., swaps $|0\rangle$ and $|1\rangle$. It can be represented by:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.5.1}$$

2. **Phaseflip gate**: It puts a - in front of $|1\rangle$. It can be represented by:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.5.2}$$

3. **Phase gate**: It rotates the phase of the $|1\rangle$-state by an angle θ:

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{1.5.3}$$

4. **Hadamard gate**: It is specified by:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.5.4}$$

The last one, the Hadamard gate, is possibly the most important 1-qubit gate. If we apply H to an initial state $|0\rangle$ and then measure, we have the same probability of observing $|0\rangle$ or $|1\rangle$, and analogously if we apply it to initial $|1\rangle$. However, when applied to the superposition state

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

the Hadamard gate provides the value $|0\rangle$. The effect that we get in this case (both positive and negative amplitudes for $|1\rangle$ cancelling out) is called *interference.* It is completely analogous to the interference patterns that one can notice in light or sound waves.

We can further define gates that act on 2 qubits:

5. **CNOT (Controlled not)**: Given two input bits, this gate is used to negate the second bit if the first one is 1, and to leave it invariant if the first bit is 0. It can be represented by

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{1.5.5}$$

In this scenario, the first qubit is called the *control* qubit, since it is the one that determines the effect of the gate, and the second one is called the *target* qubit, as it is the one that receives the effect.

In general, if U is a 1-qubit gate (as the ones that we have defined above), then the we can define the 2-qubit controlled-U gate analogously to the previous one, i.e., if the first bit is 0 it does nothing, and, if it is 1, the gate applies the unitary to the second bit. We can represent it in the following matrix form:

6. **Controlled-U gate**: If the first bit is 0 it does nothing, and, if it is 1, the gate applies the unitary to the second bit. It is given by

$$C_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} \tag{1.5.6}$$

Another way to understand the quantum CNOT gate is as a generalization of the classical XOR gate. Note, however, that there are some classical gates, like NAND or XOR, which cannot be understood as unitary gates in a sense similar to the way the quantum NOT gate represents the classical NOT gate. The reason is because these two gates are essentially irreversible.

We can see that in the following example: Given an output $A \oplus B$ of a XOR gate, it is not possible to determine what the inputs A and B were. This can be also stated by saying that there is a loss of information associated with the irreversible action of the XOR gate. On the other hand, since quantum gates are described by unitary matrices, it is important to remark that they can always be inverted by another quantum gate.

Further we name the following 3-qubit gate, which is particularly interesting as it is classically universal. This means every classical computation can be implemented by a sequence of Toffoli gates.

7. **Toffoli gate or CCNOT (Controlled-Controlled-NOT gate)**: It negates the third bit of its input if both the first two bits are 1.

All those gates mentioned above can be composed into bigger unitary operations in the following ways:

- By taking *tensor products*, if the gates are applied *in parallel.*
- By taking *matrix products*, if the gates are applied *sequentially.*

We show now an example of these operations. If we apply a Hadamard gate H to each bit in a register of n zeros, we get

$$\frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} |j\rangle,$$

a superposition of all n-bit strings, whereas applying $H^{\otimes n}$ to an initial state $|i\rangle$, with $i \in \{0,1\}^n$ gives us

$$H^{\otimes n} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle,$$

with $i \cdot j = \sum\limits_{k=1}^{n} i_k j_k$ the inner product of the n-bit strings $i, j \in \{0,1\}^n$. In this case, one can also notice that the Hadamard is its own inverse. Thus, if we apply it again on the right-hand side of the previous expression, we get the initial $|i\rangle$. This makes the Hadamard gate quite useful for the development of algorithms, as we will see in the following section.

To sum up, as in the case for classical circuits, one can define a quantum circuit in the following form.

Definition. 1.5.2 (Quantum circuit)
A *quantum circuit* is a finite directed acyclic graph composed by:

- **Input nodes.** Some of these nodes (n nodes) contain the input, and some more nodes are initially $|0\rangle$ (they are called the *workspace*).
- **Quantum gates.** Each of them operates on, at most, two or three qubits of the state.
- **Output nodes.** The previous gates transform the initial state vector into a final state, which will generally be a superposition.

Let us see now how one can draw these circuits. We usually consider that time progresses from left to right. As briefly mentioned above, each qubit is represented as a wire, and the circuit prescribes which gates are applied to each wire.

With this notation of wires, it is clear that 1-qubit gates act on just one wire, whereas 2-qubit and 3-qubit gates act, respectively, on 2 or 3 wires. Moreover, when a gate acts on more than 1 qubit, and one of them is the *control* one, its wire is drawn with a dot linked vertically to the *target* qubits, i.e., the qubits where this effect is applied.

We show an example of this notation in the following figure.

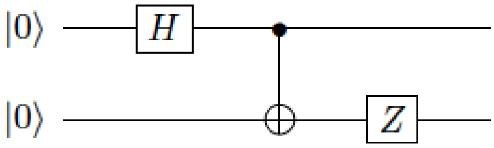

fig. 1.2: Circuit used to turn $|00\rangle$ into $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

In this example, and in general, we denote the quantum CNOT by $\oplus$. If we study every step separately, and taking into account the definition for every gate mentioned above, we can see that, after each step, the resulting state is:

- **Step 0.** We start with $|\varphi_0\rangle = |00\rangle$.
- **Step 1.** After the Hadarmard gate, we have $|\varphi_1\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$.
- **Step 2.** When we apply the CNOT gate, we get $|\varphi_2\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- **Step 3.** Finally, after the Z gate, we have $|\varphi_3\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47 (1935), p. 777.

[2] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667. URL: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf.

[3] C. Palazuelos. *Introduction to Quantum Information Theory*. 2013.

[4] J. Preskill. *Quantum Computation. Lecture Notes*. 2015.

[5] P. W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: SIAM Journal on Computing.26(5) (1997), pp. 1484–1509.

[6] U. Vazirani. *Notes of the Course CS294-2 Quantum Computation*. University of Berkeley, 2004.

[7] Mark M. Wilde. "Preface to the Second Edition". In: *Quantum Information Theory*. Cambridge University Press, pp. xi–xii. DOI: 10.1017/9781316809976.001. URL: https://arxiv.org/pdf/1106.1445.pdf.

[8] R. de Wolf. *Quantum Computing: Lecture Notes*. 2011.