

A. KELLER

UNIVERSITÉ PARIS-SACLAY

QUANTUM COMPUTATION *LECTURE NOTES*

MASTER PHYSICS OF COMPLEX SYSTEMS

Contents

1	<i>Quantum mechanics of isolated systems</i>	5
2	<i>Qubits and quantum gates</i>	21
3	<i>Some Quantum Algorithms</i>	35
4	<i>Appendix</i>	51
5	<i>Bibliography</i>	53

1

Quantum mechanics of isolated systems

IN THIS CHAPTER we will recall basic concepts of quantum mechanics. We will restrict to an isolated system which evolution is unitary. In this context we will recall how the measurement process is formalized. We end this chapter introducing the density operator describing non-pure state, the reduction and purification processes. This allows to present the Schmidt decomposition and solve the problem of characterizing the entanglement of pure states.

1.1 States space

The states of an isolated system are the unit vectors $|\psi\rangle$ in an Hilbert space \mathcal{H} :

$$|\psi\rangle \in \mathcal{H}; \langle\psi|\psi\rangle = 1.$$

Remark. — This definition is not exactly correct as $|\psi'\rangle = e^{i\phi}|\psi\rangle$ describes the same state as $|\psi\rangle$. One way to circumvent this ambiguity is to consider that the state of a system is given by the rank-one projection operator $\rho = |\psi\rangle\langle\psi|$, acting on \mathcal{H} . Indeed we have: $|\psi\rangle\langle\psi| = |\psi'\rangle\langle\psi'|$. The operator ρ is called the density operator, or the density matrix. We will see more on this later in the course (see section 1.7, page 13).

Example. — The minimal system is a qubit, that is a 2-dimensional system. The states $|\psi\rangle$ can be considered as unit vectors in \mathbb{C}^2 . Let $\{|0\rangle, |1\rangle\}$ an orthonormal basis, then an arbitrary qubit state can be written as

$$|\psi\rangle = a|0\rangle + b|1\rangle; \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1.$$

Once the basis has been fixed, the state can be written as a 2-rows vector $\begin{pmatrix} a \\ b \end{pmatrix}$.

The density matrix $\rho = |\psi\rangle\langle\psi|$ is given by :

$$|\psi\rangle\langle\psi| = |a|^2 |0\rangle\langle 0| + |b|^2 |1\rangle\langle 1| + ab^* |0\rangle\langle 1| + a^*b |1\rangle\langle 0|$$

where a^* is the complex conjugate of a . Once the basis $\{|0\rangle, |1\rangle\}$ has been fixed, the density matrix can be written as the 2×2 matrix: $\begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}$.

1.2 Unitary evolution

The evolution of an isolated system from time t_1 to time t_2 is described by a unitary operator $U(t_2, t_1)$:

$$|\psi(t_2)\rangle = U(t_2, t_1)|\psi(t_1)\rangle$$

with the following properties :

$$UU^\dagger = U^\dagger U = \mathbb{1}; \quad [U(t_2, t_1)]^\dagger = U(t_1, t_2).$$

where $\mathbb{1}$ represents the identity operator on \mathcal{H} . The generator of the evolution is the Hamiltonian, an hermitian operator H , such that

$$i\hbar \frac{d}{dt} U(t, t_1) = H(t)U(t, t_1),$$

this equation is the Schrodinger equation. When the systems is isolated, H does not depend on time t and

$$U(t_2, t_1) = e^{-iH(t_2-t_1)}.$$

1.3 Measurements

1.3.1 Projective measurement

Let O an observable, that is an hermitian operator ($O^\dagger = O$) on \mathcal{H} . It can be written as :

$$O = \sum_n \lambda_n P_n,$$

where λ_n are the eigenvalues of O and P_n is the projector on the eigenspace corresponding to eigenvalue λ_n . As O is hermitian, $\lambda_n \in \mathbb{R}$ and the projectors are orthogonal: $P_n P_m = \delta_{nm} P_n$. Furthermore, they form a complete decomposition of \mathcal{H} , that is $\sum_n P_n = \mathbb{1}$.

When a measurement of the observable O is performed on the system in the state $|\psi\rangle$

- **The outcome** is one of the eigenvalues λ_n of O .
- **The probability** p_n to obtain this outcome λ_n is given by

$$p_n = \langle \psi | P_n | \psi \rangle \tag{1.1}$$

- **The state** $|\psi_n\rangle$ after the measurement becomes

$$|\psi_n\rangle = \frac{1}{\sqrt{p_n}} P_n |\psi\rangle \quad (1.2)$$

the factor $\frac{1}{\sqrt{p_n}}$ ensures the normalization of $|\psi_n\rangle$.

Exercise 1. — Show that if the state is described by the density matrix $\rho = |\psi\rangle\langle\psi|$ then the probability p_n of the outcome λ_n is given, by

$$p_n = \text{Tr}[P_n \rho]$$

where $\text{Tr}[A]$ is the trace of the operator A .

Show that the state ρ_n after the measurement is given by

$$\rho_n = \frac{1}{p_n} P_n \rho P_n.$$

Some immediate consequences of the projective measurement definition are:

- The probability to obtain the outcome λ_n is equal to one, if and only the state $|\psi\rangle$ is an eigenvector of O corresponding to the eigenvalue λ_n . In that case

$$(\Delta O)_{|\psi\rangle} \equiv \langle\psi|O^2|\psi\rangle - \langle\psi|O|\psi\rangle^2 = 0.$$

- **Heisenberg inequality:** if A and B are 2 observables such that $[A, B] \neq 0$ ($[A, B] = AB - BA$) then A and B can not share a common basis of eigenvectors, and we have

$$(\Delta A)_{|\psi\rangle} (\Delta B)_{|\psi\rangle} \geq \frac{1}{2} |\langle\psi|[A, B]|\psi\rangle| \quad (1.3)$$

The meaning of this relation is: if we prepare a large number of quantum systems in the state $|\psi\rangle$ and we perform a measurement of A on half of them and a measurement of B on the others, then the standard deviations ΔA and ΔB satisfy the Heisenberg inequality.

- To specify a measurement, rather than giving an observable O , we can give the list of orthogonal projectors P_n such that $P_n P_m = \delta_{nm} P_n$ and $\sum_n P_n = \mathbb{1}$. In this case, the implicit observable is $O = \sum_m m P_m$, and the values taken by m are the possible outcomes. We also say that "the measurement is performed in the basis $|m\rangle$ ", where $|m\rangle$ form an orthonormal basis of \mathcal{H} , and it is equivalent to the specification the set of projectors $P_m = |m\rangle\langle m|$.

- **Projective measurements are repeatable:** If a first measurement of O gives the outcomes λ_n , the a second measurement of O will give the same outcome with certainty (with probability $p_n = 1$).

Remark. — often in real experiments measurements are not repeatable. A large class of measurement are destructive; the quantum system is destroyed by the measurement. For instance, the absorption of a photon by a photocathode, or the detection of an atom by ionization.

1.3.2 Generalized measurement

To answer the question posed by the last remark, the description of the measurement is generalized as follows.

A quantum measurement in which outcomes are the N real values λ_m ($m = 1, 2, \dots, N$) is described by N measurement operators M_m (which are not required to be hermitian) such that

$$\sum_{m=1}^N M_m^\dagger M_m = \mathbb{1}. \quad (1.4)$$

- **The probability** p_n to obtain the outcome λ_n is given by

$$p_n = \langle \psi | M_n^\dagger M_n | \psi \rangle. \quad (1.5)$$

The requirement given by Eq. (1.4) ensures that $\sum_{n=1}^N p_n = 1$.

- **The state** $|\psi_n\rangle$ after the measurement becomes

$$|\psi_n\rangle = \frac{1}{\sqrt{p_n}} M_n |\psi\rangle. \quad (1.6)$$

The factor $\frac{1}{\sqrt{p_n}}$ ensures the normalization of $|\psi_n\rangle$.

Remark. — These rules constitute a generalization of the projective measurement. Indeed, replacing operators M_n by a complete set of orthogonal projectors P_n gives us the usual rules of projective measurement.

Example (Photon count detector). — The electronic current induced by the light received by the detector is proportional to the number of photons. The photons are destroyed by this measurement device. This destructive measurement can be described by the operator

$$M_n = |vac\rangle \langle n|,$$

where $|n\rangle$ is the state of n photons and $|vac\rangle$ is the vacuum state of the quantum electromagnetic field.

Exercise 2. — Show that M_n is a plausible measurement operator describing a photocount detector.

1.3.3 POVM

When we are not interested about the state after the measurement, it is sufficient to specify a set of N positive¹ operators E_m ($m = 1, 2, \dots, N$), one for each possible outcomes, satisfying

$$\sum_{m=1}^N E_m = \mathbb{1}. \quad (1.7)$$

The probability p_n to obtain the outcome n , when the state of the systems is $|\psi\rangle$ is given by

$$p_n = \langle \psi | E_m | \psi \rangle, \quad (1.8)$$

and Eq. (1.7) ensures that $\sum_{m=1}^N p_m = 1$. The set of N operators E_m ($m = 1, 2, \dots, N$), is called a Positive Operator Valued Measure (POVM).

Remarks:

Relations between POVM, generalized and projective measurements:

- If we know the measurement operator M_m defined in section 1.3.2 then we can define a POVM as the set $E_m = M_m^\dagger M_m$. Indeed the operators $M_m^\dagger M_m$ are hermitian and positive and as the operators M_m satisfy Eq. (1.4) then the set of operator E_m fulfills Eq. (1.7).
- At the contrary, from the POVM E_m we can always define measurement operators $M_m = \sqrt{E_m}$. The square root can be defined in the following way: $\sqrt{E_m} = U_m^{-1}(\Lambda_m)^{\frac{1}{2}}U_m$, where U_m is the unitary operator which diagonalizes E_m and Λ_m is the diagonal matrix defined by $\Lambda_m = U_m E_m U_m^{-1}$.
This definition is not unique, and given an arbitrary set of unitaries V_m , the set of operators M'_m such that $M'_m = V_m M_m$ will do the job. That is $M_m'^\dagger M'_m = E_m$.
But $M_m = U_m^{-1}(\Lambda_m)^{\frac{1}{2}}U_m$ are the only hermitian operators such that $M_m^\dagger M_m = E_m$.
- A projective measurement is a particular case of a POVM with $E_m = P_m$.
- A projective measurement is a particular case of a generalized measurement with $M_m = P_m$.

Example (State discrimination). — Suppose that Alice encode a message using 2 states $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $\langle \psi_1 | \psi_2 \rangle \neq 0$. She send $|\psi_1\rangle$ or $|\psi_2\rangle$ to Bob. To decode the message Bob needs to discriminate which states $|\psi_1\rangle$ and $|\psi_2\rangle$ Alice sent.

¹ A positive operator is an hermitian operator with a positive spectrum.

Suppose that he tries to discriminate with certainty using a POVM with 2 elements E_1 and E_2 , such that $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and $\langle \psi_2 | E_2 | \psi_2 \rangle = 1$. We will show that this is not possible.

Indeed, as $\langle \psi_1 | E_1 | \psi_1 \rangle = 1$ and $E_1 \geq 0$ then there is a positive operator A such that

$$E_1 = |\psi_1\rangle\langle\psi_1| + A \text{ and } A|\psi_1\rangle = 0$$

but then

$$\langle \psi_2 | E_1 | \psi_2 \rangle = |\langle \psi_1 | \psi_2 \rangle|^2 + \langle \psi_2 | A | \psi_2 \rangle \geq |\langle \psi_1 | \psi_2 \rangle|^2 > 0$$

We conclude that due to the non-orthogonality of $|\psi_1\rangle$ and $|\psi_2\rangle$ Bob will sometimes makes an error in the state identification.

It is possible to perform an unambiguous state discrimination at the cost of rejecting some of the measurement outcomes which are identified as non conclusive. This can be done as follows. Consider the POVM with 3 elements:

$$\begin{aligned} E_1 &= p |\psi_2^\perp\rangle\langle\psi_2^\perp| \\ E_2 &= p |\psi_1^\perp\rangle\langle\psi_1^\perp| \\ E_3 &= 1 - E_1 - E_2 \end{aligned}$$

where $p > 0$ and $\langle \psi_i | \psi_i^\perp \rangle = 0$, ($i = 1, 2$).

Let see how it works. Suppose that the state is $|\psi_1\rangle$ with probability $p_1 = p |\langle \psi_1 | \psi_2^\perp \rangle|^2$ Bob will obtain the outcome $m = 1$, and with probability $p_3 = 1 - p |\langle \psi_1 | \psi_2^\perp \rangle|^2$ he will obtain the outcome $m = 3$. He will never obtain $m = 2$, that is $p_2 = 0$.

Now, if the state is $|\psi_2\rangle$ then the measurement outcomes are $m = 2$ with probability $p_2 = p |\langle \psi_2 | \psi_1^\perp \rangle|^2$ and $m = 3$ with probability $p_3 = 1 - p |\langle \psi_2 | \psi_1^\perp \rangle|^2$. The outcome $m = 1$ never occurs, that is $p_1 = 0$.

Considering the outcomes $m = 3$ as non conclusive and rejecting them, allows a unambiguous states discrimination. The rate of rejection is $1 - p (|\langle \psi_2 | \psi_1^\perp \rangle|^2 + |\langle \psi_1 | \psi_2^\perp \rangle|^2)$

Exercise 3. — Show that for $\mathcal{H} = \mathbb{C}^2$, that is for 2 qubit states discrimination, the maximum value of p is $(1 + |\langle \psi_1 | \psi_2 \rangle|)^{-1}$.

1.4 Composite systems

The state space of a composite system is the tensor product of the spaces of each system.

If the states of the system S_1 are in \mathcal{H}_1 and those of system S_2 are in \mathcal{H}_2 then the states of $S_1 \cup S_2$ are in $\mathcal{H}_1 \otimes \mathcal{H}_2$. Let $|\psi_i\rangle$ ($i = 1, 2, \dots, N$)

an orthonormal basis of \mathcal{H}_1 and $|\phi_j\rangle$ ($j = 1, 2, \dots, M$) an orthonormal basis of \mathcal{H}_2 ; then the $N \times M$ states

$$|\chi_{ij}\rangle = |\psi_i\rangle \otimes |\phi_j\rangle \quad (i = 1, 2, \dots, N; j = 1, 2, \dots, M)$$

constitute an orthonormal basis of $\mathcal{H}_1 \otimes \mathcal{H}_2$. The dimension of $\mathcal{H}_1 \otimes \mathcal{H}_2$ is the product of the dimensions of \mathcal{H}_1 and \mathcal{H}_2 .

Exercise 4. — Let $\mathcal{H}_1 = \mathcal{H}_2 = \mathbb{C}^2$. and $\{|0\rangle, |1\rangle\}$ an orthonormal basis of \mathbb{C}^2 . Calculate the expectation value of the operator $X \otimes Z$ for the state $\frac{1}{\sqrt{2}}[|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle]$, where the matrix representations of X and Z in the $\{|0\rangle, |1\rangle\}$ basis are:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

1.4.1 Entangled states

There are states in $\mathcal{H}_1 \otimes \mathcal{H}_2$ which can not be written as a product $|\psi_1\rangle \otimes |\psi_2\rangle$ of states in \mathcal{H}_1 and \mathcal{H}_2 , respectively.

For instance the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle] \in \mathbb{C}^2 \otimes \mathbb{C}^2$$

is entangled. How to determine that a state is entangled ? We will address this question later on.

1.5 No cloning theorem

This theorem prevent the copy of an arbitrary (unknown in advance) quantum state.

Theorem 1 (No cloning). — Let's \mathcal{H}_A and \mathcal{H}_B two Hilbert spaces. The theorem says that there is no unitary operation ² that can perform the following operation:

$$|\psi\rangle_A \otimes |e\rangle_B \rightarrow |\psi\rangle_A \otimes |\psi\rangle_B, \forall |\psi\rangle_A \in \mathcal{H}_A$$

where $|e\rangle_B$ is some initial state in \mathcal{H}_B .

Proof. Suppose that there is an unitary operator U , and let's a pair of states $|\psi\rangle$ and $|\phi\rangle$. We can use U to clone both states, so

$$U[|\psi\rangle_A \otimes |e\rangle_B] = e^{i\alpha(|\psi\rangle, |e\rangle)} |\psi\rangle_A \otimes |\psi\rangle_B \quad (1.9)$$

$$U[|\phi\rangle_A \otimes |e\rangle_B] = e^{i\alpha(|\phi\rangle, |e\rangle)} |\phi\rangle_A \otimes |\phi\rangle_B \quad (1.10)$$

$$(1.11)$$

² The theorem is more general and prohibits the cloning for all quantum operations

where α is a real number depending on the two input states.

Computing the scalar product of the two states, we have

$$\langle e| \otimes \langle \phi| U^\dagger U |\psi\rangle_A \otimes |e\rangle_B = e^{i(\alpha(\langle \phi|\psi\rangle, |e\rangle) - \alpha(\langle \phi|, |e\rangle))} |\langle \phi|\psi\rangle|^2$$

as U is unitary, we obtain:

$$|\langle \phi|\psi\rangle| = |\langle \phi|\psi\rangle|^2$$

Hence, there are only two possibilities: $|\langle \phi|\psi\rangle| = 1$ or $|\langle \phi|\psi\rangle| = 0$. In the first case, both elements represents the same state, that $\exists \beta \in \mathbb{R}; |\phi\rangle = e^{i\beta}|\psi\rangle$. In the second case, both states are orthogonal. \square

1.6 Naimark theorem

The Naimark theorem provides a link between the projective measurement and the POVM measurement. It says that

Theorem 2 (Naimark). — *Any POVM measurement can be considered as a projective measurement in an enlarged Hilbert space.*

Proof. Let E_i ($i = 1, 2, \dots, N$) a POVM. (positive operators on \mathcal{H} such that $\sum_{i=1}^N E_i = \mathbb{1}$). Let $|i\rangle$ ($i = 1, 2, \dots, N$) an orthonormal basis of an ancilla Hilbert space \mathcal{A} .

Consider the isometry $U : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{A}$ such that

$$\forall |\psi\rangle \in \mathcal{H}; \quad U|\psi\rangle = \sum_{i=1}^N \sqrt{E_i} |\psi\rangle \otimes |i\rangle$$

It is not difficult to prove that the projective measurement on the basis $|i\rangle$ corresponding to the set of operators $P_i = \mathbb{1} \otimes |i\rangle\langle i|$ on $\mathcal{H} \otimes \mathcal{A}$ is equivalent to the POVM E_i on \mathcal{H} .

Indeed, using the rule of projective measurements on $\mathcal{H} \otimes \mathcal{A}$, we have that the probability p_i to obtain the outcome i when the state is $U|\psi\rangle$, is given by

$$\langle \psi| U^\dagger P_i U |\psi\rangle = \sum_{i,j} \left[\langle \psi| \sqrt{E_j} \otimes \langle j| \right] \left[\sqrt{E_i} |\psi\rangle \otimes |i\rangle \right] = \langle \psi| E_i |\psi\rangle$$

\square

Remark. — U is indeed an isometry as it preserves the norm. Let $|\psi\rangle \in \mathcal{H}$ and let $|\Phi\rangle = U|\psi\rangle$, then

$$\begin{aligned} \langle \Phi|\Phi\rangle &= \sum_{i,j} \langle \psi| \sqrt{E_j} \sqrt{E_i} |\psi\rangle \langle j|i\rangle = \sum_{i,j} \langle \psi| \sqrt{E_j} \sqrt{E_i} |\psi\rangle \delta_{ij} = \sum_i \langle \psi| E_i |\psi\rangle \\ &= \langle \psi| \sum_i E_i |\psi\rangle = \langle \psi| \mathbb{1} |\psi\rangle = \langle \psi|\psi\rangle \end{aligned}$$

Another way to see that, is to remark that $U^\dagger : \mathcal{H} \otimes \mathcal{A} \rightarrow \mathcal{H}$ is defined as $U^\dagger = \sum_i \sqrt{E_i} \otimes \langle i|$. Computing $U^\dagger U$ we obtain

$$U^\dagger U = \sum_{ij} \sqrt{E_j} \sqrt{E_i} \langle j|i \rangle = \sum_i E_i = \mathbb{1}$$

In fact, we can write

$$U^\dagger (\mathbb{1} \otimes |i\rangle\langle i|) U = E_i$$

check that.

1.7 Density operator – Ensemble of quantum states

The density operator (or density matrix) is a convenient way to describe the relevant features of a statistical ensemble of systems. Suppose that we have an ensemble \mathcal{E} of quantum systems. We have a probabilistic description as follows: with probability p_i the system is in state $|\psi_i\rangle$ ($i = 1, 2, \dots, N$). If we perform a projective measurement of the observable $O = \sum_{k=1}^M \lambda_k P_k$, then we expect to obtain the eigenvalue λ_k with probability $P_{\mathcal{E}}(\lambda_k)$ given by:

$$P_{\mathcal{E}}(\lambda_k) = \sum_{i=1}^N p_i \langle \psi_i | P_k | \psi_i \rangle$$

where P_k is the projector on the eigenspace corresponding to the eigenvalue λ_k .

We can check that

$$\sum_{k=1}^M P_{\mathcal{E}}(\lambda_k) = \sum_{i=1}^N p_i \langle \psi_i | \sum_{k=1}^M P_k | \psi_i \rangle = \sum_{i=1}^N p_i \langle \psi_i | \psi_i \rangle = \sum_{i=1}^N p_i = 1$$

It is convenient to write the probability $P_{\mathcal{E}}(\lambda_k)$ as:

$$P_{\mathcal{E}}(\lambda_k) = \text{Tr} [P_k \rho_{\mathcal{E}}] \text{ with } \rho_{\mathcal{E}} = \sum_{i=1}^N p_i |\psi_i\rangle\langle\psi_i|.$$

The density operator $\rho_{\mathcal{E}}$ describes the statistical mixture of quantum states $|\psi_i\rangle$ ($i = 1, 2, \dots, N$).

If the density operator has only one term, $\rho_{\mathcal{E}} = |\psi\rangle\langle\psi|$, we say that the state of the system is pure. If there is more than one terms we often say that the state of the system is a "mixed state" or a mixture. But this is a shortcut, and one must remember that the density operator describe a statistical ensemble of systems.

This statistical description often occurs because we lack some information about the system. For instance, there can be some noisy fluctuations in the apparatus that prepare the system. In more general terms, this lack of information come from an interaction of the considered system with another systems which properties are only partially known. We will address this problem later on the course.

Definition (Density operator). — *The density operator ρ on the Hilbert space \mathcal{H} , is a positive-semidefinite operator on \mathcal{H} with unit trace.*

$$\langle \psi | \rho | \psi \rangle \geq 0 \forall |\psi\rangle \in \mathcal{H} \text{ and } \text{Tr} [\rho] = 1.$$

1.7.1 Properties of the density operator

1. The density operator is hermitian. This is a property of positive-semidefinite operators on separable Hilbert space.
2. The density operator can be written as a convex combination of pure states

$$\sum_i p_i |\psi_i\rangle \langle \psi_i|; \text{ with } 0 \leq p_i \leq 1 \text{ and } \sum_i p_i = 1.$$

where the $|\psi_i\rangle$ are not required to be orthogonal.

3. As ρ is hermitian it can be made diagonal. The spectral representation of the density operator reads:

$$\rho = \sum_k \lambda_k |k\rangle \langle k|$$

where the $|k\rangle$ are the eigenvectors that constitutes an orthonormal basis and the eigenvalues λ_k are positive and $\text{Tr} [\rho] = \sum_k \lambda_k = 1$.

4. If $\text{Tr} [\rho^2] = 1$ then the state is pure, otherwise $\text{Tr} [\rho^2] < 1$ and the state is a mixture. Indeed, as $\sum_k \lambda_k = 1$, then $\sum_k \lambda_k^2 \leq 1$ and the equality occurs only if there is only one eigenvalue $\lambda = 1$. But, $\text{Tr} [\rho^2] = \sum_k \lambda_k^2$, hence $\text{Tr} [\rho^2] \leq 1$, and $\text{Tr} [\rho^2] = 1$ if and only if there is only one eigenvalue $\lambda = 1$. We conclude that ρ is pure if and only if $\rho^2 = \rho$.

Definition (Purity). — *$\text{Tr} [\rho^2]$ is the purity of the state ρ on the Hilbert space \mathcal{H} . we have*

$$\frac{1}{N} \leq \text{Tr} [\rho^2] \leq 1$$

where N is the dimension of \mathcal{H} . $\text{Tr} [\rho^2] = 1$ when ρ is a pure state and $\text{Tr} [\rho^2] = \frac{1}{N}$ when ρ is the maximally mixed state $\rho = \frac{1}{N} \mathbb{1}$.

1.7.2 Generalized measurement and density operator

Suppose that the state of the system ensemble \mathcal{E} is described by the density operator $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ and let M_m the measurement operators.

1. **Probability of the outcome m :**

When the system is in the pure state $|\psi_i\rangle$, in accordance with Eq. (1.5), the probability that the outcome is m is given by

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = \text{Tr} \left[M_m^\dagger M_m |\psi_i\rangle \langle \psi_i| \right].$$

Therefore the probability to obtain the outcome m for the ensemble \mathcal{E} is

$$p(m) = \sum_i p(m|i) p_i = \sum_i p_i \text{Tr} \left[M_m^\dagger M_m |\psi_i\rangle \langle \psi_i| \right] = \text{Tr} \left[M_m^\dagger M_m \sum_i p_i |\psi_i\rangle \langle \psi_i| \right]$$

which finally can be written as

$$p(m) = \text{Tr} \left[M_m^\dagger M_m \rho \right] = \text{Tr} \left[M_m \rho M_m^\dagger \right] = \text{Tr} \left[\rho M_m^\dagger M_m \right] \quad (1.12)$$

where we have used the property of the trace: $\text{Tr} [AB] = \text{Tr} [BA]$.

2. **State after the measurement outcome** Let $|\psi_i^m\rangle$ the state after the measurement when the state before the measurement was the pure state ψ_i then, using Eq. (1.6), we can write

$$|\psi_i^m\rangle = \frac{1}{\sqrt{p(m|i)}} M_m |\psi_i\rangle$$

The density operator ρ_m describing the state of the ensemble after the measurement when the outcome is m can then be written as

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle \psi_i^m|,$$

therefore:

$$\rho_m = \sum_i \frac{p(i|m)}{p(m|i)} M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger$$

but the joint probability $p(m, i) = p(m|i) p_i = p(i|m) p_m$ hence

$$\rho_m = \sum_i \frac{p_i}{p_m} M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger = \frac{1}{p_m} M_m \left(\sum_i p_i |\psi_i\rangle \langle \psi_i| \right) M_m^\dagger$$

and as $p_m = \text{Tr} [M_m \rho M_m^\dagger]$, finally

$$\rho_m = \frac{1}{\text{Tr} [M_m \rho M_m^\dagger]} M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger \quad (1.13)$$

1.7.3 Density operator of a subsystem – Partial trace

Let 2 quantum systems A and B , whose pure states are in the Hilbert space \mathcal{H}^A and \mathcal{H}^B respectively. We consider an ensemble \mathcal{E} of quantum systems $S = A \cup B$. The quantum states of this ensemble are described by a density operators ρ^{AB} on $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$.

The reduced operator ρ^A on \mathcal{H}^A is defined as:

$$\rho^A = \text{Tr}_B [\rho^{AB}]$$

where the partial trace over B can be defined using an orthonormal basis $\{|k\rangle\} \in \mathcal{H}^B$ as

$$\text{Tr}_B [\rho^{AB}] = \sum_k \langle k | \rho^{AB} | k \rangle.$$

If ρ^{AB} is a product state, $\rho^{AB} = \rho^A \otimes \rho^B$ then

$$\text{Tr}_B [\rho^A \otimes \rho^B] = \text{Tr} [\rho^B] \rho^A = \rho^A$$

The reduced state ρ^A describes all the observations that can be obtained by measuring the subsystem A only.

Indeed, Let $O^A = \sum_\lambda \lambda P_\lambda^A$ an observable on \mathcal{H}^A , where P_λ^A is the projector on the eigenspace corresponding to the eigenvalue λ . Then on $\mathcal{H}^A \otimes \mathcal{H}^B$ we can define the observable $O = O^A \otimes \mathbb{1} = \sum_\lambda \lambda P_\lambda$, where $P_\lambda = P_\lambda^A \otimes \mathbb{1}$.

The probability p_λ that the outcome is λ when the measurement of observable O^A is performed on a system in the state $\rho \in \mathcal{H}^A \otimes \mathcal{H}^B$ is given by

$$p_\lambda = \text{Tr} [P_\lambda \rho] = \text{Tr} [(P_\lambda^A \otimes \mathbb{1}) \rho] = \text{Tr}_A [P_\lambda^A \text{Tr}_B [\rho]] = \text{Tr}_A [P_\lambda^A \rho^A]$$

Example. — We have seen that when ρ is a product state $\rho = \rho^A \otimes \rho^B$ then

$$\text{Tr}_A [\rho^A \otimes \rho^B] = \rho^B, \text{ and } \text{Tr}_B [\rho^A \otimes \rho^B] = \rho^A$$

Suppose that in addition to be a product, ρ is a pure state, that is

$$\rho = |\psi^A\rangle\langle\psi^A| \otimes |\psi^B\rangle\langle\psi^B|$$

then the reduced states are also pure,

$$\text{Tr}_A [\rho] = |\psi^B\rangle\langle\psi^B| \text{ and } \text{Tr}_B [\rho] = |\psi^A\rangle\langle\psi^A|$$

Now consider the entangled state $|\psi\rangle$ defined as

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2$$

where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis of \mathbb{C}^2 . The corresponding density operator is $\rho = |\psi\rangle\langle\psi|$. Computing the partial trace we obtain:

$$\text{Tr}_A [\rho] = \text{Tr}_B [\rho] = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \mathbb{1}.$$

Check that.

We see that the reduced state is a mixture, it is the maximal mixed state.

The reverse is also true: if the reduced state ρ^A (or ρ^B) is a mixture then the state ρ is entangled.

Theorem 3 (Pure entangled states characterization). — *A bipartite pure state is entangled if and only if its reduced state is not pure.*

The purity of the reduced state ρ^A (or ρ^B) is a measure of the entanglement of the pure state $\rho = |\psi\rangle\langle\psi|$.

1.8 Schmidt decomposition

The Schmidt decomposition provides a specific answer to the question of determining if a pure state is entangled. Moreover, it provides an entanglement measure, that characterizes the amount of entanglement carried by a pure state.

Theorem 4 (Schmidt decomposition). — *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, a state of a bipartite system AB . There are 2 orthonormal bases $|i\rangle_A$ ($i = 1, 2, \dots, N_A$) and $|j\rangle_B$ ($j = 1, 2, \dots, N_B$) of \mathcal{H}_A and \mathcal{H}_B respectively, such that $|\psi\rangle$ can be written as*

$$|\psi\rangle = \sum_{k=1}^{\min(N_A, N_B)} \lambda_k |k\rangle_A \otimes |k\rangle_B \text{ with } \lambda_k \geq 0. \quad (1.14)$$

Definition (Schmidt coefficient and Schmidt rank). — *The coefficients λ_k are called the Schmidt coefficients. The number of non zero Schmidt coefficients is called the Schmidt rank (or Schmidt number).*

Remark. — *The Schmidt decomposition is very peculiar and different from the usual expansion using 2 arbitrary orthonormal bases of \mathcal{H}_A and \mathcal{H}_B :*

$$|\psi\rangle = \sum_{ij} c_{ij} |i\rangle_A \otimes |j\rangle_B$$

indeed, here the coefficients c_{ij} are complex numbers and the number of coefficients is the product of the \mathcal{H}_A and \mathcal{H}_B dimensions. In the Schmidt decomposition the coefficients λ_k are positive real numbers and the number of those coefficients are at most the smallest of the \mathcal{H}_A and \mathcal{H}_B dimensions.

Proof. Let $\{|a_i\rangle (i = 1, 2, \dots, N_A)\}$ and $\{|b_j\rangle (j = 1, 2, \dots, N_B)\}$ two orthonormal bases of \mathcal{H}_A and \mathcal{H}_B , respectively. The decomposition of $|\psi\rangle$ reads:

$$|\psi\rangle = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} M_{ij} |a_i\rangle \otimes |b_j\rangle.$$

Define the $N_A \times N_B$ matrix M , with complex matrix elements M_{ij} . By the singular decomposition of M , there exist a $N_A \times N_A$ unitary matrix U , a $N_B \times N_B$ unitary matrix V and a diagonal positive $N_B \times N_B$ matrix D , such that

$$M = U \begin{pmatrix} D \\ 0 \end{pmatrix} V^\dagger. \quad (1.15)$$

where we have supposed that $N_A \geq N_B$ and O is a $N_A \times N_B$ zero matrix.

Let $\lambda_k (k = 1, 2, \dots, N_B)$ the diagonal element of D (the singular values of M) then Eq. (1.15) can be written as

$$M_{ij} = \sum_{k=1}^{N_B} U_{ik} \lambda_k V_{kj}^\dagger$$

hence

$$|\psi\rangle = \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \sum_{k=1}^{N_B} U_{ik} \lambda_k V_{kj}^\dagger |a_i\rangle \otimes |b_j\rangle$$

defining

$$|k\rangle_A = \sum_{i=1}^{N_A} U_{ik} |a_i\rangle \text{ and } |k\rangle_B = \sum_{j=1}^{N_B} V_{kj}^\dagger |b_j\rangle$$

we obtain

$$|\psi\rangle = \sum_{k=1}^{N_B} \lambda_k |k\rangle_A \otimes |k\rangle_B$$

□

Remark (Schmidt decomposition and entanglement). — *If the Schmidt rank is equal to 1, then the state $|\psi\rangle$ is separable, otherwise the state is entangled.*

The Schmidt rank is an entanglement measure, it characterizes the amount of entanglement of the state $|\psi\rangle$.

The reduced state ρ^A or ρ^B can be computed easily using the Schmidt decomposition of $|\psi\rangle$,

$$\begin{aligned} \rho^A &= \text{Tr}_B [|\psi\rangle\langle\psi|] = \sum_k \lambda_k^2 |k\rangle_{AA} \langle k| \\ \rho^B &= \text{Tr}_A [|\psi\rangle\langle\psi|] = \sum_k \lambda_k^2 |k\rangle_{BB} \langle k| \end{aligned}$$

We see that the Schmidt basis $|k\rangle_A$ and $|k\rangle_B$ are the eigenstates of the reduced states ρ^A and ρ^B , respectively and the square of the Schmidt coefficients are the corresponding eigenvalues. We note that the eigenvalues λ_k^2 of ρ^A and ρ^B are identical.

1.8.1 Purification

The purification can be seen as the inverse process of reduction. Let ρ^A the state describing an ensemble of systems on \mathcal{H}^A . It is always possible to introduce another system E which states are in \mathcal{H}^E , and define a pure state $|\psi\rangle_{AE} \in \mathcal{H}^A \otimes \mathcal{H}^E$ such that

$$\rho^A = \text{Tr}_E [|\psi\rangle_{AE} \langle\psi|].$$

$|\psi\rangle_{AE}$ is a purification of ρ^A .

Proof. Let p_k and $|k\rangle_A$ the eigenvalues and eigenvectors of ρ^A . Let $|k\rangle_E$ an orthonormal basis of \mathcal{H}^E , then

$$|\psi\rangle_{AE} = \sum_k \sqrt{p_k} |k\rangle_A \otimes |k\rangle_E$$

is a purification of ρ^A . Check this. \square

Remarks:

The dimension of the auxiliary Hilbert space \mathcal{H}^E must be at least equal to the rank of ρ^A .

The purification allows the extension of the no-cloning theorem (see 1.5, page 11) for mixed states.

2

Qubits and quantum gates

QUANTUM COMPUTATION like classical computation can be defined in 3 steps: encoding the input information, processing this information and reading the output information. In this chapter, we will see how this can be performed using qubits. We will focus on the circuit model, but it is important to know that others equivalent models exist. For instance the Measurement Based Quantum Computing (MBQC) [9, 4].

2.1 The quantum bit – qubit

2.1.1 One qubit

A classical bit can have only 2 states, either 0 or 1. A qubit is a normalized state in the 2-dimensional Hilbert space \mathbb{C}^2 .

Let $\{|0\rangle, |1\rangle\}$ an orthonormal basis of \mathbb{C}^2 , which is often called the *computational basis*, the pure states can be written as

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle; \text{ with } \theta \in [0, \pi]; \phi \in [0, 2\pi]. \quad (2.1)$$

From Eq. (2.1), the corresponding expression for density matrix $\rho = |\psi\rangle\langle\psi|$ can be obtained (perform the calculation to check):

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2} [\mathbb{1} + \cos \theta Z + \sin \theta \cos \phi X + \sin \theta \sin \phi Y] \quad (2.2)$$

where X, Y and Z are the Pauli operators defined as:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|; \quad Y = i|1\rangle\langle 0| - i|0\rangle\langle 1|; \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (2.3)$$

It is convenient to define the unit vector $\vec{n} = \begin{pmatrix} \sin \theta \cos \phi \\ \sin \theta \sin \phi \\ \cos(\theta) \end{pmatrix} \in \mathbb{R}^3$ and

the vector of Pauli operators: $\vec{\sigma} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$ to rewrite ρ as:

$$\rho = \frac{1}{2} (\mathbb{1} + \vec{n} \cdot \vec{\sigma}) \quad (2.4)$$

We conclude that to each pure state $|\psi\rangle\langle\psi|$, we can associate an unit vector \vec{n} on the sphere, ($\theta \in [0, \pi]$ is the co-latitude and $\phi \in [0, 2\pi]$ the longitude). It is the so called *Bloch sphere*. To each point (θ, ϕ) on the Bloch sphere corresponds a pure state given by the density matrix of Eq. (2.2). It can also be shown that to each point in the Bloch ball (interior of the sphere) corresponds a mixed state ρ on \mathbb{C}^2 .

How much information is represented in one qubit? The answer to this question is not obvious because to retrieve the information, the qubit must be measured giving finally a 0 or 1 that is a bit of information. But "Nature" apparently can keep track of $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$. In each qubit there is two real numbers "hidden" by "Nature".

2.1.2 Multi-qubits

Suppose that we have 2 qubits, that is a state in $\mathbb{C}^2 \otimes \mathbb{C}^2$. In the computational basis $\{|ij\rangle \equiv |i\rangle \otimes |j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2; i, j = 0, 1\}$, it can be written as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \text{ with } \sum_{i,j=0}^1 |\alpha_{ij}|^2 = 1.$$

The measurement in the computational basis of the system in state $|\psi\rangle$ can give the results $x = 01, 01, 10$ or 11 with the respective probability $p_x = |\alpha_x|^2$.

Generalizing to a n qubits system, the computational basis is defined as

$$\{|x\rangle \equiv |x_1 x_2 \cdots x_n\rangle, x_i = 0, 1; i = 1, 2, \cdots n\} = \{|x\rangle, x \in \{0, 1\}^n\}$$

where $\{0, 1\}^n$ is the set of 2^n strings that can be formed with n bits. We have used the shorthand notation:

$$|x_1 x_2 \cdots x_n\rangle \equiv |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle. \quad (2.5)$$

A n -qubit state lives in the 2^n dimensional Hilbert space \mathbb{C}^{2^n} , which computational basis vectors can be labeled by the 2^n bit strings of length n .

Then, a general n -qubit state $|\psi\rangle$ can be written as superposition of the basis elements:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \text{ with } \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1.$$

The sum in this equation runs over the 2^n terms, corresponding to the set of integers $0, 1, \dots, 2^n - 1$ that can be coded with n bits.

When n becomes large (for instance $n = 500$ gives $2^{500} \simeq 10^{150}$), trying to store all this complex numbers α_x in a classical computer becomes a very difficult task. It seems that "Nature" is able to "evolve" and "calculate" the dynamics keeping tracks of these 2^n complex number.

Can we take advantage of this enormous computational power? This is the goal of quantum computation.

2.2 The quantum circuit model

2.2.1 Classical circuit

In the classical circuit model, the information is coded in bits. Each bit can take 2 values 0 or 1. Hence, the only one bit-gate is the **NOT** gate that transform 0 to 1 and 1 to 0. The result of the operation **NOT** a is also noted as \bar{a} .

There are several 2-bit gates, for instance: **OR**, **AND**, **XOR**, **NAND**. We recall that a **XOR** b , more commonly noted as $a \oplus b$ is equal to 1 if $a \neq b$ ($a = \bar{b}$) and is equal to 0 if $a = b$.

$$a \oplus b = \begin{cases} 1 & \text{if } a = \bar{b} \\ 0 & \text{if } a = b \end{cases}$$

it can also be considered as the addition (modulo 2).

$$a \oplus b = a + b \bmod(2)$$

The **NAND** gate is the negation of the **AND** gate:

$$a \text{ NAND } b = \overline{a \text{ AND } b} = \overline{a \cdot b}$$

where we have noted the **AND** gate by a dot, because it can be considered as the multiplication modulo 2:

$$a \text{ AND } b \equiv a \cdot b = a \times b \bmod(2)$$

We recall two important results:

Theorem 5 (**NAND** gate). — The **NAND** gate is a universal gate. That is all 1- and 2-qubit gates can be obtained using successive **NAND** gates.

Theorem 6 (F_2). — The set $\{0, 1\}$ with the two operations \oplus and **AND** is a field named $GF(2)$ (or F_2).

2.2.2 Quantum gates

Quantum gates are linear and unitary operators U :

$$U[a|\psi\rangle + b|\phi\rangle] = aU|\psi\rangle + bU|\phi\rangle \text{ and } UU^\dagger = U^\dagger U = \mathbb{1}.$$

It can be shown that an arbitrary linear unitary operator in \mathbb{C}^n can be written as a product of 1-qubit and specific 2-qubit gates which are controlled 1-qubit gates; that is 1-qubit gate which output depends on the state of an ancillary qubit.

2.2.3 1-qubit gates – $SU(2)$ – Rotations

A 1-qubit gates can be any unitary operator on \mathbb{C}^2 . All unitary operators on \mathbb{C}^2 can be written as $e^{i\alpha}U$ where α is any real phase, and U is any unitary operator with a determinant equal to 1, that is $U \in SU(2)$. Because a global phase has no physical implication, we can restrict 1-qubit gates to be unitary operators in $SU(2)$.

Parametrization of $SU(2)$: The set of 2×2 unitary matrices U with determinant equal to one can be parametrized with 2 complex numbers a and b as

$$U(a, b) = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}; \forall a, b \in \mathbb{C}; |a|^2 + |b|^2 = 1,$$

decomposing a and b in terms of their real and imaginary parts as $a = w + iz$, $b = y + ix$, we have

$$U(a, b) = \begin{pmatrix} w + iz & y + ix \\ -y + ix & w - iz \end{pmatrix} = w\mathbb{1} + i(x\sigma_1 + y\sigma_2 + z\sigma_3);$$

with $w^2 + x^2 + y^2 + z^2 = 1$ and where σ_i ($i = 1, 2, 3$) denotes a Pauli matrix:

$$\sigma_1 \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 \equiv Y = \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix}, \quad \sigma_3 \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2.6)$$

which we have already introduced in Eq. (2.3), page 21.

Let introduce the angle $\theta \in [0, \pi]$ such that $\cos(\frac{\theta}{2}) = w$ and $\sin(\frac{\theta}{2}) = \sqrt{1 - w^2} = \sqrt{x^2 + y^2 + z^2}$. And define v_x, v_y and $v_z \in \mathbb{R}$ such that $x = -v_x \sin(\frac{\theta}{2})$, $y = -v_y \sin(\frac{\theta}{2})$ and $z = -v_z \sin(\frac{\theta}{2})$, with $v_x^2 + v_y^2 + v_z^2 = 1$. We obtain:

$$U(a, b) = \cos\left(\frac{\theta}{2}\right) \mathbb{1} - i \sin\left(\frac{\theta}{2}\right) (v_x \sigma_x + v_y \sigma_y + v_z \sigma_z) = \exp\left(-i \frac{\theta}{2} \vec{\sigma} \cdot \vec{v}\right)$$

Where the last equality is proven in appendix XXX. The unitary operator

$$U_{\vec{v}}(\theta) \equiv \exp\left(-i \frac{\theta}{2} \vec{\sigma} \cdot \vec{v}\right) = \cos\left(\frac{\theta}{2}\right) \mathbb{1} - i \sin\left(\frac{\theta}{2}\right) \vec{\sigma} \cdot \vec{v} \quad (2.7)$$

where \vec{v} is the unit real vector with components $(v_x, v_y, v_z)^T$, and $\vec{\sigma}$ is the vector of Pauli matrices, acts as a rotation by an angle θ around the axis \vec{v} in the Bloch sphere.

More precisely we have the following homomorphism between $SU(2)$ and $SO(3)$ which is the group of rotations on \mathbb{R}^3 :

Theorem 7 (Homomorphism $SU(2), SO(3)$). — $\forall U \in SU(2)$, let

$$F(U) : \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

$$(x, y, z)^T \rightarrow (x', y', z')^T$$

through

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = F(U) \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

and

$$U(x\sigma_1 + y\sigma_2 + z\sigma_3)U^\dagger = x'\sigma_1 + y'\sigma_2 + z'\sigma_3$$

then

$$F(U_{\vec{v}}(\theta)) = \mathcal{R}_{\vec{v}}(\theta)$$

where $\mathcal{R}_{\vec{v}}(\theta)$ is the rotation in \mathbb{R}^3 by an angle θ around the axis \vec{v} .

Hence, if a qubit state is given by its Bloch vector \vec{n} , that is by its density matrix $\rho = \frac{1}{2}(\mathbb{1} + \vec{n} \cdot \vec{\sigma})$ (see Eq. (2.4)), then the effect of the qubit gate $U_{\vec{v}}(\theta)$ is obtained as follows,

$$U_{\vec{v}}(\theta)\rho U_{\vec{v}}^\dagger(\theta) = \frac{1}{2} [\mathbb{1} + U_{\vec{v}}(\theta)\vec{n} \cdot \vec{\sigma} U_{\vec{v}}^\dagger(\theta)] = \frac{1}{2} [\mathbb{1} + \{\mathcal{R}_{\vec{v}}(\theta)\vec{n}\} \cdot \vec{\sigma}]$$

and simply corresponds to the rotation of the vector \vec{n} by an angle θ around \vec{v} .

We see that all the 1-qubit gates can be parametrized with the help of 3 angles: two angles defining the orientation of the axis of the rotation \vec{v} and the angle θ corresponding to the rotation angle round this axis.

Another way to parametrize a rotation is by the 3 Euler angles :

Theorem 8 (Euler angles). — $U(\alpha, \beta, \gamma) \in SU(2)$ if and only if it exists $\alpha, \gamma \in [0, 2\pi]$ and $\beta \in [0, \pi]$ such that

$$U(\alpha, \beta, \gamma) = U_z(\alpha)U_y(\beta)U_z(\gamma) = \exp\left(-i\frac{\alpha}{2}\sigma_3\right)\exp\left(-i\frac{\beta}{2}\sigma_2\right)\exp\left(-i\frac{\gamma}{2}\sigma_3\right)$$

The proof is given in appendix XXX.

Some important examples of 1-qubit gates:

1. **Pauli gates:** We have already seen the Pauli gates $X = \sigma_1$, $Y = \sigma_2$ and $Z = \sigma_3$ (see Eqs. (2.6)) and Eqs. (2.3).

We recall here the main properties :

$$\sigma_i^2 = \mathbb{1} \quad (i = 1, 2, 3) \quad (2.8)$$

$$XY = iZ, YZ = iX, ZX = iY. \quad (2.9)$$

Hence, if we now how to implement Z and X gates we have also the Y gate.

The computational basis $\{|0\rangle, |1\rangle\}$ is formed by the eigenvectors of the gate Z corresponding to the eigenvalues $(1, -1)$, respectively.

The application of the X -gate on the computational basis, acts as a **NOT** gate:

$$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle$$

In a more compact form

$$X|a\rangle = |\bar{a}\rangle; \quad a = 0, 1.$$

The eigenstates of the X gate are

$$|0; X\rangle \equiv |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |1; X\rangle \equiv |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

2. **Hadamar gate H :** The Hadamar gate H transforms the Z gate into the X gate:

$$H|0\rangle = |+\rangle; \quad H|1\rangle = |-\rangle$$

hence, $H^2 = \mathbb{1}$ implying that $H^{-1} = H$ and therefore

$$HZH = X.$$

Its matrix representation in the computational basis is

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

3. **Phase gate S :** The matrix representation of the phase gate is

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

We have that $S^2 = Z$ thus $S^4 = \mathbb{1} \Rightarrow S^3 = ZS = S^{-1}$.

4. **$\frac{\pi}{8}$ -gate T :** The matrix representation of the T -gate is

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}$$

We have that, $S = T^2$ hence $T^8 = \mathbb{1}$.

The application of gates on a quantum state can be represented by a circuit diagram. The circuit diagram for a 1-qubit gate U is simply :

$$|\psi\rangle \text{---} \boxed{U} \text{---} U|\psi\rangle$$

The information flow is from left to right, $|\psi\rangle$ denotes any 1-qubit input state and $U|\psi\rangle$ is the output state, after the application of the gate U .

2.2.4 2-qubit gates – Controlled 1-qubit gates

2-qubits gates are unitary on $\mathbb{C}^2 \otimes \mathbb{C}^2$, they can be represented by 4×4 matrices in the computational basis $\{|ij\rangle \equiv |i\rangle \otimes |j\rangle; i, j \in \{0, 1\}\}$. Borrowing from the classical computation model, 2-qubit gates are implemented using controlled operations.

Example: the CNOT quantum gate The quantum CNOT gate acts on the 2 inputs qubits: $|c\rangle$ (control) and $|t\rangle$ (target) as a controlled X operator, C_X . If the control qubit is $|0\rangle$ then the target qubit is left unchanged and if the control qubit is in the state $|1\rangle$ then the gate X is applied on the target qubit, that is:

$$\begin{aligned} |0\rangle \otimes |t\rangle &\rightarrow |0\rangle \otimes |t\rangle \\ |1\rangle \otimes |t\rangle &\rightarrow |1\rangle \otimes X|t\rangle = |1\rangle \otimes |\bar{t}\rangle \end{aligned}$$

which can also be written as

$$C_X [|c\rangle \otimes |t\rangle] = |c\rangle |t \oplus c\rangle$$

In all cases the control qubit remains unchanged.

In the computational basis $\{|ij\rangle \equiv |i\rangle \otimes |j\rangle; i, j \in \{0, 1\}\}$ (eigenstates of $Z \otimes Z$), the 4×4 matrix representing the CNOT gates is:

$$C_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The circuit diagram representing the controlled X gate is as follows:

$$\begin{array}{c} |c\rangle \text{---} \bullet \text{---} |c\rangle \\ |t\rangle \text{---} \oplus \text{---} |c \oplus t\rangle \end{array}$$

where the dot indicates the control qubit and the \oplus sign indicates the X gate applied to the target qubit (as a reminder, \oplus looks like a target).

The controlled unitary gate In general, we can define a controlled arbitrary unitary gate C_U , that applies the unitary gate U to the target

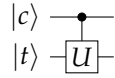
qubit if the control qubit is in the state $|1\rangle$ and does nothing if the control qubit is in the state $|0\rangle$:

$$\begin{aligned} C_U|0\rangle \otimes |t\rangle &= |0\rangle \otimes |t\rangle \\ C_U|1\rangle \otimes |t\rangle &= |1\rangle \otimes U|t\rangle \end{aligned}$$

The matrix representation of C_U , in the computational basis is

$$C_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix} \text{ where } U_{ij} = \langle i|U|j\rangle.$$

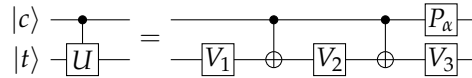
The circuit diagram representing the C_U gate is:



Theorem 9 (C_U implementation). — A C_U gate can always be implemented using C_X gates and 1-qubit gates only.

Proof. We will show that an arbitrary 2-qubit controlled unitary gate C_U can be decomposed in the product of two CNOT gates and four 1-qubit gates. The proof involves two steps:

1. We first show that for an arbitrary 1-qubit gate U , there are 3 1-qubit unitary gates V_1, V_2, V_3 and $\alpha \in [0, 2\pi]$ such that $V_3V_2V_1 = \mathbb{1}$ and $U = V_3XV_2XV_1(e^{i\alpha}\mathbb{1})$.
2. This decomposition allows to implement the C_U gate with the following circuit:



where P_α is the following unitary: $P_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$.

It can be easily checked that when $|c\rangle = |0\rangle$, $|t\rangle$ remains untouched, and when $|c\rangle = |1\rangle$ then $U = V_3XV_2XV_1(e^{i\alpha}\mathbb{1})$ is applied to $|t\rangle$.

Hence, it remains to show the first step. For this we first remark that $V_3V_2V_1 = \mathbb{1}$ implies that $V_2 = V_3^\dagger V_1^\dagger$. Then we use the parametrization of $SU(2)$ given by Eq. (2.7) and write

$$U = e^{i\alpha} (\cos \beta + i \sin \beta \vec{\sigma} \cdot \vec{v}),$$

where $\beta \in [0, \pi/2]$, \vec{v} is a unit real vector and $\vec{\sigma}$ is the vector of Pauli matrices.

Hence, we have

$$V_3 X V_2 X V_1 = V_3 X V_3^\dagger V_1^\dagger X V_1 = \cos \beta + i \sin \beta \vec{\sigma} \cdot \vec{v}$$

Let define two unit real vectors \vec{b} and \vec{c} such that $V_3 X V_3^\dagger = \vec{b} \cdot \vec{\sigma}$ and $V_1 X V_1^\dagger = \vec{c} \cdot \vec{\sigma}$. Then,

$$V_3 X V_3^\dagger V_1^\dagger X V_1 = \vec{b} \cdot \vec{\sigma} \vec{c} \cdot \vec{\sigma} = \vec{b} \cdot \vec{c} \mathbb{1} + i(\vec{b} \wedge \vec{c}) \cdot \vec{\sigma}$$

where the last equality can be explicitly checked.

We thus can choose \vec{b} and \vec{c} such that $\vec{b} \cdot \vec{c} = \cos \beta$ and $\vec{b} \wedge \vec{c} = \sin \beta \vec{v}$. That is \vec{b} and \vec{c} are in the plane orthogonal to \vec{v} and $\widehat{\vec{b}\vec{c}} = \beta$ (see Fig. 2.1). \square

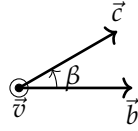


Figure 2.1: implementation of the controlled unitary operators

Notation When playing with 2-qubit gates, it is convenient to write X_1 to indicate that the gate X is applied to the first qubit. That is $X_1 = X \otimes \mathbb{1}$. In the same way, we will write $Z_2 = \mathbb{1} \otimes Z$, meaning that the Z gate is applied to the second qubit.

Exercise 5. — Check the following circuit identities:

$$\begin{aligned} C_X X_1 C_X &= X_1 X_2; & C_X Y_1 C_X &= Y_1 Y_2; & C_X Z_1 C_X &= Z_1 \\ C_X X_2 C_X &= X_2; & C_X Y_2 C_X &= Z_1 Y_2; & C_X Z_2 C_X &= Z_1 Z_2 \end{aligned}$$

2.2.5 Universal gates and efficient approximation – The Solovay-Kitaev theorem

In this section we will list some important results without giving the proof. The proof is given in Ref. [8]¹ for instance.

1. Any unitary in $SU(d)$ (Unitary on \mathbb{C}^d with unit determinant) can be written as the product of 2-qubit and 1-qubit gates.
2. Any unitary in $SU(d)$ can be expressed exactly using single qubit gates and CNOT 2-qubit gate. This is a consequence of the previous point and the theorem 9 given on page 28.

¹ M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010

3. **Universal gates:** Any unitary on \mathbb{C}^2 (1-qubit gate) can be approximated to arbitrary accuracy using Hadamard gate H , phase gate S and $\pi/8$ T -gate. The set of gates $\{H, S, T\}$ is said universal.

Definition (Universal set). — A set G of unitary operators on $SU(d)$ is said to be universal if

- $g \in G \Rightarrow g^{-1} \in G$
- The group $\langle G \rangle$ generated by the set G is dense in $SU(d)$. That is: $\forall U \in SU(d), \forall \epsilon > 0, \exists S = g_1 g_2 \cdots g_m (g_i \in G)$ such that $\|U - S\| \leq \epsilon$. (Where $\|U - S\| = \sup_{\|\psi\|=1} \|(U - S)|\psi\rangle\|$)

4. **Solovay-Kitaev theorem** This theorem insures that given an universal set G , the approximation of an arbitrary gate U as a product of gates in G can be performed efficiently. A pedagogical review is presented in Ref [5]² by C. M. Dawson and M. A. Nielsen.


Theorem 10 (Solovay-Kitaev). — Let G be an universal set of gate in $SU(d)$ and let ϵ a given accuracy, $\exists c > 0, \forall U \in SU(d)$, it exists a finite sequence of gates from G of length $\mathcal{O}(\log^c(1/\epsilon))$ such that $\|U - S\| \leq \epsilon$

In Ref. [5] a constructive proof is given, presenting an algorithm that build the sequence of gate. The value of c obtained with this proof is $c \simeq 3.97$.

The important point is that the length of the gate sequence scale polylogarithmically with the accuracy of the approximation.

² Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm, August 2005. arXiv:quant-ph/0505030

2.2.6 Measurements

The symbol  indicate a projective measurement in the computational basis $\{|0\rangle, |1\rangle\}$. The double line after the measurement symbol indicates that classical information (one bit) is transmitted. Concerning measurement operations, the following rules applies:

- Classically conditioned operations can be replaced by quantum conditional operations without changing the output of the quantum circuit
- Measurements can always be moved from intermediate stage to the end of a quantum circuit.
- Any unterminated quantum wire (qubit which is not measured) at the end of a quantum circuit may be assumed to be measurement without altering the output of the circuit.

In most cases, the measurement plays the role of an interface between the quantum and the classical word. In that case the measurement

is considered as irreversible, destroying quantum information and replacing quantum information (qubit) by classical information (bit).

But in some cases, this is not the case. For instance in teleportation or quantum error correction as we will see later. In that cases, the measurement does not reveal any information about the identity of the quantum state being measured. In order of a measurement to be a reversible operation, it must reveal no information about the quantum state being measured.

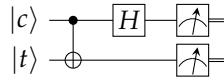
Exercise 6. — Suppose that ρ is the density matrix of a 2-qubit system. Suppose we perform a measurement of the second qubit with $P_0 = \mathbb{1} \otimes |0\rangle\langle 0|$ and $P_1 = \mathbb{1} \otimes |1\rangle\langle 1|$. Let ρ' the density matrix which would be assigned to the system after the measurement, by an observer who did not learn the measurement result. Show that

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1.$$

Also, show that the reduced density matrix for the first qubit is not affected by the measurement, that is

$$\text{Tr}_2 [\rho] = \text{Tr} [\rho']$$

Exercise 7 (Measurement in the Bell basis). — Show that the following circuit performs a measurement in the Bell basis



The Bell basis is a basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$ formed by the following vectors:

$$\begin{aligned} |\beta(0,0)\rangle &\equiv |\phi_+\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\ |\beta(0,1)\rangle &\equiv |\psi_+\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) \\ |\beta(1,0)\rangle &\equiv |\phi_-\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\ |\beta(1,1)\rangle &\equiv |\psi_-\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \end{aligned} \quad (2.10)$$

it can be written in a concise way as:

$$|\beta(i,j)\rangle = \frac{1}{\sqrt{2}} (|0,j\rangle + (-1)^i |i,\bar{j}\rangle) \quad (2.11)$$

where we have used the notation $|i,j\rangle \equiv |i\rangle \otimes |j\rangle$.

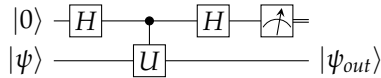
Exercise 8. — Let U the unitary operator such that

$$U|i, j\rangle = |\beta(i, j)\rangle (i, j = 0, 1).$$

where $\{|\beta(i, j)\rangle (i, j = 0, 1)\}$ denotes the Bell basis (see previous exercise).

1. Show that $U = C_X(H \otimes \mathbb{1})$ and draw the corresponding circuit.
 2. Draw the circuit diagram corresponding to U^{-1} .
 3. Deduce a general recipe to draw the circuit that allows the measurement in the basis $U|i, j\rangle$ and the circuit that produce $U|i, j\rangle$.
-

Exercise 9. — Let U a single qubit operator, which is hermitian and unitary (its eigenvalues are thus ± 1). Show that the following circuit performs the measurement of U for an arbitrary $|\psi\rangle \in \mathbb{C}^2$.



2.3 First applications

2.3.1 Quantum teleportation

Quantum teleportation allows to send an *arbitrary* quantum state from a source to a receiver. The important point is that the state $|\psi\rangle$ to be sent is *arbitrary*, and not known in advance by the source. The quantum circuit that allows this process has been presented by Charles H. Bennett et. al as publication in Phys. Rev. Lett. in 1993³ (see Ref. [1]).

In the proposed algorithm, Alice and Bob must have previously shared the Bell state $|\beta(0,0)\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$, each taking one qubit of the pair. Then Alice receives the arbitrary state $|\psi\rangle_A$ and need to send it to Bob. For this she's allowed to send only classical information to Bob.

Let's describe the algorithm step by step. We define $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ the state that Alice must send to Bob. Hence the initial state of the system shared by Alice and Bob is

$$|\Psi\rangle_{AB} = |\psi\rangle_A |\beta(0,0)\rangle = |\psi\rangle_A \otimes \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

³ Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, March 1993. Publisher: American Physical Society

Alice has 2 qubits (the state to be send and a part of the Bell state that she share with Bob) and Bob have one qubit (the other part of the Bell state).

Then Alice applies a CNOT (C_X) gate to her 2-qubit state. She thus change its second qubit only if its first qubit is $|1\rangle$, she obtain:

$$\begin{aligned} \text{CNOT}_A |\Psi\rangle_{AB} &= \frac{\alpha}{\sqrt{2}} |0\rangle_A \otimes (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \\ &\quad + \frac{\beta}{\sqrt{2}} |1\rangle_A \otimes (|1\rangle_A \otimes |0\rangle_B + |0\rangle_A \otimes |1\rangle_B) \end{aligned}$$

She then applies an Hadamard gate to its first qubit:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad |1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

and she obtain

$$\begin{aligned} (H \otimes \mathbb{1})_A \text{CNOT}_A |\Psi\rangle_{AB} &= \frac{1}{2} [|0\rangle_A \otimes |0\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) \\ &\quad + |0\rangle_A \otimes |1\rangle_A (\alpha|1\rangle_B + \beta|0\rangle_B) \\ &\quad + |1\rangle_A \otimes |0\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) \\ &\quad + |1\rangle_A \otimes |1\rangle_A (\alpha|1\rangle_B - \beta|0\rangle_B)] \end{aligned}$$

In the last step, she measures her 2 qubits in the computational basis $\{|i\rangle \otimes |j\rangle; i, j = 0, 1\}$ and communicates the result she obtain to Bob.

She can obtain 4 results and in each case the Bob state is as follows:

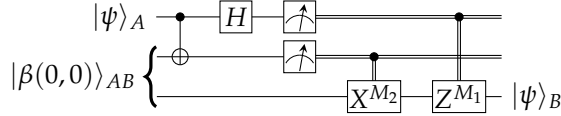
$$\begin{aligned} 00 &\rightarrow |\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B = |\psi\rangle \\ 01 &\rightarrow |\psi\rangle_B = \alpha|1\rangle_B + \beta|0\rangle_B = X|\psi\rangle \\ 10 &\rightarrow |\psi\rangle_B = \alpha|0\rangle_B - \beta|1\rangle_B = Z|\psi\rangle \\ 11 &\rightarrow |\psi\rangle_B = \alpha|1\rangle_B - \beta|0\rangle_B = XZ|\psi\rangle \end{aligned}$$

Now knowing the result of the Alice measurement, Bob can recover the state $|\psi\rangle$ by applying a one qubit specific gate to his state conditioned to the measurement result Alice have sent to him:

- If he receives 00 then Bob does nothing.
- If he receives 01 then Bob applies a X gate.
- If he receives 10 then Bob applies a Z gate.
- If he receives 11 then Bob applies first and X gate and then a Z gate.

This last step can be summarizes as: Bob applies the gate $Z^{M_1} X^{M_2}$, where $M_1 M_2$ are the measurement results that Alice have sent to Bob.

The circuit diagram that performs the teleportation is as follows:



We see that the operations performed by Alice corresponds to a measurement in the Bell Basis of its 2-qubits state (See exercise 7 on page 31).

2.3.2 superdense coding

Alice would like to send 2 (classical) bits of information but she can only send one qubit. Suppose that Alice and Bob share a pair of qubits in the entangled state Bell state $|\Psi\rangle_{AB} = |\beta(0,0)\rangle$, by sending its qubit to Bob it turns out that Alice can send 2 bits of information.

For this, Alice performs a local unitary operation on its qubit and send it to Bob. Bob then possesses a 2-qubit state. The coding is the following:

$$\begin{aligned} 00 : \mathbb{1}_A |\psi\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\ 01 : Z_A |\psi\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\ 10 : X_A |\psi\rangle &= \frac{1}{\sqrt{2}} (|1\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle) \\ 11 : X_A Z_A |\psi\rangle &= \frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) \end{aligned}$$

Bob can determine the 2 bits sent by Alice by performing a measurement in the Bell basis.

Exercise 10. — Let E a positive operator acting on Alice qubit. Show that $\langle \psi | E \otimes \mathbb{1} | \psi \rangle$ take the same value when $|\psi\rangle$ is any of the Bell state $|\beta(i,j)\rangle$, ($i,j = 1,2$).

3

Some Quantum Algorithms

In, this chapter we present some quantum algorithms.

3.1 Quantum Parallelism

3.1.1 Computing a function with a unitary operator

We would like to compute a function f :

$$\begin{aligned} f : \{0, 1\} &\rightarrow \{0, 1\} \\ x &\rightarrow f(x) \end{aligned} \quad (3.1)$$

using a unitary operation U_f , as it is the only allowed operation (except for the measurements) in quantum computation, this can be done as follows:

$$|x\rangle \otimes |y\rangle \xrightarrow{U_f} |x\rangle \otimes |y \oplus f(x)\rangle \quad (3.2)$$

We remind that \oplus is the **xor** 2-bit operation which is also the addition mod 2:

$$x \oplus y = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases}$$

which can also be defined as

$$x \oplus y = \begin{cases} y & \text{if } x = 0 \\ \bar{y} & \text{if } x = 1 \end{cases}$$

Thus $x \oplus y$ is also a classical **CNOT** 2-bit operation where x is the control and y is the target. Hence the unitary U_f can also be defined as:

$$U_f(|x\rangle \otimes |y\rangle) = \begin{cases} |x\rangle \otimes |f(x)\rangle & \text{if } y = 0 \\ |x\rangle \otimes |\overline{f(x)}\rangle & \text{if } y = 1 \end{cases} \quad (3.3)$$

You can check that U_f is indeed unitary, it preserves the norm and maps orthogonal states to orthogonal states.

Now, as U_f is also a linear operator, instead of $|x\rangle$ as input we can try to input the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. We obtain:

$$U_f \left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \otimes |0\rangle \right] = \frac{|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle}{\sqrt{2}}.$$

We have a superposition of all $(x, f(x))$ possible pair by acting U_f only once.

We have already seen the unitary operation:

$$\begin{aligned} |0\rangle &\rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle &\rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{aligned}$$

it is the Hadamard gate. If we apply The Hadamard gate on the 2 qubits initialized in the $|0\rangle \otimes |0\rangle$ state we obtain

$$\begin{aligned} H \otimes H |0\rangle \otimes |0\rangle &= \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{2} (|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \end{aligned}$$

We obtain a superposition of the 4 states of the computational basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$, by acting two Hadamard gates.

3.1.2 The n -qubit case

If we apply n Hadamard gates on n qubits, one on each qubit you can check that we obtain:

$$\underbrace{H \otimes H \otimes \cdots \otimes H}_n \underbrace{(|0\rangle \otimes |0\rangle \cdots \otimes |0\rangle)}_n = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle. \quad (3.4)$$

Applying only n Hadamard gate we have obtained the superposition of the 2^n elements $|x\rangle$ ($x \in \{0,1\}^n$) of the computational basis of \mathbb{C}^{2^n} ; where we have used the shorthand notation defined in Eq. (2.5), page 22.

Now suppose that we have a function f as follows,

$$\begin{aligned} f : \{0,1\}^n &\rightarrow \{0,1\} \\ x &\rightarrow f(x) \end{aligned}$$

and the corresponding gate U_f as defined in Eq. (3.3). Then applying U_f to the state defined in Eq. (3.4), we obtain

$$U_f(H^{\otimes n} \Pi^{\otimes n} |0\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle.$$

Applying U_f only once, we obtain the superposition of all couples (input,output) value of f . This is what is called *quantum parallelism*. Quantum mechanics allows to obtain this fantastic superposition, but can we extract useful information from this superposition and more efficiently than a classical computer. A simple projective measurement on the computational basis, will give only one $|x\rangle \otimes |f(x)\rangle$ with probability $\frac{1}{2^n}$.

Quantum parallelism is not sufficient to obtain quantum advantage, we must be clever.

3.1.3 Technical remarks on the Hadamard gate

The effect of the Hadamard gate on the computational basis $\{|x\rangle; x = 0, 1\}$, can be written as:

$$H|x\rangle = \sum_{z=0,1} \frac{(-1)^{xz}}{\sqrt{2}} |z\rangle$$

This expression becomes particularly convenient in the case n qubits case:

$$\begin{aligned} H^{\otimes n} |x_1\rangle \otimes |x_2\rangle \cdots \otimes |x_n\rangle &= \sum_{z_1=0,1} \frac{(-1)^{x_1 z_1}}{\sqrt{2}} |z_1\rangle \otimes \sum_{z_2=0,1} \frac{(-1)^{x_2 z_2}}{\sqrt{2}} |z_2\rangle \otimes \cdots \otimes \sum_{z_n=0,1} \frac{(-1)^{x_n z_n}}{\sqrt{2}} |z_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{z_1=0,1} \sum_{z_2=0,1} \cdots \sum_{z_n=0,1} (-1)^{x_1 z_1 + x_2 z_2 + \cdots + x_n z_n} |z_1 z_2 \cdots z_n\rangle \end{aligned}$$

We thus have the following result,

$$H^{\otimes n} |x_1\rangle \otimes |x_2\rangle \cdots \otimes |x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \quad (3.5)$$

where we have used the shorthand notation defined in Eq. (2.5), page 22 and we have defined $x \cdot z = x_1 z_1 + x_2 z_2 + \cdots + x_n z_n$.

3.2 Deutsch algorithm

3.2.1 the 1-qubit case

Suppose that we have a function $f(x)$ as in Eq. (3.1), and the corresponding gate U_f as defined in Eq. (3.2), the Deutsch algorithm ¹ (see Ref. [6]) allows to compute $f(0) \oplus f(1)$ using U_f only once.

Let calculate $f(0) \oplus f(1)$:

$$f(0) \oplus f(1) = \begin{cases} 0 & \text{if } f(0) = f(1) \text{ (constant function)} \\ 1 & \text{if } f(0) \neq f(1) \text{ (balanced function)} \end{cases}$$

$f(0) \oplus f(1)$ is a global information about $f(x)$ which requires the computation of f twice with a classical computer.

¹ David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992

Let start by applying U_f to the input state $|\psi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. For this we first note that

$$\begin{aligned} \forall x \in \{0,1\}, U_f|x\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} &= \frac{1}{\sqrt{2}}|x\rangle \otimes (|f(x)\rangle - |\overline{f(x)}\rangle) \\ &= \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle) \end{aligned}$$

With this result we can obtain $|\psi_2\rangle = U_f|\psi_1\rangle$:

$$|\psi_2\rangle = U_f|\psi_1\rangle = \begin{cases} \pm \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1) \end{cases}$$

Then applying the Hadamrd gate on the first qubit we obtain the desired result

$$\begin{aligned} |\psi_3\rangle &= [H \otimes \mathbb{1}] U_f|\psi_1\rangle = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1) \\ \pm|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1) \end{cases} \\ &= \pm |f(0) \oplus f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

So, by measuring the first qubit we can obtain th value of $f(0) \oplus f(1)$, using only one evaluation of U_f .

The circuit diagram for this algorithm is:

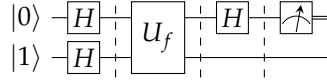


Figure 3.1: Circuit diagram for the Deutsch algorithm

3.2.2 Multiqubit case, the Deutsch-Jozsa algorithm

Now we consider a function f from $\{0,1\}^n$ and which value is 0 or 1,

$$\begin{aligned} f : \{0,1\}^n &\rightarrow \{0,1\} \\ x &\rightarrow f(x) \end{aligned}$$

furthermore, we assume that the function can be either constant or balanced. By balanced, we mean that $f(x) = 0$ for exactly half of its 2^n inputs and $f(x) = 1$ for the others. In the classical setting, we suppose that we have a black box that can give us the value of $f(x)$ for each input x . In the quantum case, we suppose that we have a black box that can compute $U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$ for all $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$ and $|y\rangle \in \mathbb{C}^2$.

The objective of the algorithm is to determine if the function f is balanced or constant. With a classical computer, in the worst case we must compute f , $2^n/2 + 1$ times.

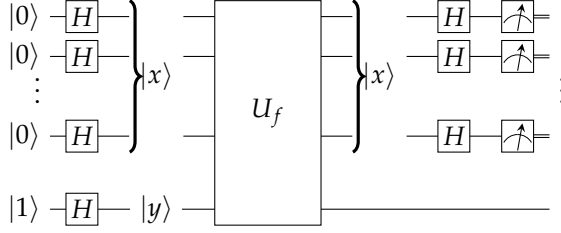


Figure 3.2: Circuit diagram for the Deutsch-Jozsa algorithm. If all the n measurements give a result $x_i = 0$ ($i = 1, 2, \dots, n$) then the function f is constant.

The quantum algorithm is a generalization of the one-qubit case, as represented by the diagram of Fig. 3.2.

It is composed by the following steps:

1. Initialization: the n first qubits are initialized in the state $|x\rangle = |0\rangle^{\otimes n}$, and the last qubit $|y\rangle = |1\rangle$. Thus, at this stage the state is

$$|\psi_1\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle$$

2. A series of Hadamard gates are applied; Hence the state becomes

$$|\psi_2\rangle = H^{\otimes n}|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes H|1\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

3. The U_f gate is applied. To compute the resulting state, we first compute the application of the gate for each term of the sum, that is $U_f|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$. We obtain

$$\begin{aligned} U_f|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) &= \frac{1}{\sqrt{2}} \left(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |\overline{f(x)}\rangle \right) \\ &= (-1)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

Hence, the state after the U_f gate is:

$$|\psi_3\rangle = U_f|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

4. The application of the n Hadamard gates on the n first qubits can be computed using the result of Eq. (3.5). We obtain

$$|\psi_4\rangle = H^{\otimes n} \otimes \mathbb{1} |\psi_3\rangle = \frac{1}{2^n} \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z + f(x)} |z\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Now suppose that $f(x)$ is a constant function f ($f = 0$ or $f = 1$), then we can factorize $(-1)^{f(x)} = (-1)^f$ and the state can be written as

$$|\psi_4\rangle = \frac{(-1)^{f(x)}}{2^n} \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right); \quad f \text{ constant}$$

The measurements of the first n qubits amount to measure $z \in \{0,1\}^n$. The probability $\Pr(z)$ to obtain the outcomes z in such a measurement is given by

$$\Pr(z) = \left| \frac{\sum_{x \in \{0,1\}^n} (-1)^{x \cdot z}}{2^n} \right|^2$$

But we note that when $z = 00 \cdots 0$, $\sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} = 2^n$ giving

$$\Pr(z = 00 \cdots 0) = 1.$$

We conclude that when f is a constant function the state is simply

$$|\psi_4\rangle = |0\rangle^{\otimes n} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right); \quad f \text{ constant}$$

and the outcomes of the measurements can only be $00 \cdots 0$.

Suppose now that $f(x)$ is a balanced function, then the probability to obtain $z = 00 \cdots 0$ is given by

$$\Pr(z = 00 \cdots 0) = \left| \frac{\sum_{x \in \{0,1\}^n} (-1)^{f(x)}}{2^n} \right|^2 = 0$$

where we have used that for a balanced function $\sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0$.

Finally, if the outcomes of the measurements are $z = 00 \cdots 0$, the function is constant. if not, the function is balanced. Using U_f only once, we can obtain an answer requiring $2^n/2 + 1$ queries (in the worst case) with a classical computer.

Remark. — *The caveats are:*

- *This problem has no application*
- *The comparison between classical or quantum is not completely fair. Indeed, how to compare the classical query which amount to compute $f(x)$ and the quantum one which amount to apply the gate U_f ?*
- *With a probabilistic classical algorithm, we can do much better than with a deterministic classical algorithm.*

3.3 Grover's search algorithm

The problem consists in finding an entry in an unstructured database. Suppose, for instance, that you have a directory, a phone book, sorted by name in alphabetic order but you only know the phone number and look for the corresponding name.

On average, this task requires $N/2$ trials, if N is the number of item in the list. In term of computational complexity one can say that the time required scales as $\mathcal{O}(N)$.

The Grover's algorithm finds the required item more quickly, in $\mathcal{O}(\sqrt{N})$ queries to the database. Furthermore, it can be shown that this scaling is optimal. No quantum algorithm can make better than a $\mathcal{O}(N)$. Here we will only present the algorithm and show that its scaling is indeed $\mathcal{O}(\sqrt{N})$. For the optimality proof see Ref. [10]².

Let us label each of the $N = 2^n$ elements of the database by an integer: $a = 1, 2, \dots, N = 2^n$. Each element can be labeled by a string of n bits. The problem can be formalized by the existence of a function f such that $f(a) = 1$ if a is the searched item and $f(a) = 0$ otherwise.

In the quantum case, to each item a we associate an element $|a\rangle$ of the computational basis $B_n = \{|a\rangle; a \in \{0, 1\}^n\}$ of $(\mathbb{C}^2)^{\otimes n}$. We suppose that we have a black box – the so-called oracle – that computes this function for every item (as in the classical case). Hence we have at our disposal the gate U_f defined as

$$U_f|a\rangle \otimes |y\rangle = |a\rangle \otimes |y \oplus f(a)\rangle; \quad \forall |a\rangle \in B_n \text{ and } y \in \{0, 1\}.$$

Now suppose that $|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, then

$$U_f|a\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)^{f(a)}|a\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

We see that with this specific $|y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, the effect of the operator U_f is to mark with a minus sign (π phase shift) the searched element a_0 corresponding to $f(a_0) = 1$.

If we prepare the input state of the database in a uniform superposition of all the elements of the orthogonal basis B_n ,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{a=0}^N |a\rangle \quad (3.6)$$

then

$$U_f|\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{N}} \sum_{a=0}^N (-1)^{f(a)}|a\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

A measurement in the computational basis of the first register ($|a\rangle$) will give all outcomes with equal probabilities $1/N$ and will not reveal the searched item $a = a_0$ corresponding $(-1)^{f(a)} = -1$. However, this can be changed by performing the so-called *diffusion unitary transformation* D on the first register, defined as:

$$D = 2|\psi\rangle\langle\psi| - \mathbb{1}^{\otimes n} \quad (3.7)$$

where $|\psi\rangle$ has been defined in Eq. (3.6) and $\mathbb{1}$ is the identity operator on \mathbb{C}^2 .

Let calculate

$$(D \otimes \mathbb{1})U_f|\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = D|\phi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \text{ with } |\phi\rangle = \sum_{a=0}^N (-1)^{f(a)}|a\rangle \quad (3.8)$$

² Christof Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, 60:2746–2751, Oct 1999

But

$$D|\phi\rangle = 2|\psi\rangle\langle\psi|\phi\rangle - |\phi\rangle$$

and

$$\begin{aligned}\langle\psi|\phi\rangle &= \frac{1}{N} \sum_{a,a'} \langle a'|a\rangle (-1)^{f(a)} = \frac{1}{N} \sum_{a,a'} \delta_{a,a'} (-1)^{f(a)} = \frac{1}{N} \sum_a (-1)^{f(a)} \\ &= \frac{1}{N} \left[\left(\sum_{a \neq a_0} 1 \right) - 1 \right] = \frac{N-2}{N}\end{aligned}$$

Hence,

$$\begin{aligned}D|\phi\rangle &= 2\frac{N-2}{N}|\psi\rangle - |\phi\rangle = \frac{1}{\sqrt{N}} \sum_a \left[2\frac{N-2}{N} - (-1)^{f(a)} \right] |a\rangle \\ &= \frac{1}{\sqrt{N}} \left[\frac{N-4}{N} \sum_{a \neq a_0} |a\rangle + \frac{3N-4}{N} |a_0\rangle \right]\end{aligned}$$

We see that the application of the operator D has amplified the amplitude of the searched component $|a_0\rangle$ from $\frac{1}{\sqrt{N}}$ to $\frac{1}{\sqrt{N}}(3 - \frac{4}{N})$. The probability has thus be amplified from $1/N$ to $\simeq 9/N$. We can now apply D , p times, to amplify the probability of this outcomes before performing the measurement in the computational basis.

To investigate how many times we must apply D such that the probability of success is sufficiently high, we will see that the full transformation G of the first register is a rotation in the two dimensional subspace spanned by the orthonormal basis $\{|a_0\rangle, |a_{0\perp}\rangle\}$ where

$$|a_{0\perp}\rangle = \frac{1}{\sqrt{N-1}} \sum_{a \neq a_0} |a\rangle.$$

For this, let us write the initial state $|\psi\rangle$ (see Eq. (3.6)) in the basis $\{|a_0\rangle, |a_{0\perp}\rangle\}$:

$$|\psi\rangle = \sqrt{\frac{N-1}{N}} |a_{0\perp}\rangle + \frac{1}{\sqrt{N}} |a_0\rangle.$$

The state $|\phi\rangle$ (see Eq. (3.8)) can also be written in the orthonormal basis $\{|a_0\rangle, |a_{0\perp}\rangle\}$ as:

$$|\phi\rangle = \sqrt{\frac{N-1}{N}} |a_{0\perp}\rangle - \frac{1}{\sqrt{N}} |a_0\rangle.$$

We see that U_f acts on the first register as a reflection with respect to $|a_{0\perp}\rangle$. The operator D is also a reflection (see Eq. (3.7)) but with respect to $|\psi\rangle$. We know that the composition of two reflections is a rotation. The angle θ of the rotation is such that (see fig. 3.3)

$$\cos(\theta/2) = \langle a_{0\perp}|\psi\rangle = \sqrt{\frac{N-1}{N}}; \quad \sin(\theta/2) = \langle a_0|\psi\rangle = \sqrt{\frac{1}{N}}.$$

We conclude that the full transformation $(D \otimes 1)U_f$ applied on the

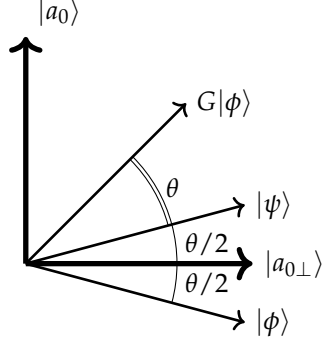


Figure 3-3: The state $|\phi\rangle$ is obtained by reflection of $|\psi\rangle$ through $|a_{0\perp}\rangle$. $|\phi\rangle$ is then reflected through $|\psi\rangle$, resulting in a rotation of $|\psi\rangle$ by an angle θ .

state $|\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ can be written as

$$(D \otimes \mathbb{1})U_f|\psi\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = [G|\psi\rangle] \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

where $|\psi\rangle$ and $G|\psi\rangle$ are given by

$$\begin{aligned} |\psi\rangle &= \cos \frac{\theta}{2} |a_{0\perp}\rangle + \sin \frac{\theta}{2} |a_0\rangle \\ G|\psi\rangle &= \cos \frac{3\theta}{2} |a_{0\perp}\rangle + \sin \frac{3\theta}{2} |a_0\rangle \end{aligned}$$

Hence, iterating p times we obtain

$$G^p|\psi\rangle = \cos \left[(2p+1) \frac{\theta}{2} \right] |a_{0\perp}\rangle + \sin \left[(2p+1) \frac{\theta}{2} \right] |a_0\rangle.$$

The probability $\Pr(a_0)$ to obtain a_0 after p application of the transformation $(D \otimes \mathbb{1})U_f$ is given by

$$\Pr(a_0) = \sin^2 \left[(2p+1) \frac{\theta}{2} \right].$$

For $\Pr(a_0)$ to reach the value 1, we must have $(2p+1) \frac{\theta}{2} \simeq \frac{\pi}{2}$. Thus the optimal number of iterations p_o is given by

$$p_o = \left\lfloor \frac{\pi}{2\theta} \right\rfloor - \frac{1}{2} \quad (3.9)$$

where $\lfloor x \rfloor$ denotes the floor of x (the greater integer less than x).

Now, if $N \gg 1$, then as $\sin \theta/2 = 1/\sqrt{N} \ll 1$, we can consider that $\sin \theta/2 \simeq \theta/2$, hence $\theta \simeq \frac{2}{\sqrt{N}}$. Inserting this result in Eq. (3.9) we conclude that the optimal number of iterations p_o is given by

$$p_o \simeq \left\lfloor \frac{\pi}{4} \sqrt{N} - \frac{1}{2} \right\rfloor$$

that is

$$p_o = \mathcal{O}(\sqrt{N}).$$

the number of iteration needed to obtain the searched item scales as \sqrt{N} . \square

The technique used in the Grover's algorithm which consists in an amplification of a probability amplitude has been generalized by G. Brassard and coll. ³, see Ref. [2].

³ Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv:quant-ph/0005055*, 2000

3.4 Quantum Fourier algorithm

The quantum Fourier algorithm is the basic tool to perform what is called quantum phase estimation which in turn allows to solve efficiently several problems as order finding, integer factoring, period finding, discrete logarithm. The quantum Fourier transform is at the hearth of the Shor's algorithm used to decompose an integer in its prime factors.

3.4.1 Classical Fourier transform

We recall the formula defining the classical discrete Fourier transform (FT). The FT takes as input x_0, x_1, \dots, x_{N-1} and returns the output $\hat{x}_0, \hat{x}_1, \dots, \hat{x}_{N-1} \in \mathbb{C}$

$$\hat{x}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}; \quad k = 0, 1, \dots, N-1$$

where each x_j and y_k are in \mathbb{C} .

3.4.2 Quantum Fourier algorithm

The quantum Fourier transform (QFT) It is a unitary operator U_{QFT} that can be defined by its action on the computational basis $\{|j\rangle; j = 0, 1, \dots, N\}$ as

$$U_{\text{QFT}}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle \equiv |\hat{j}\rangle. \quad (3.10)$$

For an arbitrary input state $|\{x_j\}\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$, by linearity, we obtain

$$U_{\text{QFT}}|\{x_j\}\rangle = U_{\text{QFT}} \sum_{j=0}^{N-1} x_j |j\rangle = \sum_{j=0}^{N-1} x_j |\hat{j}\rangle = \sum_{k=0}^{N-1} \hat{x}_k |k\rangle$$

Hence, we can write:

$$U_{\text{QFT}}|\{x_j\}\rangle = |\text{FT}[\{x_j\}]\rangle = |\{\hat{x}_k\}\rangle \quad (3.11)$$

Exercise 11. — By an explicit calculation check the precedent result. Show that U_{QFT} is a unitary operator.

Now the basis states $|0\rangle, |1\rangle, \dots, |j\rangle, \dots, |N-1\rangle$, are encoded with n qubits. That is, we assume that $N = 2^n$, and the encoding is simply

$$\begin{aligned} |j=0\rangle &\equiv |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \equiv |00\dots 0\rangle \\ |j=1\rangle &\equiv |0\rangle \otimes |0\rangle \otimes \dots \otimes |1\rangle \equiv |00\dots 1\rangle \\ &\vdots \\ |j=N-1\rangle &\equiv |1\rangle \otimes |1\rangle \otimes \dots \otimes |1\rangle \equiv |11\dots 1\rangle \end{aligned}$$

We introduce the following notation:

Definition (Base 2 notation). — Let k an integer such that $0 \leq k < 2^n$, we note $[K_{n-1}K_{n-2}\dots K_1K_0]$ its expansion in base 2, where $K_j = 0, 1$. So,

$$k = 2^{n-1}K_{n-1} + 2^{n-2}K_{n-2} + \dots + 2K_1 + K_0 = [K_{n-1}K_{n-2}\dots K_1K_0]$$

Hence the basis states $\{|k\rangle\}$ are encoded as

$$|k\rangle \rightarrow |K_{n-1}K_{n-2}\dots K_1K_0\rangle; \text{ with } k = [K_{n-1}K_{n-2}\dots K_1K_0]$$

where we have used the notation of Eq. (2.5), page 22. It is advantageous to rewrite the exponential factor $e^{i\frac{2\pi jk}{2^n}}$ appearing in the definition of the QFT in Eq; (3.10) as follows:

$$e^{i\frac{2\pi jk}{2^n}} = \exp \left\{ i2\pi j \left(\frac{K_{n-1}}{2} + \frac{K_{n-2}}{2^2} + \dots + \frac{K_1}{2^{n-1}} + \frac{K_0}{2^n} \right) \right\}$$

which in turn can be factorized as

$$e^{i\frac{2\pi jk}{2^n}} = \exp \left(i2\pi j \frac{K_{n-1}}{2} \right) \exp \left(i2\pi j \frac{K_{n-2}}{2^2} \right) \times \dots \times \exp \left(i2\pi j \frac{K_1}{2^{n-1}} \right) \exp \left(i2\pi j \frac{K_0}{2^n} \right)$$

The sum $\sum_{k=0}^{n-1}$ in the definition of the QFT in Eq; (3.10), can be performed as

$$\sum_{k=0}^{n-1} = \sum_{K_{n-1}=0}^1 \sum_{K_{n-2}=0}^1 \dots \sum_{K_0=0}^1,$$

hence, the definition of the QFT given by Eq. (3.10) can be written as:

$$U_{\text{QFT}}|j\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{i\pi j} |1\rangle \right) \left(|0\rangle + e^{i\pi j/2} |1\rangle \right) \left(|0\rangle + e^{i\pi j/2^2} |1\rangle \right) \times \dots \times \left(|0\rangle + e^{i\pi j/2^{n-1}} |1\rangle \right).$$

Now, using the expression of j in base 2: $j = [J_{n-1}J_{n-2}\dots J_0]$, and the fact that $e^{i2\pi m} = 1$ if $m \in \mathbb{Z}$, we have

$$\begin{aligned} e^{i\pi j} &= e^{i\pi J_0} \\ e^{i\pi j/2} &= e^{i\pi J_1} e^{i\pi J_0/2} = \exp \left(i\frac{\pi}{2} [J_1 J_0] \right) \\ e^{i\pi j/2^2} &= e^{i\pi J_2} e^{i\pi J_1/2} e^{i\pi J_0/2^2} = \exp \left(i\frac{\pi}{2^2} [J_2 J_1 J_0] \right) \\ &\vdots \\ e^{i\pi j/2^{n-1}} &= e^{i\pi J_{n-1}} e^{i\pi J_{n-2}/2} \times \dots \otimes e^{i\pi J_0/2^{n-1}} = \exp \left(i\frac{\pi}{2^{n-1}} [J_{n-1} J_{n-2} \dots J_1 J_0] \right) \end{aligned}$$

that is:

$$e^{i\pi j/2^k} = \prod_{m=0}^k e^{i\pi J_{k-m}/2^m}; \text{ where } j = [J_{n-1}J_{n-1} \cdots J_0]$$

so we can write U_{QFT} in the following factorized form:

$$\begin{aligned} U_{\text{QFT}}|j\rangle &= U_{\text{QFT}}|J_{n-1}\rangle \otimes |J_{n-1}\rangle \otimes \cdots \otimes |J_0\rangle \\ &= \left(|0\rangle + e^{i\pi J_0}|1\rangle\right) \otimes \left(|0\rangle + e^{i\frac{\pi}{2}[J_1J_0]}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{i\frac{\pi}{2^{n-1}}[J_0J_1 \cdots J_{n-1}]}|1\rangle\right) \end{aligned}$$

the advantage of this expression is that it can be implemented using a sequence of Hadamard and controlled phase gates.

To see this, let define the phase gate R_k defined as the following one-qubit gate:

$$R_k|0\rangle = |0\rangle; \quad R_k|1\rangle = e^{i\pi/2^k}|1\rangle$$

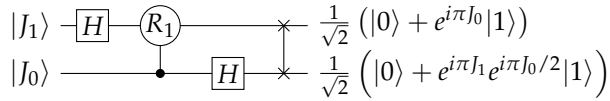
that is:

$$R_k|J\rangle = e^{i\pi J/2^k}|J\rangle; \quad (J = 0, 1).$$

Now, the controlled phase gate C_{R_k} can be defined as the following 2-qubit gates

$$C_{R_k}|0\rangle \otimes |J\rangle = |0\rangle \otimes |J\rangle; \quad C_{R_k}|1\rangle \otimes |J\rangle = e^{i\pi J/2^k}|1\rangle \otimes |J\rangle; \quad (J = 0, 1)$$

For $n = 2$ ($N = 4$), the following circuit diagram performs the QFT:

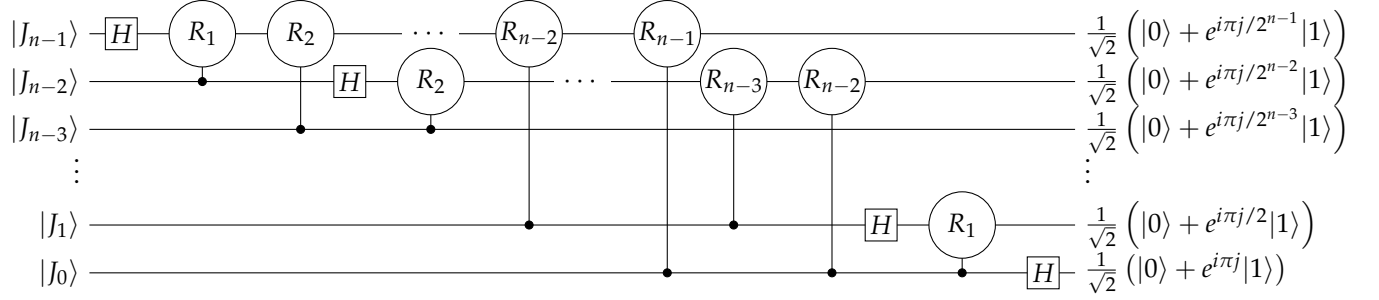


Indeed, let's take a closer look at each step:

$$\begin{aligned} |J_1\rangle \otimes |J_0\rangle &\xrightarrow{H \otimes \mathbb{1}} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{J_1}|1\rangle\right) \otimes |J_0\rangle \\ &\xrightarrow{C_{R_1}} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{J_1}e^{i\pi J_0/2}|1\rangle\right) \otimes |J_0\rangle \\ &\xrightarrow{\mathbb{1} \otimes H} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{J_1}e^{i\pi J_0/2}|1\rangle\right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi J_0}|1\rangle\right) \\ &\xrightarrow{\text{SWAP}} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi J_0}|1\rangle\right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{J_1}e^{i\pi J_0/2}|1\rangle\right) = |\hat{j}\rangle \end{aligned}$$

The last 2-qubit gate is the **swap**-gate and it is not really necessary.

For n qubits the circuit looks like:



This diagram allows an evaluation of the complexity of the QFT algorithm. Indeed, we can see that there are n H-gate and $(n-1) + (n-2) + \dots + 1 = n(n-1)/2$ C_R gates. Hence, the algorithm scales as $\mathcal{O}(n^2) = \mathcal{O}(\log^2(N))$ (where \log is the logarithm base 2).

The classical algorithm, The Fast Fourier Transform (FFT) algorithm, scales as $\mathcal{O}(N \log(N)) = \mathcal{O}(2^n n)$. Hence, the classical algorithm requires exponentially more operation than the QFT algorithm.

But, we don't know how to extract the \hat{x}_k from the \hat{x}_j using the QFT. We don't know how to compute the FFT of a function using the QFT. Nevertheless, the QFT algorithm can be useful for several tasks which are based on *phase estimation*.

3.5 Quantum phase estimation

Suppose that we are given the state $|\psi(\varphi)\rangle$ which depends on the phase φ as

$$|\psi(\varphi)\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi k\varphi} |k\rangle \text{ with } \varphi \in [0, 1[\text{ and } N = 2^n.$$

The objective is to estimate the value of φ .

When φ can be exactly expressed using n bits, that is, if it exists n binary digit $J_0, J_1, \dots, J_{n-1} = 0, 1$ such that $\varphi = \frac{j}{2^n}$ with $j = [J_{n-1}J_{n-2} \dots J_0]$ ($0 \leq j \leq 2^n - 1$). Then the state $|\psi(\varphi)\rangle$ can be written as

$$|\psi(\varphi)\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi kj/2^n} |k\rangle$$

so

$$\langle j' | \psi(\varphi) \rangle = \langle j' | U_{\text{QFT}}^\dagger | \psi(\varphi) \rangle = \delta_{jj'}.$$

Hence, a measurement in the basis $|\hat{j}\rangle = U_{\text{QFT}} |j\rangle$ ($j = 1, 2, \dots, 2^n - 1$) will give the exact result with probability 1.

If φ can not be exactly written as $\frac{j}{2^n}$ with $0 \leq j \leq 2^n - 1$, then $\langle \hat{j} | \psi(\varphi) \rangle$ will give a good approximation of the value of φ with high probability. Let's see how it works. Let's calculate $U_{\text{QFT}}^\dagger |\psi(\varphi)\rangle$:

$$U_{\text{QFT}}^\dagger |\psi(\varphi)\rangle = \sum_{\ell=0}^{2^n-1} \alpha_\ell |\ell\rangle \text{ with } \alpha_\ell = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{i2\pi k\varphi} e^{-i2\pi \frac{k\ell}{2^n}}$$

But α_ℓ can also be written as:

$$\alpha_\ell = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{i2\pi k(\varphi - \frac{\ell}{2^n})} = \frac{1}{2^n} \frac{1 - e^{i2\pi 2^n(\varphi - \frac{\ell}{2^n})}}{1 - e^{i2\pi(\varphi - \frac{\ell}{2^n})}} = \frac{1}{2^n} \frac{1 - e^{i2\pi 2^n \varphi}}{1 - e^{i2\pi(\varphi - \frac{\ell}{2^n})}}$$

let's introduce φ_n the better n -bit approximation to φ . That is, $\varphi_n = \frac{f_n}{2^n}$ with f_n an integer such that $0 \leq f_n \leq 2^n - 1$. Let's define δ the difference:

$$\delta = \varphi - \varphi_n = \varphi - \frac{f_n}{2^n} < \frac{1}{2^n},$$

defining the new index $j = \ell - f_n$, we have

$$\alpha_{f_n+j} = \frac{1}{2^n} \frac{1 - e^{i2\pi 2^n \delta}}{1 - e^{i2\pi(\delta - \frac{j}{2^n})}} =$$

and the probability that the measurement in the computational basis $\{|\ell\rangle\}$ gives the outcome $\ell = f_n + j$ is

$$|\alpha_{f_n+j}|^2 = \left(\frac{1}{2^n} \frac{\sin(\pi 2^n \delta)}{\sin(\pi[\delta - j/2^n])} \right)^2 \quad (3.12)$$

As $\delta < 1/2^n$, the maximum of the probability occurs for $j = 0$, which corresponds to the outcome $\ell = f_n$ associated with the better n -bit, approximation $\varphi_n = \frac{f_n}{2^n}$ to φ .

Now suppose that the outcome of the measurement is $j \neq 0$, we can accept it if it lies within some tolerance of the value of φ_n . Say that we consider it as an accurate estimation if $\frac{f_n+j}{2^n}$ is at least a m -bit ($m < n$) approximation of φ that is if the estimated φ lies in the range $\varphi \pm \frac{1}{2} \frac{1}{2^m}$. The failure probability is thus defined as (see Ref. ⁴ [3]):

$$\epsilon = \Pr \left(\left| \frac{j + f_n}{2^n} - \varphi \right| > \frac{1}{2} \frac{1}{2^m} \right).$$

But

$$\left| \frac{j + f_n}{2^n} - \varphi \right| > \frac{1}{2} \frac{1}{2^m} \Leftrightarrow |j + (f_n - 2^n \varphi)| > 2^{n-m-1}$$

and as the term $(f_n - 2^n \varphi)$ is strictly less than 1, we can write the failure probability as

$$\epsilon = \Pr \left(j \geq 2^{n-m-1} \text{ and } j \leq -2^{n-m-1} - 1 \right).$$

Hence,

$$\epsilon = 1 - \sum_{j=-2^{n-m-1}}^{2^{n-m-1}-1} |\alpha_{f_n+j}|^2$$

This probability of failure can be bounded in several way (see Ref. ⁵ [3, 7] for the details of the proofs)

The important point is that it can be shown that for (not so) large $a = n - m$, the probability of failure ϵ scale as:

$$\epsilon = \mathcal{O}(1/2^a).$$

⁴James M. Chappell, Max A. Lohe, Lorenz von Smekal, Azhar Iqbal, and Derek Abbott. A precise error bound for quantum phase estimation. *PLOS ONE*, (5):e19663, 2011

⁵James M. Chappell, Max A. Lohe, Lorenz von Smekal, Azhar Iqbal, and Derek Abbott. A precise error bound for quantum phase estimation. *PLOS ONE*, (5):e19663, 2011; and Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. Oxford University Press, 1. publ edition

In other words, the number of additional qubits a , we must add to the m qubits, such that the m -qubit accuracy is obtained with a failure probability less than ϵ scale as

$$a = \mathcal{O}(\log(1/\epsilon))$$

4

Appendix

4.1 Proof of Theorem 8

we will prove the following theorem,

$U(\alpha, \beta, \gamma) \in SU(2)$ if and only if it exists $\alpha, \gamma \in [0, 2\pi]$ and $\beta \in [0, \pi]$ such that

$$U(\alpha, \beta, \gamma) = U_z(\alpha)U_y(\beta)U_z(\gamma) = \exp\left(-i\frac{\alpha}{2}\sigma_3\right)\exp\left(-i\frac{\beta}{2}\sigma_2\right)\exp\left(-i\frac{\gamma}{2}\sigma_3\right)$$

Proof. By direct computation we can obtain:

$$U_z(\alpha)U_y(\beta)U_z(\gamma) = \left[\cos\frac{\gamma}{2}\cos\frac{\gamma+\beta}{2}\right]\mathbb{1} - i\left[\sin\frac{\gamma}{2}\sin\frac{\delta-\beta}{2}\right]X - i\left[\sin\frac{\gamma}{2}\cos\frac{\delta-\beta}{2}\right]Y - i\left[\cos\frac{\gamma}{2}\sin\frac{\gamma+\beta}{2}\right]Z$$

where X, Y, Z are the Pauli matrices.

We know that any $SU(2)$ operation can be written as

$$U_{\vec{n}}(\theta) = \exp(-i\vec{\sigma} \cdot \vec{n}\frac{\theta}{2}) = \cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}$$

where \vec{n} is a unit vector and σ is the vector of the Pauli matrices, $\vec{\sigma} = (X, Y, Z)^T$. Hence we have,

$$\begin{aligned}\cos\frac{\theta}{2} &= \cos\frac{\gamma}{2}\cos\frac{\gamma+\beta}{2} \\ n_x \sin\frac{\theta}{2} &= \sin\frac{\gamma}{2}\sin\frac{\delta-\beta}{2} \\ n_y \sin\frac{\theta}{2} &= \sin\frac{\gamma}{2}\cos\frac{\delta-\beta}{2} \\ n_z \sin\frac{\theta}{2} &= \cos\frac{\gamma}{2}\sin\frac{\gamma+\beta}{2}\end{aligned}$$

□

4.2 Computing $\exp\left(-i\vec{n} \cdot \vec{\sigma}\frac{\theta}{2}\right)$

We prove that

$$\exp\left(-i\vec{n} \cdot \vec{\sigma}\frac{\theta}{2}\right) = \cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\vec{n} \cdot \vec{\sigma}$$

For this, we first prove that $(\vec{n} \cdot \vec{\sigma})^2 = \mathbb{1}$.

Proof. By direct computation we have $Z^2 = \mathbb{1}$, hence $\vec{e}_z \cdot \vec{\sigma} = \mathbb{1}$, where \vec{e}_z is the unit vector in the Oz axis.

Now, Let's define R the rotation that bring \vec{e}_z to \vec{n} . That is $R[\vec{e}_z] = \vec{n}$. By the homomorphism between $SU(2)$ and $SO3$ (see theorem 7, page 25) We know that there is an unitary operator U such that

$$U\vec{e}_z \cdot \vec{\sigma} U^\dagger = [R\vec{e}_z] \cdot \vec{\sigma} = \vec{n} \cdot \vec{\sigma}$$

Hence,

$$(\vec{n} \cdot \vec{\sigma})^2 = (U\vec{e}_z \cdot \vec{\sigma} U^\dagger)^2 = UZU^\dagger UZU^\dagger = UZ^2U^\dagger = \mathbb{1}$$

□

Now we can prove that

$$\exp\left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right) = \cos \frac{\theta}{2} \mathbb{1} - i \sin \frac{\theta}{2} \vec{n} \cdot \vec{\sigma}$$

Proof. By expanding the exponential we have

$$\exp\left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right) = \sum_{k=0}^{\infty} \frac{1}{k!} \left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right)^k = \sum_{p=0}^{\infty} \frac{1}{2p!} \left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right)^{2p} + \sum_{p=0}^{\infty} \frac{1}{(2p+1)!} \left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right)^{2p+1}$$

where we have summed among even ($k = 2p$) an odd ($k = 2p + 1$) value of k separately.

As $\vec{n} \cdot \vec{\sigma}^2 = \mathbb{1}$, we have also $\vec{n} \cdot \vec{\sigma}^{2p} = \mathbb{1}$ and $\vec{n} \cdot \vec{\sigma}^{2p+1} = \vec{n} \cdot \vec{\sigma}$. Hence,

$$\exp\left(-i\vec{n} \cdot \vec{\sigma} \frac{\theta}{2}\right) = \mathbb{1} \sum_{p=0}^{\infty} \frac{1}{2p!} \left(\frac{\theta}{2}\right)^{2p} + \vec{n} \cdot \vec{\sigma} \sum_{p=0}^{\infty} \frac{1}{(2p+1)!} \left(\frac{\theta}{2}\right)^{2p+1}$$

but $\sum_{p=0}^{\infty} \frac{1}{2p!} \left(\frac{\theta}{2}\right)^{2p} = \cos \frac{\theta}{2}$ and $\sum_{p=0}^{\infty} \frac{1}{(2p+1)!} \left(\frac{\theta}{2}\right)^{2p+1} = \sin \frac{\theta}{2}$ □

Bibliography

- [1] Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, March 1993. Publisher: American Physical Society.
- [2] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *arXiv:quant-ph/0005055*, 2000.
- [3] James M. Chappell, Max A. Lohe, Lorenz von Smekal, Azhar Iqbal, and Derek Abbott. A precise error bound for quantum phase estimation. *PLOS ONE*, (5):e19663, 2011.
- [4] Andrew M. Childs, Debbie W. Leung, and Michael A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Physical Review A*, 71(3):032318, 2005.
- [5] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm, August 2005. *arXiv:quant-ph/0505030*.
- [6] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439(1907):553–558, 1992.
- [7] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. Oxford University Press, 1. publ edition.
- [8] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [9] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188–5191, 2001.

- [10] Christof Zalka. Grover's quantum searching algorithm is optimal.
Phys. Rev. A, 60:2746–2751, Oct 1999.