Lecture notes: Introduction to Quantum Computing.

By Armando Pérez

May 12, 2026

Chapter 1

Quantum Cloning and Teleportation

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 $(x, y) \longrightarrow (x, x \oplus y)$, therefore if we take $y = 0$ we have $(x, 0) \longrightarrow (x, x \oplus 0) = (x, x)$, so that we have managed to copy the bit x. Can we do something similar with the quantum CNOT gate?

If we start 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,

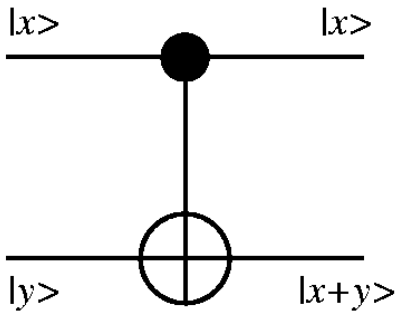

Figure 1.1: Trying to copy with CNOT

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 [13]) 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 the copy, we take a second system B with 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

$$U(|\psi\rangle\,|e\rangle\,|A\rangle) = |\psi\rangle\,|\psi\rangle\,|A(\psi)\rangle\,. \tag{1.1}$$

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

$$U(|\phi\rangle\,|e\rangle\,|A\rangle) = |\phi\rangle\,|\phi\rangle\,|A(\phi)\rangle\,. \tag{1.2}$$

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 satisfy 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 [13] 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:

$$|0\rangle_a|Q\rangle_x \longrightarrow |0\rangle_a|0\rangle_b|Q_0\rangle_x$$

$$|1\rangle_a|Q\rangle_x \longrightarrow |1\rangle_a|1\rangle_b|Q_1\rangle_x. \tag{1.3}$$

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

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

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

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

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

where

$$\big|\psi^{\perp}\big\rangle = \alpha^*\,|1\rangle - \beta^*\,|0\rangle$$

One sees immediately that the first two qubits 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

$$\rho_1 = \rho_2 = \frac{5}{6}\,|\psi\rangle\,\langle\psi| + \frac{1}{6}\,\big|\psi^{\perp}\big\rangle\,\big\langle\psi^{\perp}\big|$$

To quantify the similarity of the cloned state with respect to the initial state we use the fidelity [9], which is defined as follows. Given two quantum states, described by their respective density operators ρ and σ, the fidelity between them is given by

$$F(\rho,\sigma) = (Tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}})^2$$

If (at least) one of the two states is pure, for example $\sigma = |\phi\rangle\,\langle\phi|$, the fidelity simplifies to

$$F(\rho,\sigma) = Tr(\rho\sigma) = \langle\phi\mid\rho\mid\phi\rangle$$

If, in addition, ρ is pure $\rho = |\psi\rangle\,\langle\psi|$, the above expression further simplifies to

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

In our case, we obtain $F_1 = F_1 = \langle\psi\mid\rho_1\mid\psi\rangle = \frac{5}{6}$, which can be shown to outperform, on the average, the QCM machine (the value in that case is $\frac{3}{4}$).

Imperfect cloning can be used as an attack on quantum cryptography protocols, among other uses on quantum information [12].

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

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

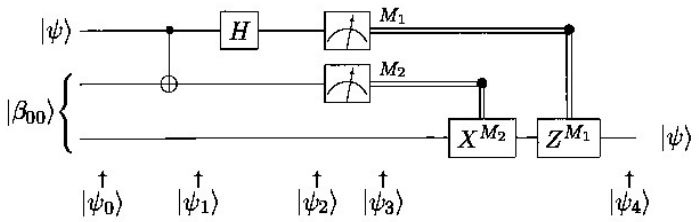

Figure 1.2: Illustration of the teleportation protocol through the use of quantum gates (Fig. from [9]).

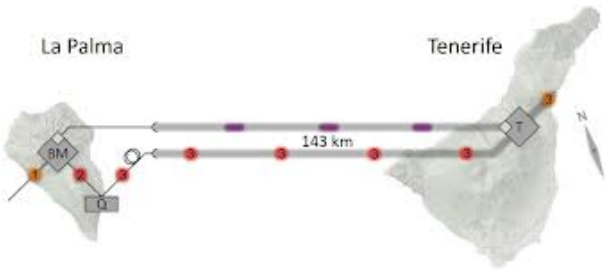

Figure 1.3: Teleportation between La Palma and Tenerife islands. Figure from [7].

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

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 [7]. The teleported state is the polarization of a photon, which can be written as

$$|\Psi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_2, \tag{1.4}$$

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

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

Ground to satellite teleportation has reached even longer distances [11]. 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.

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. Supose 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 [8]. 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.

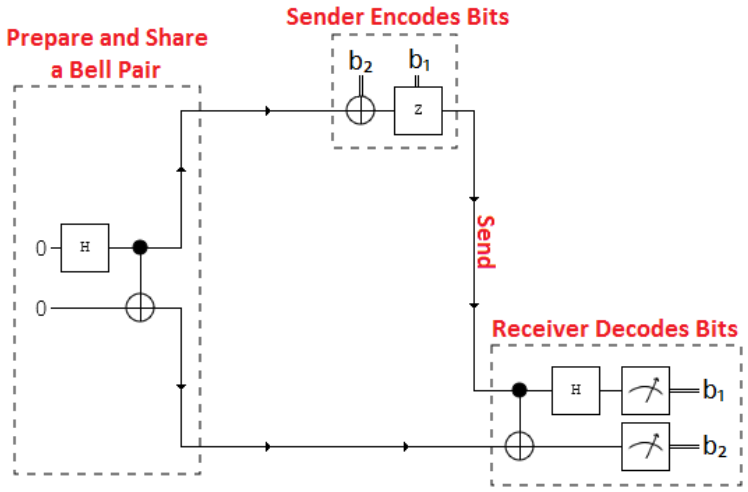

Figure 1.4: Circuit diagram for superdense coding. By Strilanc - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=37919015

Suppose Alice and Bob share the following Bell state

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

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	Z
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.

Chapter 2

Quantum algorithms: Quantum parallelism. Deutsch, Deutsch-Jozsa, Grover.

Quantum algorithms are specifically designed to run on quantum computers. They make use of properties such as superposition, entanglement or quantum parallelism.

Let us briefly discuss how a function can be constructed using a quantum circuit. We will concentrate on real functions defined over a real variable. The variable x can be approximated, up to n digits, by a sequence such as $x = \{1, 0, 0, 1, \ldots 0\}$. We will use a second register with p digits in which we will store a variable $y = \{0, 1, 0, 0, \ldots 1\}$. The first register is called the 'data' register, and the second register the 'target' register.

The computer starts on the state $|x, y\rangle$. Suppose that with an appropriate sequence of logic gates it is possible to transform this state into $|x, y \oplus f(x)\rangle$. We will denote by U_f this transformation, i.e.

$$U_f |x, y\rangle = |x, y \oplus f(x)\rangle .$$

One can prove that this operation is unitary . If $y = 0$, then the final state of the second qubit is just the value $f(x)$.

Let us first consider a simple case with $n = p = 1$, then $f(x)$ reduces to $f(x) : \{0, 1\} \longrightarrow \{0, 1\}$. A familiar example is the CNOT gate (Fig. 2). If we take $y = 0$, then the circuit just evaluates the function $f(x) = x$.

Another example, with $n = 2$ and $p = 1$ is depicted in Fig. 2. The data register contains two qubits. If we define the following values for the x variable $\{0, 0\} = 0, \{0, 1\} = 1, \{1, 0\} = 2, \{1, 1\} = 3$, one can check that this circuit will output the function $f(x)$ with $f(0) = f(1) = 0$, $f(2) = f(3) = 1$.

In the general case, the circuit to evaluate a function $f(x)$ has the structure shown in Fig. 2. Consider now the data register starting with the initial state

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle ,$$

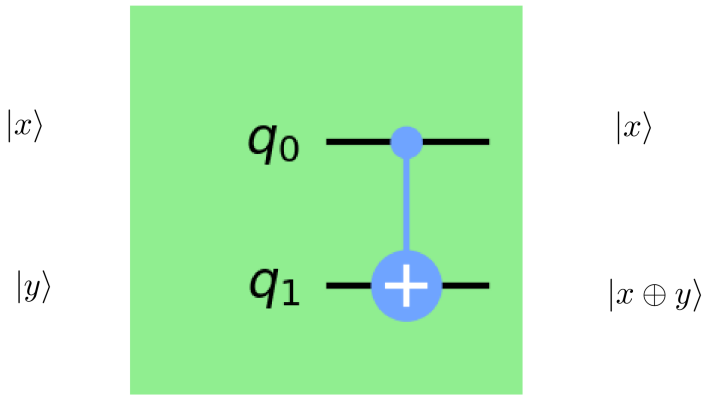

Figure 2.1: CNOT gate.

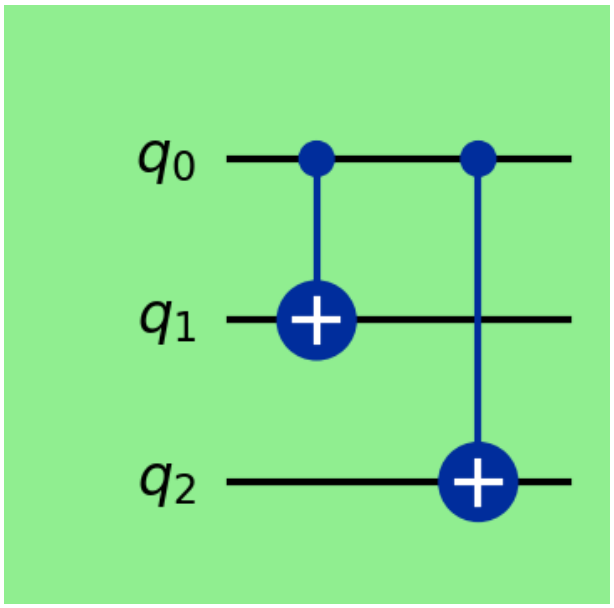

Figure 2.2: A circuit to evaluate the function $f(x)$ defined in the text.

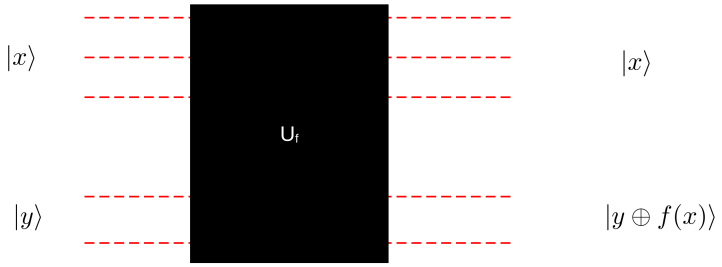

Figure 2.3: Circuit for evaluating a function $f(x)$

where the sum is over all possible values of x. This state can be prepared by applying the Hadamard gate on each of the quibits starting in the $x = |0, \ldots 0\rangle$ state. Similarly, the target register is initialized with $y = |0, \ldots 0\rangle$. In other words, we prepare the state

$$|\Psi_0\rangle = (H \otimes H \cdots \otimes H\,|0, \ldots 0\rangle) \otimes |0, \ldots 0\rangle\,.$$

The result of applying U_f to this state is

$$|\Psi_1\rangle = U_f\,|\Psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes |f(x)\rangle\,.$$

As we see, this new state contains all possible values of $f(x)$, which is referred to as quantum parallelism. Quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once. However, this parallelism is not immediately useful. In the single qubit example, a measurement of the state gives only either $|0\rangle \otimes |f(0)\rangle$ or $|1\rangle \otimes |f(1)\rangle$. Similarly, in the general case, measurement of the state $|\Psi_1\rangle$ would give only a single value of $f(x)$ corresponding to the obtained value of x. Quantum computation requires something more than just quantum parallelism to be useful; it requires the ability to extract information about more than one value of $f(x)$ from superposition states. In what follows we investigate examples of how this may be done.

2.1 Deutsch's algorithm

Let us consider the circuit in Fig. 2 with just two qubits, i.e. $n = p = 1$ and a function $f(x) : \{0, 1\} \longrightarrow \{0, 1\}$. The problem is to know whether $f(x)$ is constant: $f(0) = f(1)$ or satisfies $f(0) \neq f(1)$.

Deutsch's algorithm combines quantum parallelism with a property of quantum mechanics known as interference to solve this problem. As before, we use a Hadamard gate on the first qubit. The second qubit is assumed to start with the state $|1\rangle$, and the Hadamard gate is also applied. After this, we have the state

$$|\Psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

One can easily prove that the action of U_f on the state

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

can be written as

$$(-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Then, the action of U_f on the state $|\Psi_1\rangle$ produces

$$|\Psi_2\rangle = \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } \; f(0) = f(1) \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } \; f(0) \neq f(1) \end{cases}$$

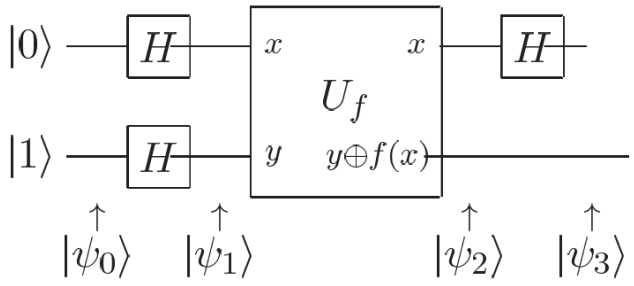

Figure 2.4: Circuit for Deutsch's algorithm. From [9].

The final step is the action of the Hadamard gate on the first qubit, which produces the result

$$|\Psi_3\rangle = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm|1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1) \end{cases}$$

so by measuring the first qubit we may determine whether $f(0) = f(1)$ or $f(0) \neq f(1)$ with a single evaluation of $f(x)$. This is faster than any classical procedure, which will require two evaluations to arrive to the same conclusion. As discussed in [9]:

"This example highlights the difference between quantum parallelism and classical randomized algorithms. Naively, one might think that the state $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ corresponds rather closely to a probabilistic classical computer that evaluates $f(0)$ with probability one-half, or $f(1)$ with probability one-half. The difference is that in a classical computer these two alternatives forever exclude one another; in a quantum computer it is possible for the two alternatives to interfere with one another to yield some global property of the function f, by using something like the Hadamard gate to recombine the different alternatives, as was done in Deutsch's algorithm. The essence of the design of many quantum algorithms is that a clever choice of function and final transformation allows efficient determination of useful global information about the function – information which cannot be attained quickly on a classical computer."

2.2 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 $f : \{0,1\}^n \longrightarrow \{0,1\}$. In other words, it takes a set of n bits, such as $10001\ldots1$, 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

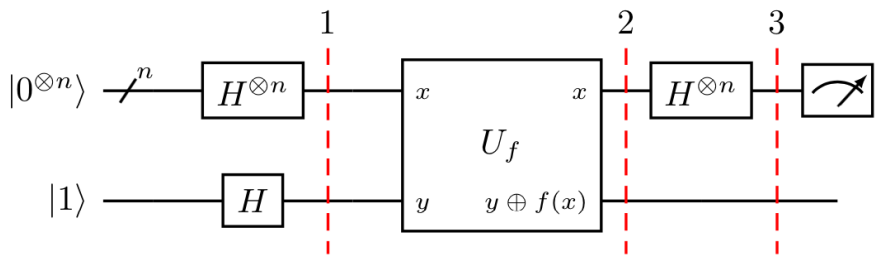

Figure 2.5: Circuit for the Deutsch-Jozsa algorithm. Source: Qiskit

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

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

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 to the previous state we get

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

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 $x\cdot y=x_0y_0\oplus\cdots\oplus x_ny_n$. 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 these qubits, and look for the probability to obtain $|y=0\rangle = |0\rangle^{\otimes n}$. This probability is given by

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

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.

2.3 Grover's algorithm

The Grover's algorithm, published in 1996 [6] 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

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

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

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

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

$$U_\omega = I - 2|\omega\rangle\langle\omega|. \tag{2.3}$$

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

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

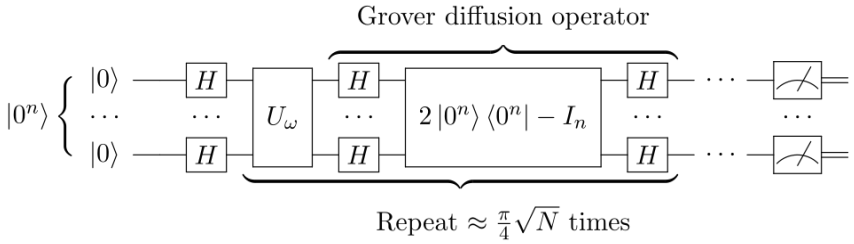

Figure 2.6: Circuit for Grover's algorithm. By Fawly - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=106362482

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

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

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. 2.6.

Chapter 3

Decoherence and quantum noise

Quantum systems (S) are never completely isolated, but rather interact with some environment (E), see figure 3.1. 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 [1].

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.

3.1 Decoherence and superpositions

Suppose a quantum system that can be in one of the states $|s_1\rangle$ or $|s_2\rangle$ belonging to the Hilbert space $\mathcal{H}_S$, and interacts with the surroundings in such a way that, if the state of S

[1] This is in fact the situation in most cases. The only exception are systems for which the evolution is non Markovian [5].

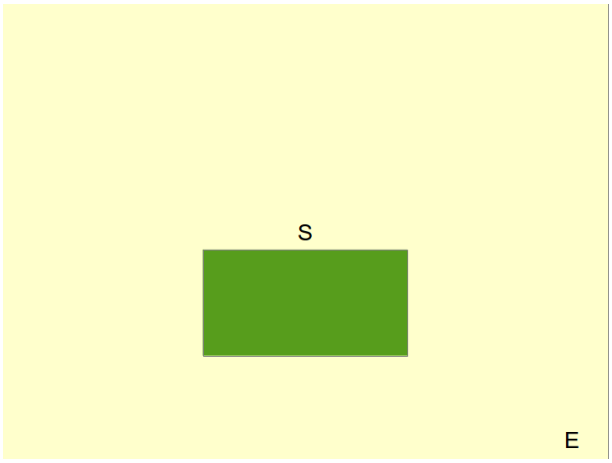

Figure 3.1: Scheme representing a quantum system S which interacts with an environment E.

is $|s_1\rangle$, the state of E (with the associated Hilbert space $\mathcal{H}_E$ 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

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

Note that the presence of correlations in ρ_S depends on the term $\langle E_1|E_2\rangle$. If this term is zero (or nearly zero, as in the case of distinct macroscopic states), the coherence between the states $|s_1\rangle$ and $|s_2\rangle$ disappears, and we are left with

$$\rho_S = |\alpha|^2\,|s_1\rangle\langle s_1| + |\beta|^2\,|s_2\rangle\langle s_2|$$

In other words, the system will experience a transition from a pure state to a mixed state.

3.2 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

$$\begin{aligned}\rho_S(t) &= \mathrm{Tr}_E \left\{ U(t) \left[\rho_S(0) \otimes \left(\sum_i p_i |E_i\rangle\langle E_i| \right) \right] U^\dagger(t) \right\} \\ &= \sum_{ij} p_i \langle E_j| U(t) |E_i\rangle \rho_S(0) \langle E_i| U^\dagger(t) |E_j\rangle . \end{aligned} \tag{3.1}$$

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

$$\rho_S(t) = \sum_k K_k(t) \rho_S(0) K_k^\dagger(t). \tag{3.2}$$

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. It is important no stress that, as can be seen from the above derivation, **the set of Kraus operators that perform a given effect on the system is not uniquely defined.** In other words, two different sets of operators may produce the same transformation on the system.

Since the evolution of SE is unitary, the Kraus operators satisfy the completeness property

$$\sum_k K_k^\dagger(t) K_k(t) = I_S, \tag{3.3}$$

where I_S is the identity operator on the Hilbert space of S.

Equation 3.2 defines, by its own, a linear transformation which is also referrer to as a map

$$\phi : \rho_S(0) \longrightarrow \rho_S(t) = \sum_k K_k(t) \rho_S(0) K_k^\dagger(t)$$

If the completeness relation 3.3 is satisfied, map ϕ is known as a superoperator and Eq. 3.2 is known as the Kraus representation (or the operator-sum representation) of the superoperator ϕ.

A superoperator maps density operators to density operators, since:

1) $\rho_S(t)$ is Hermitian if $\rho_S(0)$ is Hermitian

2) The trace is preserved

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

that is $\rho_S(t)$ has unit trace if $\rho_S(0)$ has unit trace.

3) $\rho_S(t)$ is nonnegative if $\rho_S(0)$ is nonnegative

$$\langle\psi|\,\rho_S(t)\,|\psi\rangle = \sum_k \langle\psi|\,K_k(t)\rho_S(0)K_k^\dagger(t)\,|\psi\rangle = \sum_k \langle\varphi_k(t)|\,\rho_S(0)\,|\varphi_k(t)\rangle \geq 0,$$

where $|\psi\rangle$ is any vector in $\mathcal{H}_S$ and $|\varphi_k(t)\rangle \equiv K_k^\dagger(t)\,|\psi\rangle$.

Unitary representation

We have shown that the unitary evolution of a composite system naturally gives rise to an operator-sum representation describing the evolution of a subsystem. We now tackle the converse problem: given a Kraus representation for the evolution of system S, we shall show that it is possible to introduce an auxiliary system E so that the evolution of the total system S + E is unitary. In this manner, we construct the unitary representation corresponding to a given superoperator. We define an operator U, acting as follows on states of the form $|\psi\rangle\,|E\rangle$ [2]:

$$U\,|\psi\rangle\,|E\rangle \equiv \sum_k K_k\,|\psi\rangle\,|k\rangle\,, \tag{3.4}$$

where $\{|k\rangle$ is an orthonormal basis for subsystem E, whose dimension is determined by the number of Kraus operators appearing in the operator-sum representation, and we consider a fixed time t so that we can omit the time dependence on the Kraus operators. The operator U preserves the inner product. Indeed, for arbitrary states $|\psi\rangle$ and $|\phi\rangle$ we have

$$\langle\phi|\,\langle E|\,U^\dagger U\,|\psi\rangle\,|E\rangle = (\sum_l \langle l|\,\langle\phi|\,K_l^\dagger)(\sum_k K_k\,|\psi\rangle\,|k\rangle) = \sum_k \langle\phi|\,K_k^\dagger K_k\,|\psi\rangle = \langle\phi|\psi\rangle$$

where we have used the orthonormality relation for the $\{|k\rangle\}$ basis and the completeness relation (3.3). As the operator U preserves the inner product when acting on the subspace whose states are of the form $|\psi\rangle\,|E\rangle$, it can be extended to a unitary operator acting on the entire Hilbert space (i.e., to non separable states).

As a simple example [2], let us consider a qubit which is initially in the state

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

This state can also be described by a density matrix

$$\rho = |\psi\rangle\,\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

The diagonal terms of ρ are known as populations, and give the probabilities to obtain, from a polarization measurement along the z-axis, outcomes 0 or 1, respectively. The off-diagonal terms, known as coherences, appear when the state $|\psi\rangle$ is a superposition of the states $|0\rangle$ and $|1\rangle$. We now enlarge our system with an environment described by a single qubit initially in the $|0\rangle$ state. The combined state is therefore

$$|\Psi\rangle = |\psi\rangle \otimes |0\rangle = \alpha\,|00\rangle + \beta\,|10\rangle$$

We now apply a unitary transformation $U = CNOT$ on the composite system, controlled by our qubit. The new state becomes

$$|\Psi'\rangle = \alpha\,|00\rangle + \beta\,|11\rangle$$

Note that the CNOT interaction has entangled the qubit with the environment, as the state $|\Psi'\rangle$ is non-separable. The final density matrix ρ' of the system is obtained after tracing over the environment:

$$\rho' = Tr_{env}\{|\Psi'\rangle\langle\Psi'|\} = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

As we can see, coherences are lost. The information on the relative phases of the coefficients α and β appearing in the initial state $|\psi\rangle$ is now hidden in the system–environment quantum correlations. Since we do not keep records of the state of the environment, this information is lost for us. In short, information leaks from the system into the external world.

Quantum channels

We may now state the following fundamental theorem (for a proof see [9]):

The Kraus representation theorem (Kraus, 1983): A map $\phi : \rho \to \rho'$ satisfying the following requirements: it

(1) is linear; that is, $\phi(\alpha\rho_1 + \beta\rho_2) = \alpha\phi(\rho_1) + \beta\phi(\rho_2)$,

(2) preserves hermiticity,

(3) preserves trace,

(4) is completely positive,

has an operator-sum (Kraus) representation and a unitary representation (3.4) on a larger Hilbert space, this latter generally known as Stinespring representation for ϕ.

We say that ϕ is positive if, for a non-negative ϕ , $\rho' = \phi(\rho)$ is also non-negative. The complete positivity of ϕ is a stronger requirement. It demands that, for any extension of the Hilbert space $\mathcal{H}_S$ to $\mathcal{H}_S \otimes \mathcal{H}_E$, the superoperator $\phi \otimes I_E$ is positive. That is, if we add any system E that has a trivial dynamics (the identity I_E means that no state of E is changed), independently of the dynamics of system S, the resulting superoperator $\phi \otimes I_E$ must be positive. This requirement is physically motivated since, in general, it cannot be excluded that the two systems are initially entangled. If this is the case and we call ρ_{SE} the density matrix corresponding to the initially entangled state, then $\rho_{SE}{}' = (\phi \otimes I_E)\rho_{SE}$ must also be a valid density matrix. This implies the positivity of $\phi \otimes I_E$ for any E, namely the

complete positivity of ϕ. If the above requirements are met, the map ϕ is called a quantum channel.

In Sect. 3.2 we showed that any superoperator satisfies conditions (1-3) above. One can also prove that superoperators defined by a given set of Kraus operators are also completely positive [10].

Exercise: Consider the state

$$|\psi\rangle_{SE} = \frac{1}{\sqrt{2}}(|0\rangle_s |1\rangle_E + |1\rangle_s |0\rangle_E)$$

Let ρ_1 denote the density operator for the first qubit and show that the transposition operator

$$\mathcal{T}(\rho_1) = \rho_1^T$$

is positive but not completely positive. For this purpose, it will be sufficient to show that $\mathcal{T} \otimes I_E$ is not positive.

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 measurement 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

$$K_0 \equiv \sqrt{1-p}\; I_S,$$
$$K_1 \equiv \sqrt{p}\; \Pi_1$$
$$K_2 \equiv \sqrt{p}\; \Pi_2,$$

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 iterating, 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 $t \to \infty$ limit we obtain

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

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

Quantum Channels for a qubit

The above discussion corresponds to the so-called "dephasing channel" (also called the phase-damping channel). Under the effect of a quantum channel, the qubit density matrix transforms as

$$\rho_S \longrightarrow \phi(\rho_S) = \rho'_S = \sum_k K_k \rho_S K_k^\dagger = \frac{1}{2}\sum_k K_k (I + \vec{P}\cdot\vec{\sigma}) K_k^\dagger = \frac{1}{2}\sum_k K_k K_k^\dagger + \frac{1}{2}\sum_k K_k \vec{P}\cdot\vec{\sigma} K_k^\dagger$$

To obtain the new polarization vector associated with ρ'_S, we need to calculate

$$P'_i = Tr\{\sigma_i \rho'_S\},$$

and we arrive to

$$P'_i = c_i + \sum_j M_{ij} P_j,$$

where $\vec{P}$ is the polarization vector corresponding to ρ_S, and

$$M_{ij} = \frac{1}{2}\sum_k Tr\{\sigma_i K_k \sigma_j K_k^\dagger\}$$

$$c_i = \frac{1}{2}\sum_k Tr\{\sigma_i K_k K_k^\dagger\}$$

In other words, we can simply write

$$\vec{P}' = M\vec{P} + \vec{c},$$

where one can prove (Exercise) that both the vector $\vec{c}$ and the matrix M are real. One particular case appears for the so-called unital maps, which are the ones that satisfy

$$\sum_k K_k K_k^\dagger = I.$$

(in addition to $\sum_k K_k^\dagger K_k = I$). For such kind of maps,

$$c_i = \frac{1}{2} Tr\{\sigma_i \sum_k K_k K_k^\dagger\} = \frac{1}{2} Tr\{\sigma_i\} = 0$$

For example, for the phase damping channel, one obtains

$$M = \begin{pmatrix} 1-p & 0 & 0 \\ 0 & 1-p & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \vec{c} = 0,$$

which means that it is an unital map. In other words,

$$\vec{P}' = ((1-p)P_x, (1-p)P_y, P_z),$$

so that the Bloch sphere is contracted along the x and y axis, whereas the z axis remains invariant (see Fig. 3.2).

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 [10]:

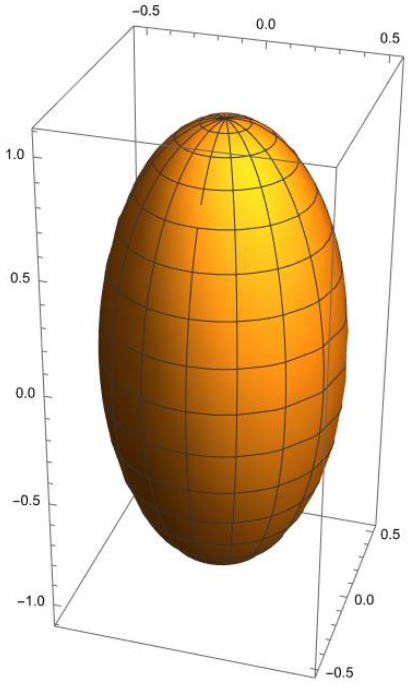

Figure 3.2: Transformation of the Bloch sphere under the phase damping channel.

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. The corresponding Kraus operators are:

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

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:

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

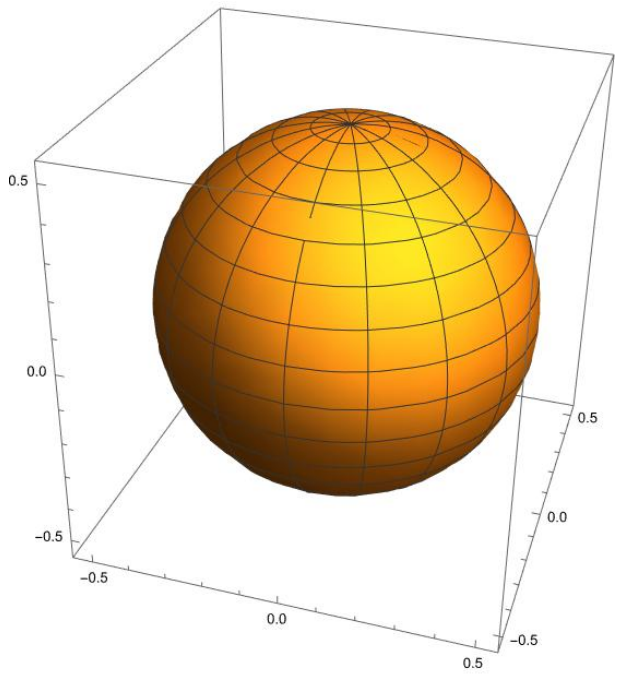

Figure 3.3: Transformation of the Bloch sphere under the depolarizing channel.

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

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 (also know as relaxation time), and "T_2" to denote the exponential decay time for the coherences (known as dephasing time). For the amplitude-damping channel these two times are related by:

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

but, in general, $T_2 \leq 2T_1$.

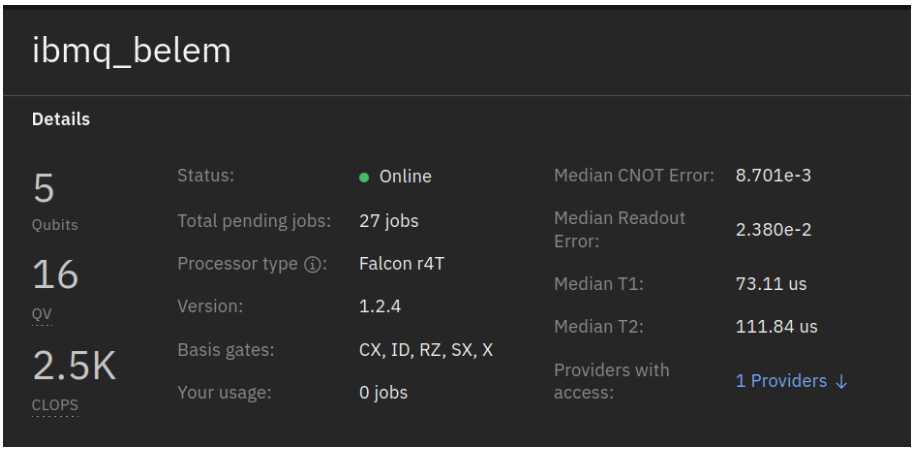

Figure 3.4: Noise characteristics for the IBM quantum processor "Belem". Source: IBM.

Example: Noise on superconducting qubits

As any quantum system, superconducting qubits in quantum computers are subject to noise, which will result in decoherence. There are many factors that contribute to this noise, such as fluctuating charges (quasiparticles, electron hopping, electric dipoles flipping, two level systems...), fluctuating magnetic spins, or fluctuating magnetic vortices. The modelization of this noise is complicated, and we will not describe it here. In Fig. 3.2 we can see some typical data for an IBM quantum processor.

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] Giuliano Benenti, Giulio Casati, Davide Rossini, and Giuliano Strini. *Principles of Quantum Computation and Information: A Comprehensive Textbook*. World Scientific, 2019.

[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] Inés de Vega and Daniel Alonso. Dynamics of non-markovian open quantum systems. *Rev. Mod. Phys.*, 89:015001, Jan 2017.

[6] 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.

[7] 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.

[8] Klaus Mattle, Harald Weinfurter, Paul G. Kwiat, and Anton Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76:4656–4659, Jun 1996.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[10] John Preskill. *Course Information for Physics 219/Computer Science 219 Quantum Computation (Caltech)*.

[11] 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.

[12] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Rev. Mod. Phys.*, 77:1225–1256, Nov 2005.

[13] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.