Quantum Computing

A stochastic guide to understand the (quantum) revolution.

Nahum Sá

January 24, 2020

Contents

0 Quick Recap of Linear Algebra and Dirac Notation 2

1 Quantum Information 5

1.1 Postulates of Quantum Mechanics . . . 5

1.2 Qubit . . . 6

1.3 Density Matrix . . . 6

1.4 Qubit Revisited . . . 9

1.5 Purification . . . 11

1.6 Entanglement . . . 12

1.7 No-go Theorems . . . 12

1.7.1 No communication Theorem . . . 12

1.7.2 No Cloning Theorem . . . 13

1.8 Channels . . . 14

2 Quantum Computing 17

2.1 Quantum Gates . . . 17

2.1.1 One Qubit Gates . . . 17

2.1.2 Two Qubit Gates . . . 19

2.2 Deutsch's Algorithm . . . 19

2.3 Deutsch-Josza Algorithm . . . 20

2.4 Grover's Algorithm . . . 23

2.4.1 Searching for 1 Item on N=4 elements . . . 23

2.4.2 Implementation on Qiskit . . . 25

2.5 Quantum Fourier Transform . . . 26

0 Quick Recap of Linear Algebra and Dirac Notation

In this section I will introduce some concepts of linear algebra that are important to understand quantum mechanics and consequently quantum computing. Full disclosure, I will not be giving a formal definition of everything, for this look at your favorite linear algebra book, my suggestion is the Serge Lang [5] book on linear algebra.

Consider a basis on $\mathbb{R}^2$ given by the vectors:

$$\mathbf{b}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \mathbf{b}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

In quantum mechanics those two vectors are usually represented by the Dirac bra-ket notation:

$$|b_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |b_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2}$$

So now any vector on $\mathbb{R}^2$ is represented by:

$$|\chi\rangle = a\,|b_1\rangle + b\,|b_2\rangle \tag{3}$$

In quantum mechanics is important to introduce its dual, that is the complex conjulgation and the transpose of the ket:

$$|\chi\rangle^\dagger = \left(\,|\chi\rangle^*\,\right)^T = \langle\chi| \tag{4}$$

So by our definition of ket, the bra of the basis defined before is:

$$\langle b_1| = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad \langle b_2| = \begin{pmatrix} 0 & 1 \end{pmatrix} \tag{5}$$

Now we can define the inner product of two vectors:

$$\langle\chi|\beta\rangle = \langle\beta|\chi\rangle^* \in \mathbb{C} \tag{6}$$

For example:

$$\langle b_1|b_1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \tag{7}$$

$$\langle b_1|b_2\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \tag{8}$$

Now we can define the outer product:

$$|b_1\rangle\,\langle b_1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 & 1\cdot 0 \\ 0\cdot 1 & 0\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{9}$$

For a general state:

$$|\psi\rangle\langle\chi| = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix} \begin{pmatrix} \chi_1^* & \chi_2^* & \dots & \chi_N^* \end{pmatrix} = \begin{pmatrix} \psi_1\chi_1^* & \psi_1\chi_2^* & \dots & \psi_1\chi_N^* \\ \psi_2\chi_1^* & \psi_2\chi_2^* & \dots & \psi_2\chi_N^* \\ \vdots & \vdots & \ddots & \vdots \\ \psi_N\chi_1^* & \psi_N\chi_2^* & \dots & \psi_N\chi_N^* \end{pmatrix} \tag{10}$$

Now we can define linear operators in terms of outer products, for instance, every linear operator A on $\mathbb{R}^2$ is defined as:

$$A = a|b_1\rangle\langle b_1| + b|b_1\rangle\langle b_2| + c|b_2\rangle\langle b_1| + d|b_2\rangle\langle b_2| = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{11}$$

Theorem 0.1 (Spectral Theorem)**.** *An hermitian operator $\Phi : \mathcal{H} \to \mathcal{H}$ can always be diagonalized, with its eigenvectors being an orthonormal basis for $\mathcal{H}$ and its eigenvalues being real.*

$$\Phi = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i| \tag{12}$$

Now we define tensor products of kets, on this example this product form an element of a basis on $\mathbb{R}^2 \otimes \mathbb{R}^2$:

$$|b_1\rangle \otimes |b_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{13}$$

Consider a more general case with $|\psi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B$, the tensor product is $|\psi\rangle \otimes |\chi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$:

$$|\psi\rangle \otimes |\chi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_N \end{pmatrix} \otimes \begin{pmatrix} \chi_1 \\ \chi_2 \\ \vdots \\ \chi_M \end{pmatrix} = \begin{pmatrix} \psi_1 \begin{pmatrix} \chi_1 \\ \chi_2 \\ \vdots \\ \chi_M \end{pmatrix} \\ \psi_2 \begin{pmatrix} \chi_1 \\ \chi_2 \\ \vdots \\ \chi_M \end{pmatrix} \\ \vdots \\ \psi_N \begin{pmatrix} \chi_1 \\ \chi_2 \\ \vdots \\ \chi_M \end{pmatrix} \end{pmatrix} \tag{14}$$

1 Quantum Information

This will be a short introduction on quantum information in order to have a theoretical basis to understand most Quantum Algorithms.

1.1 Postulates of Quantum Mechanics

As stated in Aaronson [1], there are two ways of introducing quantum mechanics: The physicist's way explaining the history behind the discovery of quantum theory and stating postulates of quantum theory as an endpoint, or showing that quantum mechanics is a generalization of probability theory. Here I will take the physicist's position and skip the history stuff and introduce the postulates of quantum theory.

The quantum mechanics postulates are, according to Nielsen and Chuang [6]:

1. Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

2. The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2 , $|\psi(t_2)\rangle = U\,|\psi(t_1)\rangle$.

3. Quantum measurements are described by a collection of POVMs $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by:

$$p(m) = \langle\psi|\, M_m^\dagger M_m \,|\psi\rangle \tag{15}$$

   And the system after the measurement is:

$$\frac{M_m\,|\psi\rangle}{\langle\psi|\, M_m^\dagger M_m\,|\psi\rangle} \tag{16}$$

   Where $\sum_m M_m^\dagger M_m = \mathbb{I}$.

4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n: $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \ldots |\psi_n\rangle$

To sum up, the first postulate states that wave functions lives in Hilbert Space, the second one states that evolutions are unitary, the third one states that the wavefunction collapses when it's measured (For a good Everretian this might seems strange) and the final one states that composite systems are described by tensor products.

1.2 Qubit

One qubit is a subspace with two dimensions, that means we can map a qubit to $\mathbf{C}^2$. We can choose a basis in order to span this vector space, we will choose the standard computational basis that will be associated to bits:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; and \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{17}$$

The general state of a qubit is a superposition of those states:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{18}$$

This state can be parameterized by two parameters and construct what we call a "Bloch Sphere":

$$|\psi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} sin\left(\frac{\theta}{2}\right)|1\rangle \tag{19}$$

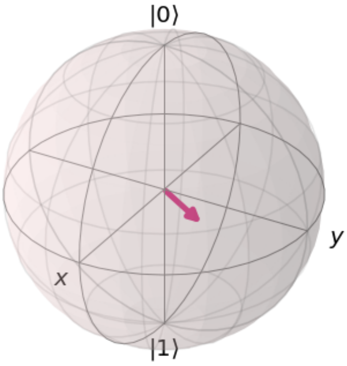


Figure 1: Graphical representation of the Bloch sphere.

1.3 Density Matrix

Density matrix is a generalization of quantum states (For the sake of simplicity, some people call the density matrix of a system the state of a system, because we can always purify it, see Sec 1.5). I will introduce this concept with an example that will be easily generalized.

Consider that you send a state $|+\rangle$ with probability p and a state $|0\rangle$ with probability $(1-p)$, where: $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, how would you describe this state as a ket? No!

Since you do not know which state came out exactly, you need to consider this uncertainty into our formulation, this is done using a density matrix ρ:

$$\rho = p\,|+\rangle\langle+| + (1-p)\,|0\rangle\langle 0| = \frac{p}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + (1-p)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1-\frac{p}{2} & \frac{p}{2} \\ \frac{p}{2} & \frac{p}{2} \end{pmatrix} \tag{20}$$

Let's consider $p = \frac{1}{2}$:

$$\rho = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \tag{21}$$

What is the probability to measure the state $|0\rangle$?

By intuition since we have probability $\frac{1}{2}$ of finding the state on $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and probability $\frac{1}{2}$ of finding the state on $|0\rangle$, the probability of measuring $|0\rangle$ in the state $|+\rangle$ is $\frac{1}{2}$ given by the second postulate of quantum mechanics, therefore the probability is given by:

$$p(0) = \frac{1}{2}\overbrace{\frac{1}{2}}^{|+\rangle} + \frac{1}{2}\overbrace{1}^{|0\rangle} = \frac{3}{4} = \langle 0|\,\rho\,|0\rangle = Tr(\rho\,|0\rangle\,\langle 0|) \tag{22}$$

Exercise 1: What is the probability of measuring the state $|1\rangle$?

Exercise 2: What is the probability of measuring the state $|1\rangle$ or the state $|0\rangle$?

Now we can generalize what a density matrix is. Consider a quantum system with i states $|\psi_i\rangle$ with respective probabilities p_i. The density matrix of this system is given by:

$$\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i| \tag{23}$$

The evolution of a quantum state is given by an unitary transformation U, then the evolution of the density matrix is given by:

$$\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i| \xrightarrow{U} \sum_i p_i U\,|\psi_i\rangle\,\langle\psi_i|\,U^\dagger = U\rho U^\dagger \tag{24}$$

Measurements, as shown above, also can be generalized for the density operator formalism. Suppose the measurement operators M_m. If the initial state was $|\psi_i\rangle$, the probability of measuring m given i is:

$$p(m|i) = \langle\psi_i|\,M_m^\dagger M_m\,|\psi_i\rangle = Tr(M_m^\dagger M_m\,|\psi_i\rangle\,\langle\psi_i|) \tag{25}$$

By the laws of probability:

$$\begin{aligned} p(m) &= \sum_i p(m|i)p_i \\ &= \sum_i p_i\ Tr(M_m^\dagger M_m\,|\psi_i\rangle\,\langle\psi_i|) \\ &= Tr(M_m^\dagger M_m \rho) \end{aligned} \tag{26}$$

Therefore, if you want to know the value of any observable A, you have:

$$\langle A\rangle = Tr(A\rho) \tag{27}$$

The class of operators that are density operators are characterized by the following useful theorem(From [6]):

Theorem 1.1 (Characterization of Density Operators)**.** *An operator ρ is the density operator associated to some ensemble $\{\ p_i\ ,\ |\psi_i\rangle\ \}$ if and only if it satisfies the conditions:*

- ***Unity Trace**: $Tr(\rho) = 1$*
- ***Positivity**: $\rho \geq 0$*

Proof. Suppose $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$. Then

- **Unity Trace**:

$$Tr(\rho) = Tr(\sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|) = \sum_i p_i \overbrace{Tr(\left|\psi_i\right\rangle \left\langle\psi_i\right|)}^{=1} = \sum_i p_i = 1 \tag{28}$$

- **Positivity**: Suppose $|\phi\rangle$ is an arbitrary state. Then:

$$\begin{aligned} \left\langle\phi\right| \rho \left|\phi\right\rangle &= \sum_i p_i \left\langle\phi|\psi_i\right\rangle \left\langle\psi_i|\phi\right\rangle \\ &= \sum_i p_i |\left\langle\phi|\psi_i\right\rangle|^2 \\ &\geq 0 \end{aligned} \tag{29}$$

Now suppose ρ is an operator that the trace is unity and is positive. Since ρ is positive, it must have a spectral decomposition:

$$\rho = \sum_i \lambda_i \left|i\right\rangle \left\langle i\right| \tag{30}$$

From the unity of the trace, we have that $\sum_i \lambda_i = 1$. Therefore, we have the ensemble $\{\ \lambda_i\ ,\ |i\rangle\ \}$ that gives rise to the density operator ρ. □

Question: Can we distinguish between two ensembles?

No! For example the ensembles:

1. $\{\ (\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\ \} \rightarrow\ \rho = \frac{1}{2}(\left|0\right\rangle \left\langle 0\right| + \left|0\right\rangle \left\langle 0\right|) = \frac{\mathbb{1}}{2}$
2. $\{\ (\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\ \} \rightarrow\ \rho = \frac{1}{2}(\left|+\right\rangle \left\langle +\right| + \left|-\right\rangle \left\langle -\right|) = \frac{\mathbb{1}}{2}$

Exercise: Work out the details of the above ensembles.

We can discriminate between two types of states:

- **Pure States**: States that we have complete knowledge.

$$\rho = \left|\psi_i\right\rangle \left\langle\psi_i\right|\ ,\ p_i = 1\ ,\ p_{j\neq i} = 0 \tag{31}$$

- **Mixed States**: States that we do not have complete knowledge.

$$\rho = \sum_i |\psi_i\rangle \langle\psi_i| \tag{32}$$

  With at least two p_i's that are different than 0.

We can quantify the purity of a state using the following measure:

$$P(\rho) = Tr(\rho^2) \tag{33}$$

Example 1 (Pure State): $\rho = |\psi\rangle \langle\psi|$

$$P(|\psi\rangle \langle\psi|) = Tr((|\psi\rangle \langle\psi|)^2) = Tr(|\psi\rangle \overbrace{\langle\psi| |\psi\rangle}^{=1} \langle\psi|) = Tr(|\psi\rangle \langle\psi|) = 1 \tag{34}$$

Example 2 (Mixed State): Since ρ is hermitian we can consider its spectral decomposition $\rho = \sum_i \lambda_i |\phi_i\rangle \langle\phi_i|$, where $\langle\phi_i|\phi_j\rangle = \delta_{ij}$, $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. Therefore:

$$P(\rho) = Tr((\sum_i \lambda_i |\phi_i\rangle \langle\phi_i|)^2) = Tr(\sum_i \sum_j \lambda_i\lambda_j |\phi_i\rangle \overbrace{\langle\phi_i| |\phi_j\rangle}^{=\delta_{ij}} \langle\phi_j|) = Tr(\sum_i \lambda_i^2 |\phi_i\rangle \langle\phi_i|) = \sum_i \lambda_i^2 \leq 1 \tag{35}$$

Exercise: Find the purity of the maximally mixed state $\rho = \mathbb{1}/d$, where d is the dimension of the finite Hilbert Space.

If you tried to do the exercise, you will find that the purity of a d-dimensional state lies between two fixed values $\frac{1}{d} \leq P(\rho) \leq 1$.

1.4 Qubit Revisited

In section 1.2 we introduced the concept of qubits, but we didn't have the density operator formalism yet, now we take a more detailed look on qubits and the bloch sphere.

The density matrix of a qubit is a $2x2$ matrix:

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} = \sum_{i=0}^{1}\sum_{j=0}^{1} \rho_{ij} |i\rangle \langle j| \tag{36}$$

Since it is a density matrix, we have that: $\rho_{00} + \rho_{11} = 1$ and $\rho_{ij}^* = \rho_{ji}$

We can expand the density matrix on the pauli matrices basis: $\mathcal{B}_{2x2} = \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$.

The Pauli Matrices are:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{37}$$

And they have the following properties:

- Hermitian: $\sigma_i = \sigma_i^\dagger$, $\forall i$;
- $Tr(\sigma_i) = 0$, $\forall i \in \{x, y, z\}$;
- $Tr(\sigma_i^\dagger \sigma_j) = 2\delta_{ij}$;
- $\sigma_i\sigma_j = \delta ij\mathbb{1} + i\epsilon_{ijk}\sigma_k$, $i, j, k \in \{x, y, j\}$, in particular $\sigma_i^2 = \mathbb{1}$.

Writing the qubit on the Pauli Matrices basis, we have:

$$\rho = r_0\mathbb{1} + r_1\sigma_x + r_2\sigma_y + r_3\sigma_z \tag{38}$$

Applying the unit trace condition, we have:

$$Tr(\rho) = 1 \Rightarrow 2r_0 = 1 \Rightarrow r_0 = \frac{1}{2} \tag{39}$$

Therefore:

$$\rho = \frac{1}{2}\mathbb{1} + r_1\sigma_x + r_2\sigma_y + r_3\sigma_z \tag{40}$$

Using that the density matrix is Hermitian, we have that:

$$\rho = \rho^\dagger \Rightarrow \frac{1}{2}\mathbb{1} + r_1\sigma_x + r_2\sigma_y + r_3\sigma_z = \frac{1}{2}\mathbb{1} + r_1^*\sigma_x + r_2^*\sigma_y + r_3\sigma_z^* \Rightarrow r_1, r_2, r_3 \in \mathbb{R} \tag{41}$$

We choose $r_1 = \frac{1}{2}r_x$, $r_2 = \frac{1}{2}r_y$, $r_3 = \frac{1}{2}r_z$, then our qubit density matrix is written as:

$$\rho = \frac{1}{2}\Big(\mathbb{1} + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\Big) = \frac{1}{2}\Big(\mathbb{1} + \mathbf{r}\cdot\sigma\Big) \tag{42}$$

Writing as a matrix, we have:

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{pmatrix} \tag{43}$$

So now, in order to know where the state is in the Bloch sphere we just write the density matrix and find r_x, r_y and r_z.

It is interesting to note that pure and mixed states stay on different regions of the Bloch sphere, let's calculate the puryti of an generic qubit:

$$
\begin{aligned}
P(\rho) = Tr(\rho^2) = Tr\Bigg[\bigg(\frac{1}{2}(\mathbb{1} + \mathbf{r}\cdot\sigma\bigg)\Bigg] &= \frac{1}{4}\,Tr\bigg(\mathbb{1} + \mathbf{r}\cdot\sigma\bigg)\bigg(\mathbb{1} + \mathbf{r}\cdot\sigma\bigg) \\
&= \frac{1}{4}\,Tr\bigg(\mathbb{1} + 2\mathbf{r}\cdot\sigma + \sum_{ij} r_i r_j \sigma_i \sigma_j\bigg) \\
&= \frac{1}{4}\,Tr\bigg(\mathbb{1} + 2\mathbf{r}\cdot\sigma + \sum_{i\neq j} r_i r_j \sigma_i \sigma_j + \sum_i r_i^2 \overbrace{\sigma_i^2}^{=\mathbb{1}}\bigg) \\
&= \frac{1}{4}(2 + 2\sum_i r_i^2) = \frac{1}{2}(1 + |\mathbf{r}|^2)
\end{aligned}
\tag{44}
$$

Therefore we have two situations:

- Pure States: If $|\mathbf{r}| = 1$, therefore it is in the spherical shell.
- Mixed States: If $|\mathbf{r}| < 1$, those states are inside the Bloch sphere in a spherical shell("isopure shells").

1.5 Purification

Given a density matrix $\rho_A \in \mathcal{L}(\mathcal{H}_A)$, there always is an pure state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that: $\rho_A = Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$.

For instance, consider $\rho_A = \sum_{i=1}^N p_i |\phi_i\rangle\langle\phi_i|$ with $p_i \geq 0$ and $\sum_{i=1}^N p_i = 1$. We can suppose that there is an orthonormal basis $\{|i\rangle\}_{i=1}^N \in \mathcal{H}_B$, then we can take the pure state as:

$$
|\psi_{AB}\rangle = \sum_{i=1}^N \sqrt{p_i}\,|\phi_i\rangle \otimes |i\rangle \tag{45}
$$

Checking that this is a purification of ρ_A:

$$
\begin{aligned}
Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|) &= Tr_B\big\{\sum_{i,j}\sqrt{p_i p_j}\,|\phi_i\rangle\langle\phi_j| \otimes |i\rangle\langle j|\,\big\} \\
&= \sum_{i,j}\sqrt{p_i p_j}\,|\phi_i\rangle\langle\phi_j|\,\overbrace{Tr\big(\,|i\rangle\langle j|\,\big)}^{\delta_{ij}} \\
&= \sum_i p_i\,|\phi_i\rangle\langle\phi_i| \\
&= \rho_A
\end{aligned}
\tag{46}
$$

It is important to note that there are infinite purifications for the density matrix $\rho_A \in \mathcal{L}(\mathcal{H}_A)$.

Theorem 1.2 (Non unicity of purifications). *If $|\psi_{AB}\rangle$ is such that $\rho_A = Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$, then $\mathbb{1} \otimes U_B|\psi_{AB}\rangle$ is also a valid purification with $U_B^\dagger U_B = \mathbb{1}$.*

Proof. Suppose that $\rho_A = Tr_B(|\psi_{AB}\rangle \langle\psi_{AB}|)$, then:

$$\begin{aligned}
&Tr_B\big\{(\mathbb{1}\otimes U_B)\,|\psi_{AB}\rangle\langle\psi_{AB}|\,(\mathbb{1}\otimes U_B^\dagger)\big\} = \\
&Tr_B\big\{\,|\psi_{AB}\rangle\langle\psi_{AB}|\,(\mathbb{1}\otimes U_B^\dagger)(\mathbb{1}\otimes U_B)\big\} = \\
&Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|) = \rho_A
\end{aligned} \tag{47}$$

Where we used the cyclic property of the trace. □

1.6 Entanglement

Definition 1.1 (Product State)**.** A given state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be a product state if $\exists\,|\phi\rangle \in \mathcal{H}_A$ and $\exists\,|\chi\rangle \in \mathcal{H}_B$, such that: $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$.

Example 1 (Product State): Consider the following state:

$$\begin{aligned}
|\psi\rangle =& \frac{1}{2}\bigg(\,|00\rangle + |01\rangle\bigg) \\
=& \frac{1}{2}\bigg(\,|0\rangle \otimes (|0\rangle + |1\rangle))\bigg)
\end{aligned} \tag{48}$$

Definition 1.2 (Entangled State)**.** A given state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be entangled if $\nexists\,|\phi\rangle \in \mathcal{H}_A$ and $\nexists\,|\chi\rangle \in \mathcal{H}_B$, such that: $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$.

Example 1 (Entangled State): Consider the following state:

$$\begin{aligned}
|\psi\rangle =& \frac{1}{2}\bigg(\,|00\rangle + |01\rangle + |10\rangle - |11\rangle\bigg) \\
=& \frac{1}{2}\bigg(\,|0\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)\bigg)
\end{aligned} \tag{49}$$

1.7 No-go Theorems

1.7.1 No communication Theorem

Consider that you have a composite physical system with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and those states are finite dimensional. A general state on $\mathcal{H}$ is given by: $\rho = \sum_i \sigma_i \otimes \omega_i$, where $\sigma_i \in \mathcal{L}(\mathcal{H}_A)$ and $\omega_i \in \mathcal{L}(\mathcal{H}_B)$.

The observer in A makes a measurement only on her subsystem:

$$P(\rho) = \sum_j (K_j \otimes \mathbb{1}_B)^\dagger \rho (K_j \otimes \mathbb{1}_B) \tag{50}$$

Where K_j are Kraus Operators(See 1.8) with the property: $\sum_j K_j K_j^\dagger = \mathbb{1}$.

Now the state for an observer in B is given by the partial trace over A:

$$\rho_B = Tr_A(P(\rho)) \tag{51}$$

So let's see if there is any difference on the B state:

$$\begin{aligned}
\rho_B &= Tr_A(\sum_j (K_j \otimes \mathbb{1}_B)^\dagger \rho (K_j \otimes \mathbb{1}_B)) \\
&= Tr_A(\sum_i \sum_j K_j^\dagger \sigma_i K_j \otimes \omega_i) \\
&= \sum_i \sum_j Tr(K_j^\dagger \sigma_i K_j) \otimes \omega_i \\
&= \sum_i Tr(\overbrace{\sum_j K_j K_j^\dagger}^{=\mathbb{1}} \sigma_i) \otimes \omega_i \\
&= \sum_i Tr(\sigma_i) \otimes \omega_i \\
&= Tr_A(\rho)
\end{aligned} \tag{52}$$

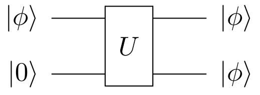
Since the state before and after the local operations are indistinguishable for B, an observer in A doesn't have a way to communicate with and observer in B by using local operations. **There is no faster than light communication on Quantum Mechanics!**.

1.7.2 No Cloning Theorem

Theorem 1.3 (No cloning Theorem)**.** *There is no unitary U acting on $\mathcal{H} \otimes \mathcal{H}$ such that for all $|\phi\rangle \in \mathcal{H}$ we have:*

$$U |\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle \tag{53}$$

This theorem can be represented by the following circuit:



Proof. This theorem is prooved by contradiction. Suppose that exists this unitary, so given $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, we have that:

$$\begin{aligned}
U |\phi\rangle \otimes |0\rangle &= |\phi\rangle \otimes |\phi\rangle \\
U |\psi\rangle \otimes |0\rangle &= |\psi\rangle \otimes |\psi\rangle
\end{aligned} \tag{54}$$

Taking the scalar product:

$$\begin{aligned}(\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) &= (\langle\phi| \otimes \langle 0| U^{\dagger})(U|\psi\rangle \otimes |0\rangle)\\ \langle\phi|\psi\rangle \langle\psi|\phi\rangle &= \langle\phi|\psi\rangle \langle 0|0\rangle\\ \Rightarrow \langle\phi|\psi\rangle^2 &= \langle\phi|\psi\rangle\end{aligned} \tag{55}$$

This is a equation $x^2 - x = 0$, so there are two possible solutions:

- $\langle\phi|\psi\rangle = 0$, therefore $|\phi\rangle$, $|\psi\rangle$ are ortogonal;
- $\langle\phi|\psi\rangle = 1$, therefore $|\phi\rangle$, $|\psi\rangle$ are identical;

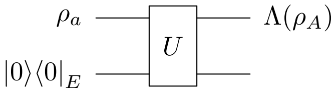
This is a contradiction, because we supposed that U would work for every state.

□

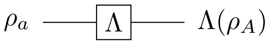
The No-Cloning theorem is really important in Quantum Cryptography. Because you cannot clone quantum states, it is impossible for a eavesdropper to hear your communication without you knowing. See BB84 Protocol [4].

1.8 Channels

Suppose a system with an environment state on a global unitary $U : \mathcal{H}_A \otimes \mathcal{H}_B \rightarrow \mathcal{H}_A \otimes \in H_B$:



or



So we throw away the E part because we are only interested on part A. Therefore we will trace out the environment E:

$$\lambda(\rho_A) = Tr_B(U\rho_A \otimes |0\rangle\langle 0|_E U^{\dagger}) \tag{56}$$

Let's derive the formula for this channel:

$$U = \sum_{k,l,m,n} U^{kl}_{mn} |kl\rangle\langle mn| \tag{57}$$

Using equation 57 on equation 56:

$$\begin{aligned}
\Lambda(\rho_A) =& \sum_i (\mathbb{1}\otimes\langle i|)\left[\sum_{k,l,m,n} U^{kl}_{mn}\,|kl\rangle\langle mn|\,(\rho_A\otimes|0\rangle\langle 0|_E)\left(\sum_{r,s,p,q}U^{rs}_{pq}\,|rs\rangle\langle pq|\right)^\dagger\right](\mathbb{1}\otimes|i\rangle)\\
=& \sum_i (\mathbb{1}\otimes\langle i|)\left[\sum_{k,l,m,n} U^{kl}_{mn}\,|kl\rangle\langle mn|\,(\rho_A\otimes|0\rangle\langle 0|_E)\left(\sum_{r,s,p,q}(U^{rs}_{pq})^*\,|pq\rangle\langle rs|\right)\right](\mathbb{1}\otimes|i\rangle)\\
=& \sum_i\sum_{k,l,m,n}\sum_{r,s,p,q} U^{kl}_{mn}(U^{rs}_{pq})^*\,|k\rangle\langle m|\,\rho_A\,|p\rangle\langle r|\otimes\langle i|l\rangle\,\langle n|0\rangle\,\langle 0|q\rangle\,\langle s|i\rangle\\
=& \sum_i\sum_{k,m}\sum_{r,p} U^{ki}_{m0}(U^{ri}_{p0})^*\,|k\rangle\langle m|\,\rho_A\,|p\rangle\langle r|\\
=& \sum_i\left(\sum_{k,m}U^{ki}_{m0}\,|k\rangle\langle m|\right)\rho_A\left(\sum_{r,p}U^{ri}_{p0}\,|p\rangle\langle r|\right)^\dagger\\
\equiv& \sum_i K_i\rho_A K_i^\dagger
\end{aligned}\tag{58}$$

Then we define the Kraus Operator $K_i:\mathcal{H}_A\to\mathcal{H}_A$:

$$K_i=\sum_{k,m}U^{ki}_{m0}\;\;|k\rangle\langle m| = \langle i|_E\,U\,|0\rangle_E \tag{59}$$

Properties of quantum channels:

- Linearity:

$$\Lambda(\sum_j p_j\rho_j)=\sum_i K_i(\sum_j p_j\rho_j)K_i^\dagger=\sum_j\left(\sum_i K_i\rho_jK_i^\dagger\right)=\sum_j p_j\Lambda(\rho_j) \tag{60}$$

- Preserves Hermicity: If $\rho=\rho^\dagger\Rightarrow\Lambda(\rho)^\dagger=\Lambda(\rho)$

$$\Lambda(\rho)^\dagger=\left(\sum_i K_i\rho K_i^\dagger\right)^\dagger=\sum_i K_i\rho K_i^\dagger=\Lambda(\rho) \tag{61}$$

- Preserves the Trace:

$$Tr(\Lambda(\rho))=Tr(\sum_i K_i\rho K_i^\dagger)=Tr(\sum_i K_i^\dagger K_i\rho) \tag{62}$$

Using $K_i=\langle i|_B\,U\,|0\rangle_B$, we have that:

$$\sum_i K_i^\dagger K_i=\sum_i\langle 0|_B\,U^\dagger\,|i\rangle_B\,\langle i|_B\,U\,|0\rangle_B=\langle i|_B\,U^\dagger U\,|0\rangle_B=\langle i|_B\,|0\rangle_B=\mathbb{1}_A \tag{63}$$

Therefore:

$$Tr(\Lambda(\rho))=Tr(\rho) \tag{64}$$

- Preserves Positivity: $\rho \geq 0 \Rightarrow \Lambda(\rho) \geq 0$

$$\Lambda(\rho) = \sum_i K_i \rho K_i^\dagger = \sum_i K_i \sqrt{\rho}\sqrt{\rho} K_i^\dagger \tag{65}$$

Then, $\forall \left|\psi\right\rangle$:

$$\left\langle\psi\right| \Lambda(\rho) \left|\psi\right\rangle = \sum_i \left\langle\psi\right| K_i \sqrt{\rho}\sqrt{\rho} K_i^\dagger \left|\psi\right\rangle = \sum_i || \sqrt{\rho} K_i \left|\psi\right\rangle || \geq 0 \tag{66}$$

But in order to define an physically valid quantum channel, we have that the channel must return states even when applied to subsystems.

Channels which $\forall n \in \mathbb{N} : \Lambda \otimes \mathbb{1}_n(\rho) \geq 0$ are said to be Completely Positive Maps.

2 Quantum Computing

Now we will focus on Quantum Computing and Algorithms for the Circuit model.

2.1 Quantum Gates

2.1.1 One Qubit Gates

Since everything must be done in the realm of Quantum Mechanics the one qubit gates should be unitary 2x2 matrices, following the 2nd postulate.

The first gate is the *Hadamard Gate*, defined as the matrix:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{67}$$

This gate changes the computational basis $\{0, 1\}$ (Z basis) to a new basis: $\{+, -\}$ (X basis).

$$\begin{aligned} H\left|0\right\rangle &= \frac{1}{\sqrt{2}}\big(\left|0\right\rangle + \left|1\right\rangle\big) \equiv \left|+\right\rangle \\ H\left|0\right\rangle &= \frac{1}{\sqrt{2}}\big(\left|0\right\rangle - \left|1\right\rangle\big) \equiv \left|-\right\rangle \end{aligned} \tag{68}$$

Another important property of the Hadamard gate is that $H^2 = \mathbb{1}$, so the inverse transformation is the Hadamard gate itself, $H^\dagger = H$.

The next gate is the *Phase Shift Gate*:

$$R_z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \tag{69}$$

This gate adds a phase only if the state is $\left|1\right\rangle$, Therefore for a general state $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$:

$$R_z(\delta)\left|\psi\right\rangle = \alpha\left|0\right\rangle + e^{i\delta}\beta\left|1\right\rangle \tag{70}$$

Since this is a relative phase, it is observed when you measure on the Z basis.

It is important to notice that every single qubit unitary operation can be made by only Phase Shift and Hadamard Gates: For instance:

$$R_z(\frac{\pi}{2} + \phi) H R_z(\theta) H \left|0\right\rangle = e^{i\frac{\theta}{2}}\big(cos\frac{\theta}{2}\left|0\right\rangle + e^{i\phi}\left|1\right\rangle\big) \tag{71}$$

Let's show this:

$$
\begin{aligned}
R_z(\frac{\pi}{2}+\phi)HR_z(\theta)H\left|0\right\rangle =&R_z(\frac{\pi}{2}+\phi)HR_z(\theta)\frac{1}{\sqrt{2}}\big(\left|0\right\rangle+\left|1\right\rangle\big)\\
=&R_z(\frac{\pi}{2}+\phi)H\frac{1}{\sqrt{2}}\big(\left|0\right\rangle+e^{i\theta}\left|1\right\rangle\big)\\
=&R_z(\frac{\pi}{2}+\phi)\frac{1}{2}\big((\left|0\right\rangle+\left|1\right\rangle)+e^{i\theta}(\left|0\right\rangle-\left|1\right\rangle)\big)\\
=&R_z(\frac{\pi}{2}+\phi)e^{i\frac{\theta}{2}}\big(cos\frac{\theta}{2}\left|0\right\rangle-isin\frac{\theta}{2}\left|1\right\rangle)\big)\\
=&e^{i\frac{\theta}{2}}\big(cos\frac{\theta}{2}\left|0\right\rangle-e^{i\frac{\pi}{2}}e^{i\phi}isin\frac{\theta}{2}\left|1\right\rangle)\big)\\
=&e^{i\frac{\theta}{2}}\big(cos\frac{\theta}{2}\left|0\right\rangle+e^{i\phi}sin\frac{\theta}{2}\left|1\right\rangle)\big)
\end{aligned}
\tag{72}
$$

The most general class of 1 qubit unitary transformation are the rotations of the Bloch Sphere. Consider an operator $\mathcal{O}$ such that $\mathcal{O}^2=\mathbb{1}$ and the Taylor expansion of the following operator:

$$
e^{-i\alpha\mathcal{O}}=\left[1-\frac{1}{2!}\alpha^2+\dots\right]\mathbb{1}-i\left[\alpha-\frac{1}{3!}\alpha^3+\dots\right]\mathcal{O}=cos\ \alpha\ \mathbb{1}-isin\ \alpha\ \mathcal{O}
\tag{73}
$$

So if you want to rotate counter clockwise about the Z direction, we use the Pauli Z matrix:

$$
e^{-i\frac{\delta}{2}Z}=cos\ \frac{\delta}{2}\ \mathbb{1}-isin\ \frac{\delta}{2}\ Z=e^{-i\frac{\delta}{2}}\begin{pmatrix}1&0\\0&e^{i\delta}\end{pmatrix}\equiv R_z(\delta)
\tag{74}
$$

This is the same definition given above for the phase shift gate with a global phase that can be ignored because it is of no physical significance.

If you want to rotate counter clockwise about the X direction, we use the Pauli X matrix:

$$
e^{-i\frac{\delta}{2}X}\equiv R_x(\delta)
\tag{75}
$$

If you want to rotate counter clockwise about the Y direction, we use the Pauli Y matrix:

$$
e^{-i\frac{\delta}{2}Y}\equiv R_y(\delta)
\tag{76}
$$

A rotation counter clockwise about an arbitrary direction can be done combining rotations about X,Y and Z axis:

$$
R_n(\epsilon)\approx R_x(n_x\epsilon)R_y(n_y\epsilon)R_z(n_z\epsilon)
\tag{77}
$$

The taylor expansion gives:

$$
R_n(\epsilon)\approx\mathbb{1}-i\frac{\epsilon}{2}(\mathbf{n}\cdot\sigma)
\tag{78}
$$

Then we have that:

$$R_n(\delta) = cos\ \frac{\delta}{2}\ \mathbb{1} - isin\ \frac{\delta}{2}\ (\mathbf{n} \cdot \sigma) \tag{79}$$

We can see that the Hadamard gate written in terms of rotations is written with $\delta = \pi$ and $\tilde{n} = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$:

$$H = \frac{1}{\sqrt{2}}(Z + X) \tag{80}$$

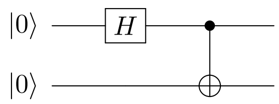
This transformation rotates the X-axis to Z and vice versa.

2.1.2 Two Qubit Gates

The most important two qubit gate is the Controled-NOT(C-NOT) gate. The *C-NOT* is a generalization of a XOR classic gate:

$$CNOT\,|A\rangle\,|B\rangle = |A\rangle\,|B \oplus A\rangle \tag{81}$$

This gate is responsible for entanglement in Circuit Quantum Computing. It is easy to show that using this gate we can construct an entangled state given by the following circuit:



In the first part we have:

$$|\psi_0\rangle = |00\rangle \tag{82}$$

After the Hadamard gate on the first qubit:

$$|\psi_1\rangle = H \otimes \mathbb{1}\,|\psi_0\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes |0\rangle \tag{83}$$

Applying the CNOT gate:

$$|\psi_2\rangle = \text{CNOT}\,|\psi_1\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle \otimes |0 \oplus 0\rangle + |1\rangle \otimes |0 \oplus 1\rangle\,\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \tag{84}$$

So, using the CNOT gate we have just created an entangled state also known as one of the bell states.

2.2 Deutsch's Algorithm

Problem: Consider an oracle evaluating a 1 bit boolean function $f : \{0, 1\} \to \{0, 1\}$ we want to know if the function is constant ($f(0) = 0$ and $f(1) = 1$) or balanced ($f(0) = 1$ and $f(1) = 0$).

For a classical computer it is needed two queries, that means, you need to test 2 diferent bits and see the outputs, for instance if $f(0) = 0$ and $f(1) = 1$ you know that the function is constant.

For a quantum computer this can be done with only one query. This is done with the Deutsch algorithm, the idea is to check if it is balanced, if it is not balanced it is constant.

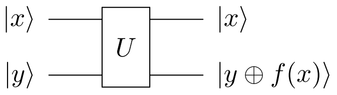
Solution: The Deutsch's Algorithm is the following:

1. Start with the state $|\psi\rangle = |10\rangle$:
2. Apply a Hadamard on both qubits, the state will be: $|\psi_2\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)$
3. Apply a Unitary operator such that: $U_f \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|x\rangle = (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|x\rangle$. The phase factor is "kicked back" on the front of the state, this will be useful to evaluate $f(x)$ with only one query. The state after U_f is: $|\psi_3\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes \left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)$
4. Apply a Hadamard on the first Qubit: $|\psi_3\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes \left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right]$

So now if $f(0) = f(1)$ we will measure $|0\rangle = |f(0) \bigoplus f(1)\rangle$ and if $f(0) \neq f(1)$ we will measure $|1\rangle = |f(0) \bigoplus f(1)\rangle$.

In this implementation the oracle (U_f) is a C-NOT gate, this will measure if the function is balanced.

This can be extended for a function with more inputs, not only two. In this case, the solution is the Deutsch–Jozsa Algorithm.



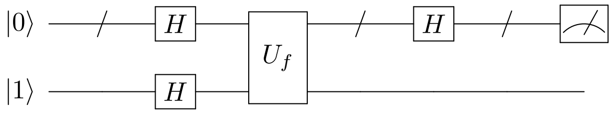
2.3 Deutsch-Josza Algorithm

In the Deutsch's Algorithm we had only 1 bit boolean function, for the Deutsch-Josza case, we have a N bit boolean function $f : \{0,1\}^N \to \{0,1\}$, where f is constant or balanced:

- f is constant if $\forall x \in \{0,1\}^N$, $f(x) = b \in \{0,1\}$
- f is balanced if $f(x) = b$ for half of the inputs and $f(x) = b \oplus 1$ for the other half.

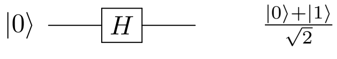
Classicaly, for a deterministic algorithm, it is needed $\frac{2^N}{2} + 1 = 2^{N-1} + 1$ queries.

The Deutsch-Josza Algorithm is represented by the following circuit:

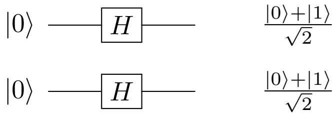


The slash on the circuit represent N qubits. Observe that:

For 1 qubit:



For 2 qubits:



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

Therefore, for N qubits we have a combination of all possible strings:

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} |x\rangle \tag{85}$$

So in the first step of the algorithm, we have:

$$|\psi_0\rangle = |0\rangle^{\otimes N} |1\rangle \tag{86}$$

After the Hadamard gates:

$$|\psi_1\rangle = H^{\otimes N+1} |\psi_0\rangle = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \tag{87}$$

In the next step we use the oracle as on the Deutsch's Algorithm, since the oracle must be linear, we only need to check one term of the sum:

$$U_f |x\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = \frac{|x\rangle |0 \oplus f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle}{\sqrt{2}} \tag{88}$$

We have two cases:

- If $f(x) = 0$, then:

$$U_f |x\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{89}$$

- If $f(x) = 1$, then:

$$U_f |x\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{-|0\rangle + |1\rangle}{\sqrt{2}} \right) = -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{90}$$

We can represent both cases by:

$$U_f |x\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{91}$$

Therefore, after the Oracle:

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{92}$$

Before the next step, observe that:

$$\begin{aligned} H\left|0\right\rangle &= \frac{(-1)^{0\cdot 0}\left|0\right\rangle + (-1)^{0\cdot 1}\left|0\right\rangle}{\sqrt{2}} \\ H\left|1\right\rangle &= \frac{(-1)^{1\cdot 0}\left|0\right\rangle + (-1)^{1\cdot 1}\left|0\right\rangle}{\sqrt{2}} \end{aligned} \tag{93}$$

Therefore:

$$H\left|b\right\rangle = \sum_{b'=0}^{1} \frac{(-1)^{b\odot b'}\left|b'\right\rangle}{\sqrt{2}} \tag{94}$$

Where $\odot$ is the bitwise sum.

Now we can apply the Haddamard gate to all N qubits:

$$\begin{aligned} \left|\psi_3\right\rangle =& H^{\otimes N}\otimes \mathbb{1}\left|\psi_2\right\rangle = \frac{1}{2^{N/2}}\sum_{x_1,\dots,x_N=0}^{1}(-1)^{f(x)}H\left|x_1\right\rangle\otimes H\left|x_2\right\rangle\otimes\cdots\otimes H\left|x_N\right\rangle\otimes\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right) \\ =& \frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\left(\sum_{z_1=0}^{1}\frac{(-1)^{z_1\cdot x_1}\left|z_1\right\rangle}{\sqrt{2}}\right)\otimes\left(\sum_{z_2=0}^{1}\frac{(-1)^{z_2\cdot x_2}\left|z_2\right\rangle}{\sqrt{2}}\right)\otimes\cdots\otimes\left(\sum_{z_N=0}^{1}\frac{(-1)^{z_N\cdot x_N}\left|z_N\right\rangle}{\sqrt{2}}\right)\otimes\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right) \\ =& \frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\sum_{z=0}^{2^N-1}(-1)^{z_1\cdot x_1+\cdots+z_N\cdot x_N}\left|z_1\dots z_N\right\rangle\otimes\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right) \end{aligned} \tag{95}$$

Therefore:

$$\left|\psi_3\right\rangle = \frac{1}{2^N}\sum_{x=0}^{2^N-1}\sum_{z=0}^{2^N-1}(-1)^{f(x)}(-1)^{z\odot x}\left|z\right\rangle\otimes\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right) \tag{96}$$

The probability to measure $\left|00\dots00\right\rangle$ is given by:

$$Pr(00\dots00) = \left|\frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}\right|^2 \tag{97}$$

We have two cases as before:

- If f is constant:

$$\sum_{x=0}^{2^N-1}(-1)^{f(x)} = (-1)^{f(x)}2^N \tag{98}$$

  Therefore: $Pr(00\dots00) = 1$

- If f is balanced:

$$\sum_{x=0}^{2^N-1}(-1)^{f(x)} = \frac{1}{2}\sum_{x=0}^{(2^N-1)/2}1 - \frac{1}{2}\sum_{x=0}^{(2^N-1)/2}1 = 0 \tag{99}$$

  Therefore: $Pr(00\dots00) = 0$

So we know that the function is constant if we measure $|00\dots00\rangle$, any other result the function is balanced. Since with only one query we can know if the function is constant or balanced, we have an exponential gain compared with the classical deterministic case.

2.4 Grover's Algorithm

Grover's algorithm is useful for searching an unstructured database with N elements. For instance, you have a phone number and want to find the corresponding name associated to this phone number, since it is unstructured you need to check every element (in the worst case scenario), but if you have the solution it is easy to check, this shows that the problem is NP.

In order to show Grover's algorithm we need to rephrase as an oracle problem: Labelling each element of the database $\{0,1,\dots,N-1\}$ and x_0 the unknown marked item. The oracle f computes the following binary function:

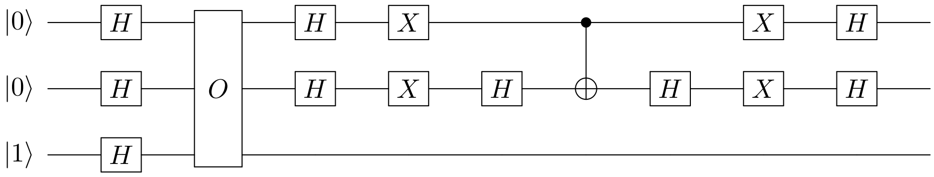
$$f:\{0,1\}^N \to \{0,1\} \quad , \quad \text{with} \qquad f(x)=\begin{cases}1, & \text{if } x=x_0\\ 0, & \text{otherwise}\end{cases} \tag{100}$$

For a classical computer, the probability to find x_0 is $\frac{1}{N}$, so to find x_0 with probability p is needed $pN=\mathcal{O}(N)$ oracle queries. Grovers showed that on a quantum computer we can have a quadratic speedup, then we will need $\mathcal{O}(\sqrt{N})$ queries. This is not massive, but we can compare this speedup with the breakthrough that Fast Fourier Transform(FFT) did for signalling processing.

To understand the more general algorithm we start with an example:

2.4.1 Searching for 1 Item on N=4 elements

The circuit for this example is(Reference [3]):



So we start with two qubits in the state $|00\rangle$ and an ancilliary state $|1\rangle$:

$$|\psi_0\rangle = |00\rangle\,|1\rangle \tag{101}$$

Then we apply in all qubits Hadamard gates in order to have all possible bit strings:

$$|\psi_1\rangle = H^{\otimes 3}\,|\psi_0\rangle = \frac{1}{2}\big(\,|00\rangle+|01\rangle+|10\rangle+|11\rangle\,\big)\frac{1}{\sqrt{2}}\big(\,|0\rangle-|1\rangle\,\big) \tag{102}$$

The oracle query works to mark down the searched state:

$$O\,|x\rangle\,|y\rangle = |x\rangle\,|y\oplus f(x)\rangle \tag{103}$$

Since the ancillary state is $\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$ it is the same if $f(x) = 0$ but changes sign if $f(x) = 1$. Suppose the item that we are searching is $x_0 = (1, 0) \to |10\rangle$, after the oracle query we have:

$$|\psi_2\rangle = O\,|\psi_1\rangle = \frac{1}{2}\big(\,|00\rangle + |01\rangle - |10\rangle + |11\rangle\,\big)\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \tag{104}$$

This is the same process of kicking back the sign that we have on the Deutsch's Algorithm. Since the ancillary state is the same, we will ignore it on the calculation.

Since in Quantum Mechanics the probability of measuring a state is the absolute value squared we cannot distinguish between the four state superposition. The first part of the algorithm is to mark the state that we are interested and the last part is to amplify its probability to be measured.

This is done by means of the unitary transformation:

$$D_{ij} = -\delta_{ij} + \frac{2}{2^N} \tag{105}$$

For $N = 2$, we have that:

$$D = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \tag{106}$$

It is usually not easy to find the circuit representation of unitary transformations, but after some work and some experience we can decompose D:

$$D = H^{\otimes 2}\; D'\; H^{\otimes 2} \tag{107}$$

Where D' is:

$$D' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{108}$$

This is a controlled phase shift through an angle π in the coefficient in front of the basis element $|00\rangle$. Again we need to decompose D':

$$D' = X^{\otimes 2}\; (I \otimes H)\; CNOT\; (I \otimes H)\; X^{\otimes 2} \tag{109}$$

This comes from the $CMINUS$ gate, that is:

$$CMINUS = (I \otimes H)\ CNOT\ (I \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{110}$$

The NOT (X) gates places the phase factor in front of the $|00\rangle$ instead of the $|11\rangle$.

So applying D on our state $|\psi_2\rangle$, we have:

$$D\ \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{111}$$

So if we measure the two qubits, we have that the outcome will be $|10\rangle$ with 100% certainty.

For a Classical algorithm we would need on average $N_c = \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{2} \cdot 3 = 2.25$ queries. In the Quantum algorithm we would only need one query, thus $N_Q = 1$.

2.4.2 Implementation on Qiskit

Here I will follow the Qiskit Book [2] and we will focus on the implementation for $N = 4$ as the example before, but the algorithm implementation is not hard to scale up for any N.

The first part of the algorithm is to build an oracle that marks the desired state, let's consider the marked up state $|11\rangle$.

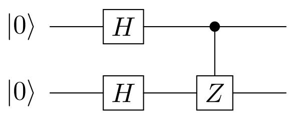
Therefore, we need that the oracle acts as follows:

$$O\,|s\rangle = O\ \frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big) = \frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\Big) \tag{112}$$

This is the same as a controled Z gate, that means if your first qubit is $|1\rangle$, then you apply an Z operator on the seccond qubit:

$$\text{CZ} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes Z \tag{113}$$

Therefore, the circuit for this part is:



The next part is the amplitude augmentation, since the only the sign is changed, there is no difference between this state and the state with all superpositions upon measurement. We need to grow the marked state probability to be measured.

This can be done by the reflection: $D = 2\,|s\rangle\langle s| - \mathbb{1}$. As shown on the previous section, we have that: $D = H^{2\otimes} D' H^{2\otimes}$, where:

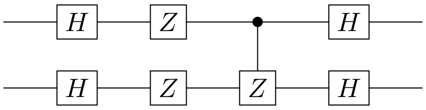
$$D' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{114}$$

Therefore:

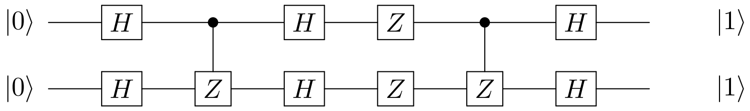
$$D' |s\rangle = \frac{1}{2}\Big(|00\rangle - |01\rangle - |10\rangle - |11\rangle \Big) \tag{115}$$

We know that the state $|00\rangle$ is the only one that changes the sign and we also know that we can change the sign of $|11\rangle$ by an CZ gate. The other signs can be changed using Z gates on each qubit, because $Z|i\rangle = (-1)^i |i\rangle$.

Therefore the circuit for the reflection is the following:



Now we have our full circuit:



The qiskit implementation is on the following notebook.

2.5 Quantum Fourier Transform

Fourier transform is a very important tool to signal processing.

Here we will build a quantum version of a discrete fourier transform, this will be used in many quantum algorithms.

Discrete fourier transform is the map between two strings $F : (x_0, x_1, \ldots, x_{N-1}) \to ((y_0, y_1, \ldots, y_{N-1}))$.

$$F(x_k) = y_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x_l \omega_N^{lk} \tag{116}$$

Where: $\omega_N^{lk} = exp\left(2\pi i \frac{lk}{N}\right)$

Quantum Fourier transform does the same thing, but using quantum states: $F : \sum_{i=0}^{N-1} x_i |i\rangle \to \sum_{i=0}^{N-1} y_i |i\rangle$

$$F(x_k) = y_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x_l \omega_N^{lk} \tag{117}$$

Where: $\omega_N^{lk} = exp\left(2\pi i \frac{lk}{N}\right)$

This can be represented by an unitary matrix:

$$F = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega_N^{lk} \left| y \right\rangle \left\langle x \right| \tag{118}$$

To find the circuit representation of the Fourier transform we need to see how it works on 2^N qubits first:

$$\begin{aligned} F\left(\left| m \right\rangle_n\right) &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{km} \left| k \right\rangle_n \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} exp\left(i\frac{2\pi}{N}mk\right) \left| k \right\rangle_n \\ &= \frac{1}{\sqrt{N}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} exp\left(i\frac{2\pi}{N}m\sum_{l=1}^{n}\frac{k_{n-l}}{2^l}\right) \left| k_{n-1}\dots k_0 \right\rangle_n \\ &= \frac{1}{\sqrt{N}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} \bigotimes_{l=1}^{n} exp\left(i\frac{2\pi}{N}m\frac{k_{n-l}}{2^l}\right) \left| k_{n-l} \right\rangle_n \\ &= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[\left|0\right\rangle + exp\left(i\frac{2\pi m}{2^l}\right)\left|1\right\rangle\right] \end{aligned} \tag{119}$$

Now we use the binary representation of $\frac{m}{2^l}$:

$$\begin{aligned} \frac{m}{2^l} &= \sum_{p=1}^{n} m_{n-p}2^{n-p-l} = m_{n-1}2^{n-1-l} + \cdots + m_l 2^0 + \cdots + m_0 2^{-l} \equiv m_{n-1}\dots m_l.m_{l-1}\dots m_0 \\ &= \sum_{p=1}^{n-l} m_{n-p}2^{n-p-l} + \sum_{p=1}^{l}\frac{m_{l-p}}{2^l} \end{aligned} \tag{120}$$

Therefore:

$$exp\left[i\frac{2\pi m}{2^l}\right] = exp\left[i2\pi\sum_{p=1}^{n-l} m_{n-p}2^{n-p-l}\right] exp\left[i2\pi\sum_{p=1}^{l}\frac{m_{l-p}}{2^l}\right] = exp\left[i2\pi\sum_{p=1}^{l}\frac{m_{l-p}}{2^l}\right] \tag{121}$$

Now, we have that:

$$F(\left|m\right\rangle_n) = \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left[\left|0\right\rangle + exp\left[i2\pi\sum_{p=1}^{l}\frac{m_{l-p}}{2^l}\right]\left|1\right\rangle\right] \tag{122}$$

Consider first acting on 2 qubits(n=2):

$$\begin{aligned} F(\left|m\right\rangle_n) &= \frac{1}{\sqrt{4}} \bigotimes_{l=1}^{2} \left[\left|0\right\rangle + exp\left[i2\pi\sum_{p=1}^{l}\frac{m_{l-p}}{2^l}\right]\left|1\right\rangle\right] \\ &= \frac{1}{2}\left[\left|0\right\rangle + exp\left[i2\pi 0.m_0\right]\left|1\right\rangle\right] \otimes \left[\left|0\right\rangle + exp\left[i2\pi 0.m_1 m_0\right]\left|1\right\rangle\right] \end{aligned} \tag{123}$$

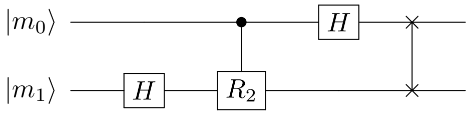
Consider the following gate:

$$\begin{aligned} R_k^{(0,1)} \left| m \right\rangle \left| 0 \right\rangle &= \left| 0 \right\rangle \\ R_k^{(0,1)} \left| m \right\rangle \left| 1 \right\rangle &= exp\left[i2\pi \frac{m}{2^k} \right] \left| 1 \right\rangle \end{aligned} \tag{124}$$

We can write the QFT as:

$$F = SWAP[H^{(0)} R_2^{(0,1)} H^{(1)} \left| m \right\rangle_2] \tag{125}$$

Where the SWAP gate changes the order of the qubits. This is represented by the following circuit:



This can be easily generalized for n qubits.

References

[1] Scott Aaronson. *Quantum Computing Since Democritus.* Cambridge University Press, New York, NY, USA, 2013.

[2] Abraham Asfaw, Luciano Bello, Yael Ben-Haim, Sergey Bravyi, Lauren Capelluto, Almudena Carrera Vazquez, Jack Ceroni, Jay Gambetta, Shelly Garion, Leron Gil, Salvador De La Puente Gonzalez, David McKay, Zlatko Minev, Paul Nation, Anna Phan, Arthur Rattew, Javad Shabani, John Smolin, Kristan Temme, Madeleine Tod, and James Wootton. Learn quantum computation using qiskit, 2019.

[3] Giuliano Benenti, Giulio Casati, and Giuliano Strini. *Principles of Quantum Computation and Information.* WORLD SCIENTIFIC, 2004.

[4] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014.

[5] Serge Lang. *Introduction to Linear Algebra.* Springer New York, 1986.

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