PHY580
Physics of Quantum Information

Laurent Sanchez-Palencia
lsp@cpht.polytechnique.fr

Lecture 1: The language of quantum information

January 4$^{\text{th}}$ 2022

Quantum information employs a specific language, adapted to the manipulation of qubits, which are the basic elements of information in the quantum field. This chapter is an introduction to this language. After a brief reminder of elementary notions about quantum state, unitary evolution, quantum coherence, and measurement theory, we introduce those of qubit and Bloch sphere, universally used in this field. We then describe elementary single-qubit and multi-qubit operations that allow us to efficiently manipulate quantum information. These form the elementary building blocks of quantum circuits, which are discussed at the end of the chapter.

1 Apetizer

The state of a generic quantum system is represented by a ket $|\psi\rangle \in \mathbb{C}^N$, where N is the dimension of the relevant Hilbert space $\mathscr{E}$. It may be expanded in an orthonormal basis $\{|n\rangle\,, n \in \mathbb{N}\}$ of $\mathscr{E}$ and reads as

$$|\psi\rangle = \sum_n c_n\,|n\rangle \qquad \text{with} \qquad \sum_n |c_n|^2 = 1. \tag{1}$$

Such a state is said to be a *coherent superposition* of the basis states $|n\rangle$. We shall see later that in the case of an open system, i.e. a system that is coupled to another one, the notion of state should be extended to that of density matrices.

1.1 State and measurements

More precisely, the quantum measurement theory states that a physical quantity $\mathcal{O}$ is represented by an Hermitian operator $\hat{\mathcal{O}}$ whose eigenvalues $\{\mathcal{O}_j, j \in \mathbb{N}\}$ form the set of possible results of the measurement of $\mathcal{O}$. The spectral theorem allows us to write the operator as

$$\hat{\mathcal{O}} = \sum_j \mathcal{O}_j \hat{\mathcal{P}}_j, \tag{2}$$

where $\hat{\mathcal{P}}_j$ is the projection operator onto the eigenstate of $\hat{\mathcal{O}}$ associated to the eigenvalue $\mathcal{O}_j$. This form is called the *spectral decomposition* of the observable $\hat{\mathcal{O}}$. A given eigenvalue $\mathcal{O}_j$ is obtained with a probability equal to the square modulus of the projection of the state $|\psi\rangle$ onto the corresponding eigen-subspace of $\hat{\mathcal{O}}$,

$$P_j = \left|\hat{\mathcal{P}}_j|\psi\rangle\right|^2. \tag{3}$$

After a measurement, the ket is projected onto the latter, $|\psi'\rangle \propto \hat{\mathcal{P}}_j|\psi\rangle$, and renormalized to ensure $\langle\psi'|\,\psi'\rangle = 1$, where $|\psi'\rangle$ is the after measurement state. The average of a series of measurements performed on the same system prepared each time in the same state $|\psi\rangle$ then reads as

$$\langle\mathcal{O}\rangle = \sum_j P_j\mathcal{O}_j = \langle\psi|\hat{\mathcal{O}}|\psi\rangle, \tag{4}$$

where we have used the spectral expansion (2).

1.2 Evolution operator

In between two measurements, the evolution of the state is governed by the Schrödinger equation

$$i\hbar\frac{d\,|\psi(t)\rangle}{dt} = \hat{H}(t)\,|\psi(t)\rangle\,, \tag{5}$$

where $\hat{H}(t)$ is the Hamiltonian. This evolution is unitary, i.e. it preserves the normalization of the ket, $\langle\psi(t)|\,\psi(t)\rangle = 1$ at any time t. This is a direct consequence of the fact that $\hat{H}(t)$ is an Hermitian operator ($\hat{H}^\dagger = \hat{H}$),

$$i\hbar\frac{d\,\langle\psi(t)|\,\psi(t)\rangle}{dt} = \underbrace{i\hbar\frac{d\,\langle\psi(t)|}{dt}}_{-\langle\psi(t)|\hat{H}^\dagger(t)}|\psi(t)\rangle + \langle\psi(t)|\underbrace{i\hbar\frac{d\,|\psi(t)\rangle}{dt}}_{+\hat{H}(t)|\psi(t)\rangle} = 0.$$

In quantum information theory, we shall, in many cases, disregard the time evolution and focus on processes changing the system from a certain state to another state. This is decribed by a unitary operator, known as the *evolution operator* $\hat{U}$.

From a general point of view, we may describe the action of a certain Hamiltonian onto the system from time t_0 to time t by

$$|\psi(t)\rangle = \hat{U}(t,t_0)\,|\psi(t_0)\rangle\,. \tag{6}$$

The existence of $\hat{U}(t,t_0)$ is a direct consequence of the linearity of the Schrödinger equation. For instance, it may be defined by its action on the states of a basis of $\mathscr{E}$. Moreover, norm conservation implies that $\hat{U}(t,t_0)$ is a unitary operator, i.e.

$$\hat{U}(t,t_0)^\dagger\hat{U}(t,t_0) = 1. \tag{7}$$

The equation of motion of $\hat{U}(t,t_0)$ is given by inserting Eq. (6) into the Schrödinger equation (5), which yields

$$\boxed{i\hbar\frac{\partial \hat{U}(t,t_0)}{\partial t} = \hat{H}(t)\hat{U}(t,t_0)}\,, \tag{8}$$

with the initial condition $\hat{U}(t_0,t_0) = 1$. In the simplest case where the Hamiltonian $\hat{H}$ is time-independent, the solution reads as[1]

$$\hat{U}(t,t_0) = \exp\left[-\frac{i}{\hbar}\hat{H}(t-t_0)\right]. \tag{9}$$

Assuming that the interaction time $t - t_0$ may be controlled, the evolution operator can be continuously tuned.

In the remainder of this chapter, we shall mainly work with evolution operators, rather than Hamiltonians, to describe the action of an aparatus onto the quantum system.

1.3 When does quantum coherence matter?

The state $|\psi\rangle$ defined in Eq. (1) is usually described saying that ”the system may be in any of the basis states $|n\rangle$ with probability $|c_n|^2$”. This is indeed what we obtain if we have at our disposal an observable $\hat{\mathcal{O}}$ that is diagonal in the basis $\{|n\rangle\}$ with nondegenerate eigenvalues, O_n. In such a case the measurement of the physical quantity $\mathcal{O}$ can return any of the values O_n with probability $P_n = |\hat{\mathscr{P}}_n\,|\psi\rangle\,|^2 = |c_n|^2$, where $\hat{\mathscr{P}}_n$ is the projector onto the eigenspace associated to O_n, here $\hat{\mathscr{P}}_n = |n\rangle\langle n|$. Such a description is, however, rather *classical* in the sense that we would obtain the same result assuming that the system is not a coherent superposition but just exactly in one of the states $|n\rangle$, each produced with probability P_n.

Observing quantum coherence

In order to fully appreciate the quantum nature – i.e. the quantum coherence – of the state in Eq. (1), it is necessary to use an observable $\hat{\mathcal{O}}$ that is nondiagonal in the basis $\{|n\rangle\}$. In practice, it amounts to perform an interference experiment. Consider for instance the observable

$$\hat{\mathcal{O}} = |+\rangle\langle +| - |-\rangle\langle -|\,, \tag{10}$$

[1] This formula is straightforwardly extended to the case where two Hamiltonians at any times commute, $[\hat{H}(t),\hat{H}(t')] = 0$, as

$$\hat{U}(t,t_0) = \exp\left[-\frac{i}{\hbar}\int_{t_0}^{t} dt\,\hat{H}(t')\right].$$

Note that this formula breaks down if two Hamiltonians at any times do not commute.

where

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \tag{11}$$

are the so-called *Hadamard states.* The operator $\hat{\mathcal{O}}$ returns $+1$ if the system is in the state $|+\rangle$, -1 if it is in the state $|-\rangle$, and 0 if it is in any state $|n\rangle$ with $n \geq 2$. The probability that the system in the state $|\psi\rangle$ as defined in Eq. (1) is measured in the state $|\pm\rangle$ is then

$$P_\pm = |\langle\pm|\psi\rangle|^2 = \frac{|c_0 \pm c_1|^2}{2} = \frac{|c_0|^2 + |c_1|^2 \pm 2\,|c_0|\,|c_1|\cos\left(\varphi_1 - \varphi_0\right)}{2}, \tag{12}$$

where φ_n is the phase of c_n, such that $c_n = |c_n|\mathrm{e}^{i\varphi_n}$. Here the probability of measuring such or such a value for the physical quantity $\mathcal{O}$ hence does not only depend on the probabilities $P_n = |c_n|^2$ but also on the relative phases $\varphi_n - \varphi_m$. Note that in contrast the gobal phase of the ket is irrelevant, since the probability of any measurement, $P_j(\mathcal{O}) = |\hat{\mathscr{P}}_j\,|\psi\rangle\,|^2$, is unaffected by the unitary transfrom $|\psi\rangle \to \mathrm{e}^{i\Phi}\,|\psi\rangle$.

A direct generalization is that two kets $|\psi\rangle$ and $|\psi'\rangle$ represent the same quantum state if and only if they differ only by a global phase, $|\psi'\rangle = \mathrm{e}^{i\Phi}\,|\psi\rangle$. Otherwise, one can always find a set of observables that allows us to distinguish them, see exercise 1, page 24. An immediate consequence is that a quantum system in a Hilbert space of dimension strictly higher than one contains a continuous infinite amount of information. For instance, a qubit, of state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, has four real-valued, continuous degrees of freedom (the real and imaginary parts of α and β) and only two constraints (the norm and the arbitrary phase which can be fixed by convention). This is to be distinguished from a classical bit, which contains a single binary information: It is either in the state 0 or 1. More generally, while the state of N classical bits is described by N binary values, that of N quantum bits is described by $2^{N+1} - 2$ continuous, real-valued, quantities.

The case discussed above is just the simplest example of a general statement, namely that taking advantage of quantum coherence beyond classical-like probabilities requires to perform measurements on sets of observables that do not commute with each other, so that there is no basis where they are all diagonal.

A useful trick

This may be a problem in practice. Assume for instance that you have a single observable $\hat{\mathcal{O}}$ at your disposal, an eigenbasis of which is $\{|n\rangle\,, n \in \mathbb{N}\}$, so that

$$\hat{\mathcal{O}} = \sum_n O_n\,|n\rangle\,\langle n|\,. \tag{13}$$

How can we appreciate the quantum coherence of the state $|\psi\rangle$? Since we do not have at our disposal a nondiagonal observable, we may instead manipulate the state and apply a unitary transform $|\psi\rangle \to \hat{U}^{-1}\,|\psi\rangle$ so as to rotate the state in the Hilbert space and transform the states $|\pm\rangle$ we would like to measure into the bais states $|0\rangle$ and $|1\rangle$ we can measure. This corresponds to the operation[2]

$$\hat{U}^{-1} \;=\; |0\rangle\langle +| \;+\; |1\rangle\langle -| \;+\; \sum_{n>1} |n\rangle\langle n| \,. \tag{14}$$

Hence, measuring, respectively, $|0\rangle$ and $|1\rangle$ after the rotation is equivalent to having measured, respectively, $|+\rangle$ and $|-\rangle$ before the rotation. We can thus have a signature of the quantum state coherence performing first the rotation $\{|+\rangle, |-\rangle; |n\rangle, n > 1\} \longrightarrow \{|0\rangle, |1\rangle; |n\rangle, n > 1\}$ and then the measurement in the the basis $\{|0\rangle, |1\rangle; |n\rangle, n > 1\}$.

Note that the transformation $\hat{U}^{-1}$, and equivalently the transformation $\hat{U}$, is a legitimate operation since it is unitary. It indeed transforms the orthonormal basis $\{|+\rangle; |-\rangle; |n\rangle, n > 1\}$ into the orthonormal basis $\{|n\rangle, n \in \mathbb{N}\}$. The unitarity of $\hat{U}^{-1}$ can be checked directly by writting that $\hat{U}$ realizes the opposite of $\hat{U}^{-1}$, i.e.

$$\hat{U} \;=\; |+\rangle\langle 0| \;+\; |1\rangle\langle -| \;+\; \sum_{n>1} |n\rangle\langle n| \,, \tag{15}$$

so that

$$\hat{U}^{\dagger}\hat{U} = |0\rangle\langle 0| \;+\; |1\rangle\langle 1| \;+\; \sum_{n>1} |n\rangle\langle n| = 1. \tag{16}$$

The generalization of this operation is straightforward: In order to measure a state in a *measurement basis* $\{|m_j\rangle, j \in \mathbb{N}\}$, we can first apply the unitary transformation from $\{|m_j\rangle, j \in \mathbb{N}\}$ to $\{|n\rangle, n \in \mathbb{N}\}$ and then realize the mesurement in the latter. One may, optionally get back from the basis $\{|n\rangle, n \in \mathbb{N}\}$ to the basis $\{|m_j\rangle, j \in \mathbb{N}\}$ using the inverse transformation.

Summary

1. The state of a quantum system contains a continuous infinity of information. It is encapsulated in the N complex-valued coefficients of its expansion in a basis, where N is the dimension of the Hilbert space. Only the global phase is irrelevant.

2. Quantum coherence is appreciated by using a set of observables that do not commute with each other.

3. Measuring in a certain basis means measuring an observable that is diagonal in this basis. If we do not have such an observable at our disposal, we may first rotate the state and measure it in another basis.

[2] The sum term is written in gray because it is irrelevant here and can be disregarded in the discussion.

2 Qubits and Bloch sphere

In the remainder of this chapter and many of the following ones, we shall restrict ourselves to qubits.

2.1 What is a qubit?

A qubit – i.e. a quantum bit – is just the simplest realization of a system hosting quantum coherence, namely a quantum system living in a $N = 2$-dimensional Hilbert space. Any state of a qubit may be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha\begin{bmatrix}1\\ 0\end{bmatrix} + \beta\begin{bmatrix}0\\ 1\end{bmatrix}, \tag{17}$$

with $|\alpha|^2 + |\beta|^2 = 1$ and $\{|0\rangle, |1\rangle\}$ is an arbitrarily chosen orthonormal basis. In the following, it is called the *computational basis.* Since the absolute phase of the qubit is irrelevant, we may arbitrary decide that α is a real, nonnegative number and write the state as

$$\boxed{|\psi\rangle = \underbrace{\cos(\theta/2)}_{\alpha}\,|0\rangle + \underbrace{\sin(\theta/2)\mathrm{e}^{i\varphi}}_{\beta}\,|1\rangle}\,, \tag{18}$$

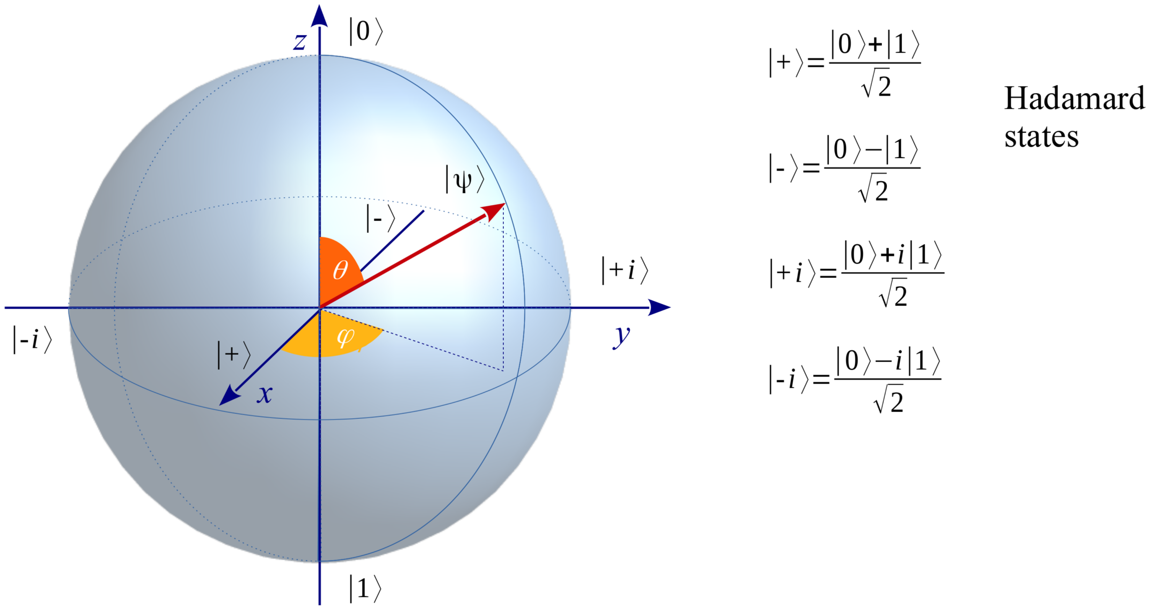
with $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi[$. The angle θ serves to determine the relative weights of the states $|0\rangle$ and $|1\rangle$, and the cos and sin assure normalization. The angle φ determines the relative phase. The interest of such a notation should not be underestimated and will appear clearer below.

The name ”qubit” was coined by analogy with classical bits used in computer science. Digital information is usually encoded in a series of 0's and 1's. Each digit is a bit. In classical physics, there are just only two possibilities : It can be either 0 or 1. A qubit can instead be in 0 or 1 or any quantum superposition of the two. A discussed above, the qubit state may be parametrized by the angles $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi[$. This illustrates the twofold continuous infinity of information contained in a qubit. Hence a *quantum register* – i.e. a set of qubits – can, in principle, contain infinitely more information than its classical counterpart.

2.2 Bloch sphere picture

Since the state $|\psi\rangle$ is fully determined by two angles, reminiscent of the polar and azimutal angles in spherical coordinates, it can be represented by the vector

$$\vec{\psi} = (1, \theta, \varphi) \tag{19}$$



$|0\rangle$
z
$|\psi\rangle$
$|-\rangle$
θ
$|+i\rangle$
$|-i\rangle$
$|+\rangle$
φ
x
y
$|1\rangle$
$|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
$|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
$|+i\rangle=\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$
$|-i\rangle=\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$
Hadamard states

Figure 1: Bloch sphere. The qubit state (18) is represented by the unit vector $\vec{\psi}$ of polar angle θ and azimutal angle φ. The positive axis vectors are $|+\rangle$, $|+i\rangle$, and $|0\rangle$, respectively. The negative ones are $|-\rangle$, $|-i\rangle$, and $-|1\rangle$, respectively.

in spherical coordinates on the unit sphere, see Fig. 1. The vector $\vec{\psi}$ is known as the *Bloch vector*. It yields an extremely fruitful geometrical representation of the qubit state and is widely used in quantum information science to represent the qubit state and operations on it. It was first introduced in the context of classical optics by Poincaré. It was then extended to quantum spin systems and popularized by Félix Bloch in the context of nuclear magnetic resonance. In the context of quantum information, it is known as the *Bloch sphere*. The *Poincaré sphere* is sometimes used in quantum optics, which corresponds to a slightly different parametrization of the angles.

A few states

Note that the vector opposite to the vector $\vec{\psi}=(\theta,\varphi)$ is

$$-\vec{\psi}=(\pi-\theta,\varphi+\pi), \tag{20}$$

where we have dropped the radial coordinate, which is irrelevant here. The associated state is

$$\begin{aligned} |-\psi\rangle &= \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle+\sin\left(\frac{\pi-\theta}{2}\right)\mathrm{e}^{i(\varphi+\pi)}\,|1\rangle \qquad (21)\\ &= \sin(\theta/2)\,|0\rangle-\cos(\theta/2)\mathrm{e}^{i\varphi}\,|1\rangle \qquad (22)\end{aligned}$$

Hence, we find $\langle -\psi|\psi\rangle = 0$. It follows that

$$\boxed{\text{Orthogonal qubit states are represented by opposite Bloch vectors.}}$$

We may now examine some particular and useful states:

- The state $|+\vec{e}_z\rangle$ corresponds to $\theta = 0$ and φ is irrelevant, i.e.

  $$|+\vec{e}_z\rangle = |0\rangle\,.$$

  By convention, we shall choose $\varphi = -\pi$.

- The state $|-\vec{e}_z\rangle$ corresponds to $\theta = \pi$ and φ is undetermined. Consistently with Eq. (20) and the arbitrary convention above, we shall choose $\varphi = 0$

  $$|-\vec{e}_z\rangle = |1\rangle\,.$$

- The state $|+\vec{e}_x\rangle$ corresponds to $\theta = \pi/2$ and $\varphi = 0$, i.e.

  $$|+\vec{e}_x\rangle \equiv |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

  which is one of the Hadamard states introduced above, see Eq. (11).

- The state $|-\vec{e}_x\rangle$ corresponds to $\theta = \pi/2$ and $\varphi = \pi$, i.e.

  $$|-\vec{e}_x\rangle \equiv |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

  which is the second Hadamard state introduced above, see Eq. (11).

- The state $|+\vec{e}_y\rangle$ corresponds to $\theta = \pi/2$ and $\varphi = \pi/2$, i.e.

  $$|+\vec{e}_y\rangle \equiv |+i\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}.$$

- Finally, the state $|-\vec{e}_y\rangle$ corresponds to $\theta = \pi/2$ and $\varphi = 3\pi/2$, i.e.

  $$|-\vec{e}_y\rangle \equiv |-i\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}.$$

These states are all shown in Fig. 1.

Qubit states in the spin representation

In some occasions, it is fruitful to assimilate a qubit to a 1/2-spin and use the correspondance $|0\rangle = |{\uparrow}\rangle_z$ and $|1\rangle = |{\downarrow}\rangle_z$. The states $|{\uparrow}\rangle_z$ and $|{\downarrow}\rangle_z$, which may also be denoted $|\pm\rangle_z$, are the polarized states along $+\mathrm{e}_z$ and $-\mathrm{e}_z$, respectively. The state $|\psi\rangle$ in Eq. (18) is nothing but the polarized state along its associated Bloch vector $\vec{\psi}$, i.e. the eigenstate associated to the eigenvalue +1 of the corresponding spin operator $\vec{\psi}\cdot\hat{\vec{\sigma}}$, where $\hat{\vec{\sigma}} = \hat{X}\vec{\mathrm{e}}_x + \hat{Y}\vec{\mathrm{e}}_y + \hat{Z}\vec{\mathrm{e}}_z$ and

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \quad \hat{Y} = \begin{bmatrix} 0 & -i \\ +i & 0 \end{bmatrix} \quad , \quad \hat{Z} = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix} \tag{23}$$

are the Pauli matrices. This is easily checked by showing $\left(\vec{\psi}\cdot\hat{\vec{\sigma}}\right)|\psi\rangle = |\psi\rangle$. Moreover, it immediately follows that $(-\vec{\psi})\cdot\hat{\vec{\sigma}}\ |\psi\rangle = -|\psi\rangle$ so that

$$|\psi\rangle = |+\rangle_{+\vec{\psi}} = |-\rangle_{-\vec{\psi}}\,, \tag{24}$$

that is $|\psi\rangle$ is the eigenstate of $(-\vec{\psi})\cdot\hat{\vec{\sigma}}$ of eigenvalue -1. It may finally be checked that $\vec{\psi}$ is nothing but the average spin vector of the state $|\psi\rangle$,

$$\langle\psi|\,\hat{\vec{\sigma}}\,|\psi\rangle = \vec{\psi}. \tag{25}$$

A direct consequence is that the state of a 1/2-spin is completely determined by the average value of the spin vector operator, up to the gobal phase. All these properties are shown in exercise 2, page 24.

Bloch sphere representation

In summary, the quantum state of a qubit,

$$|\psi\rangle = \underbrace{\cos(\theta/2)}_{\alpha}|0\rangle + \underbrace{\sin(\theta/2)\mathrm{e}^{i\varphi}}_{\beta}|1\rangle\,,$$

may be represented by a vector pointing at the surface of the Bloch sphere. It corresponds to the unit vector $\vec{\psi} = (\theta,\varphi)$ in spherical coordinates. The qubit state is the eigenstate of the spin operator projected onto the direction of $\vec{\psi}$, i.e. $|\psi\rangle = |+\rangle_{\vec{\psi}}$. The Bloch vector $\vec{\psi}$ is the quantum average of the spin operator,

$$\vec{\psi} = \langle\psi|\hat{\vec{\sigma}}|\psi\rangle\,,$$

where $\hat{\vec{\sigma}} = \hat{X}\vec{\mathrm{e}}_x + \hat{Y}\vec{\mathrm{e}}_y + \hat{Z}\vec{\mathrm{e}}_z$ and the operators

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \quad \hat{Y} = \begin{bmatrix} 0 & -i \\ +i & 0 \end{bmatrix} \quad \text{, and} \quad \hat{Z} = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}$$

are the Pauli matrices.

2.3 Manipulation and measurement of a qubit

Since any qubit states is represented by a vector pointing at the surface of the Bloch sphere, any operation performed on a single qubit can always be seen as a rotation on the surface of the Bloch sphere. For instance, one can transform the state $|0\rangle$ into the state $|+\rangle$ or $|-\rangle$ by the $\pi/2$-rotation of the Bloch vector $\vec{\psi}$ around the y axis in the anticlockwise or clockwise direction, respectively. On can transform the same state $|0\rangle$ into the state $|+i\rangle$ or $|-i\rangle$ by a $\pi/2$-rotation of the Bloch vector $\vec{\psi}$ around the x axis in the clockwise or anticlockwise direction, respectively. The implementation of such a rotation depends on the physical realization of the qubit. In the case of a physical 1/2-spin, it may be realized by a Larmor precession induced by an appropriate magnetic field.

Rotation on the Bloch sphere

Generally, the transformation of a state into another is represented by a rotation of the Bloch vector around an axis orthogonal to both the initial and final Bloch vectors:

The transformation of any qubit state $|\psi\rangle$ into any other state $|\psi'\rangle$ is represented by the rotation of the Bloch vector around the axis oriented by $\vec{n} = \frac{\vec{\psi}\times\vec{\psi}'}{|\vec{\psi}\times\vec{\psi}'|}$ in the anticlockwise direction by the angle $\alpha = \arccos\left(\vec{\psi}\cdot\vec{\psi}'\right)$, see Fig. 2(a).

We recall that such a rotation is generated by the dynamical equation

$$\frac{d\vec{\psi}}{dt} = \omega\,\vec{n}\times\vec{\psi}, \tag{26}$$

which describes the precession of the Bloch vector $\vec{\psi}$ around the unit vector $\vec{n}$ at the angular velocity ω. The rotation of angle α is thus obtained by applying this precession for a duration $t = \alpha/\omega$. This rotation applies to the Bloch vector in the 3D geometrical space.

Consider now an arbitrary quantum operation on the qubit, generated by some Hamitonian $\hat{H}$. Since the Pauli matrices complemented by the identity form a generator of the ensemble of Hermitian operators acting on any two-dimensional Hilbert space, one can always write $\hat{H} = h_0\hat{1} + h_x\hat{X} + h_y\hat{Y} + h_z\hat{Z}$ or, equivalently,

$$\hat{H} = h_0\hat{1} + \frac{\hbar\omega}{2}\vec{n}\cdot\hat{\vec{\sigma}}, \tag{27}$$

where $\omega \in \mathbb{R}_+$ and $\vec{n}$ is a unit, real-valued, three-dimensional vector. The evolution operator $\hat{U} = \mathrm{e}^{-i\hat{H}t/\hbar}$ then reads as

$$\hat{U} = \mathrm{e}^{i\Phi}\hat{R}_{\vec{n}}(\alpha) \qquad \text{with} \qquad \hat{R}_{\vec{n}}(\alpha) = \exp\left(-i\frac{\alpha\vec{n}\cdot\hat{\vec{\sigma}}}{2}\right) \qquad \text{and} \qquad \alpha = \omega t\ . \tag{28}$$

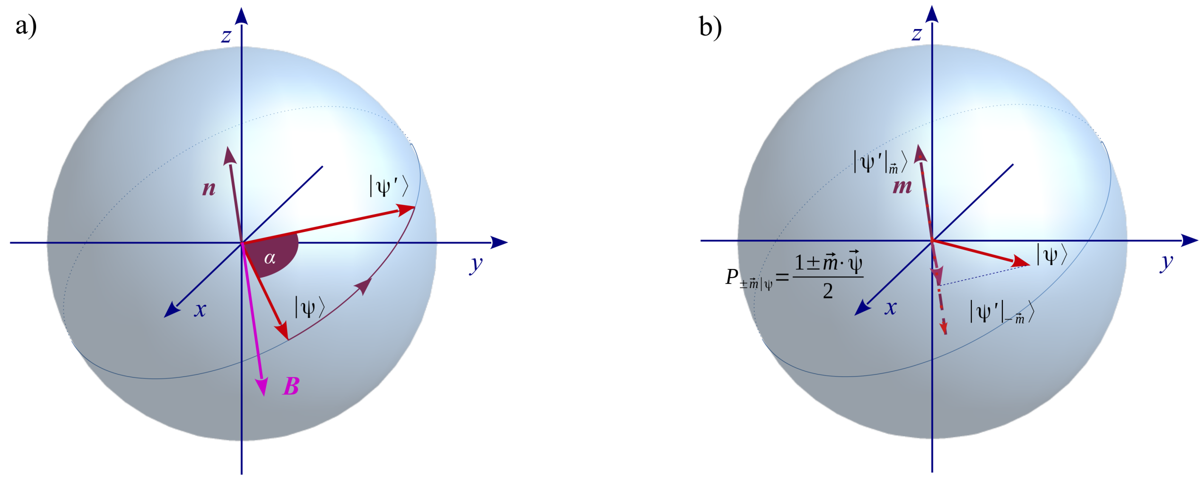

a)
z
n
|ψ'⟩
α
y
x
|ψ⟩
B
b)
z
$|\psi'|_{\vec{m}}\rangle$
m
$|\psi\rangle$
y
$P_{\pm\vec{m}|\psi}=\frac{1\pm\vec{m}\cdot\vec{\psi}}{2}$
x
$|\psi'|_{-\vec{m}}\rangle$

Figure 2: Manipulation of a qubit state within the Bloch sphere. (a) Single-qubit gate. Any unitary transformation of the qubit state from $|\psi\rangle$ to $|\psi'\rangle$ is represented by the rotation of angle $\alpha = \arccos\left(\vec{\psi}\cdot\vec{\psi}'\right)$ in the anticlockwise direction around the axis oriented by $\vec{n} = \frac{\vec{\psi}\times\vec{\psi}'}{\left|\vec{\psi}\times\vec{\psi}'\right|}$. For a physical spin associated to a magnetic momentum, it can be realized by a Larmor precession driven by an appropriate magnetic field $\vec{B}$. (b) Measurement. A measurement is represented by a projection followed by the renormalization of the Bloch vector to preserve its norm. If the spin along $\vec{m}$ is measured, one projects the Bloch vector $\vec{\psi}$ onto the measurement axis $\vec{m}$. The probability to measure ± 1 is $P_{\pm\vec{m}|\psi} = \frac{1\pm\vec{m}\cdot\vec{\psi}}{2}$. It ± 1 is measured, the after measurement Bloch vector is $\vec{\psi}'_{\pm\vec{m}} = \pm\vec{m}$.

The global phase, $\Phi = -h_0 t/\hbar$, generated by the identity component of the Hamiltonian, see Eq. (27), is irrelevant. The operator $\hat{R}_{\vec{n}}(\alpha)$ represents the rotation of the qubit state by the angle α around the unit vector $\vec{n}$ in Hilbert space. This can be checked using the Ehrenfest theorem,

$$\frac{d\langle\hat{\vec{\sigma}}\rangle}{dt} = \frac{1}{i\hbar}\left\langle\left[\hat{\vec{\sigma}},\hat{H}\right]\right\rangle . \tag{29}$$

Using the commutation relations of the Pauli matrices and the Bloch vector identity $\vec{\psi} = \langle\hat{\vec{\sigma}}\rangle$, it yields Eq. (26), see exercise 3, page 24.

Rotation on the Bloch sphere
Any operation on a qubit is generated by some Hamiltonian, which can be cast, without loss of generality, in the form

$$\hat{H} = h_0 \hat{1} + \frac{\hbar\omega}{2} \vec{n} \cdot \hat{\vec{\sigma}}, \tag{30}$$

where $\omega \in \mathbb{R}_+$ and $\vec{n}$ is a unit, real-valued, vector. The evolution operator then reads as

$$\hat{U} = \mathrm{e}^{i\Phi} \hat{R}_{\vec{n}}(\alpha) \qquad \text{with} \qquad \hat{R}_{\vec{n}}(\alpha) = \exp\left(-i \frac{\alpha \vec{n} \cdot \hat{\vec{\sigma}}}{2}\right) . \tag{31}$$

Up to the irrelevant global phase Φ, it is represented by the rotation of the Bloch vector $\vec{\psi} = \langle \hat{\vec{\sigma}} \rangle$ by the angle α around the axis oriented by the vector $\vec{n}$.

Note that $\hat{R}_{\vec{n}}(\alpha)$ is the rotation operator to be applied onto the quantum qubit state $|\psi\rangle$ in the Hilbert space. It has to be distinguished from the rotation operator to be applied onto the Bloch vector in geometrical space, $\mathcal{R}_{\vec{n}}(\alpha)$. The matrix representations of the two are of course different. For instance, for a rotation of angle α along axis z, we have

$$\hat{R}_z(\alpha) = \begin{bmatrix} \mathrm{e}^{-i\alpha/2} & 0 \\ 0 & \mathrm{e}^{+i\alpha/2} \end{bmatrix} \qquad \text{and} \qquad \mathcal{R}_{\vec{n}}(\alpha) = \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{32}$$

Finally, it is worth noting that the rotation operator in the Hilbert space can be written

$$\boxed{\hat{R}_{\vec{n}}(\alpha) = \cos(\alpha/2)\ \hat{I} - i \sin(\alpha/2)\ \vec{n} \cdot \hat{\vec{\sigma}}} \ . \tag{33}$$

This can be shown using standard properties of the Pauli matrices, see exercise 4, page 25.

Measurement

In contrast, the effect of a measurement on the Bloch sphere representation is more tricky. Assume the qubit is in the state $|\psi\rangle$ as written in Eq. (18) and measure the spin along the axis oriented by the unit vector $\vec{m} = (\theta', \varphi')$. It is straightforward to show that the probabilities to measure ±1 are

$$\boxed{P_{\pm\vec{m}|\psi} = \frac{1 \pm \vec{m} \cdot \vec{\psi}}{2}} , \tag{34}$$

respectively, see exercise 5, page 25. The probability of measuring +1 is thus given by the projection of the Bloch vector $\vec{\psi}$ onto the measurement direction $\vec{m}$. The Bloch vector after the measurement is then $\vec{\psi}' = \vec{m}$ with probability $P_{+\vec{m}|\psi}$ and $\vec{\psi}' = -\vec{m}$ with probability $P_{-\vec{m}|\psi}$, see Fig. 2(b).

Summary
The Bloch sphere is a very useful – and widely used – representation of a single-qubit states. Almost any unitary operation on the qubit can be represented by a rotation of the Bloch vector. The only exception is the application of a global phase. While it is irrelevant for a single qubit, it may be useful in quantum circuits.

3 Quantum gates

We now discuss a number of operations that can be performed on qubits. As discussed above, the elementary quantum operations are described by unitary operators $\hat{U}$. In the context of quantum information, such operations are called *quantum gates.* The main ones are single or two, or even three, qubit gates, which we discuss below. It is essential to get used to them and learn how to read and manipulate them in order to simplify the design of efficient quantum circuits and algorithms. In addition, there are measurement operations, which are neither unitary nor reversible, but also play a decisive role in reading the results of operations.

3.1 Single-qubit gates

Unitary operations on a qubit may be realized by application of an appropriate Hamiltonian for a certain time. Since the latter can be controlled, such transformations are continuous. In quantum information theory, a unitary operation on one qubit is called a *single-qubit gate.* As discussed above, it is nothing but a rotation on the Bloch sphere surface. In quantum circuits, it is schematically represented by a box with an incoming line and and outgoing line:

$$|\psi\rangle \;-\!\boxed{U}\!\rightarrow \hat{U}\,|\psi\rangle \;\;.$$

In order to ease the graphical representation of quantum algorithms, one defines a number of elementary single-qubit gates. The most famous ones are described in table 1.

A few single-qubit gates

The first ones are the generators of the rotations on the Bloch sphere, namely the Pauli matrices $\hat{X}$, $\hat{Y}$, and $\hat{Z}$. In particular, the Pauli-X gate exchanges the two basis states $|0\rangle$ and $|1\rangle$. It is also called the NOT gate by analogy with classical gates: $|\text{NOT } 0\rangle = |1\rangle$ and $|\text{NOT } 1\rangle = |0\rangle$. The Pauli-$Z$ gate imprints a phase flip π to the qubit state $|1\rangle$ while preserving the state $|0\rangle$. The gates S and T, and more generally the arbitrary phase gate

$$-\boxed{\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{i\varphi}\end{bmatrix}}-$$

Name (nick-name)	Gate	Matrix	Action
Pauli-X (NOT)	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	Exchanges the states $\lvert 0\rangle$ and $\lvert 1\rangle$; Note that $\lvert \text{NOT } 0\rangle = \lvert 1\rangle$ and vice-versa.
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	Exchanges the states $\lvert 0\rangle$ and $\lvert 1\rangle$ and imprints the phases $\pm\pi/2$.
Pauli-Z (PHASE FLIP)	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	Imprints the phase π onto $\lvert 1\rangle$, while preserving $\lvert 0\rangle$.
Phase (S)	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$	Imprints the phase $\pi/2$ onto $\lvert 1\rangle$, while preserving $\lvert 0\rangle$.
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\pi/4} \end{bmatrix}$	Imprints the phase $\pi/4$ onto $\lvert 1\rangle$, while preserving $\lvert 0\rangle$.
Rotation	$-\boxed{R_{\vec{n}}(\alpha)}-$	$\begin{bmatrix} \cos\left(\frac{\alpha}{2}\right) - in_z \sin\left(\frac{\alpha}{2}\right) & -\sin\left(\frac{\alpha}{2}\right)(in_x + n_y) \\ -\sin\left(\frac{\alpha}{2}\right)(in_x - n_y) & \cos\left(\frac{\alpha}{2}\right) + in_z \sin\left(\frac{\alpha}{2}\right) \end{bmatrix}$	Rotates the qubit (Bloch vector) by an angle α around the axis oriented by $\vec{n}$.
Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	Basis transform from $\{\lvert 0\rangle, \lvert 1\rangle\}$ to $\{\lvert +\rangle, \lvert -\rangle\}$ and vice-versa.

Table 1: Single qubit gates. The matrix representations are written in the computational basis $\{\lvert 0\rangle, \lvert 1\rangle\}$, in this order.

are generalizations of the Pauli-Z gate imprinting a phase $\pi/2$, $\pi/4$, and φ onto the sole qubit state $\lvert 1\rangle$ while preserving the qubit state $\lvert 0\rangle$.[3] The general rotation gate, $\hat{R}_{\vec{n}}(\alpha)$,

[3] The gate T is called $\pi/8$ while a $\pi/4$ appears in its matrix repesentation because, in a more symmetric manner, we may write

$$\hat{T} = \mathrm{e}^{i\pi/8}\begin{bmatrix} \mathrm{e}^{-i\pi/8} & 0 \\ 0 & \mathrm{e}^{+i\pi/8} \end{bmatrix}.$$

amounts to rotate the Bloch vector by angle α around the axis oriented by $\vec{n}$, see Sec. 2.3.

Combining single-qubit gates

It is worth noting that the various gates are not independent of each other. Indeed, some gates may be realized by combining other ones. For instance, we find

$$-\boxed{T}-\boxed{T}- = \qquad\qquad , \tag{35}$$

and

$$-\boxed{Z}-\boxed{X}- = \qquad\qquad , \tag{36}$$

see exercise 6, page 25. Note that the gates are chained from left to right, while the operators are chained from right to left. Hence, the circuit above applies first $\hat{Z}$ and then $\hat{X}$.

Hadamard gate and relatives

Another class of single-qubit gates are the basis changing gates. The most popular one is the *Hadamard gate*, which transforms the eigenbasis of $\hat{Z}$, i.e. the computational basis $\{|0\rangle\,, |1\rangle\}$, into that of $\hat{X}$, i.e. $\{|+\rangle\,, |-\rangle\}$ as defined in Fig 1,

$$-\boxed{\{|0\rangle\,, |1\rangle\} \leftrightarrow \{|+\rangle\,, |-\rangle\}}- = -\boxed{H}- \,. \tag{37}$$

Similarly, one can construct the gate that changes the eigenbasis of $\hat{Z}$ into that of $\hat{Y}$. It is nothing but

$$-\boxed{\{|0\rangle\,, |1\rangle\} \rightarrow \{|+i\rangle\,, |-i\rangle\}}- = \qquad\qquad , \tag{38}$$

see exercise 7, page 25. Note that the Hadamard (H) and phase (S) gates do not commute.

A few simple properties of single-qubit gates

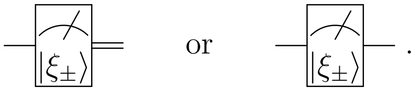
Let us conclude this section by a few straightforward properties of single-qubit gates.

> All single-qubit gates are
>
> (i) deterministic,
>
> (ii) unitary and thus reversible,
>
> (iii) continuous in the sense discussed above.

These properties can be easily checked for all single-qubit gates listed in table 1. For instance, the $\hat{X}$, $\hat{Y}$, $\hat{Z}$, and $\hat{H}$ gates are involutory, i.e. they are their own inverse. In contrast, we have $\hat{S}^{-1} = \hat{S}^{\dagger}$, $\hat{T}^{-1} = \hat{T}^{\dagger}$, and $\hat{R}_{\vec{n}}(\alpha)^{-1} = \hat{R}_{\vec{n}}(-\alpha)$.

3.2 Measurements

A completely different class of operations that are useful to perform on single-qubits is that of measurement operations. It is repesented by the symbol



where $|\xi_\pm\rangle$ indicates the measurement basis. The two outgoing lines represent the two possible outcomes of the measurement. This is a classical channel due to the decoherence effect induced by the measurement. When not useful, however, it may be represented by a single outgoing line. In direct opposition to the the gates discussed above

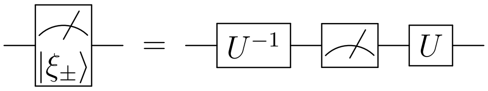
A measurement operation is

(i) nondeterministic,

(ii) nonunitary and irreversible,

(iii) discrete.

The measurement basis is not shown for a measurement in the computational basis, i.e. for $|\xi_+\rangle = |0\rangle$ and $|\xi_-\rangle = |1\rangle$. A measurement in a basis different from the computational basis may be represented by the simple quantum circuit



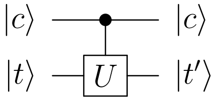
where $\hat{U}$ is the unitary operation transforming the computation basis $\{|0\rangle, |1\rangle\}$ into the measurement basis $\{|\xi_+\rangle, |\xi_-\rangle\}$, see discussion in Sec. 1.3, page 4.

3.3 Multi-qubit gates

So far, we have focused on single-qubit gates. With a view towards building a quantum computer, however, we would like to make several qubits interact with each other and hence build multi-qubit gates.

Controlled gates

In analogy with classical computing, an important class of two-qubit gates is made of so-called *controlled gates*, i.e. gates that act on a *target qubit* $|t\rangle$ depending on the state of a *control qubit* $|c\rangle$. Such an operation is represented by

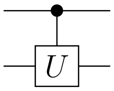


where $|t'\rangle = |t\rangle$ if $|c\rangle = |0\rangle$ and $|t'\rangle = \hat{U}\,|t\rangle$ if $|c\rangle = |1\rangle$, and $\hat{U}$ is a single-qubit gate. The two-qubit gate above is called the *controlled-U gate*. Since the two-qubit gate is linear, for $|c\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, we have

$$\boxed{|c\rangle \otimes |t'\rangle = \alpha\;\; |0\rangle \otimes |t\rangle \;\;+\;\; \beta\;\; |1\rangle \otimes \hat{U}\,|t\rangle}\,. \tag{39}$$

Note that the state of the control qubit is never affected by a controlled gate.

It may also be useful to represent the gate in its matrix form. For the controlled-U gate, it reads as



$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{$\hat{U}$}} \\ 0 & 0 & & \end{bmatrix},$$

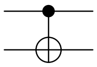
in the basis $\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}$. Indeed, a two-qubit state such that $|c\rangle = |0\rangle$ is represented as follows and is unchanged,

$$\begin{bmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{bmatrix} \longrightarrow \begin{bmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{bmatrix}.$$

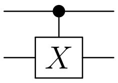
In contrast, a two-qubit state such that $|c\rangle = |1\rangle$ is represented and transforms as follows:

$$\begin{bmatrix} 0 \\ 0 \\ \alpha \\ \beta \end{bmatrix} \longrightarrow \begin{bmatrix} 0 \\ 0 \\ \hat{U} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \end{bmatrix}.$$

Some of the most useful two-qubit controlled gates are listed in table 2. The most celebrated one is the so-called CNOT gate,



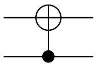
$=$



$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{40}$$

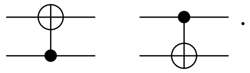
which applies the Pauli-X (NOT, see table 1) to the target qubit if and only if the control qubit is in the state $|1\rangle$.

Note that the control qubit is not necessarily placed on the top line. Exchanging the roles of the control and target qubits, one finds



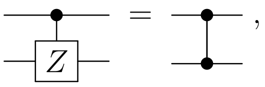
$$= \qquad\qquad\qquad . \tag{41}$$

Note that the two above gates are



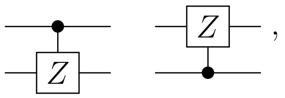
$$. \qquad (42)$$

Another useful example is the CPHASE gate,



$$, \qquad (43)$$

which applies the Pauli-Z gate if and only if the control qubit is in the state $|1\rangle$. The CPHASE is symmetric by exchange of the control and target qubits,

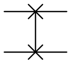


$$, \qquad (44)$$

hence the simplified notation above, see exercise 9, page 25. This is obvious from the matrix representation, which reads exactly the same in the reversed computational basis $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$, see table 2.

Other multi-qubit gates

There also exist two-qubit gates other than controlled gates. A celebrated example is the SWAP gate

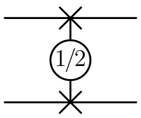


$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} ,$$

which exchanges the single-qubit basis states of the two qubits, i.e.

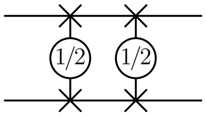
$$|00\rangle \to |00\rangle \quad , \quad |01\rangle \to |10\rangle \quad , \quad |10\rangle \to |01\rangle \quad , \quad |11\rangle \to |11\rangle \ .$$

Another example is the so-called $\sqrt{\text{SWAP}}$ gate,



$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & \frac{1+i}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} ,$$

which performs half the way of the SWAP gate, so that



$$= \qquad , \qquad (45)$$

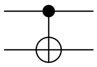
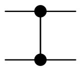
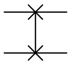
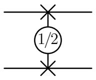
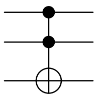
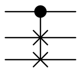
Name (nickname)	Gate	Matrix	Action
Controlled NOT (CNOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	Applies the single-qubit NOT gate to the target qubit iff the control qubit is in the state $\|1\rangle$.
Controlled Z (CPHASE)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	Applies the single-qubit Pauli-Z gate to the target qubit iff the control qubit is in the state $\|1\rangle$.
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	Exchanges the single-qubit basis state of the two qubits.
$\sqrt{\text{SWAP}}$		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & \frac{1+i}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	Performs half the way of the SWAP gate.
Toffoli (CCNOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	Applies the single-qubit NOT gate to the third qubit iff both the first and second qubits are in the state $\|1\rangle$.
Fredkin (CSWAP)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	Applies the two-qubit SWAP gate to the second and third qubits iff the first qubit is in the state $\|1\rangle$.

Table 2: Multi-qubit gates. The matrix representations are written in the basis that fixes the state of the first qubit, then the state of the second qubit and so on, starting with $|0\rangle$ and ending with $|1\rangle$, i.e. for instance $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, ...

see exercise 10, page 25.

Many other two-qubit gates can be built. In fact, it can be shown that any two-qubit gate can be constructed from a set of universal gates. More generally, multi-qubit gates are constructed by a direct extension of two-qubit gates. Celebrated examples are the Toffoli and Fredkin three-qubit gates, which are constructed by adding an additional control qubit, see table 2.

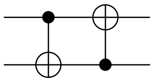
4 Circuits

Having introduced the main single- and multi-qubit gates, we may now combine them and construct quantum circuits. They are basic *quantum algorithms*. Here, we just show how elementary gates can be combined to realize some simple tasks.

4.1 Playing around with somes gates

To start with, let us combine a certain number of single- and two-qubit gates and see what they do.

Consider first the following circuit made of two CNOT gates alternating the control and target qubits. Its action may be found using the matrix representation of each of the gates, see Eqs. (40) and (41). It yields



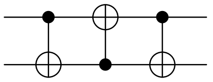
$$= \qquad\qquad\qquad\qquad , \tag{46}$$

see exercise 11a, page 26. Note that the order of the matrices is the opposite of that of the gates (remember that the circuit is read from left to right, while a product of evolution operators is read from right to left. While such an approach is a good check, it is usually easier to directly write the action of the circuit (or at least a part of it) directly on the computation basis states:

$$\begin{array}{lll} |00\rangle & \to \qquad & \to \\ |01\rangle & \to \qquad & \to \\ |10\rangle & \to \qquad & \to \\ |11\rangle & \to \qquad & \to \end{array} \qquad . \tag{47}$$

This is known as the *truth table* of the gate. Of course, the two approaches are equivalent as can be easily checked. Note, however, that the latter is in general easier than the former. On the one hand, it avoids the dangerous direction swap between the circuit and matrix representation. On the other hand, the gate matrices are usually sparse and the direct calculations avoids adding many zeros.

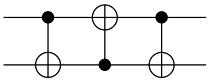
Consider now the same circuit with an additional CNOT gate where the control and target qubits are, respectively the first and the second qubits, as in the first gate,

 .

The action of such a circuit is readily found pursuing the previous one. It yields

$$\begin{array}{lll} |00\rangle & \cdots & \to \\ |01\rangle & \cdots & \to \\ |10\rangle & \cdots & \to \\ |11\rangle & \cdots & \to \end{array} \qquad , \tag{48}$$

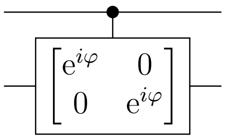
where the $\cdots$ represents the action of the previous circuit. We thus find that the circuit exchanges the states of the two qubits. This is nothing but



$$= \qquad\qquad . \tag{49}$$

This can be double checked using the matrix representation, see exercise 11b, page 26. An important conclusion of this simple exercise is that the writting of a circuit is not unique and can, in some cases, be considerably simplified.

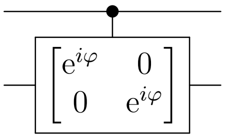
Consider another enlightening example. Assume you want to apply a phase to the second qubit provided the first qubit is in the state $|1\rangle$. This is nothing but the controlled two-qubit gate


$\begin{bmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$

Its action on the computational basis reads as

$$\begin{array}{ll} |00\rangle & \to \\ |01\rangle & \to \\ |10\rangle & \to \\ |11\rangle & \to \end{array} \tag{50}$$

Hence the circuit is diagonal in the computation basis and applies a phase that depends only on the state of the control qubit. It can be written as

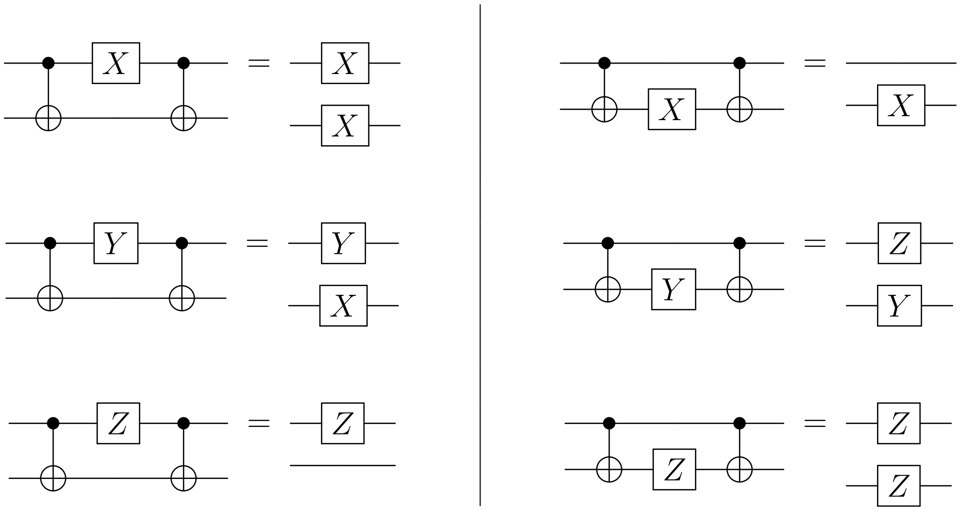

$\begin{bmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$

$$= \qquad\qquad , \tag{51}$$

see exercise 12, page 26. The circuit is thus just a single-qubit $\varphi/2$ phase gate applied to the first qubit.

4.2 Circuit identities

The obvious conclusion of these simple examples is that it is always worth trying to simplify a quantum circuit as much as possible before analyzing or using it. There exists a number of rules to do this, known as circuit identities, a first example of which is the identity (49). Other important examples are some that allows us to reduce two-qubit circuits to two parallel single-qubit gates, e.g.



These identities are proven in exercise 13, page 26. As can be seen from these simple examples, it is clear that the simplication of quantum circuits may not be a trivial task.

4.3 Designing circuits

Another approach to quantum circuits aims at designing dedicated quantum circuits to realize a certain specific task. Let us discuss a few examples.

Bell states

Assume first you want to desgin a circuit to create two-qubit entangled states from non-entangled qubit states. More specifically, assume you have the two-qubit state $|00\rangle$ at your disposal and aim at creating the state $|\mathcal{B}\rangle_1 = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, which is maximally entangled[4]. A way to design the circuit is to think of single-qubit or two-qubit operations to turn from the former to the latter. More generally, it is straightforward to write down the truth

[4] A more precise definition of what *maximally entangled states* mean will discussed later.

table of this circuit,

$$\begin{array}{ll} |00\rangle & |\mathcal{B}_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \\ |01\rangle & |\mathcal{B}_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}} \\ |10\rangle & |\mathcal{B}_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}} \\ |11\rangle & |\mathcal{B}_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}} \end{array} \tag{52}$$

see exercise 14, page 26. Hence, the circuit transforms the product two-qubit computational basis into the basis of maximally entangled states, known as the *Bell states*.

GHZ states

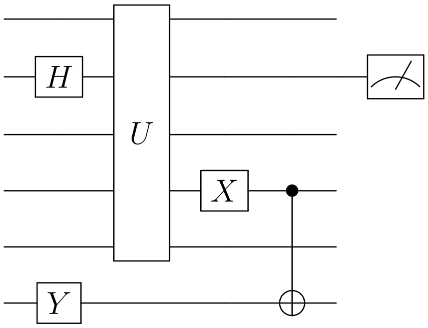
Another example is the realization of so-called Greenberger-Horne-Zeilinger (GHZ) states. The simplest one is the three-qubit GHZ state,

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \tag{53}$$

In order to generate such a state, we may apply

Towards more elaborated quantum circuits

One can then realize a number of quantum circuits and quantum algorithms and build things such as



where the gate U is a multi-qubit gate (here acting on 5 qubits). As it can be easily anticipated, it becomes rapidely difficult to build quantum circuits that (i) are useful, (ii) work, (iii) are optimized, and (iv) can be realized on existing platforms.

A Exercises

A.1 Quantum states

1. *Identical quantum states.* Show that two kets $|\psi\rangle$ and $|\psi'\rangle$ represent the same quantum state if and only if they only differ by a global phase, $|\psi'\rangle = \mathrm{e}^{i\theta}\,|\psi\rangle$.

A.2 Bloch sphere

2. *Bloch vector.* Consider a spin realization of the qubit, with the state correspondance $|0\rangle = |{\uparrow}\rangle$ and $|1\rangle = |{\downarrow}\rangle$.

   (a) Show that the state $|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\mathrm{e}^{i\varphi}\,|1\rangle$ is an eigenstate of the spin operator along the corresponding Bloch vector $\vec{\psi} = (1, \theta, \varphi)$. What is the eigenvalue?

   (b) Show that the Bloch vector associated to the ket $|\psi\rangle$ is the average of the spin vector operator, i.e. $\langle\psi|\hat{\vec{\sigma}}|\psi\rangle = \vec{\psi}$.

   Hint: Use $\big|\,|\psi\rangle\,\big| = 1$ and $\big|\langle\hat{\vec{\sigma}}\rangle\big| \leq 1$. Note that, using rotation invariance, it is sufficient to show it for a Bloch vector aligned with a given axis, for instance z.

3. *Precession of the Bloch vector.* Using the Ehrenfest theorem, show that the effect of the generic qubit Hamiltonian $\hat{H} = h_0\hat{1} + \frac{\hbar\omega}{2}\vec{n}\cdot\hat{\vec{\sigma}}$ is represented by the precession of its Bloch vector and determine the rotation axis as well as the angular velocity.

4. *Rotation operator.* Show that the qubit rotation operator of axis $\vec{n}$ and angle α [second formula of Eq. (31)] reads as

$$\hat{R}_{\vec{n}}(\alpha) = \cos(\alpha/2)\ \hat{I} - i\sin(\alpha/2)\ \vec{n}\cdot\hat{\vec{\sigma}}. \tag{54}$$

   Hint: It is useful to start writting some commutation and anti-commutation rules of the Pauli matrices. For instance, show the following relations

$$[\hat{X},\hat{Y}] = 2i\hat{Z} \quad , \quad \{\hat{X},\hat{Y}\} \equiv \hat{X}\hat{Y} + \hat{Y}\hat{X} = 0 \quad \text{and} \quad \{\hat{X},\hat{X}\} = 2$$

   using the matrix representations of the Pauli matrices, see box on page 9. Then, Taylor expand the exponential in the definition of the rotation operator, Eq. (33) and find Eq. (54).

5. *Bloch vector and measurement process.* Show that, for a qubit in the state $|\psi\rangle$, the probability to measure the spin ±1 along the axis oriented by the unit vector $\vec{m}$ is

$$P_{\pm\vec{m}|\psi} = \frac{1 \pm \vec{m}\cdot\vec{\psi}}{2}, \tag{55}$$

   where $\vec{\psi}$ is the Bloch vector associated to $|\psi\rangle$. Note that it is sufficient to consider the case $\vec{m} = \vec{e}_z$.

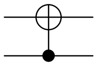
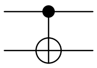
   Hint: Compute the probability of finding ±1 when measuring the spin component along z and show that it can be written as in Eq. (55) with $\vec{m} = \vec{e}_z$.

A.3 Single-qubit gates

6. Prove the circuit identities of Eqs (35) and (36) on page 15.

7. Build up a simple sequence of gates (circuit) that transforms the standard basis $\{|0\rangle, |1\rangle\}$ into the basis $\{|+i\rangle, |-i\rangle\}$.

A.4 Multi-qubit gates

8. Write down the truth table (action) of the gate . Is it the same as the CNOT gate,  ?

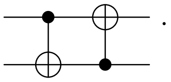
9. Check Eq. (44) on page 18 and justify the short-hand notation of Eq. (43).

10. Check the identity (45) on page 18.

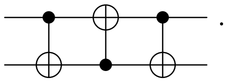
A.5 Circuit identities

11. *CNOT gates.*

    (a) Write down the matrix representation and the truth table of

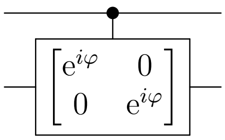
    

    (b) Write down the truth table of

    Do you recognize a known gate?

12. Write the truth table of

    
    $\begin{bmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$

    and show that it can be expressed as two independent single-qubit gates.

13. Prove the six circuit identities in the table of page 22.

A.6 Simple circuits

14. *Bell states.* Build up a simple circuit that transforms the two-qubit computational basis into the Bell basis.

15. *Greenberger-Horne-Zeilinger states.*

    (a) Build up at least two simple circuits able to transform the first state of the computational basis into the 3-qubit Greenberger-Horne-Zeilinger (GHZ) state,

    $$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \tag{56}$$

    (b) Are these circuits equivalent?

    (c) Generalize the circuits to the N-qubit GHZ state.