

Lecture notes: Introduction to Quantum Computing. By
Armando Pérez

May 6, 2022

Chapter 1

Quantum protocols

1.1 No cloning theorem

One property which seems evident in classical information, is that bits can be easily copied: we do it with photocopiers, with information files on a hard disk, on USB sticks, etc... We can now ask ourselves about the possibility of copying qubits of information, leaving the original unchanged. As we will see below, this operation is very limited when dealing with quantum information. This is the so-called non-cloning theorem, which prevents the creation of identical copies of an arbitrary unknown quantum state, and has important consequences for the manipulation of quantum information.

Suppose we start from two classical bits (x, y) . The classical computing CNOT gate performs the transformation $(x, y) \rightarrow (x, x \oplus y)$, therefore if we take $y = 0$ we have $(x, 0) \rightarrow (x, x \oplus 0) = (x, x)$, so that we have managed to copy the bit x . Can we do something similar with the quantum CNOT gate?

If we start, as indicated in the figure, from the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as the first qubit and $|0\rangle$ in the second, we will finally obtain the state $\alpha|00\rangle + \beta|11\rangle$, which is not equal to the wanted state $|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$, so both states only coincide if $\alpha = 0$ or $\beta = 0$, that is, we can clone the states of the computational basis, but not a generic state $|\psi\rangle$. Although we have verified that the CNOT gate cannot clone arbitrary states, we are left wondering if we can build another type of operation that does the cloning. However, as we will show below, the no-cloning theorem greatly limits the possibilities, since it states that

Theorem: (no cloning theorem [17]) A quantum system only allows the exact cloning of a set of mutually orthogonal states.

The proof is simple. Let us imagine a state in system A, given by $|\psi\rangle$ that we intend to copy. To make

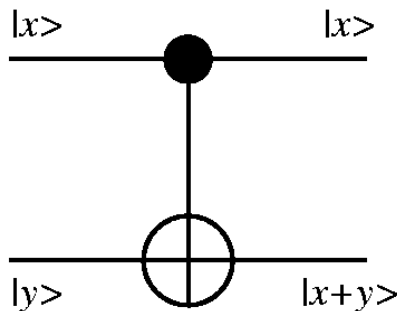


Figure 1.1: Trying to copy with CNOT

the copy, we take a second system B with a Hilbert space equal to that of B, and a state $|e\rangle$ representing the “white paper”, and possibly includes an auxiliary state $|A\rangle$. The composite system AB is thus described by the tensor product

$$|\psi\rangle |e\rangle |A\rangle,$$

where we have omitted the \otimes symbol for simplicity. There are two types of operations that we can perform on this state. We can make a measurement, although this will cause an irreversible collapse towards one of the eigenstates of the observable, thus altering the information contained in the state $|\psi\rangle$, and we are left without a copy. Instead, we must consider a unitary transformation U such that

$$U(|\psi\rangle |e\rangle |A\rangle) = |\psi\rangle |\psi\rangle |A(\psi)\rangle. \quad (1.1)$$

Let us now take a second state $|\phi\rangle$ and suppose that U can also copy this state:

$$U(|\phi\rangle |e\rangle |A\rangle) = |\phi\rangle |\phi\rangle |A(\phi)\rangle. \quad (1.2)$$

Now, a unitary transformation preserves the scalar product, so the scalar product of the initial states in equations (1.1) and (1.2) must coincide with the scalar product of the final states, which implies

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2 \langle A(\phi)|A(\psi)\rangle.$$

One possibility is $\langle\phi|\psi\rangle = 0$, which implies that U can be designed to copy states which are orthogonal to each other. If we exclude this possibility, we have the condition

$$1 = \langle\phi|\psi\rangle \langle A(\phi)|A(\psi)\rangle.$$

This equation can only be satisfied if both $|\langle A(\phi)|A(\psi)\rangle| = 1$ and $|\langle\phi|\psi\rangle| = 1$, which implies $|\phi\rangle = |\psi\rangle$ (except for a phase), and does not add anything new. Therefore U does not copy generic states. The **exact copy** reduces to states orthogonal to each other.

Consequences

The non-cloning theorem prevents us from using classical error correction techniques on quantum states. For example, we cannot create backup copies of a state during quantum computing, and use them to correct later errors. Error correction is vital to practical quantum computing, and for some time it was thought that this could be a serious limitation. In 1995, Shor and Steane revived the prospects for quantum computing by independently writing the first quantum error-correcting code, which avoids the pitfalls of the no-cloning theorem.

In contrast, the no-cloning theorem is a vital ingredient in quantum cryptography, as it prohibits potential eavesdroppers from creating copies of transmitted quantum encryption keys so that they can be decrypted later.

1.2 Quantum cloning

Although it is impossible to make perfect copies of an unknown quantum state, it is still possible to produce imperfect copies. For example, the Wootters-Zurek copying machine [17] is input-state dependent. Let us restrict ourselves to qubits with basis vectors $|0\rangle_a$ and $|1\rangle_a$, for system A, and define the cloning machine in the following way:

$$\begin{aligned} |0\rangle_a |Q\rangle_x &\longrightarrow |0\rangle_a |0\rangle_b |Q_0\rangle_x \\ |1\rangle_a |Q\rangle_x &\longrightarrow |1\rangle_a |1\rangle_b |Q_1\rangle_x. \end{aligned} \quad (1.3)$$

As a consequence of the unitarity of the transformation process and the normalization of the basis states $|0\rangle_a$ and $|1\rangle_a$ it follows that the copying-machine states $|Q_0\rangle_x$ and $|Q_1\rangle_x$ are normalized to unity, provided that ${}_x\langle Q|Q\rangle_x = 1$, i.e. we can assume that

$${}_x\langle Q|Q\rangle_x = {}_x\langle Q_0|Q_0\rangle_x = {}_x\langle Q_1|Q_1\rangle_x = 1.$$

The Wootters-Zurek (WZ) quantum copying machine (QCM) is defined in such a way that the basis vectors $|0\rangle_a$ and $|1\rangle_a$ are copied ideally. However, this is not true for a general state $|s\rangle_a$

$$|s\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$$

Using the transformation relation (1.3) we obtain:

$$|s\rangle_a|Q\rangle_x \longrightarrow \alpha|0\rangle_a|0\rangle_b|Q_0\rangle_x + \beta|1\rangle_a|1\rangle_b|Q_1\rangle_x \equiv |\Psi\rangle_{abx}^{(out)},$$

which clearly differs from the ideal copying result

$$|s\rangle_a|Q\rangle_x \longrightarrow |s\rangle_a|s\rangle_a|Q\rangle_s,$$

as can be checked after expanding the above equation ¹.

As an alternative, Bužek and Hillery [4] introduce an "Universal Quantum Copying Machine" (UQCM). This machine needs just one auxiliary qubit. Its action in the computational basis of the original qubit is

$$\begin{aligned} |0\rangle|e\rangle|Q\rangle &\rightarrow \sqrt{\frac{2}{3}}|0\rangle|0\rangle|1\rangle - \sqrt{\frac{1}{3}}|\Psi^+\rangle|0\rangle \\ (-|1\rangle)|e\rangle|Q\rangle &\rightarrow \sqrt{\frac{2}{3}}|1\rangle|1\rangle|0\rangle - \sqrt{\frac{1}{6}}|\Psi^+\rangle|1\rangle \end{aligned}$$

where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle + |0\rangle|1\rangle]$. By linearity, these two relations induce the following action on the most general input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$|\psi\rangle|e\rangle|Q\rangle \rightarrow \sqrt{\frac{2}{3}}|\psi\rangle|\psi\rangle|\psi^\perp\rangle - \sqrt{\frac{1}{6}}[|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle]|\psi\rangle,$$

where

$$|\psi^\perp\rangle = \alpha^*|1\rangle - \beta^*|0\rangle$$

One sees immediately that A and B can be exchanged, and, in addition, that the transformation has the same form for all input states $|\psi\rangle$. Thus this QCM is symmetric and universal. The partial states for the original and the copy are

$$\rho_A = \rho_B = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^\perp\rangle\langle\psi^\perp|$$

the fidelity is $F_A = F_B = \langle\psi|\rho_A|\psi\rangle = \frac{5}{6}$, which can be shown to outperform, on the average, the QCM machine.

Imperfect cloning can be used as an attack on quantum cryptography protocols, among other uses on quantum information [14].

1.3 Teleportation

We already know that it is not possible to clone an arbitrary unknown state. However, there is the possibility of transferring the quantum state of one qubit to a distant one, at the price of altering the initial qubit (not cloning!). To do this, suppose that Alice has a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ that she wishes to teleport to Bob. We are going to require that both share an entangled state which, to fix ideas, is the Bell state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. So Alice owns the qubit that is entangled with Bob's, and the qubit that she wishes to teleport. In total, the state of these three qubits is

$$|\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle).$$

Let us now take the two Alice qubits, and perform a CNOT operation, followed by a Hadamard gate on the first, as illustrated in figure 1.2

¹A more detailed comparison can be made after tracing out the auxiliary system [4]

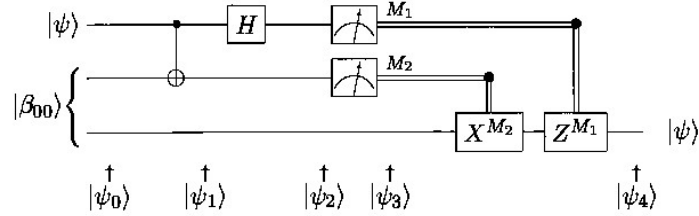


Figure 1.2: Illustration of the teleportation protocol through the use of quantum gates (Fig. from [11]).

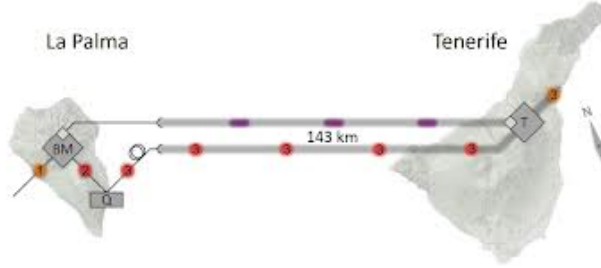


Figure 1.3: Teleportation between La Palma and Tenerife islands. Figure from [9].

The combination of these two operations can be written as

$$|\psi_2\rangle = \frac{1}{2} [|00\rangle |\psi\rangle + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)],$$

being the first two qubits from A and the third one from B. Next, Alice measures her two qubits in the computational basis, obtaining two bits M_1 and M_2 that can each take the values 0 or 1. These bits are sent to Bob using a classic channel (telephone, radio waves, e-mail, etc...). When Bob receives these two bits, he performs the operation $Z^{M_1} \cdot X^{M_2}$ (in this order, note that time runs from left to right in the figure) on his qubit. As can be easily verified, the result of this last operation always produces the result $\alpha |0\rangle + \beta |1\rangle = |\psi\rangle$.

To date, teleportation experiments have been performed with photons, with atoms, with ions, arrays of atoms, light packets, and solid-state qubits. The greatest distance on the ground corresponds to the experiment with photons between La Palma and Tenerife [9]. The teleported state is the polarization of a photon, which can be written as

$$|\Psi\rangle_1 = \alpha |H\rangle_1 + \beta |V\rangle_2, \quad (1.4)$$

in terms of the horizontal $|H\rangle$ and vertical $|V\rangle$ polarization states. The two parties shared the Bell state

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}} (|H\rangle_2 |V\rangle_3 - |V\rangle_2 |H\rangle_3). \quad (1.5)$$

Ground to satellite teleportation has reached even longer distances [13]. In this case, The photon prepared in the state (1.4) is generated in a laboratory in Ngari, Tibet. The goal was to teleport the quantum information of the qubit to the Micius satellite that was launched on August 16, 2016 at an altitude of around 500 km. The distance between the ground station and the satellite changes from 500 km to 1,400 km.

Observations

After teleportation, Bob's qubit becomes state $\alpha |0\rangle + \beta |1\rangle$, and Alice's qubit has collapsed. Teleportation does not result in qubit copying, and is therefore consistent with the no-cloning theorem.

There is no transfer of matter or energy in the process. Alice's particles have not physically moved to Bob, and only their state has been transferred. The term "teleportation", coined by Bennett, Brassard, Crépeau, Jozsa, Peres and Wootters, reflects the indistinguishability of particles in quantum mechanics.

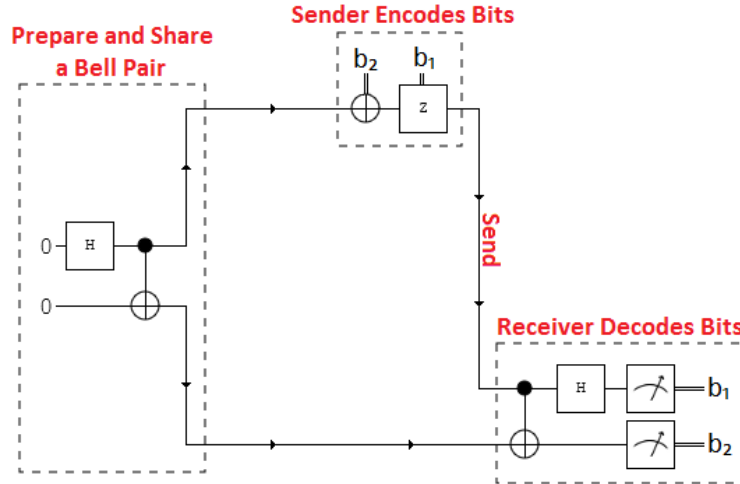


Figure 1.4: Circuit diagram for superdense coding. By Strilanc - Own work, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=37919015>

The teleportation scheme combines the resources of two procedures that are impossible separately. If the entangled shared state of Alice and Bob is removed, the process becomes classical teleportation, which is impossible. On the other hand, if the classical channel is eliminated, then it becomes an attempt to achieve superluminal communication, again impossible.

For each teleported qubit, Alice needs to send Bob two classical bits of information. These two classical bits do not have complete information about the qubit to be teleported. If an attacker intercepts both bits, he/she can know exactly what Bob needs to do to get back to the desired state. However, this information is useless if he cannot interact with the entangled particle in Bob's possession.

1.4 Superdense coding

Superdense coding is a method to transmit a given number of classical bits by sending a smaller number of qubits from sender to receiver. Suppose Alice wishes to transmit two classical bits to Bob using a classical channel: She would have to use two bits. With superdense coding, however, she can communicate the two bits with the transmission of just one qubit. This protocol was proposed by Bennett and Wiesner [3], and experimentally realized in 1996 by Mattle, Weinfurter, Kwiat and Zeilinger using entangled photon pairs [10]. Superdense coding can be thought of as the opposite of quantum teleportation, in which one transfers one qubit from Alice to Bob by communicating two classical bits, as long as Alice and Bob have a pre-shared Bell pair. To achieve superdense coding, Alice first prepares an EPR pair, which is then shared with Bob. She then performs one of four operations on her half of the pair. Let's say that these are a pair of photons. Now Alice chooses which of four classical states she wishes to transmit to Bob as the intended message. Depending on the message she chooses to send, Alice applies a specific quantum operator to her photon.

Suppose Alice and Bob share the following Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Now Alice chooses which of four classical states she wishes to transmit to Bob as the intended message. Depending on the two-bit message she chooses to send, Alice applies a specific quantum operator to her photon.

Alice wants to send	She applies
00	I
01	X
10	Y
11	ZX (first X, then Z)

Next she sends her photon to Bob via a quantum communications channel that preserves entanglement. After receiving the photon, Bob applies the Hadamard to this photon and then a CNOT across the photon pair. He then performs a measurement. The result will be two classical bits of information.

1.5 Quantum cryptography (quantum key distribution or QKD)

Cryptography is the discipline that deals with the transmission and storage of data in such a way that it cannot be understood or modified by third parties. The different cryptographic methods currently in use require two people who wish to communicate information to securely exchange one or more keys; once the keys have been exchanged, the interlocutors can transfer information with a known level of security [16]. But this way of working bases the security of transmissions exclusively on the security of the key exchange. There are two types of cryptography: public key (or asymmetric) and private key (symmetric). Public keys, such as those provided by the RSA algorithm, are based on the difficulty of performing certain operations efficiently (in this case, factoring a large number). The name RSA is an acronym formed by the initials of the first surname of its founders, Ron Rivest, Adi Shamir and Len Adleman. The RSA algorithm starts with two large prime numbers p and q . We form the product $N=pq$ and, by means of modular arithmetic operations, we obtain two other numbers d and e . The private key is formed by the pair (N,d) , and the public key is formed by (N,e) . The party that wants to receive the message sends the public key, and the other party encrypts it. The message can be decrypted using the private key. If a third party could factor N into p and q , he/she would be able to generate the private key and thus decrypt the message. Factorization of large numbers with the known algorithms on classical computers is extraordinarily complex (although it would be an efficient task with a quantum computer, thanks to Shor's algorithm!).

The most secure way to exchange a private key is in person, but this is not possible in most cases, given the multiple number of interlocutors with whom you want to exchange confidential information (banks, internet stores, work colleagues at distant locations, etc...). So the point where there is the least security in the exchange of confidential information is in the process of exchanging and transmitting the keys. If we have a private key, there is a method of encryption, the so-called Vernam encryption or "One-time pad", which can be proven to be undecipherable provided that: a) the key used is sufficiently random and b) it is used only once per message.

Suppose we want to send the word "Hi". We transcribe both letters to the ascii code

H : 72 i : 105

Now we convert to 8-digit binary code ($2^8=256$)

H : 01001000 i : 01101001

i.e. : 0100100001101001

We generate now a random key of equal length

101010010100110

and we add them bitwise, so that $1+1=0$:

0100100001101001

1101010010100110

1001110011001111

It can be shown that the result contains no information about the message. The original message can be recovered by adding the key back to the encrypted message.

Quantum cryptography uses principles of quantum mechanics to guarantee the absolute confidentiality of transmitted information. Current quantum cryptography techniques allow two people to securely create a shared secret key that can be used as a key to encrypt and decrypt messages using symmetric cryptography

methods. Quantum cryptography as an idea was proposed in the 1970s, but it was not until 1984 that the first protocol was published.

One of the most important properties of quantum cryptography is that if a third party attempts to intercept the communication during the creation of the secret key, the process is altered and the intruder is detected before private information is transmitted, because the measurement process in a quantum system disturbs the system.

The security of quantum cryptography rests on the foundations of quantum mechanics, unlike traditional public key cryptography, which rests on assumptions of unproven computational complexity of certain mathematical problems. We now describe two different protocols.

BB84 protocol https://en.wikipedia.org/wiki/Quantum_key_distribution

This protocol was published in 1984 by Charles Bennett and Gilles Brassard, and marks the birth of quantum cryptography. In this protocol, transmission is achieved using polarized photons sent between the sender (Alice) and the receiver (Bob) through a quantum channel, for example, an optical fiber. On the other hand, there also needs to be a public channel (not necessarily quantum) between Alice and Bob, such as the Internet or radio waves, which is used to send information required for the construction of the shared secret key. None of the channels need to be secure, i.e., it is assumed that an intruder (Eve) can tap into them in order to obtain information.

Each photon represents one bit of information, zero or one, and the information is achieved by encoding in orthogonal states, for example rectilinear (horizontally and vertically) or diagonal (at 45° and 135° angles), as shown in the table below. Circular polarization (clockwise or counterclockwise) can also be used.

Basis	0	1
+	↑	→
x	↗	↘

First step: the protocol starts when Alice decides to send a sequence of polarized photons to Bob. To do so, Alice generates a random sequence of chosen bases, for example, between straight (+) and diagonal (x), which is stored temporarily. Once this is done, Alice uses the quantum channel to emit to Bob a randomly polarized photon using the bases she generated (one photon for each base), recording the polarization with which it was emitted.

Alice then has the sequence of bases used and the polarization of the photons emitted.

Quantum mechanics says that it is not possible to make a measurement that distinguishes between 4 different polarization states if they are not orthogonal to each other. In other words, the only possible measurement is between two orthogonal (base) states. Thus, for example, if measured on a rectilinear basis, the only possible results are horizontal or vertical. If the photon was created with a horizontal or vertical polarization (with a rectilinear state generator), then this measurement will yield the correct result. But if the photon was created with a polarization of 45° or 135° (diagonal generator), then the rectilinear measurement will yield a result of horizontal or vertical at random. Moreover, after this measurement, the photon will remain polarized in the state in which it was measured (horizontal or vertical), losing all the initial polarization information.

Second step: as Bob does not know the bases that Alice used to generate the photons, he has no choice but to measure the polarization of the photons using a random base generated by him (rectilinear or diagonal).

Bob records the bases he used to measure the photons and also the results of each measurement.

Third step: Alice and Bob contact each other through the public channel to communicate the bases they used to generate and measure, respectively: Bob sends the bases he used and Alice sends the bases she used.

Both discard the measurements (bits) where the bases did not match (on average half of the bits are discarded). The remaining bits were generated and measured with the same base, so the recorded polarization is the same for Alice and Bob.

Up to this step, in an ideal communication, Alice and Bob already have a shared secret key determined by the remaining bits.

Alice random bits	0	1	1	0	1	0	0	1
Alice basis	+	+	x	+	x	x	x	+
Photons sent by Alice	↑	→	↘	↑	↘	↗	↗	→
Bob random basis	+	x	x	x	+	x	+	+
Bob measurements	↑	↗	↘	↗	→	↗	→	→
Basis are made public								
Secret shared key	0		1			0		1

Fourth step: since there may be some errors in the quantum channel or, worse, an intruder may have intercepted the transmission of photons, the polarization of the photons may have been altered, so Alice and Bob must check that indeed the bits that were not discarded coincide in their value.

If an intruder tries to measure the photons sent by Alice, as in the case of Bob she does not know on what basis they were generated, so she has to make her measurements using random bases, which will inevitably introduce a perturbation in the photons sent by Alice if they do not match on the basis. She could not generate Alice's original photons, since the non-cloning theorem guarantees that it is impossible to reproduce (clone) the transmitted information without knowing in advance the quantum state describing the light.

If an intruder tries to obtain information from the photons then, with a high probability, Alice's and Bob's bit sequences do not match. In order to detect the presence of the intruder, Alice and Bob reveal segments of the generated key. If they differ by more than a certain minimum, then an intruder is assumed and the communication is aborted. If this minimum is not exceeded, it is possible to repair the bit sequence in the event of a mismatch (e.g., in the case of jamming). There are techniques to keep the information revealed in the key as low as possible. This is what we call "privacy amplification". Note that the ability to evaluate the information that Eve has acquired is possible thanks to the use of quantum transmission of the key, and that **this ability does not exist in classical transmission**.

Fifth step: to encode a message one can use the same quantum channel with polarized photons, or use the public channel by encrypting the message with an encryption algorithm, since the key for encryption has been transmitted in an absolutely secure way.

Alice random bits	0	1	1	0	1	0	0	1
Alice basis	+	+	x	+	x	x	x	+
Photons sent by Alice	↑	→	↘	↑	↘	↗	↗	→
Eve random basis	+	x	+	+	x	+	x	+
State found and resend by Eve	↑	↗	→	↑	↘	→	↗	→
Bob random basis	+	x	x	x	+	x	+	+
Bob measurements	↑	↗	↗	↘	→	↗	↑	→
Basis are made public								
Secret shared key	0		0			0		1
Errors on the key	OK		NO			OK		OK

E91 protocol

In the BB84 protocol, the security is guaranteed by the non-cloning principle of quantum states, namely, the cloning is not possible for two non-orthogonal quantum states. A. K. Ekert in 1991 proposed a key distribution protocol with entangled quantum states: the so-called EPR pairs [5]. The protocol can be discussed using either spin directions or photon polarizations. We will consider the first possibility, so that Alice Bob measure the spin of a pair coupled to total spin 0, which constitutes an EPR pair and can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$$

Let us use the unit vectors \vec{a}_i and \vec{b}_i ($i = 1, 2, 3$) to express the directions of the detectors, and assume that \vec{a}_i and \vec{b}_i are taken in the xy-plane perpendicular to the z-axis. Alice uses \vec{a}_i while Bob uses \vec{b}_j to measure

the direction of spin. The correlation between upward + and downward – is defined by

$$E(\vec{a}_i, \vec{b}_j) \equiv E_{++}(\vec{a}_i, \vec{b}_j) + E_{--}(\vec{a}_i, \vec{b}_j) - E_{+-}(\vec{a}_i, \vec{b}_j) - E_{-+}(\vec{a}_i, \vec{b}_j)$$

where, for example, $E_{++}(\vec{a}_i, \vec{b}_j)$ means the observation of spin direction with \vec{a}_i being + and that with \vec{b}_j being +. For the singlet state defined above, it takes the value

$$E(\vec{a}_i, \vec{b}_j) = -\vec{a}_i \cdot \vec{b}_j$$

The detectors with Alice and Bob are arranged at angles $(\vec{a}_1, \vec{a}_2, \vec{a}_3) = (\varphi_1 = 0, \varphi_2 = \pi/4, \varphi_3 = \pi/2)$ and $(\vec{b}_1, \vec{b}_2, \vec{b}_3) = (\theta_1 = \pi/4, \theta_2 = \pi/2, \theta_3 = 3\pi/4)$, respectively, from the x-axis. Let us note that the directions a_2 and b_1 have the same direction, as well as a_3 and b_2 . Now, let us define

$$S \equiv E(\vec{a}_1, \vec{b}_1) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_3, \vec{b}_1) + E(\vec{a}_3, \vec{b}_3),$$

which means that Alice and Bob must perform measurement on the EPR pair with four different sets of the specific directions. If one assumes a theory with local realism, then

$$|S| \leq 2,$$

which is the so-called the CHSH inequality (J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt inequality), and is a variation of Bell's inequality.

For the above detector arrangements, quantum mechanics gives instead

$$S = -2\sqrt{2}.$$

The violation of this inequality is a signature of quantum behavior, and can be used to detect entanglement.

The E91 protocol is as follows:

Step 1 : Alice and Bob perform measurements with their own detectors arranged as shown above.

Step 2 : Alice and Bob make public the direction of the detectors. They classify the results of measurements into two groups: (a) results by detectors at different directions, (b) results by detectors at the same directions.

Step 3 : Alice and Bob make public only those results in group (a), and check whether the CHSH inequality S is satisfied.

Step 4 : They adopt the results of group (b) as the secret key only if the CHSH inequality $S = -2\sqrt{2}$ is satisfied.

The eavesdropper can try to measure both particles using **random directions**, and send to Alice and Bob new particles according to these results. However, one can show that this strategy results in a new value S' which is restricted to

$$|S'| \leq \sqrt{2} < 2,$$

which is in contradiction with the quantum mechanical result. In this way, Alice and Bob can recognize the presence of a tapper by making use the CHSH inequality. The measurement of the EPR pair by Eve results in determining the direction of the spin at each measurement. The average over the resulting states which are sent to Alice and Bob has completely different description that the one corresponding to the initial entangled state, so that the CHSH inequality is not violated. The capability of recognizing eavesdroppers by the measurement at a certain number of different directions is a wonderful application of the principles of quantum mechanics with the entangled states. Another advantage of this protocol is that the key is generated "naturally at random" since it is impossible to know in advance what polarization each photon will have.

Obtaining the key

Let us offer some idea of how Alice and Bob can establish a secret key. As mentioned above, once the "sifted key" is obtained (i.e., after the bases have been announced), Alice and Bob publicly compare a

randomly chosen subset of it. In this way, they estimate the error rate. These publicly disclosed bits are then discarded. If the discrepancy is above some threshold, as quantified by their mutual information [7], they stop the protocol. Otherwise, they proceed with the last step in a quantum cryptography protocol, which uses classical algorithms, first to correct the errors, and then to reduce Eve’s information on the final key, a process called privacy amplification. One of these procedures (just to give a simple example) is the one we describe below [15, 7]. More elaborated procedures are discussed in [2].

Error correction (also called information reconciliation)

The obtained key can be treated in such a way as to minimize errors in it, without completely revealing it, at the price of reducing the size of the key. Suppose that Alice and Bob have obtained, by the procedure explained above, the keys $\{a_i\}_{i=1\dots N}$ and $\{b_i\}_{i=1\dots N}$, respectively, and that both keys are not identical. Suppose the probability of matching any two bits is $p(a_i = b_i) = p > \frac{1}{2}$. The goal is to produce more correlated keys. To do this, Alice randomly chooses pairs of bits and announces their XOR value $A = a_1 \oplus a_2$. Bob replies either “accept” if he has the same XOR value $B = b_1 \oplus b_2$ for his corresponding bits, or “reject” if not. In the first case, Alice and Bob keep the first bit: $a'_1 = a_1, b'_1 = b_1$ and discard the other one. If $A \neq B$, they discard both bits. As can be shown, the new key satisfies

$$p(a'_1 = b'_1) = \frac{p^2}{p^2 + (1-p)^2} > p,$$

so the probability that the keys match has increased, at the price of discarding more than half of the bits. This procedure can be iterated until arbitrarily identical keys are obtained.

Privacy amplification

Suppose now that Alice and Bob have corrected all their errors: $p(a_i = b_i) = 1$. Eve still has information about Alice’s bits, which we assume: $p(e_i = a_i) = q > \frac{1}{2}$. To decrease the information available to Eve, they apply the procedure next: As before, Alice again randomly chooses pairs of bits and computes their XOR value. But, in contrast to error correction, she does not announce this XOR value. She only announces which bits she chose (e.g., bits number 103 and 537). Alice and Bob then replace the two bits by their XOR value, i.e. they compute $A = a_1 \oplus a_2$ and $B = b_1 \oplus b_2$. Since their keys match, $A = B$ holds. Now they take $a'_1 = A, b'_1 = B$. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even less. If she tries to figure out the new bit a'_1 by defining $e'_1 = e_1 \oplus e_2$, it can be shown that

$$p(e'_1 = a'_1) = q^2 + (1-q)^2 < q,$$

if $q > \frac{1}{2}$. That is, the probability that Eve guesses the bit has decreased. Again, the price is that the new key has been made shorter by a factor of 2. If this procedure is iterated, one gets the limit $p(e'_i = a'_i) \rightarrow 1/2$.

Practical QKD:

Quantum key distribution has reached the commercial era. See <https://www.ventureradar.com/keyword/Quantum%20cryptography> and https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_or_communication. Recently, quantum secure direct communication over a 100km fiber has been achieved [18].

Chapter 2

Quantum algorithms: Deutsch, Grover.

2.1 Deutsch-Jozsa algorithm

In the Deutsch–Jozsa problem, we are given a black box quantum circuit, also known as an oracle, that implements some function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. In other words, it takes a set of n bits, such as 10001...1, and gives as result either 0 or 1. We are promised that the function is either constant (0 on all outputs or 1 on all outputs) or balanced (returns 1 for half of the input domain and 0 for the other half: notice that the number of total inputs is 2^n). The task then is to determine whether f is constant or balanced by using the oracle. For a conventional classical algorithm $2^{n-1} + 1$ evaluations of f will be required in the worst case. To prove that f is constant, just over half the set of inputs must be evaluated and their outputs found to be identical. The best case occurs where the function is balanced and the first two output values that happen to be selected are different. The Deutsch–Jozsa quantum algorithm produces an answer that is always correct with a single evaluation of f , which therefore represents an exponential speedup, although no practical applications have been found so far. The Deutsch–Jozsa Algorithm generalizes earlier (1985) work by David Deutsch, which provided a solution for the simple case where $n = 1$.

To perform the algorithm, we need $n + 1$ qubits, which are initially in the $|0\rangle^{\otimes n} |1\rangle$ state. Next we apply the Hadamard gate H on each qubit to obtain the state

$$\frac{1}{\sqrt{2^n + 1}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle).$$

The oracle is constructed such that it transforms each state $|x\rangle |y\rangle$ to $|x\rangle |y \oplus f(x)\rangle$. After applying the oracle

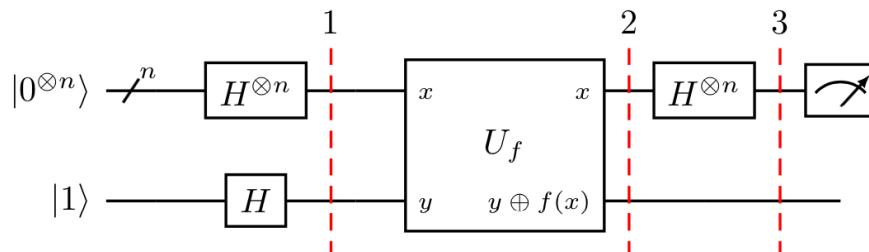


Figure 2.1: Circuit for the Deutsch-Jozsa algorithm. Source: Qiskit

to the previous state we get

$$\frac{1}{\sqrt{2^n+1}} \sum_{x=0}^{2^n-1} |x\rangle (|f(x)\rangle - |1 \oplus f(x)\rangle) = \frac{1}{\sqrt{2^n+1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle).$$

The last qubit can be therefore factored out, which allows us to concentrate on the first n qubits, described by the state

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle.$$

We now apply a Hadamard gate on each one of these qubits, which can be proven to act as

$$|x\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle,$$

where $x \cdot y = x_0 y_0 \oplus \dots \oplus x_n y_n$. Then we arrive at

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle.$$

Finally, we measure the qubits, and look for the probability to obtain $|y=0\rangle = |0\rangle^{\otimes n}$. This probability is given by

$$P(0) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2.$$

Let us examine this result in detail. If $f(x)$ is constant, so is the sign $(-1)^{f(x)}$, and the sum results in $P(0) = 1$ (constructive interference), which implies that $y = 0$ is the only possible result. On the other hand, if $f(x)$ is balanced, half of the terms contribute with $+$, while the other half contributes with $-$, which results in a destructive interference producing $P(0) = 0$, then $y = 0$ cannot be obtain. These two cases are clearly distinguishable, and allows to solve the problem with just one run of the oracle function.

2.2 Grover's algorithm

The Grover's algorithm, published in 1996 [8] is usually introduced as the problem of unstructured search on a database, i.e. the problem of finding a particular, or "marked" item ω out of a set $\{x\}$. It is however preferable to recast the goal as a satisfiability problem, since this allows to apply it to a wider class of problems (such as boolean satisfiability problems). In this way, one is given with a function $f : \{0, 1, \dots, N-1\} \longrightarrow \{0, 1\}$. We will assume that there is one particular element ω such that

$$f(x) = \begin{cases} 1 & x = \omega \\ 0 & x \neq \omega \end{cases} \quad (2.1)$$

This function is commonly referred to as a "black box" or an "oracle", meaning that one can interrogate the box to find the solution to the problem. Our goal is to make it part of a quantum algorithm such that the solution becomes amplified. A first important comment is that having such an oracle at our disposal does not immediately imply that we will find the solution in an efficient way. In other words: being able to recognize the solution is not quite the same as looking for it! For example, a classical strategy consists in looking, one by one, at the possible values of x . In the average, this implies $N/2 = \mathcal{O}(N)$ evaluations. The Grover algorithm allows to find the correct answer in $\mathcal{O}(\sqrt{N})$ evaluations.

To start with, we define the unitary operator U_ω such that

$$U_\omega |x\rangle = e^{i\pi f(x)} |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} -|x\rangle & x = \omega \\ |x\rangle & x \neq \omega \end{cases}, \quad (2.2)$$

which constitutes a possible quantum version of the oracle. We have the following identity

$$U_\omega = I - 2|\omega\rangle\langle\omega|. \quad (2.3)$$

One comment is in order. In many examples which describe the Grover algorithm, one starts by defining the state $|\omega\rangle$ and proceeds with the rest. As a consequence, one may think that the whole procedure is meaningless, as we already know the solution. As stated at the beginning, one has to consider the oracle as a black box, such that the solution is not known at the beginning. In fact, we can consider the following example, which constitutes a physical implementation of the Grover's algorithm [1]. In this work, the authors propose a genuine application of Grover's algorithm to solving the NP-complete number partitioning problem. They specify each problem instance by a list of n weights w_i , $i \in]0, 1]$, and search for a partition into two sublists of equal total weight (sum). Then the operator

$$S_z \equiv \frac{1}{2} \sum_{i=1}^n w_i \sigma_i^z$$

represents the imbalance between the subsets, and the solution corresponds to $S_z|\omega\rangle = 0$. In other words, $f(x) = \delta(S_z|x\rangle)$, or

$$U_\omega|x\rangle = e^{i\pi\delta(S_z|x\rangle)}$$

As we can see, the oracle can be constructed without knowledge of the solution!

The Grover algorithm proceeds in the following way:

1. Initialize the system to the uniform superposition over all states

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

As we know, this can be done by applying the Hadamard gate to each of the qubits in the initial state $|0\rangle^{\otimes n}$.

2. Apply t times the Grover operator $U = U_s U_\omega$, where $U_s = 2|s\rangle\langle s| - I$.
3. Perform a measurement on the computational base.

Let us examine the action of these operators. As can be seen from the above equations, the action of these operators can be restricted to the subspace spanned by $\{|\omega\rangle, |s\rangle\}$, although it is more convenient to analyze the evolution in terms of $\{|\omega\rangle, |\omega_\perp\rangle \equiv \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle\}$. One can check that $|s\rangle = \sin\theta|\omega\rangle + \cos\theta|\omega_\perp\rangle$, where we have introduced $\sin\theta \equiv 1/\sqrt{N}$. In this basis

$$U_s = \begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

$$U_\omega = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$U = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}.$$

We need now to calculate the power U^t . Since U represents a rotation, obviously

$$U^t = \begin{pmatrix} \cos 2\theta t & \sin 2\theta t \\ -\sin 2\theta t & \cos 2\theta t \end{pmatrix}.$$

The probability to measure $|\omega\rangle$, after t iterations, starting from $|s\rangle$ is given by

$$P_\omega(t) = |\langle\omega|U^t|s\rangle|^2 = \sin^2[(2t+1)\theta],$$

which is obviously an oscillatory function. The first maximum appears at $2t+1 \simeq \frac{\pi}{2\theta}$. For $N \gg 1$, this corresponds to $t \simeq \frac{\pi\sqrt{N}}{4}$.

The circuit that implements the algorithm is depicted in Fig. 2.2.

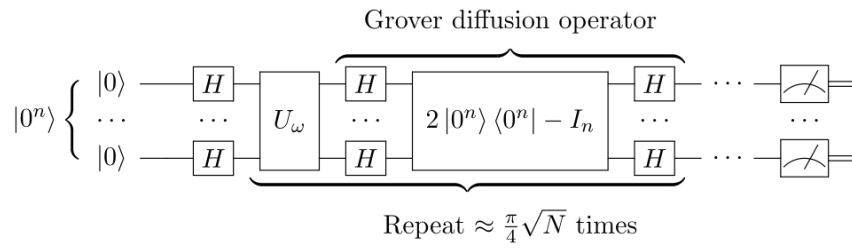


Figure 2.2: Circuit for Grover's algorithm. By Fawly - Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=106362482>

Chapter 3

Quantum information theory

3.1 Density matrix

The description of the possible states in quantum mechanics as vectors of a Hilbert space falls short when it comes to describing some situations. As an example, consider observing direct sunlight, which is unpolarized. At the quantum level, one might try to describe the photons which constitute sunlight in terms of horizontal $|H\rangle$ and vertical $|V\rangle$ photon polarization states with the same amplitudes, i.e. by a combination such as $\frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle$. However, such a combination represents linearly polarized light at 45° . In fact, any combination of the form $\alpha|H\rangle + \beta|V\rangle$ represents light which is polarized in some way! This clearly illustrates the need to introduce a new formalism to describe a wider class of states. These are the so-called mixed states, and are described with the help of the density matrix formalism.

Another example appears when the system we are studying is entangled with a second one. Suppose that the system of two electrons: A and B, is described by the singlet state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$. We know that this state is entangled, so there are no $|\psi\rangle_A$ and $|\psi\rangle_B$ such that $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. As a consequence, observations made exclusively on A cannot be described by a pure state: they are given by a mixing set. The same happens in an open quantum system (that is, a system which is in contact with its environment), since the system is entangled with the environment, and its description must be done using the mixing state formalism.

From the above discussion, we would like to have a way of describing a set of photons (or, in general, identical but completely independent physical systems) for which we can only say are in the state $|\psi_1\rangle$ with probability p_1 , in state $|\psi_2\rangle$ with probability p_2 , and so on. The first condition we need is that the p_n are probabilities, that is $1 \geq p_n \geq 0$ and $\sum_n p_n = 1$. The next property that would have to be fulfilled is that the expected value of an observable, A, in this mixture set, could be calculated by adding the expected values of the observable in each of the states multiplied by the probability of each state, that is:

$$\langle A \rangle = \sum_n p_n \langle \psi_n | A | \psi_n \rangle .$$

Using that for any state $\text{Tr} \{ |\psi\rangle \langle \psi | A \} = \langle \psi | A | \psi \rangle$, we can write

$$\langle A \rangle = \sum_n p_n \text{Tr} \{ |\psi_n\rangle \langle \psi_n | A \} = \text{Tr} \left\{ \left(\sum_n p_n |\psi_n\rangle \langle \psi_n | \right) A \right\}$$

Thus, if we define a Hilbert space operator, (this operator characterizes the mixture set and is called the density operator) as $\rho = \sum_n p_n |\psi_n\rangle \langle \psi_n |$ and we define the expectation value of an arbitrary operator on this mixed set as $\langle A \rangle_\rho = \text{Tr} \{ \rho A \}$ we will automatically have the desired property.

If we now use in the above equation the spectral theorem for A :

$$A = \sum_a a \Lambda_a,$$

where Λ_a represents the projector on the subspace corresponding to the a eigenvalue, we obtain

$$\langle A \rangle_\rho = \sum_a a \text{Tr} \{ \rho \Lambda_a \}$$

which indicates that the probability of obtaining a given eigenvalue, a , in a measurement of an operator is given by $P(a) = \text{Tr} \{ \rho \Lambda_a \}$.

Incidentally, the case of unpolarized light could be described by the density operator

$$\rho = \frac{1}{2} |H\rangle \langle H| + \frac{1}{2} |V\rangle \langle V| = \frac{1}{2} I$$

It thus represents a completely isotropic set: there is no preferred direction, as it is evident when we express it as the identity.

Thus, we will take these properties as definitions of the density operator:

Properties

1. Self-adjoint: $\rho^\dagger = \rho$
2. Positively defined: $\forall |\psi\rangle, \langle \psi | \rho | \psi \rangle \geq 0$
3. $\text{Tr} \{ \rho \} = 1$
4. $\text{Tr} \{ \rho^2 \} \leq 1$

The first three properties are immediate to prove from the definition.

Since ρ is self-adjoint (1) and positive definite (2), it is diagonalizable and its eigenvalues, ω , are real and positive. In addition, we can build an orthonormal basis with the corresponding eigenvectors, $|\omega\rangle$, (if an eigenvalue ω is degenerate, an additional label will have to be added to characterize the different elements of the basis). By (3) we will also have that $\sum_\omega \omega = 1$ since the trace of an operator is independent of the base (and if it is diagonalizable, it is the sum of its eigenvalues). The fact that the trace is 1 guarantees us that the spectrum of ρ is discrete (although the space over which it is defined can be of infinite dimension) since the trace of a positive definite operator with a continuous spectrum is necessarily infinite (for example if we calculate the trace of X^2 , we have $\text{Tr} \{ X^2 \} = \int dx \langle x | X^2 | x \rangle = \int dx x^2 \delta(0)$ which is infinite). Thus, the ω are discrete and $0 \leq \omega \leq 1$ (since they have to add up to 1) and can be interpreted as the probabilities of the different states $|\omega\rangle$. We also see that the same density operator can be expressed in different ways, and that in particular there is a special way that is its decomposition into eigenstates.

If a set is formed by a single state (a “pure state”) we will have $\rho = |\psi\rangle \langle \psi|$ and then ρ is a projector, since $\rho^2 = \rho$. In this case, it is clear that $\text{Tr} \{ \rho^2 \} = \text{Tr} \{ \rho \} = 1$. It is easy to see that the condition $\text{Tr} \{ \rho^2 \} = 1$ is also sufficient for ρ to describe a pure state. Indeed, if we use the basis of eigenvectors to calculate the trace we have

$$1 = \text{Tr} \{ \rho^2 \} = \sum_\omega \omega^2.$$

The only way to fulfill this equation is that only one of the ω is 1 and all the rest are zero, so this density matrix describes a pure state. In short, the necessary and sufficient condition for a pure state is that $\text{Tr} \{ \rho^2 \} = 1$.

3.2 Measurements on a composite system. Partial trace and reduced operator density

Consider the combination of two quantum systems, which we will call A and B, with associated Hilbert spaces \mathcal{H}_A and \mathcal{H}_B , respectively. The Hilbert space corresponding to the total system AB is given by $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Suppose that the state of the joint system is described by the density operator ρ_{AB} , and that we perform measurements (not necessarily simultaneous) on both systems. On system A, the observable is represented by the operator M_A , which has an orthonormal basis of eigenvectors $\{|a\rangle\}$, so that $M_A |a\rangle = a |a\rangle$. Similarly, we measure on B an observable M_B that has an orthonormal basis of eigenvectors $\{|b\rangle\}$, so that $M_B |b\rangle = b |b\rangle$. Let us represent by Λ_a the projector on the eigenvalue subspace a, and similarly Λ_b the projector on the eigenvalue subspace b. The set of vectors $\{|a\rangle \otimes |b\rangle \equiv |a, b\rangle\}$ constitutes a basis of the total space, with eigenvalues a and b defined in both spaces. In this way, the projector corresponding to these two eigenvalues is $|a, b\rangle \langle a, b| = \Lambda_a \otimes \Lambda_b$, where we have assumed that there is no degeneracy, although the reasoning can be extended to the case where there is.

The probability that in the joint measurement of the observables M_A and M_B the values a and b are obtained is given by

$$p(a, b|M_A, M_B) = \text{Tr}\{(\Lambda_a \otimes \Lambda_b)\rho_{AB}\}$$

We now ask ourselves what is the probability of obtaining the result a, regardless of what happens in system B. In probability theory, this operation is described by the marginal probability on that variable, and is obtained by adding on the other variable: $p(a|M_A, M_B) = \sum_b p(a, b|M_A, M_B)$

The meaning is simple: if we obtain the result a many times, it corresponds to different values of a , and all of them contribute in the same way, so in the calculation of $p(a)$ we are counting them all: that is where the sum comes from.

If we take into account that $\sum_b \Lambda_b = I_B$, we obtain

$$p(a|M_A, M_B) = \sum_b p(a, b|M_A, M_B) = \text{Tr}\{(\Lambda_a \otimes \sum_b \Lambda_b)\rho_{AB}\} = \text{Tr}\{(\Lambda_a \otimes I_B)\rho_{AB}\} \equiv p(a|M_A) \quad (3.1)$$

Note that the above result is independent of the observable M_B chosen in B, hence the last notation $p(a|M_A)$ introduced above. This implies that the measurement probabilities at A are not affected by what measurements are made at B, or even by whether such measurements are made or not. Of course, the same is true when looking at the situation from B. As a consequence, we cannot send signals between A and B by measurements on one of the parties. This is a very important property of quantum mechanics, called "non-signalling", and it prevents the transmission of information at speeds greater than the speed of light.

On the other hand, the equation (3.1) implies that the projector corresponding to the measurements when we are only concerned with system A is $\Lambda_a \otimes I_B$. From here, by means of the spectral theorem we can obtain the operator that corresponds to this type of measurement, and that we will represent by \tilde{M}_A

$$\tilde{M}_A = \sum_a a(\Lambda_a \otimes I_B) = \left(\sum_a a\Lambda_a\right) \otimes I_B = M_A \otimes I_B,$$

a quite intuitive result. Since the description of the measures seen from only one of the parts does not need the other one, we wonder if the joint state ρ_{AB} can be simplified in this context. More specifically, we wonder if it is possible to calculate the probabilities of a measure of $\tilde{M}_A = M_A \otimes I_B$, using a density operator ρ_A on \mathcal{H}_A , which we will call reduced operator, so that

$$p(a|M_A) = \text{Tr}\{(\Lambda_a \otimes I_B)\rho_{AB}\} \stackrel{?}{=} \text{Tr}_A\{\Lambda_a \rho_A\}$$

Before proceeding, we need to introduce the concept of partial trace. Let $\{|\alpha_i\rangle\}$ be an orthonormal basis of \mathcal{H}_A , and $\{|\beta_j\rangle\}$ be an orthonormal basis of \mathcal{H}_B : the set $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ forms an orthonormal basis of \mathcal{H} . Let us now consider a product operator, of the form $X \otimes Y$. Its trace will be given by

$$\text{Tr}\{X \otimes Y\} = \sum_{i,j} (\langle \alpha_i | \otimes \langle \beta_j |) X \otimes Y (|\alpha_i\rangle \otimes |\beta_j\rangle) = \text{Tr}_A\{X\} \text{Tr}_B\{Y\},$$

where $Tr_A\{X\} = \sum_i \langle \alpha_i | X | \alpha_i \rangle$, and $Tr_B\{Y\} = \sum_j \langle \beta_j | Y | \beta_j \rangle$.

We define the partial trace over B of this operator, and represent it as Tr_B , as follows

$$Tr_B\{X \otimes Y\} \equiv X Tr_B\{Y\}, \quad (3.2)$$

where the latter operation is referred only to system B. In a similar way, we can define the partial trace on A:

$Tr_A\{X \otimes Y\} \equiv Tr_A\{X\} Y$. Since the trace is always a linear operation, we can compute the partial trace for any operator, even if is not of the form $X \otimes Y$.

Let us observe that equation (3.2) transforms an operator that acts on the total space into another that only acts on \mathcal{H}_A . To illustrate this, suppose that the operator above corresponds to a product of density operators

$$\rho_{AB} = \sigma \otimes \tau, \quad (3.3)$$

being σ and τ density operators on A and B, respectively. Then

$$Tr_B\{\rho_{AB}\} = \sigma Tr_B\{\tau\} = \sigma,$$

as expected.

Let us write

$$\rho_{AB} \equiv \sum_{i,j,k,l} \rho_{ij,kl} (|\alpha_i\rangle \langle \alpha_j| \otimes |\beta_k\rangle \langle \beta_l|). \quad (3.4)$$

As a consequence,

$$p(a|M_A) = Tr\{(\Lambda_a \otimes I_B)\rho_{AB}\} = \sum_{i,j,k,l} \rho_{ij,kl} Tr_A\{\Lambda_a |\alpha_i\rangle \langle \alpha_j|\} Tr_B\{|\beta_k\rangle \langle \beta_l|\} = \quad (3.5)$$

$$\sum_{i,j,k} \rho_{ij,kk} Tr_A\{\Lambda_a |\alpha_i\rangle \langle \alpha_j|\} = Tr_A\{\Lambda_a \sum_{i,j,k} \rho_{ij,kk} |\alpha_i\rangle \langle \alpha_j|\} = Tr_A\{\Lambda_a \rho_A\},$$

with

$$\rho_A = \sum_{i,j,k} \rho_{ij,kk} |\alpha_i\rangle \langle \alpha_j| = \sum_{i,j,k,l} \rho_{ij,kl} |\alpha_i\rangle \langle \alpha_j| Tr_B\{|\beta_k\rangle \langle \beta_l|\} = Tr_B\{\rho_{AB}\}$$

In this way, the calculation of expected values or measurement probabilities for observables that act only on system A can be done with the reduced density operator for that system. In other words, ρ_A is what the system A of the total AB observes, making local measurements (restricted to its system).

3.3 Schmidt's Theorem (Schmidt Decomposition)

For any $|\psi\rangle_{AB}$, there exist two orthonormal sets $|u_i\rangle_A$ and $|v_j\rangle_B$ such that $|\psi\rangle_{AB} = \sum_i \sqrt{p_i} |u_i\rangle_A \otimes |v_i\rangle_B$,

where the coefficients p_i are positive real numbers, satisfying $\sum_i p_i = 1$.

Demonstration. Let's write

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |\alpha_i\rangle \otimes |\beta_j\rangle,$$

where $\{|\alpha_i\rangle\}$ is an orthonormal basis of \mathcal{H}_A and $\{|\beta_j\rangle\}$ is an orthonormal basis of \mathcal{H}_B . Suppose $dim(\mathcal{H}_A) \leq dim(\mathcal{H}_B)$ (otherwise we would choose the space \mathcal{H}_B in what follows), and construct the reduced density operator $\rho_A = Tr_B\{\rho_{AB}\}$, where $\rho_{AB} = |\psi\rangle_{AB} \langle \psi|$. We know that ρ_A admits an orthogonal basis $\{|u_i\rangle\}$ of eigenvectors, so that

$$\rho_A = \sum_i p_i |u_i\rangle \langle u_i|, \quad (3.6)$$

where $p_i \geq 0$ are the weights, satisfying $\sum p_i = 1$. If we write the vectors $\{|\alpha_i\rangle\}$ in this new basis:

$$|\alpha_i\rangle = \sum_k \gamma_{ik} |u_k\rangle$$

and we substitute in the expression of $|\psi\rangle_{AB}$, we have

$$|\psi\rangle_{AB} = \sum_{i,j,k} \gamma_{ik} c_{ij} |u_k\rangle \otimes |\beta_j\rangle = \sum_{k,j} d_{kj} |u_k\rangle \otimes |\beta_j\rangle,$$

having defined $d_{kj} \equiv \sum_i \gamma_{ik} c_{ij}$. If we now recalculate ρ_A , we get

$$\rho_A = \sum_{k,j,l} d_{kj} d_{lj}^* |u_k\rangle \langle u_l|$$

Comparing with equation (3.6), we obtain that

$$\sum_j d_{kj} d_{lj}^* = p_k \delta_{kl} \quad (3.7)$$

For every $p_k \neq 0$, we introduce in the space \mathcal{H}_B the vectors

$$|v_k\rangle \equiv \sum_j \frac{d_{kj}}{\sqrt{p_k}} |\beta_j\rangle$$

It can be shown that they are orthogonal to each other using the (3.7) property. We finally arrive at

$$|\psi\rangle_{AB} = \sum_k \sqrt{p_k} |u_k\rangle \sum_j \frac{d_{kj}}{\sqrt{p_k}} |\beta_j\rangle = \sum_k \sqrt{p_k} |u_k\rangle \otimes |v_k\rangle$$

Thus, the Schmidt coefficients $\sqrt{p_i}$ are the square roots of the eigenvalues of the two partial traces $\rho_{AB} = |\psi\rangle_{AB} \langle \psi|$, $\rho_A = Tr_B \{\rho_{AB}\} = \sum_i p_i |u_i\rangle \langle u_i|$ and $\rho_B = Tr_A \{\rho_{AB}\} = \sum_i p_i |v_i\rangle \langle v_i|$, having the same multiplicity those that are not zero. Note that null eigenvalues can be discarded from the Schmidt decomposition, since they do not contribute. The vectors $|u_i\rangle$ are the eigenvectors of ρ_A , and $\{|v_i\rangle\}$ are the eigenvectors of ρ_B . Note that the maximum number of nonzero Schmidt coefficients (and, therefore, of terms in the Schmidt decomposition) is bounded by the space having the lower dimension.

The Schmidt decomposition is useful to characterize the separability of pure states in some particular cases:

- 1) The state $|\psi\rangle_{AB}$ is separable if and only if there is a unique non-zero Schmidt coefficient: $\exists i / p_i = 1, p_j = 0 \quad \forall j \neq i$.
- 2) If more than one of them is not null, the state is entangled.
- 3) If all the Schmidt coefficients in the lower dimensional space are non-zero and equal, the state is said to be maximally entangled.

Examples:

I) The singlet spin state results in $p_1 = p_2 = 1/2$, so it is maximally entangled. Note that the state $|\psi\rangle \equiv \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$ also gives rise to the same reduced matrices as in the singlet case: $\rho_A = \frac{1}{2} I_A, \rho_B = \frac{1}{2} I_B$ (also maximally entangled). This implies that, when there is degeneracy in the Schmidt coefficients, there is an ambiguity when reconstructing the original state, and we need additional information (for example, the total spin of the system).

II) Let the two-photon state be $|\psi\rangle = (|HH\rangle + |HV\rangle)/\sqrt{2}$. This state is obviously separable: $|\psi\rangle = |H\rangle \otimes |d\rangle$, with $|d\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. The density operator is $\rho_{AB} = \frac{1}{2}(|HH\rangle + |HV\rangle)(\langle HH| + \langle HV|) = \frac{1}{2}(|HH\rangle \langle HH| + |HV\rangle \langle HH| + |HH\rangle \langle HV| + |HV\rangle \langle HV|)$, and the reduced operators $\rho_A = |H\rangle \langle H|$ and $\rho_B = \frac{1}{2}(|H\rangle \langle H| + |H\rangle \langle V| + |V\rangle \langle H| + |V\rangle \langle V|)$. In array notation, $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\rho_B = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Both have the same eigenvalues (1 and 0), which corresponds to a separable state. Also, the eigenvector of ρ_B with nonzero eigenvalue is $|d\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, so we can write $\rho_B = |d\rangle \langle d|$.

3.4 Measurements in quantum mechanics

We start this section by formulating the general postulate of measurement in quantum mechanics.

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators, called **Kraus operators**, that act on the space of the quantum system being measured, and satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I \quad (3.8)$$

The index m refers to all measurement outcomes that may occur. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

The state of the system immediately after the measurement is given by

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$$

The above postulate is generalized for an initial state described by a density operator ρ . The probability for an outcome m becomes

$$p(m) = \text{Tr}\{M_m \rho M_m^\dagger\},$$

and the final state becomes

$$\frac{M_m \rho M_m^\dagger}{p(m)}.$$

Projective measurements constitute a particular case of measurements, where the operators M_m are represented by projectors: $M_m = P_m$, with the condition that

$$P_m P_l = \delta_{ml} P_m,$$

and correspond to measurements of the operator $A = \sum_m m P_m$.

Projective measurements do not comprise all possible situations. As we will show below, one can obtain information about the state even if the set of measurement operators are not mutually orthogonal. **Positive Operator Valued Measurements** (POVMs) can be used to take account for such situations. At variance with projective measurements, the state of the system is generally not defined after the measurement. But again, there are some situations where such information is of no interest. As an example, imagine an experiment where a photon impacts on a screen: since the photon is absorbed, it cannot be described by a projective measurement.

A POVM is a set of positive Hermitian operators $\{E_m\}$ such that

$$\sum_m E_m = I,$$

and the probability of outcome m is given by

$$p(m) = \langle \psi | E_m | \psi \rangle$$

when the state $|\psi\rangle$ is measured.

Given a set of POVM operators, one can define $M_m \equiv \sqrt{E_m}$, which implies that $M_m^\dagger M_m = E_m$, and also that (3.8) is fulfilled. This shows that POVM constitute a particular case of the general postulate. Notice, however, that the operators M_m are not uniquely defined from E_m . In fact, given an unitary operator U , the new operator $M'_m \equiv U M_m$ also satisfies $M_m'^\dagger M'_m = M_m^\dagger M_m = E_m$. In other words, the post-measurement state is not determined by the POVM itself, but rather by the M_m operators that physically realizes it. Since there are infinitely many different sets of such operators that realize the same POVM, the operators E_m alone do not determine what the post-measurement state will be.

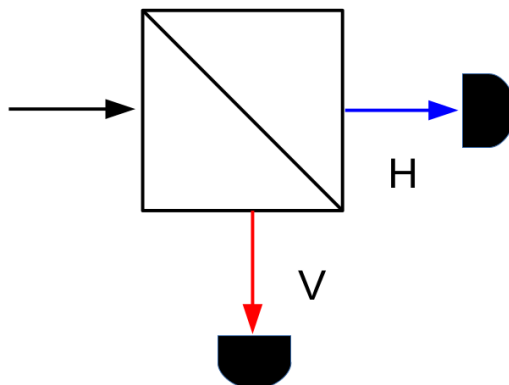


Figura 3.1: Scheme of a polarization beam splitter.

On the other side, given a set of general measurement operators M_m , it is possible to define the POVM set E_m as $E_m \equiv M_m^\dagger M_m$. This case is a bit trivial, as the replacement of $\{M_m\}$ by $\{E_m\}$ represents a loss of information. In this case, we would know the resulting state only if we do not forget about the original measurement operators M_m ! One should also mention that POVM can be obtained from projective measurements acting on a larger space (this is the so-called Neumark's Theorem [6]).

In the latest two classes (projective and POVM), each operator E_m and each operator M_m is positive and Hermitian, while these conditions are not required in the general case.

Example: Suppose we want to measure the polarization of photons. The standard method consists in making use of a polarization beam splitter, shown in Fig. 3.1

This corresponds to a projective measurement over the $|H\rangle$ and $|V\rangle$ states. What happens if we are instead allowed to make measurements using the non-orthogonal states $|\phi_1\rangle = |H\rangle$ and $|\phi_2\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$? For definiteness, we will perform measurements on the photon states $|\psi_1\rangle = |V\rangle$, and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$.

We can define the following operators

$$E_1 = \alpha |\phi_1\rangle \langle \phi_1|$$

$$E_2 = \beta |\phi_2\rangle \langle \phi_2|$$

$$E_3 = I - E_1 - E_2,$$

for some constants α and β such that the above operators conform a POVM. The choice for α and β is not unique. A possible choice is, for example, $\alpha = 1/2$, $\beta = 2/3$.

One can check that

$$\langle \psi_1 | E_1 | \psi_1 \rangle = \langle \psi_2 | E_2 | \psi_2 \rangle = 0.$$

In other words, if we obtain a non-zero result for E_1 , we can safely conclude that the initial photon state must have been $|\psi_2\rangle$. Similarly, if the measurement outcome E_2 occurs, the initial photon state must have been $|\psi_1\rangle$. Sometimes, however, we will obtain the measurement outcome E_3 , and we can infer nothing about the identity of the initial state. The key point, however, is that we never make a mistake identifying the initial state. This property comes at the price that sometimes we obtain no information about the identity of the state. This simple example demonstrates the utility of the POVM formalism as a simple and intuitive way of gaining insight into quantum measurements in instances where only the measurement statistics matter. For a discussion about the different kinds of measurements, please read Box 2.5 in [11].

Chapter 4

Decoherence and quantum noise

Quantum systems (S) are never completely isolated, but rather interact with some environment (E), see figure 4.1. This interaction will produce an entanglement between the states of the system and those of the environment, which is characterized by a large number of degrees of freedom. This entanglement prevents, as we will show later, the occurrence of interference phenomena in certain magnitudes, especially those that have a clear classical correspondence, such as position. This process is what we call decoherence. This is how we expect non-classical correlations to be suppressed, as in the well-known Schrödinger cat-like states. In this way, we think we can explain the consistency between classical predictions and quantum mechanics, since the decoherence phenomenon is, in fact, a quantum phenomenon, different from other classical phenomena such as dissipation. Thus, we would be explaining the transition between the quantum world and the classical one.

Decoherence processes are usually very efficient. Even though they do not produce a visible effect on dynamic variables (the evolution of an expected value, for example), the system becomes entangled with the environment very quickly. Furthermore, because the environment is a large system, the very states of E with which our quantum system had become entangled rapidly evolve, effectively dissipating information about S, and rendering it virtually unrecoverable.

In addition, the superposition between quantum states is necessary for most experiments on quantum information, so that decoherence usually manifests as a stumbling block in the design of these experiments, which must be designed in order to minimize interaction with the environment. In this way, the understanding of the decoherence phenomenon is crucial in quantum information.

4.1 Decoherence and superpositions

Suppose a quantum system that can be in one of the states $|s_1\rangle$ or $|s_2\rangle$, and which interacts with the surroundings in such a way that, if the state of S is $|s_1\rangle$, the state of E is $|E_1\rangle$; Similarly, if the state of S is $|s_2\rangle$, the state of E is $|E_2\rangle$. As a result of the interaction, we have the correspondence $|s_1\rangle \longrightarrow |s_1\rangle|E_1\rangle$ and $|s_2\rangle \longrightarrow |s_2\rangle|E_2\rangle$. If S starts from the state $\alpha|s_1\rangle + \beta|s_2\rangle$, and E starts from the state $|E_0\rangle$, the composite state of S+E will evolve as

$$|\Psi_0\rangle = (\alpha|s_1\rangle + \beta|s_2\rangle)|E_0\rangle \longrightarrow |\Psi\rangle = \alpha|s_1\rangle|E_1\rangle + \beta|s_2\rangle|E_2\rangle$$

Our observations on the system S are defined by the reduced density operator

$$\begin{aligned}\rho_S &= \text{Tr}_E(\rho_{SE}) = \text{Tr}_E\{|\Psi\rangle\langle\Psi|\} \\ &= |\alpha|^2|s_1\rangle\langle s_1| + |\beta|^2|s_2\rangle\langle s_2| \\ &\quad + \alpha\beta^*|s_1\rangle\langle s_2|\langle E_2|E_1\rangle + \alpha^*\beta|s_2\rangle\langle s_1|\langle E_1|E_2\rangle.\end{aligned}$$

Note that the presence of correlations in ρ_S depends on the term $\langle E_1|E_2\rangle$. If this term is zero, the coherence between the states $|s_1\rangle$ and $|s_2\rangle$ disappears.

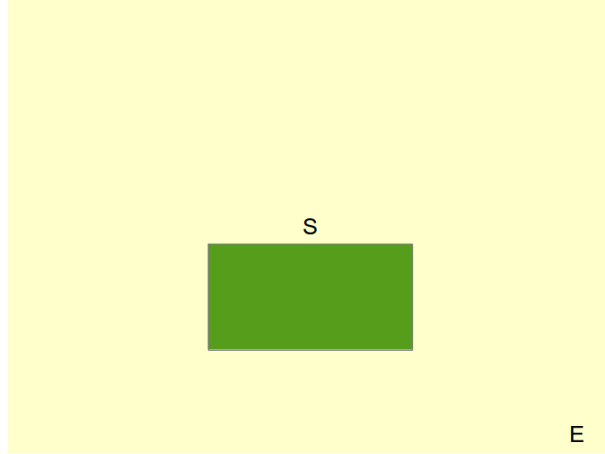


Figure 4.1: Scheme representing a quantum system S which interacts with an environment E.

Generalizing the above description to an arbitrary system, we would write that the decoherence process corresponds to the process

$$\left(\sum_i c_i |s_i\rangle \right) |E_0\rangle \longrightarrow \sum_i c_i |s_i\rangle |E_i(t)\rangle,$$

where we have introduced time, so that at $t=0$ all $|E_i(0)\rangle = |E_0\rangle$, which indicates that the system and the environment start from an uncorrelated state, while the interaction establishes correlations when $t > 0$. Due to the interactions within the environment, the overlap between the different states $|E_i(t)\rangle$ decays rapidly. More precisely, in many models this decay is exponential.

$$\langle E_i(t) | E_j(t) \rangle \propto e^{-t/\tau_d} \quad \text{for } i \neq j,$$

where τ_d is the decoherence time scale for the system.

4.2 Kraus operators

We are now going to describe the decoherence process more rigorously, using the formalism of Kraus operators. Suppose that, at $t = 0$, there are no correlations between the system and the environment, that is $\rho_{SE}(0) = \rho_S(0) \otimes \rho_E(0)$. Let us write $\rho_E(0)$ in its diagonal decomposition, $\rho_E(0) = \sum_i p_i |E_i\rangle \langle E_i|$, where $\sum_i p_i = 1$ and the states $|E_i\rangle$ form an orthonormal basis of the Hilbert space of E. If H represents the Hamiltonian (assumed to be constant in time) of SE and $U(t) = e^{-iHt/\hbar}$ represents the time evolution operator, the density operator of S evolves as

$$\begin{aligned} \rho_S(t) &= \text{Tr}_E \left\{ U(t) \left[\rho_S(0) \otimes \left(\sum_i p_i |E_i\rangle \langle E_i| \right) \right] U^\dagger(t) \right\} \\ &= \sum_{ij} p_i \langle E_j | U(t) | E_i \rangle \rho_S(0) \langle E_i | U^\dagger(t) | E_j \rangle. \end{aligned} \quad (4.1)$$

Let us define the Kraus operators as $K_{ij}(t) \equiv \sqrt{p_i} \langle E_j | U(t) | E_i \rangle$. In this way, we can write

$$\rho_S(t) = \sum_{ij} K_{ij}(t) \rho_S(0) K_{ij}^\dagger(t)$$

It is usual to combine the two indices i and j into a single index, which will take N^2 values, where N is the dimension of the Hilbert space of E. Thus,

$$K_k(t) \equiv \sqrt{p_{i_k}} \langle E_{j_k} | U(t) | E_{i_k} \rangle,$$

so that

$$\rho_S(t) = \sum_k K_k(t) \rho_S(0) K_k^\dagger(t).$$

The Kraus operator formalism represents the effect of the environment by means of a (generally non-unitary) sequence of transformations on ρ_S generated by the operators K_k , which contain information about the dynamics of the joint system SE. Since the evolution of SE is unitary, the Kraus operators satisfy the property

$$\sum_k K_k^\dagger(t) K_k(t) = I_S, \quad (4.2)$$

where I_S is the identity operator on the Hilbert space of S. The latter property implies that

$$\text{Tr}\{\rho_S(t)\} = \text{Tr}\{\rho_S(0) \sum_k K_k^\dagger(t) K_k(t)\} = \text{Tr}\{\rho_S(0)\},$$

that is, it guarantees the conservation of the trace of $\rho_S(t)$.

As we have said before, the Kraus operators contain all the information of the interaction with the environment. However, to know them we need the operator $U(t)$, as well as the detailed structure of the environment, given by the states $|E_i\rangle$. Usually, all this detailed description is not available to us, so we resort to introducing the operators in a phenomenological way.

For example, suppose that the system S corresponds to a qubit, whose basis are the states $\{|0\rangle, |1\rangle\}$. With probability p we perform a non-filtering measure on the base states, and with probability $1 - p$ no operation is performed. These operations are performed periodically with period τ . The Kraus operators are thus

$$\begin{aligned} K_0 &\equiv \sqrt{1-p} I_S, \\ K_1 &\equiv \sqrt{p} \Pi_1 \\ K_2 &\equiv \sqrt{p} \Pi_2, \end{aligned}$$

with $\Pi_1 = |0\rangle\langle 0|$ and $\Pi_2 = |1\rangle\langle 1|$. Therefore

$$\rho_S(t + \tau) = \sum_k K_k \rho_S(t) K_k^\dagger = (1-p) \rho_S(t) + p \sum_{i=1}^2 \Pi_i \rho_S(t) \Pi_i.$$

After iteration, we arrive to

$$\rho_S(t) = (1-p)^t \rho_S(0) + [1 - (1-p)^t] \sum_{i=1}^2 \Pi_i \rho_S(0) \Pi_i.$$

In other words,

$$\rho_S(t) = \begin{pmatrix} \rho_{00}(0) & (1-p)^t \rho_{01}(0) \\ (1-p)^t \rho_{10}(0) & \rho_{11}(0) \end{pmatrix}.$$

In the $t \rightarrow \infty$ limit we obtain

$$\lim_{t \rightarrow \infty} \rho_S(t) = \begin{pmatrix} \rho_{00}(0) & 0 \\ 0 & \rho_{11}(0) \end{pmatrix},$$

which corresponds to a matrix with no coherences (there are no off-diagonal elements).

Quantum Channels

The above discussion constitutes an example of a “quantum channel”, which are defined as completely positive trace-preserving maps. It corresponds to the so-called “dephasing channel”. We give below two additional examples acting on a single qubit, which are of interest in the theory of open quantum systems and quantum computers [12]:

Depolarizing channel

We can describe this channel by saying that, with probability $1 - p$, the qubit remains intact, while with probability p an “error” occurs. The error can be either 1) a bit flip error $|0\rangle \longleftrightarrow |1\rangle$, 2) a phase flip error $|1\rangle \longrightarrow -|1\rangle$, or 3) both. They are represented, in the $\{|0\rangle, |1\rangle\}$ basis, by σ_x , σ_z and σ_y , respectively. In other words, the corresponding Kraus operators are:

$$K_0 = \sqrt{1-p}I \quad K_1 = \sqrt{\frac{p}{3}}\sigma_x, \quad K_2 = \sqrt{\frac{p}{3}}\sigma_y, \quad K_3 = \sqrt{\frac{p}{3}}\sigma_z.$$

Under this action, the polarization vector transforms as

$$\vec{P}' = (1 - \frac{4}{3}p)\vec{P}.$$

In other words, the Bloch sphere contracts uniformly under the action of the channel (for $p \leq 3/4$); the spin polarization shrinks by the factor $1 - \frac{4}{3}p$ (which is why we call it the depolarizing channel).

Amplitude-damping channel

The amplitude-damping channel can be viewed as a simple model to describe the decay of an excited state of a (two-level) atom due to spontaneous emission of a photon. Let us consider the Kraus operators:

$$K_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}$$

$$K_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}$$

Then

$$\rho_S(t + \tau) = \sum_k K_k \rho_S(t) K_k^\dagger = \begin{pmatrix} \rho_{00}(t) + p\rho_{11}(t) & \sqrt{1-p}\rho_{01}(t) \\ \sqrt{1-p}\rho_{10}(t) & (1-p)\rho_{11}(t) \end{pmatrix}.$$

After iterating, at time given by $t = n\tau$, one arrives to

$$\rho_S(t) = \begin{pmatrix} \rho_{00}(0) + [1 - (1-p)^n]\rho_{11}(0) & (1-p)^{n/2}\rho_{01}(0) \\ (1-p)^{n/2}\rho_{10}(0) & (1-p)^n\rho_{11}(0) \end{pmatrix}.$$

If Γ is the spontaneous decay time per unit time, then the decay occurs with probability $p = \Gamma\tau$ during a small time interval τ . In the limit of large n , we can replace $(1-p)^n = (1 - \Gamma\tau/n)^n \longrightarrow e^{-\Gamma t}$, which is the exponential decay law. The coherences decay as $(1-p)^{n/2} \longrightarrow e^{-\Gamma t/2}$. In other words,

$$\rho_S(t) = \begin{pmatrix} \rho_{00}(0) + (1 - e^{-\Gamma t})\rho_{11}(0) & e^{-\Gamma t/2}\rho_{01}(0) \\ e^{-\Gamma t/2}\rho_{10}(0) & e^{-\Gamma t}\rho_{11}(0) \end{pmatrix}.$$

One normally uses “ T_1 ” to denote the exponential decay time for the excited population, and “ T_2 ” to denote the exponential decay time for the coherences. In some systems where dephasing is very rapid T_2 is much shorter than T_1 , but for the amplitude-damping channel these two times are related and comparable:

$$T_2 = 2\Gamma^{-1} = 2T_1.$$

4.3 Master equation

The Kraus operators formalism is a very useful tool to describe the dynamics of open quantum systems. However, it is more useful to be able to translate this description into a formulation in terms of differential equations, similar to the von Neumann equation for the density operator. The *master equations* are of this

type. It is possible to obtain them using time dependent perturbation theory. We, however, are going to get a master equation using a simplified procedure [12]. In what follows, we will use the notation $\rho(t)$ to represent the operator density of the system, instead of $\rho_S(t)$.

At an instant dt from the initial time, the evolution of the operator density of the quantum system will be of the form

$$\rho(dt) = \sum_{\mu} K_{\mu}(dt)\rho_0 K_{\mu}^{\dagger}(dt) = \rho_0 + \mathcal{O}(dt) \quad (4.3)$$

where $\mathcal{O}(dt) = dt\dot{\rho}_0$ is an operator of order dt , and ρ_0 is the density operator on $t = 0$. We can choose one of the Kraus operators, which we will represent by K_0 , that includes the identity operator and gives rise to the term ρ_0 in the above equation. This operator, in general, can include another order term dt , so as to obtain a correction of order dt when multiplied by the identity. This is:

$$K_0 = I + \left(-\frac{i}{\hbar}H + W \right) dt \quad (4.4)$$

We have separated the order contribution dt into two parts (real and imaginary), so that the operators H and W are both Hermitian¹. The rest of the Kraus operators must be of order \sqrt{dt} , so that its contribution is of order dt :

$$K_{\mu} = L_{\mu}\sqrt{dt}, \quad \mu > 0 \quad (4.5)$$

Condition (4.2) gives

$$\begin{aligned} I &= \sum_{\mu} K_{\mu}^{\dagger}K_{\mu} = I + dt \left(2W + \sum_{\mu>0} L_{\mu}^{\dagger}L_{\mu} \right) \\ W &= -\frac{1}{2} \sum_{\mu>0} L_{\mu}^{\dagger}L_{\mu} \end{aligned} \quad (4.6)$$

Upon substitution of (4.4, 4.5, 4.6) into (4.3) we obtain:

$$d\rho(dt) = \rho(dt) - \rho_0 = -\frac{i}{\hbar}[H, \rho_0]dt + \sum_{\mu>0} \left(L_{\mu}\rho_0 L_{\mu}^{\dagger} - \frac{1}{2}L_{\mu}^{\dagger}L_{\mu}\rho_0 - \frac{1}{2}\rho_0 L_{\mu}^{\dagger}L_{\mu} \right) dt.$$

Therefore, the master equation we arrive to is:

$$\boxed{\frac{d\rho}{dt} \equiv \mathcal{L}[\rho] = -\frac{i}{\hbar}[H, \rho] + \sum_{\mu>0} \left(L_{\mu}\rho L_{\mu}^{\dagger} - \frac{1}{2}\{L_{\mu}^{\dagger}L_{\mu}, \rho\} \right)}, \quad (4.7)$$

where $\{, \}$ is the anticommutator, and the L_{μ} are named *Lindblad operators*. Each term $L_{\mu}\rho L_{\mu}^{\dagger}$ describes a possible quantum transition of the system, and $-\frac{1}{2}\{L_{\mu}^{\dagger}L_{\mu}, \rho\}$ ensures that time evolution preserves normalization. The operator \mathcal{L} is the Lindbladian, an operator that transforms the density operator, similarly to how the Hamiltonian generates the time evolution of an isolated system. If the Lindbladian does not depend on time, that is if H, L_{μ} are constant operators, the formal solution of the master equation (4.7) is:

$$\rho(t) = e^{\mathcal{L}t}[\rho_0]$$

Note that, in the general case, the H operator will not coincide with the Hamiltonian of the system, since it can contain additional terms that come from interaction with the environment.

Let's consider an example that illustrates the master equation (4.7) for a qubit with a single Lindblad operator L , which we take as

¹The factor $-\frac{1}{\hbar}$ has been introduced for convenience, in order to identify the equation obtained with the von equation Neumann when there is no interaction with the environment.

$$L \equiv \sqrt{\gamma}\sigma_x \quad (4.8)$$

in the basis of the Hamiltonian of the qubit, which we assume to be given by $H = \frac{\hbar\omega}{2}\sigma_z$. Thus, $\hbar\omega$ is the difference between eigenenergies. From the master equation, we see that the real parameter γ has dimensions of $[\text{time}]^{-1}$. The action of L swaps the energy eigenstates. If we substitute the operators H and L in the master equation (4.7) we get:

$$\frac{d\rho}{dt} = -i\frac{\omega}{2}[\sigma_z, \rho] + \gamma(\sigma_x\rho\sigma_x - \rho),$$

where we have used that the Pauli matrices satisfy that $\sigma_i = \sigma_i^\dagger$ and $\sigma_i^2 = \sigma_i$. The term proportional to γ in the above equation is called a “pure phase shift”. Let’s see the effect it produces. If we substitute the explicit form of the matrices, and we represent by ρ_{ij} the elements of the density operator on the same basis, we arrive at the following set of differential equations:

$$\frac{d}{dt} \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} = \begin{pmatrix} \gamma(\rho_{22} - \rho_{11}) & -i\omega\rho_{12} + \gamma(\rho_{21} - \rho_{12}) \\ i\omega\rho_{21} + \gamma(\rho_{12} - \rho_{21}) & \gamma(\rho_{11} - \rho_{22}) \end{pmatrix}.$$

The conditions $\rho_{11} + \rho_{22} = 1$ (unit trace) and $\rho_{12} = \rho_{21}^*$ (self-adjoint) allows the reduction of the four differential equations to only two. If we define the difference between the diagonal elements (called “populations”) $D \equiv \rho_{11} - \rho_{22}$, we are left with two equations:

$$\dot{D} = -2\gamma D \quad (4.9)$$

$$\dot{\rho}_{12} = -i\omega\rho_{12} - 2i\gamma \text{Im}\{\rho_{12}\}. \quad (4.10)$$

The first one gives an exponential decay:

$$D(t) = D_0 e^{-2\gamma t}, \quad (4.11)$$

with $D_0 \equiv D(t=0)$. Together with the initial condition $\rho_{11}(0) + \rho_{22}(0) = 1$, we obtain

$$\rho_{11}(t) = \frac{1}{2}[1 + e^{-2\gamma t}(2\rho_{11}(0) - 1)]$$

$$\rho_{22}(t) = \frac{1}{2}[1 - e^{-2\gamma t}(2\rho_{11}(0) - 1)]$$

Let us split the second equation into its real and imaginary parts ($\rho_{12} \equiv x + iy$), leading to

$$\dot{x} = \omega y \quad (4.12)$$

$$\dot{y} = -\omega x - 2\gamma y \quad (4.13)$$

From them, it is possible to arrive to a differential equation of second order for x :

$$\ddot{x} + 2\gamma\dot{x} + \omega^2 x = 0$$

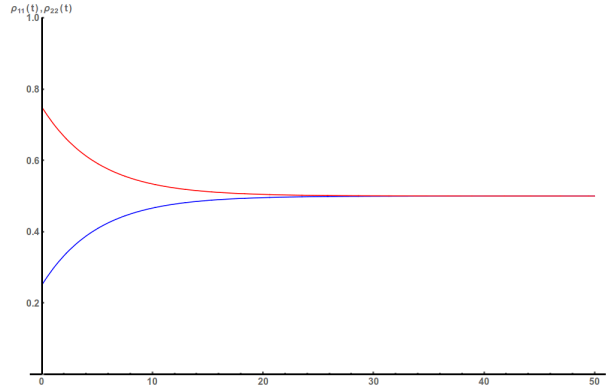
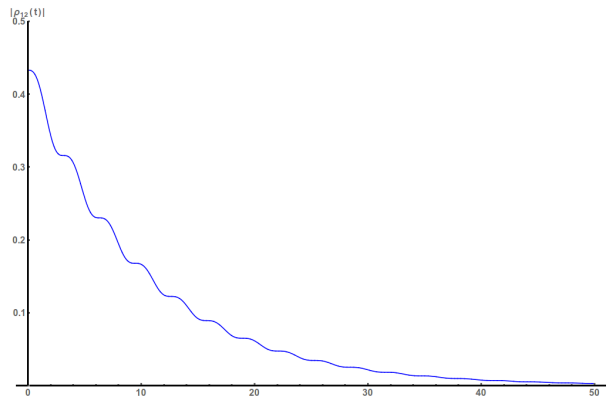
and the same equation for y . Putting again together the real and imaginary parts, we have

$$\ddot{\rho}_{12} + 2\gamma\dot{\rho}_{12} + \omega^2\rho_{12} = 0, \quad (4.14)$$

which is the differential equation of a damped harmonic oscillator. The solution is well known, and consists on an oscillatory term modulated by an exponential damping $e^{-\gamma t}$. More specifically, we get

$$\rho_{12}(t) = \frac{e^{-\gamma t}}{\Omega} [\Omega \cos(\Omega t)\rho_{12}(0) + \sin(\Omega t)(\gamma\rho_{21}(0) - i\omega\rho_{12}(0))]$$

$$\rho_{21}(t) = \frac{e^{-\gamma t}}{\Omega} [\Omega \cos(\Omega t)\rho_{21}(0) + \sin(\Omega t)(\gamma\rho_{12}(0) + i\omega\rho_{21}(0))],$$

Figure 4.2: Populations $\rho_{11}(t)$ (blue) and $\rho_{22}(t)$ (red).Figure 4.3: Absolute value of the coherence $\rho_{12}(t)$.

where $\Omega \equiv \sqrt{\omega^2 - \gamma^2}$.

Thus, regardless of the initial state of the qubit, both the difference D between populations (4.11) as the coherences ρ_{12} (4.14) are exponentially damped, so that in a time $t \gg \gamma^{-1}$ it converges towards the state of maximum entropy $\rho = \frac{I}{2}$, where I is the identity matrix in two dimensions. The interaction with the environment that describes the Lindbladian operator above leads to a loss of coherence on a characteristic time scale γ^{-1} , and describes a simple example of decoherence for a qubit. The figures 4.2 and 4.3 show the resolution of the example discussed earlier. We start from the state pure $|\psi(0)\rangle = \frac{1}{2}|+\rangle + \frac{\sqrt{3}}{2}|-\rangle$, being the states $\{|+\rangle, |-\rangle\}$ the base of eigenstates of σ_z , and the values $\omega = 1$, $\gamma = 0.1$ have been adopted for representation. We clearly see how populations evolve towards the common value $1/2$, and that the coherence $\rho_{12}(t)$ tends to zero (the same happens with $\rho_{21}(t)$: both have the same module). Figure 4.4 shows that the entropy starts from the value zero (initially the state is pure) and tends to unity, which is the maximum value for a qubit, corresponding to the state $\lim_{t \rightarrow \infty} \rho(t) = \frac{I}{2}$

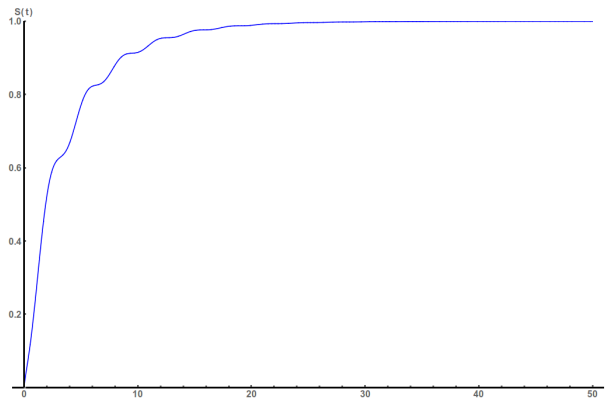


Figura 4.4: Entropy of the qubit.

Bibliography

- [1] Galit Anikeeva, Ognjen Marković, Victoria Borish, Jacob A. Hines, Shankari V. Rajagopal, Eric S. Cooper, Avikar Periwal, Amir Safavi-Naeini, Emily J. Davis, and Monika Schleier-Smith. Number partitioning with grover’s algorithm in central spin systems. *PRX Quantum*, 2:020319, May 2021.
- [2] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.
- [3] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.
- [4] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, Sep 1996.
- [5] Artur K. Ekert. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.
- [6] I. M. Gelfand and M. A. Neumark. On the imbedding of normed rings into the ring of operators in hilbert space. *Matematicheskij sbornik*, 54(2):197–217, 1943.
- [7] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.
- [8] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC ’96, pages 212–219, New York, NY, USA, 1996. Association for Computing Machinery.
- [9] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin, and Anton Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, September 2012.
- [10] Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, and Anton Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76:4656–4659, Jun 1996.
- [11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [12] John Preskill. *Course Information for Physics 219/Computer Science 219 Quantum Computation (Caltech)*.
- [13] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, Kui-Xing Yang, Xuan Han, Yong-Qiang Yao, Ji Li, Hai-Yan Wu, Song Wan, Lei Liu, Ding-Quan Liu, Yao-Wu Kuang, Zhi-Ping He, Peng Shang, Cheng Guo, Ru-Hua Zheng, Kai Tian, Zhen-Cai Zhu, Nai-Le Liu, Chao-Yang Lu, Rong Shu, Yu-Ao Chen, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, September 2017.

- [14] Valerio Scarani, Sofyan Iblidir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Rev. Mod. Phys.*, 77:1225–1256, Nov 2005.
- [15] Valerio Scarani, Chua Lynn, and Liu Shi Yang. *Six Quantum Pieces: A First Course in Quantum Physics*. World Scientific, 2010.
- [16] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, 2000.
- [17] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.
- [18] Haoran Zhang, Zhen Sun, Ruoyang Qi, Liuguo Yin, Gui-Lu Long, and Jianhua Lu. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light: Science & Applications*, 11(1):83, April 2022.