

Contents

1. Mathematical Background 2

 1.1. Complex numbers 2

 1.2. Hilbert spaces 3

 1.3. Operators 5

 1.4. Bra-ket notation 7

2. Qubits 8

 2.1. Single qubit systems 8

 2.2. Multiple qubits systems 12

 2.3. Qubit measurement 14

 2.4. Qubit manipulations 18

3. Quantum Theory 22

 3.1. Basics 22

 3.2. Complexity 23

1. Mathematical Background

1.1. Complex numbers

In mathematics, a **complex number** is an element of a number system that extends the real numbers with a specific element denoted i , called the **imaginary unit** and satisfying the equation $i^2 = -1$. The set of complex numbers is denoted by the symbol \mathbb{C} .

Every complex number z can be expressed in the form $a + bi$, where a and b are real numbers and are referred to as its **real part** and its **imaginary part**, respectively. The real part of a complex number z is denoted $\Re(z)$, the imaginary part $\Im(z)$. A complex number with imaginary part equal to 0 is simply a real number; a complex number with real part equal to 0 is said to be a **purely imaginary** number.

Addition, subtraction and multiplication of complex numbers can be naturally defined by using the rule $i^2 = -1$ along with the associative, commutative, and distributive laws.

A complex number z can be identified with the ordered pair of real numbers $(\Re(z), \Im(z))$, which may be interpreted as coordinates of a point in a Euclidean plane with standard coordinates, which is then called the **complex plane** or **Argand diagram**. The horizontal axis is generally used to display the real part, with increasing values to the right, and the imaginary part marks the vertical axis, with increasing values upwards.

Given a complex number $z = a + ib$, the **complex conjugate** of z is the number $z^* = a - ib$, obtained by changing the sign of the imaginary part of z . Geometrically, z is the “reflection” of z about the real axis. It is trivial to see that, for any complex number z , $(z^*)^* = z$. A complex number is real if and only if it equals its own conjugate.

The square root of the product between a complex number z and its complex conjugate z^* is a non negative real number called **modulus** or **magnitude**:

$$|z| = \sqrt{z \cdot z^*} = \sqrt{(\Re(z) + i\Im(z))(\Re(z) - i\Im(z))} = \sqrt{\Re(z)^2 + \Im(z)^2}$$

By Pythagoras’ theorem, $|z|$ is the distance from the origin to the point representing the complex number z in the complex plane.

The **argument** of z (sometimes called the “phase” φ), denoted as $\arg(z)$, is the angle formed by the vector $(\Re(z), \Im(z))$ with the positive real axis in the complex plane:

$$\arg(z) = \tan^{-1} \left(\frac{\Im(z)}{\Re(z)} \right)$$

Note that any rotation of $2k\pi$ with $k \in \mathbb{Z}$ is equivalent to performing no rotation at all, therefore the argument is often required to be specified in the interval $(-\pi, \pi]$.

A complex number $z = a + ib$ is said to be written in **rectangular form**, or **algebraic form**. Another way to express a complex number is the **polar form**; given a complex number z with modulus $r = |z|$ and argument $\varphi = \arg(z)$, the polar form of z is:

$$z = r(\cos(\varphi) + i \sin(\varphi))$$

A third way to express complex numbers is the **exponential form**:

$$z = re^{i\varphi}$$

Where the complex exponential $e^{i\varphi}$ is also referred to as the **phase factor**.

The fourth way to express a complex number is the **matrix form**. Given a complex number $z = a + ib$, it can be written as a 2×2 matrix as follows:

$$a + ib = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

The complex conjugate of a complex number in matrix form is simply its matrix transpose.

It is also possible to transition immediately from the exponential form to the matrix form:

$$re^{i\varphi} = r \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} = r \cos(\theta) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r \sin(\theta) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Which also means that the real unit and the imaginary unit are simply:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

This representation is consistent with respect to standard complex number operations. For example, to show that $zz^* = a^2 + b^2$:

$$\begin{aligned} zz^* &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^T = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} aa + (-b)(-b) & ab + (-b)a \\ ba + a(-b) & bb + aa \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & ab - ab \\ ab - ab & a^2 + b^2 \end{pmatrix} = \\ &= \begin{pmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{pmatrix} = (a^2 + b^2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a^2 + b^2 \end{aligned}$$

The inverse of a matrix representing a complex number is the reciprocal of the number itself. Given a complex number $z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \frac{z^*}{zz^*} = \frac{1}{z}$$

1.2. Hilbert spaces

Given a vector space V and two vectors $x, y \in V$, their **inner product** $\langle x, y \rangle$ is given by:

$$\langle x, y \rangle = x^\dagger y = (x_1^* \dots x_n^*) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^n x_i^* y_i$$

In the context of quantum mechanics, vector spaces are assumed to be on the field \mathbb{C} . In this context, the inner product is also referred to as the **scalar product** (because the value returned is a single number) or **dot product** (because it is sometimes denoted with a dot), even though in general the scalar/dot product is a special case of inner product.

The inner product is a mathematical operation that satisfies (at least) this three properties:

- Invariance with respect to conjugation: $\langle x, y \rangle = \langle x, y \rangle^*$;
- Linearity in the second position: $\langle x, \alpha y + \beta z \rangle = \alpha \langle x, y \rangle + \beta \langle x, z \rangle$;
- Antilinearity in the first position: $\langle \alpha x + \beta y, z \rangle = \alpha^* \langle x, z \rangle + \beta^* \langle y, z \rangle$;
- $\langle x, x \rangle \geq 0$ for any $x \in \mathbb{C}$;
- $\langle x, x \rangle = 0$ if $x = \mathbf{0}$.

The square root of the inner product of a vector x with itself is called the **norm** of the vector:

$$|x| = \sqrt{\langle x, x \rangle} = \sqrt{(x_1^* \dots x_n^*) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}$$

Any vector space that possesses an inner product is called an **Hilbert space**. Hilbert spaces are so obiquitous that, when not specified, any vector space is assumed to be an Hilbert space.

The **direct sum** of two vectors spaces V and W having bases $A = \{\alpha_1, \dots, \alpha_n\}$ and $B = \{\beta_1, \dots, \beta_m\}$ respectively, denoted as $V \oplus W$, is the vector space spanned by the basis $A \cup B = \{\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m\}$.

Every element $x \in V \oplus W$ can be written as $v \oplus w$, for some $v \in V$ and some $w \in W$. The dimension of $V \oplus W$ is simply given by $\dim(V) + \dim(W)$.

Addition and scalar multiplication are defined by performing the operation on the two component vector spaces separately and adding the results. When V and W are inner product spaces, the standard inner product on $V \oplus W$ is given by:

$$(v_2^\dagger \oplus w_2^\dagger)(v_1 \oplus w_1) = \langle v_2, v_1 \rangle + \langle w_2, w_1 \rangle$$

The vector spaces V and W embed in $V \oplus W$ in the obvious canonical way, and the images are orthogonal under the standard inner product.

Theorem 1.2.1 (Direct sum decomposition): For any finite inner product vector space S of dimension n , there exist a set of orthogonal subspaces $\{V_1, \dots, V_k\}$ for some $k \leq n$ such that $S = V_1 \oplus \dots \oplus V_k$

The **tensor product** between two vectors v and w is the vector $v \otimes w$ constructed as:

$$v \otimes w = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = (v_1 w_1 \dots v_1 w_m \dots v_n w_1 \dots v_n w_m)^T$$

The tensor product between vectors satisfies the following relations:

- $(v_1 + v_2) \otimes v_3 = v_1 \otimes v_3 + v_2 \otimes v_3$
- $(av_1) \otimes v_2 = v_1 \otimes (av_2) = a(v_1 \otimes v_2)$

When there is no ambiguity, the tensor product of two vectors v and w is simply denoted as vw .

Exercise 1.2.1: What is the tensor product of the two following vectors?

$$v = \begin{pmatrix} \frac{1}{\sqrt{5}} \\ -\frac{2}{\sqrt{5}} \end{pmatrix} \quad w = \begin{pmatrix} -\frac{1}{\sqrt{10}} \\ \frac{3}{\sqrt{10}} \end{pmatrix}$$

Solution:

$$v \otimes w = \left(\frac{1}{\sqrt{5}} \left(-\frac{1}{\sqrt{10}} \right) \quad \frac{1}{\sqrt{5}} \left(\frac{3}{\sqrt{10}} \right) \quad -\frac{2}{\sqrt{5}} \left(-\frac{1}{\sqrt{10}} \right) \quad -\frac{2}{\sqrt{5}} \left(\frac{3}{\sqrt{10}} \right) \right)^T = \left(-\frac{1}{5\sqrt{2}} \quad \frac{3}{5\sqrt{2}} \quad \frac{2}{5\sqrt{2}} \quad -\frac{6}{5\sqrt{2}} \right)^T$$

□

The **tensor product** of two vector spaces V and W , having bases $A = \{v_1, v_2, \dots, v_n\}$ and $B = \{w_1, w_2, \dots, w_m\}$ respectively, is a nm -dimensional vector space denoted as $V \otimes W$.

The basis of $V \otimes W$ is constituted by all of possible tensor products between the vectors of the two original bases. Explicitly, the basis of $V \otimes W$ is:

$$\{v_1 \otimes w_1, \dots, v_n \otimes w_1, \dots, v_1 \otimes w_m, \dots, v_n \otimes w_m\}$$

With $v_1, \dots, v_n \in A$ and $w_1, \dots, w_m \in B$.

This means that any generic vector of $V \otimes W$ can be written as:

$$\lambda_{1,1}(v_1 \otimes w_1) + \dots + \lambda_{n,1}(v_n \otimes w_1) + \dots + \lambda_{1,m}(v_1 \otimes w_m) + \dots + \lambda_{n,m}(v_n \otimes w_m)$$

For nm coefficients $\lambda_{i,j}$ with $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$.

If V and W are two vector spaces for whose an inner product is defined (like Hilbert spaces), then it is possible to define an inner product for $V \otimes W$ as the product of the inner products with respect to those spaces.

The tensor product has many properties that are of interest for quantum state analysis.

Lemma 1.2.1: The tensor product of two unit vectors is also a unit vector.

Lemma 1.2.2: Let V and W be two vector spaces having bases $A = \{v_1, v_2, \dots, v_n\}$ and $B = \{w_1, w_2, \dots, w_m\}$ respectively. If A and B are both orthonormal, then the basis:

$$C = \{v_1 \otimes w_1, \dots, v_n \otimes w_1, \dots, v_1 \otimes w_m, \dots, v_n \otimes w_m\}$$

Of $V \otimes W$ is also orthonormal.

The **outer product** of two vectors v and w , denoted as $|v\rangle\langle w|$, is given by:

$$|v\rangle\langle w| = vv^\dagger = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}^\dagger = \begin{pmatrix} v_1 w_1^* & v_1 w_2^* & \dots & v_1 w_n^* \\ v_2 w_1^* & v_2 w_2^* & \dots & v_2 w_n^* \\ \vdots & \vdots & \ddots & \vdots \\ v_m w_1^* & v_m w_2^* & \dots & v_m w_n^* \end{pmatrix}$$

Where m is the dimension of v and n is the dimension of w .

1.3. Operators

Lemma 1.3.1: Given two vector spaces V and W , let O be an operator $O : V \rightarrow W$. For any two vectors $v \in V$ and $w \in W$, the following holds:

$$\langle v, Ow \rangle = (\langle w, v \rangle)^\dagger$$

The **conjugate transpose** of a matrix A , denoted as A^\dagger , is the matrix obtained from transposing A and then applying complex conjugation to each element of the resulting matrix:

$$A^\dagger = A^{T*} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}^{T*} = \begin{pmatrix} a_{1,1}^* & a_{2,1}^* & \dots & a_{m,1}^* \\ a_{1,2}^* & a_{2,2}^* & \dots & a_{m,2}^* \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n}^* & a_{2,n}^* & \dots & a_{m,n}^* \end{pmatrix}$$

Exercise 1.3.1: What is the conjugate transpose of the following matrix?

$$A = \begin{pmatrix} 1 & -2-i & 5 \\ 1+i & i & 4-2i \end{pmatrix}$$

Solution:

$$A^\dagger = \begin{pmatrix} 1 & -2-i & 5 \\ 1+i & i & 4-2i \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 1+i \\ -2-i & i \\ 5 & 4-2i \end{pmatrix}^* = \begin{pmatrix} 1 & 1-i \\ -2+i & -i \\ 5 & 4+2i \end{pmatrix}$$

□

A square matrix A is said to be **Hermitian** if $A^\dagger = A$. It is said to be **unitary** if $A^\dagger = A^{-1}$.

Any matrix is equivalent to an operator given a fixed basis and vice versa, therefore it is also possible to define the conjugate transpose of an operator. Since trasposing an operator in matrix form exchanges domain

and codomain, the conjugate transpose of an operator $O : V \rightarrow W$ is the operator $O^\dagger : W \rightarrow V$. The matrix representation of O^\dagger is, as expected, the conjugate transpose of the matrix representation of O .

Theorem 1.3.1: An Hermitian matrix has all real eigenvalues.

Proof: Let $O : V \rightarrow V$ be a linear self-adjoint operator in matrix representation, and let λ be one of its eigenvalues. Recall that, given an eigenvector $v \in V$ associated to λ , $Ov = \lambda v$. Consider $\lambda \langle x, x \rangle$:

$$\lambda \langle v, v \rangle = \langle \lambda v, v \rangle = \langle Ov, v \rangle = \langle v, O^\dagger v \rangle = \langle v, Ov \rangle = \langle v, \lambda v \rangle = \lambda^* \langle v, v \rangle$$

By definition of eigenvector, v cannot be the null vector. Also, since the inner product between a vector and itself is not null, it is allowed to simplify

$$\lambda \cancel{\langle v, v \rangle} = \lambda^* \cancel{\langle v, v \rangle} \Rightarrow \lambda = \lambda^*$$

Which means that λ is a real number, because it is equal to its complex conjugate. \square

Lemma 1.3.2: If A and B are two unitary matrices, then $(AB)^\dagger AB = I$. In other words, the product of two unitary matrices is a unitary matrix.

Proof: By definition, $A^\dagger A = I$ and $B^\dagger B = I$. Then:

$$(AB)^\dagger AB = B^\dagger A^\dagger AB = B^\dagger (A^\dagger A) B = B^\dagger I B = B^\dagger B = I$$

\square

Lemma 1.3.3: The columns/rows of a unitary matrix form an orthonormal basis of \mathbb{C}^n with respect to the inner product.

The conjugate transpose of an operator is also called its **adjoint operator**. If an operator is equal to its adjoint (or equivalently, if its matrix representation is Hermitian), it is said to be **self-adjoint**.

Hermitian operators define a unique orthogonal subspace decomposition called **eigenspace decomposition**. Moreover, for every such decomposition, there exists a Hermitian operator whose eigenspace decomposition is this decomposition.

Theorem 1.3.2: Let $O : V \rightarrow V$ be an Hermitian operator in matrix form, having eigenvalues $\lambda_1, \dots, \lambda_n$. Let S_{λ_i} be the subspace generated by the i -th eigenvalue, and let $\{S_{\lambda_i}\}$ be the set that contains those subspaces. $\{S_{\lambda_i}\}$ is an orthogonal set and:

$$S_{\lambda_1} \oplus S_{\lambda_2} \oplus \dots \oplus S_{\lambda_n} = V$$

This decomposition is unique.

Proof: First, note how two eigenspaces of a matrix are necessarily disjoint. Given a unit vector x and two distinct eigenvalues λ_1 and λ_2 , if $Ox = \lambda_1 x$ and $Ox = \lambda_2 x$ then $\lambda_1 x = \lambda_2 x$, but this is only possible if $\lambda_1 = \lambda_2$.

For any Hermitian operator, the eigenvectors for distinct eigenvalues must be orthogonal. Let v_1 be an eigenvector for λ_1 and v_2 an eigenvector for λ_2 . Then:

$$\lambda_1 \langle v_1, v_2 \rangle = \langle v_1^* O^\dagger, v_2 \rangle = \langle v_1, Ov_2 \rangle = \lambda_2 \langle v_1, v_2 \rangle$$

Since λ_1 and λ_2 were assumed to be distinct, $\lambda_1 \langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \lambda_2 \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$ is possible only if $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = 0$.

□

1.4. Bra-ket notation

A more comfortable formalism for denoting vectors is the **bra-ket** notation. The **ket** associated to a state Ψ , denoted as $|\Psi\rangle$, is just its column vector representation. The **bra** of a state Ψ , denoted as $\langle\Psi|$, is the transposed conjugate of the corresponding ket:

$$|\Psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \qquad \langle\Psi| = |\Psi\rangle^\dagger = (\psi_1^* \ \psi_2^* \ \dots \ \psi_n^*)$$

If a state Ψ belongs to an Hilbert space H , its conjugate Ψ^* belongs to the **dual space** H^* of the Hilbert space H . Another way of expressing it is that if a ket $|\Psi\rangle$ belongs to H , then the corresponding bra $\langle\Psi|$ belongs to H^* .

The dual space is constituted by linear functionals X over the kets in H : if $|\Psi\rangle \in H$ then $X(\Psi) \in \mathbb{C}$:

$$X(\alpha_1 |\Psi_1\rangle + \alpha_2 |\Psi_2\rangle) = X(\alpha_1 |\Psi_1\rangle) + X(\alpha_2 |\Psi_2\rangle)$$

The inner product of two kets $|\Psi_1\rangle$ and $|\Psi_2\rangle$ is simply denoted as $\langle\Psi_1|\Psi_2\rangle$, and is called **braket**. The outer product of two kets $|\Psi_1\rangle$ and $|\Psi_2\rangle$ is simply denoted as $|\Psi_1\rangle\langle\Psi_2|$, and is called **ketbra**:

$$\langle|\Psi_1\rangle, |\Psi_2\rangle\rangle = |\Psi_1\rangle^\dagger |\Psi_2\rangle = \langle\Psi_1|\Psi_2\rangle \qquad \rangle |\Psi_1\rangle, |\Psi_2\rangle\langle = |\Psi_1\rangle|\Psi_2\rangle^\dagger = |\Psi_1\rangle\langle\Psi_2|$$

The bra-ket notation is particularly comfortable to work with, because it represents the conjugate transpose of a vector as “flipping” its symbol left-to-right. In particular, the inner product “flips” the ket on the left side of the operation, whereas the outer product “flips” the ket on the right side of the operation.

2. Qubits

2.1. Single qubit systems

Consider any physical system that can be observed in only two possible states. Systems such as these can be constructed in many different ways, such as inspecting the spin of the electron (only spin up and spin down exist, no other spins can be found) or inspecting the energy levels of the electrons of very simple atoms (only a ground state and an excited state exist, no other states can be found). Systems such as these are called **two-state quantum systems**, or just two-state systems.

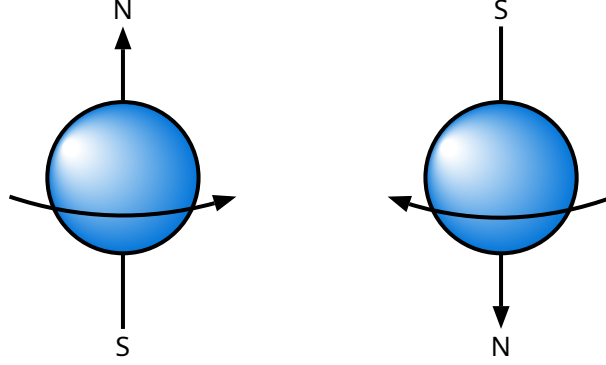


Figure 1: The spin is an intrinsic property of fundamental particles. Electrons have a value of spin that is either equal to $1/2$ or $-1/2$, also referred to as “up” and “down” respectively.

The term “two-state system” is somewhat misleading. Indeed, until measurement happens, the number of states in which a physical system can find itself is infinite; it is only *after* the measurement is performed that the system will be found in one of the two states. Therefore, “two-state” refers to the state of the system after the measurement has taken place.

More precisely, following the principles of quantum mechanics, these two “special” states, called **base states**, form a basis for the Hilbert space that contains the possible states in which the system can be *before* measurement happens. Any of these states can be constructed as a linear combination of the aforementioned basis, normalized according to Born’s rule. In this respect, the term “two-state” refers to the number of dimensions of the Hilbert space

Let $|\varphi_1\rangle$ and $|\varphi_2\rangle$ be two base states. Any linear combination of the two is also a legitimate state $|\Psi\rangle$, as long as the normalization condition is respected:

$$|\Psi\rangle = \alpha |\varphi_1\rangle + \beta |\varphi_2\rangle, \text{ with } \alpha, \beta \in \mathbb{C} \text{ such that } |\alpha|^2 + |\beta|^2 = 1$$

According to Born’s rule, the probability of finding $|\Psi\rangle$ in the state $|\varphi_1\rangle$ when measured is given by $|\alpha|^2$, whereas the probability of finding it in the state $|\varphi_2\rangle$ when measured is given by $|\beta|^2$. Later chapters will expand on this formalism, but the statement just given is, for the moment, sufficient.

A two-state quantum system is also referred to as **qubit**. The name “qubit” comes from its classical counterpart, the “bit”, but while a bit is either 0 or 1, a qubit is in an indeterminate state until the measurement is performed¹.

It is therefore valid to refer to a state such as the $|\Psi\rangle$ described above as a qubit. In particular, being the result of a linear combination of basis, any state/qubit $|\Psi\rangle$ can be entirely represented (with respect to that basis) as the coefficients of the linear combination itself:

$$|\Psi\rangle = \alpha |\varphi_1\rangle + \beta |\varphi_2\rangle \iff \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_{\{|\varphi_1\rangle, |\varphi_2\rangle\}}$$

Any pair of states that form a basis for a two-dimensional Hilbert space and are also orthogonal to each other (in other words, form an orthonormal basis) can be used as base states. The simplest choice is the pair of vectors

¹A n -state quantum system is called a **qudit**, and it has the same computational power of a qubit.

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, commonly denoted as $|0\rangle$ and $|1\rangle$ respectively².

Theorem 2.1.1: The set $\{|0\rangle, |1\rangle\}$ forms an orthonormal basis for any two-dimensional Hilbert space.

Proof: The null vector of any two-dimensional Hilbert space is $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Constructing the null combination gives:

$$\mathbf{0} = k_1 |0\rangle + k_2 |1\rangle \Rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} = k_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \begin{cases} 0 = k_1 \cdot 1 + k_2 \cdot 0 \\ 0 = k_1 \cdot 0 + k_2 \cdot 1 \end{cases} \Rightarrow \begin{cases} 0 = k_1 \\ 0 = k_2 \end{cases}$$

Being linearly independent, they do form a basis. They are also orthonormal:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \cdot 1 + 0 \cdot 0 = 1$$

$$\langle 0|1\rangle = \langle 1|0\rangle = 1 \cdot 0 + 0 \cdot 1 = 0$$

□

This basis is used obiquitously, and is therefore referred to as the **standard basis**. When the basis at play is not specified, it is assumed that the basis is the standard basis. Also, since orthonormality is a necessary condition for being a physically meaningful basis, when talking about a basis it will be implicitly assumed (unless stated otherwise) that the basis is orthonormal.

Another useful basis is the one denoted as $\{|+\rangle, |-\rangle\}$:

$$|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix} \quad |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix}$$

Theorem 2.1.2: The set $\{|+\rangle, |-\rangle\}$ forms an orthonormal basis for any two-dimensional Hilbert space.

Proof: The basis $\{|0\rangle, |1\rangle\}$ can be written as a linear combination of $\{|+\rangle, |-\rangle\}$:

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

Therefore, $\{|+\rangle, |-\rangle\}$ is a basis as well. It's also orthonormal:

$$\langle +|+\rangle = \langle -|-\rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = 1 \quad \langle +|-\rangle = \langle -|+\rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = 0$$

□

Another relevant basis is $\{|\mathfrak{O}\rangle, |\mathfrak{V}\rangle\}$, defined as:

$$|\mathfrak{O}\rangle = \frac{\sqrt{2}}{2}(|0\rangle + i|1\rangle) = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ i\frac{\sqrt{2}}{2} \end{pmatrix} \quad |\mathfrak{V}\rangle = \frac{\sqrt{2}}{2}(|0\rangle - i|1\rangle) = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -i\frac{\sqrt{2}}{2} \end{pmatrix}$$

Theorem 2.1.3: The set $\{|\mathfrak{O}\rangle, |\mathfrak{V}\rangle\}$ forms an orthonormal basis for any two-dimensional Hilbert space.

Proof: This set is indeed a basis since the basis $\{|0\rangle, |1\rangle\}$ can be written as a linear combination of $\{|\mathfrak{O}\rangle, |\mathfrak{V}\rangle\}$:

²The name emphasises the analogy with the classical bit, but the choice of assigning these vectors to their respective symbols is completely arbitrary.

$$|0\rangle = \frac{\sqrt{2}}{2}(|\oslash\rangle + i|\mathfrak{D}\rangle)$$

$$|1\rangle = \frac{\sqrt{2}}{2}(|\oslash\rangle - i|\mathfrak{D}\rangle)$$

Therefore, $\{|\oslash\rangle, |\mathfrak{D}\rangle\}$ is a basis as well. It's also orthonormal:

$$\langle\oslash|\oslash\rangle = \langle\mathfrak{D}|\mathfrak{D}\rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \cdot i \frac{\sqrt{2}}{2} = 1 \quad \langle\oslash|\mathfrak{D}\rangle = \langle\mathfrak{D}|\oslash\rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \cdot i \frac{\sqrt{2}}{2} = 0$$

□

Exercise 2.1.1: Write the state $|\Psi\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$ as a linear combination of the basis $\{|\oslash\rangle, |\mathfrak{D}\rangle\}$. What are the probabilities of obtaining the respective measurements?

Solution: There must exist two coefficients, α and β , such that:

$$\alpha|\oslash\rangle + \beta|\mathfrak{D}\rangle = |\Psi\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) = \frac{\sqrt{2}}{2} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix}$$

That is:

$$\begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix} = \alpha \begin{pmatrix} \frac{\sqrt{2}}{2} \\ i\frac{\sqrt{2}}{2} \end{pmatrix} + \beta \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -i\frac{\sqrt{2}}{2} \end{pmatrix} \Rightarrow \begin{cases} \frac{\sqrt{2}}{2} = \alpha\frac{\sqrt{2}}{2} + \beta\frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} = \alpha i\frac{\sqrt{2}}{2} - \beta i\frac{\sqrt{2}}{2} \end{cases} \Rightarrow \begin{cases} 1 = \alpha + \beta \\ i = \alpha - \beta \end{cases} \Rightarrow \begin{cases} \alpha = \frac{1+i}{2} \\ \beta = \frac{1-i}{2} \end{cases}$$

Which gives:

$$|\Psi\rangle = \frac{1+i}{2}|\oslash\rangle + \frac{1-i}{2}|\mathfrak{D}\rangle$$

The probabilities of getting each result when measured is given by:

$$P_{|\oslash\rangle} = \left| \frac{1+i}{2} \right|^2 = \left(\frac{1}{2} \right)^2 + \left(\frac{1}{2} \right)^2 = \frac{1}{2} \quad P_{|\mathfrak{D}\rangle} = \left| \frac{1-i}{2} \right|^2 = \left(\frac{1}{2} \right)^2 + \left(-\frac{1}{2} \right)^2 = \frac{1}{2}$$

□

Any vector that results from a non-trivial linear combination of a basis, that is, when both coefficients of the linear combination are not zero, is said to be in a **superposition** of the states that comprise the basis. A basis is always necessary to be specified when talking about superposition: a state can be the result of a superposition with respect to a certain basis but not with respect to another basis.

Exercise 2.1.2: Consider the states $|\Psi_1\rangle$ and $|\Psi_2\rangle$. Are they in a superposition with respect to the basis $\{|0\rangle, |1\rangle\}$?

$$|\Psi_1\rangle = \frac{\sqrt{2}}{2}(|+\rangle + |-\rangle)$$

$$|\Psi_2\rangle = \frac{\sqrt{3}}{2}|+\rangle - \frac{1}{2}|-\rangle$$

Solution: Note how:

$$|\Psi_1\rangle = \frac{\sqrt{2}}{2}(|+\rangle + |-\rangle) = \frac{\sqrt{2}}{2} \left(\begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix} + \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix} \right) = \frac{\sqrt{2}}{2} \begin{pmatrix} \sqrt{2} \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

This means that the state is one of the base states that constitutes the bases, and therefore there is no superposition. Indeed, trying to write it as a linear combination of the vectors that constitute the basis would give:

$$|\Psi_1\rangle = 1 |0\rangle + 0 |1\rangle$$

Which is trivial. On the other hand:

$$|\Psi_2\rangle = \frac{\sqrt{3}}{2} |+\rangle - \frac{1}{2} |-\rangle = \frac{\sqrt{3}}{2} \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix} - \frac{1}{2} \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{6}}{4} \\ \frac{\sqrt{6}}{4} \end{pmatrix} - \begin{pmatrix} \frac{\sqrt{2}}{4} \\ -\frac{\sqrt{2}}{4} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{6}-\sqrt{2}}{4} \\ \frac{\sqrt{6}+\sqrt{2}}{4} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}-1}{2\sqrt{2}} \\ \frac{\sqrt{3}+1}{2\sqrt{2}} \end{pmatrix}$$

Which gives a non-trivial combination:

$$|\Psi_2\rangle = \frac{\sqrt{3}-1}{2\sqrt{2}} |0\rangle + \frac{\sqrt{3}+1}{2\sqrt{2}} |1\rangle$$

□

When a measurement is not performed, the system is in a superposition of base states, and the state in which the system is found when measured can be predicted only within a certain probability. When the system is measured, there is no ambiguity, because any repeated measurement will always give the same result.

It should also be noted that, despite the existence of superpositions, a qubit still holds a single bit of information. Indeed, the state in which the qubit is prior to measurement is unknown and unknowable, and when measurement happens the value of the qubit is always one out of two allowed values. It would therefore be incorrect to state that a qubit holds an infinite amount of information.

That the same quantum state is represented by more than one vector means that there is a critical distinction between the complex vector space in which qubit values are written and the quantum state space itself. In particular, any unit vector multiplied by a phase factor is equivalent to the original vector, and therefore represents the same state.

The multiple by which two vectors representing the same quantum state differ is called the **global phase** and has no physical meaning. The notation $|v\rangle \sim |v'\rangle$ denotes the fact that the two vectors are equivalent up to a global phase $e^{i\varphi}$, that is $|v\rangle = e^{i\varphi} |v'\rangle$. The space in which two two-dimensional complex vectors are considered equivalent if they are multiples of each other is called **complex projective space** of dimension one.

Two complex vectors that differ from a phase factor belong to the same equivalence class with respect to the aforementioned relation. Each of these equivalence classes are the members of a quotient space, denoted as CP^1 :

$$CP^1 = \{\alpha |\varphi_1\rangle + \beta |\varphi_2\rangle\} / \sim$$

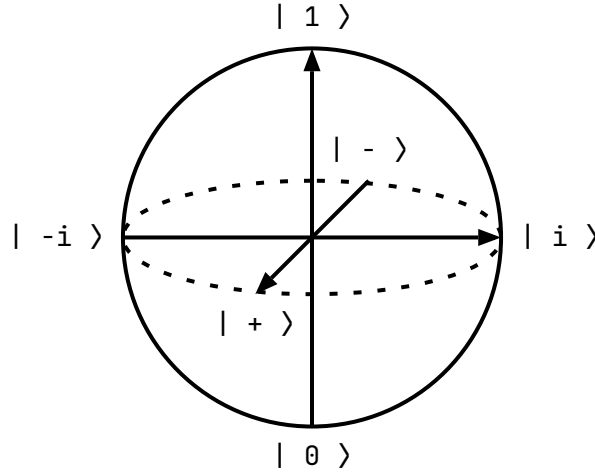
Therefore, the quantum state space for a single-qubit system is in one-to-one correspondence with the points of the complex projective space CP^1 .

A physical quantity that, unlike the global phase, is *not* irrelevant, is the **relative phase** of a single-qubit state. The relative phase of a superposition $\alpha |v_1\rangle + \beta |v_2\rangle$ is a measure of the angle in the complex plane between the two complex numbers α and β . More precisely, the relative phase is the complex number $e^{i\varphi}$ (that is, having modulus equal to one) such that:

$$\frac{\alpha}{\beta} = e^{i\varphi} \frac{|\alpha|}{|\beta|} \Rightarrow e^{i\varphi} = \frac{\alpha|\beta|}{|\alpha|\beta}$$

Two superpositions $\alpha |v_1\rangle + \beta |v_2\rangle$ and $\alpha' |v_1\rangle + \beta' |v_2\rangle$ whose amplitudes have the same magnitudes but that differ in a relative phase represent different states. On the other hand, if two superpositions (with respect to the same basis) have the same relative phase, they represent the same state.

Bases can be represented graphically as coordinates on a sphere, called **Bloch sphere**:



2.2. Multiple qubits systems

Consider two Hilbert spaces H_1 and H_2 , each describing the state space of a qubit. The Hilbert space describing the state of the two qubits is given by the tensor product of the two Hilbert spaces. If the two qubits have $\{|\varphi_1\rangle_1, |\varphi_2\rangle_1\}$ and $\{|\varphi_1\rangle_2, |\varphi_2\rangle_2\}$ respectively as bases, the basis of $H_1 \otimes H_2$ is:

$$\{|\varphi_1\rangle_1 \otimes |\varphi_1\rangle_2, |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_2, |\varphi_2\rangle_1 \otimes |\varphi_1\rangle_2, |\varphi_2\rangle_1 \otimes |\varphi_2\rangle_2\}$$

Which, in turn, means that any description of the state of two qubits at once is in the form:

$$\lambda_{1,1}|\varphi_1\rangle_1 \otimes |\varphi_1\rangle_2 + \lambda_{1,2}|\varphi_1\rangle_1 \otimes |\varphi_2\rangle_2 + \lambda_{2,1}|\varphi_2\rangle_1 \otimes |\varphi_1\rangle_2 + \lambda_{2,2}|\varphi_2\rangle_1 \otimes |\varphi_2\rangle_2$$

In general, the subscript from the basis is dropped, since the ordering of the states mirrors the orders of the qubits. Also, it is convenient to use the shorthand $|vw\rangle$ for $|v\rangle \otimes |w\rangle$, allowing the basis of the two-qubit system to be written more compactly:

$$\{|\varphi_1\varphi_1\rangle, |\varphi_1\varphi_2\rangle, |\varphi_2\varphi_1\rangle, |\varphi_2\varphi_2\rangle\}$$

Note that, due to Lemma 1.2.1 and Lemma 1.2.2, tensor product preserves both the unity of vectors and the orthonormality of bases. This means that the tensor product of two qubit state spaces is also guaranteed to be a valid state space.

This can be extended naturally to the case of a system having $n > 2$ qubits. If each of those qubits is represented by a Hilbert space H_i , with $i \in \{1, \dots, n\}$, the state space of the entire system is $H_n \otimes H_{n-1} \otimes \dots \otimes H_1$. Its basis can be written as:

$$\{|\varphi_1\varphi_1\dots\varphi_n\rangle, |\varphi_1\varphi_2\dots\varphi_n\rangle, \dots, |\varphi_2\varphi_1\dots\varphi_n\rangle, |\varphi_2\varphi_2\dots\varphi_n\rangle, \dots, |\varphi_n\varphi_1\dots\varphi_n\rangle, |\varphi_n\varphi_2\dots\varphi_n\rangle\}$$

As it is the case for a single qubit, a state of an n qubit system is in a superposition with respect to a certain basis if the linear combination:

$$\lambda_{1,1,\dots,n} |\varphi_1\varphi_1\dots\varphi_n\rangle + \lambda_{1,2,\dots,n} |\varphi_1\varphi_2\dots\varphi_n\rangle + \dots + \lambda_{n,1,\dots,n} |\varphi_n\varphi_1\dots\varphi_n\rangle + \lambda_{n,2,\dots,n} |\varphi_n\varphi_2\dots\varphi_n\rangle$$

Is not trivial, meaning that at least two coefficients are not zero. As expected, superposition is basis-dependent.

When the basis under consideration is the standard basis, it is possible to write the basis of an n -qubit state space even more compactly. Recall that the two standard base states for a qubit are $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. For a two qubit system, it is possible to use integers 0, 1, 2, 3 in the same way:

$$|00\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

In general, for a n qubit state it is possible to write its standard basis as $\{|0\rangle, |1\rangle, \dots, |2^n - 2\rangle, |2^n - 1\rangle\}$, where each ket contains the integer representation of the binary number constructed by just apposing the binary digits of the state of each qubit:

$$|00\dots 0\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |00\dots 1\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \vdots \quad |11\dots 0\rangle = |2^n - 2\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\dots 1\rangle = |2^n - 1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Note that, to use this shorthand notation, it is necessary to also specify the number of qubits of the state. Therefore, it should be employed when the number of qubits is either denoted explicitly or known from context.

Exercise 2.2.1: How would the matrix representation of the following state be?

$$\frac{1}{2} |00\rangle + \frac{1}{2}i |01\rangle + \frac{\sqrt{2}}{2} |11\rangle$$

Solution: Each ket has two digits, therefore this is a two qubit state:

$$\frac{1}{2} |00\rangle + \frac{1}{2}i |01\rangle + \frac{\sqrt{2}}{2} |11\rangle = \frac{1}{2} |0\rangle + \frac{1}{2}i |1\rangle + \frac{\sqrt{2}}{2} |3\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2}i \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix}$$

□

It is possible to use the n -dimensional standard basis to describe the state of n -qubits, but just like the case of a single qubit there are other bases that are useful to employ. One such basis for the case of a 2 qubit system is the following:

$$|\Phi^+\rangle = \frac{\sqrt{2}}{2}(|00\rangle + |11\rangle) \quad |\Phi^-\rangle = \frac{\sqrt{2}}{2}(|00\rangle - |11\rangle) \quad |\Psi^+\rangle = \frac{\sqrt{2}}{2}(|01\rangle + |10\rangle) \quad |\Psi^-\rangle = \frac{\sqrt{2}}{2}(|01\rangle - |10\rangle)$$

These states are called **Bell states**, and the basis that they form is called **Bell basis**.

Any unit vector of the 2^n -dimensional state space represents a possible state of an n -qubit system, but just as in the single-qubit case there is redundancy. In the multiple-qubit case, not only do vectors that are multiples of each other refer to the same quantum state, but properties of the tensor product also mean that phase factors distribute over tensor products; the same phase factor in different qubits of a tensor product represent the same state:

$$|v\rangle \otimes (e^{i\theta} |w\rangle) = e^{i\theta}(|v\rangle \otimes |w\rangle) = (e^{i\theta} |v\rangle) \otimes |w\rangle$$

Phase factors in individual qubits of a single term of a superposition can always be factored out into a single coefficient for that term.

Just as in the single-qubit case, vectors that differ only in a global phase represent the same quantum state; the space of distinct quantum states of an n -qubit system is a complex projective space of dimension $2^n - 1$, but in general it is easier to consider the Hilbert space directly but taking into account possible duplicate vectors.

Even though the tensor product of n single qubit states represents a state of a n -qubit system, a state of a n -qubit system might not be decomposable into a tensor product of n single qubit states. This means that there are states of n -qubit systems that cannot be conceived as simply the result of the combined contribution of each qubit, but are instead entities on their own. States like these are called **entangled states**, and indeed the majority of states of a n -qubit system are entangled states. For example, Bell states are entangled states.

Exercise 2.2.2: Consider this two 2-qubit states. Are they entangled states?

$$|\varphi_1\rangle = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle + \frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle \quad |\varphi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Solution: $|\varphi_1\rangle$ is not an entangled state, because it can be decomposed into two single (identical) qubit states as follows:

$$|\varphi_1\rangle = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle + \frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle = \left(\frac{1}{\sqrt{8}} |0\rangle + \sqrt{\frac{7}{8}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{8}} |0\rangle + \sqrt{\frac{7}{8}} |1\rangle \right)$$

On the other hand, the state $|\varphi_2\rangle$ is entangled. Attempting a decomposition gives:

$$\begin{aligned} (a |0\rangle + b |1\rangle) \otimes (c |0\rangle + d |1\rangle) &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \Rightarrow \\ ac |00\rangle + ad |01\rangle + bc |10\rangle + bd |11\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \Rightarrow \\ ac \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + ad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + bc \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + bd \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} &= \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right) \Rightarrow \\ \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \Rightarrow \begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases} \end{aligned}$$

Which is an impossible system of equations to solve. □

In the case of a two-qubit system, there is one and only decomposition (two one-qubit systems), therefore there is no ambiguity. In general, a state can be said to be entangled only with respect to a specific decomposition. More formally, a state $|\Psi\rangle$ member of a state space H decomposed as $H_1 \otimes H_2 \otimes \dots \otimes H_n$ is said to be *separable* or *unentangled* if:

$$|\Psi\rangle = (|v_1\rangle \in H_1) \otimes (|v_2\rangle \in H_2) \otimes \dots \otimes (|v_n\rangle \in H_n)$$

Otherwise, it is said to be entangled. When non specified, saying that a n -qubit state is entangled means “entangled with respect to the decomposition into n individual qubit states”.

Despite being decomposition-dependent, entanglement is basis-independent, since the chosen basis plays no role in the definition of entanglement (even though some bases might be more comfortable than others when working with entangled states).

2.3. Qubit measurement

In the first section, the issue of measuring the state of a single-qubit system was introduced. Measuring the state of a n -qubit system follows the same idea, but the set of possible measurements and measurement outcomes is significantly larger. It also serves the purpose of describing in greater detail the formal process of measuring in general.

First, recall from Theorem 1.2.1 that any vector space can be decomposed into a direct sum of one or more of its orthogonal subspaces. This means that the state space of an n -qubit system, having dimension 2^n , can be decomposed into $k \leq 2^n$ of its orthogonal subspaces. The number k corresponds to the maximum number of possible measurement outcomes for a state measured with that particular device. This number varies from device to device, even between devices measuring the same system.

As a matter of fact, the observation that any device has an associated direct sum decomposition is just a generalization of the single-qubit case. Every device measuring a single-qubit system has an associated orthonormal basis $\{|v_1\rangle, |v_2\rangle\}$ for the state space V of the system, having dimension 2. Each of these vectors generate a one-dimensional subspace, S_1 and S_2 , consisting of all $\alpha |v_1\rangle$ and $\beta |v_2\rangle$ respectively, with $\alpha, \beta \in \mathbb{C}$, and $V = S_1 \oplus S_2$. Furthermore, the only nontrivial (with no subspaces of dimension 0) possible decompositions of V are the ones into two subspaces of dimension 1, and any choice of unit length vectors, one from each of the subspaces, yields an orthonormal basis.

Exercise 2.3.1: Rephrase the measurement of the single-qubit state $|\Psi\rangle = \frac{\sqrt{2}}{2} |0\rangle + \frac{\sqrt{2}}{2} |1\rangle$ under this formalism.

Solution: Let V be the vector space associated with said single-qubit system. A device that measures a qubit in the standard basis has associated the direct sum decomposition:

$$V = S_1 \oplus S_2 = \text{span}\{|0\rangle\} \oplus \text{span}\{|1\rangle\} = \text{span}\{|0\rangle, |1\rangle\}$$

The state $|\Psi\rangle$ measured by such a device will be $|0\rangle$ with probability $\left|\frac{\sqrt{2}}{2}\right|^2 = \frac{1}{2}$, the amplitude of $|\Psi\rangle$ in the subspace S_1 , and $|1\rangle$ with probability $\left|\frac{\sqrt{2}}{2}\right|^2 = \frac{1}{2}$, the amplitude of $|\Psi\rangle$ in the subspace S_2 . \square

When a measuring device with associated direct sum decomposition $V = S_1 \oplus \dots \oplus S_k$ interacts with an n -qubit system in state $|\Psi\rangle$, the interaction changes the state to one entirely contained within one of the subspaces, and chooses the subspace with probability equal to the square of the absolute value of the amplitude of the component of $|\Psi\rangle$ in that subspace.

More formally, any state $|\Psi\rangle$ in V has a unique direct sum decomposition $|\Psi\rangle = a_1 |\varphi_1\rangle \oplus \dots \oplus a_k |\varphi_k\rangle$, where each $|\varphi_i\rangle$ is a unit vector in S_i and a_i is a real and non-negative number. When $|\Psi\rangle$ is measured, the state $|\varphi_i\rangle$ is obtained with probability equal to $|a_i|^2$. This is not a fact that can be deduced from theory, but is instead an axiom of quantum mechanics.

Exercise 2.3.2: Rephrase the measurement of the 2-qubit state $|\Psi\rangle = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle + \frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle$ under this formalism.

Solution: Let V be the vector space associated with said 2-qubit system. A device that measures the first qubit in the standard basis has associated the direct sum decomposition:

$$\begin{aligned} V = S_1 \oplus S_2 &= (|0\rangle \otimes \text{span}\{|0\rangle, |1\rangle\}) \oplus (|1\rangle \otimes \text{span}\{|0\rangle, |1\rangle\}) = \text{span}\{|00\rangle, |01\rangle\} \oplus \text{span}\{|10\rangle, |11\rangle\} = \\ &= \text{span}\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} \end{aligned}$$

To denote more explicitly what happens when a measurement is performed on the first qubit, the state can be rewritten as $|\Psi\rangle = c_1 |\Psi_1\rangle + c_2 |\Psi_2\rangle$, or more explicitly:

$$|\Psi\rangle = \sqrt{\left|\frac{1}{8}\right|^2 + \left|\frac{\sqrt{7}}{8}\right|^2} \left(\frac{\frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle}{\sqrt{\left|\frac{1}{8}\right|^2 + \left|\frac{\sqrt{7}}{8}\right|^2}} \right) + \sqrt{\left|\frac{\sqrt{7}}{8}\right|^2 + \left|\frac{7}{8}\right|^2} \left(\frac{\frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle}{\sqrt{\left|\frac{\sqrt{7}}{8}\right|^2 + \left|\frac{7}{8}\right|^2}} \right)$$

In this way, the state is correctly normalized and the probabilities for the two possible outcomes for the first qubit can be computed as:

$$P_1 = \left|\frac{1}{8}\right|^2 + \left|\frac{\sqrt{7}}{8}\right|^2 = \frac{1}{64} + \frac{7}{64} = \frac{1}{8} \qquad P_2 = \left|\frac{\sqrt{7}}{8}\right|^2 + \left|\frac{7}{8}\right|^2 = \frac{7}{64} + \frac{49}{64} = \frac{7}{8}$$

\square

Recall that the outer product of two kets results in a matrix. Since any matrix is a representation of a linear operator, this must mean that the outer product of two kets results in an operator. More operators can be constructed by summing outer products. An operator is also represented by denoting how each vector of the basis is mapped to its result.

Exercise 2.3.3: Consider the operator $X = |10\rangle\langle 00| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01|$. What's the corresponding matrix?

Solution: X exchanges the ket $|10\rangle$ with the ket $|00\rangle$ and vice versa, while leaving $|11\rangle$ and $|01\rangle$ unchanged. Keep in mind that the operator is constructed with respect to the standard basis.

$$\begin{aligned}
 X &= |10\rangle\langle 00| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01| = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}^\dagger + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}^\dagger + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}^\dagger + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}^\dagger = \\
 &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} (1 \ 0 \ 0 \ 0) + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} (0 \ 0 \ 1 \ 0) + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} (0 \ 0 \ 0 \ 1) + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} (0 \ 1 \ 0 \ 0) = \\
 &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
 \end{aligned}$$

This can also be represented as:

$$|10\rangle \rightarrow |00\rangle \qquad |00\rangle \rightarrow |10\rangle \qquad |11\rangle \rightarrow |11\rangle \qquad |01\rangle \rightarrow |01\rangle$$

□

Results in Exercise 2.3.3 can be generalized as follows. In an n -qubit system, an operator $O : V \rightarrow V$ for the basis $\{|\varphi_i\rangle\}$ on the state space V can be written as:

$$O = \sum_{i=1}^N \sum_{j=1}^N p_{ij} |\varphi_i\rangle\langle\varphi_j|$$

Where N is the dimension of V . The matrix for O with respect to the basis $\{|\varphi_i\rangle\}$ has the value p_{ij} in the (i, j) -th cell.

Any ket $|\Psi\rangle \in V$ can be written as a linear combination $\sum_{k=1}^N p_k |\varphi_k\rangle$. Applying O to this vector is equal to:

$$O|\Psi\rangle = \left(\sum_{i=1}^N \sum_{j=1}^N p_{ij} |\varphi_i\rangle\langle\varphi_j| \right) \left(\sum_{k=1}^N p_k |\varphi_k\rangle \right) = \sum_{i=1}^N \sum_{j=1}^N \sum_{k=1}^N p_{ij} p_k |\varphi_i\rangle\langle\varphi_j| |\varphi_k\rangle = \sum_{i=1}^N \sum_{j=1}^N p_{ij} p_j |\varphi_i\rangle$$

Again from Theorem 1.2.1, for any vector space V there exist a subspace S of V such that $V = S \oplus S^\perp$, where S^\perp is the vector space that contains all vectors perpendicular to S . This means that any vector $|v\rangle \in V$ can be written in a unique way as $s_1 + s_2$, with $s_1 \in S$ and $s_2 \in S^\perp$.

For any S of the sort it is possible to construct a linear operator $P_S : S \rightarrow V$, called **projection operator**, or *projectors* for short, that maps $|v\rangle$ to s_1 . To construct a projector, it is sufficient to take the outer product of a vector with itself. As a matter of fact, a projector simply “extracts” the “contribution” given by a basis to the state: the product between said basis and the component of the state with respect to the basis.

In general, given a state space V , for any direct sum decomposition $V = S_1 \oplus \dots \oplus S_k$ into orthogonal subspaces, there exist k distinct projection operators P_i , each mapping a state $|v\rangle \in V$ to a vector s_i belonging

the i -th subspace S_i . Framed this way, a measuring device with direct sum decomposition $V = S_1 \oplus \dots \oplus S_k$ acting on a state $|\Psi\rangle$ results in the state

$$|\phi_i\rangle = \frac{P_i |\Psi\rangle}{|P_i |\Psi\rangle|}$$

With probability $|P_i |\Psi\rangle|^2$. Given one of the subspaces S and a basis $\{|\alpha_1\rangle, \dots, |\alpha_s\rangle\}$ for this subspace, the projector P_S that returns the contribution given by $\{|\alpha_1\rangle, \dots, |\alpha_s\rangle\}$ to $|\Psi\rangle$ is simply given by:

$$P_S = \sum_{i=1}^s |\alpha_i\rangle\langle\alpha_i| = |\alpha_1\rangle\langle\alpha_1| + \dots + |\alpha_s\rangle\langle\alpha_s|$$

Indeed, since the base vectors are all orthogonal, applying P_S to a generic state $|\Psi\rangle$ nulls all contributions given by basis absent in S . This also means that a projector is well-defined, since applying a projector two times results in no difference. Note that applying a projector to a state might not return a normalized vector.

Exercise 2.3.4: Consider the two-qubit state $|\Psi\rangle = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle + \frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle$ and the subspace spanned by $\{|00\rangle, |01\rangle\}$. What is the projector with respect to the basis? What is its effect on $|\Psi\rangle$?

Solution: The projector with respect to S is given by $P_S = |00\rangle\langle 00| + |01\rangle\langle 01|$. Applying to $|\Psi\rangle$ gives:

$$P_S |\Psi\rangle = (|00\rangle\langle 00| + |01\rangle\langle 01|) \left(\frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle + \frac{\sqrt{7}}{8} |10\rangle + \frac{7}{8} |11\rangle \right) = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle$$

Note how this state is not normalized. Note also how applying P_S to the result does not change the state:

$$\begin{aligned} P_S(P_S |\Psi\rangle) &= (|00\rangle\langle 00| + |01\rangle\langle 01|) \left(\frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle \right) = \frac{1}{8} |00\rangle\langle 00|00\rangle + \frac{\sqrt{7}}{8} |00\rangle\langle 00|01\rangle + \\ &\quad \frac{1}{8} |01\rangle\langle 01|00\rangle + \frac{\sqrt{7}}{8} |01\rangle\langle 01|01\rangle = \frac{1}{8} |00\rangle + \frac{\sqrt{7}}{8} |01\rangle = P_S |\Psi\rangle \end{aligned}$$

□

Any projector is not only a projector in the mathematical sense, but is also self-adjoint. It is therefore easy to compute $|P_S |\Psi\rangle|^2$:

$$|P_S |\Psi\rangle|^2 = (P_S |\Psi\rangle)^\dagger P_S |\Psi\rangle = \langle\Psi|P_S|\Psi\rangle$$

Exercise 2.3.5: Consider the state $|\Psi\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle$ and a decomposition $S_{00} \oplus S_{01} \oplus S_{10} \oplus S_{11}$. Consider the projector P_{01} and describe the assigned measurement.

Solution: Applying the projection P_{01} to $|\Psi\rangle$ gives:

$$\begin{aligned} P_{01} |\Psi\rangle &= |01\rangle\langle 01| (a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle) = \\ &= a_{00} |01\rangle\langle 01|00\rangle + a_{01} |01\rangle\langle 01|01\rangle + a_{10} |01\rangle\langle 01|10\rangle + a_{11} |01\rangle\langle 01|11\rangle = a_{01} |01\rangle \end{aligned}$$

The state $\frac{P_{01} |\Psi\rangle}{|P_{01} |\Psi\rangle|}$ is measured with probability:

$$|P_{01} |\Psi\rangle|^2 = \langle\Psi|P_{01}|\Psi\rangle = \langle\Psi| (|01\rangle\langle 01|) |\Psi\rangle = \langle\Psi|01\rangle\langle 01|\Psi\rangle = a_{01}^\dagger a_{01} = |a_{01}|^2$$

□

Recall that, for any Hermitian operator, Theorem 1.3.2 describes a unique decomposition into its eigenspaces. Given this correspondence, Hermitian operators can be used to describe measurements.

Let P_i be the projectors onto the subspaces S_i , and let $\{\lambda_1, \dots, \lambda_k\}$ be a set of distinct real values. Then, the Hermitian operator $O = \sum_{i=1}^k \lambda_i P_i$ has $S_1 \oplus \dots \oplus S_k$ as its direct sum decomposition. Thus, when describing a measurement, instead of directly specifying the associated subspace decomposition, it is sufficient to specify a Hermitian operator whose eigenspace decomposition is that decomposition.

Any Hermitian operator with the appropriate direct sum decomposition can be used to specify a given measurement; in particular, the values of the λ_i are irrelevant as long as they are distinct. The λ_i should be thought of simply as labels for the corresponding subspaces, or equivalently as labels for the measurement outcomes³.

It is important to stress that it is not an Hermitian operator that acts on a state when measured, but instead the projectors associated to said operator. The Hermitian operator is just a way (frequently used in quantum mechanics) to write in compact form the projectors associated to a measuring apparatus.

2.4. Qubit manipulations

Manipulating the state of a qubit is performed through a **quantum transformation**. A quantum transformation is simply an operator that, when applied to a quantum state, results in a new state that is still valid. In particular, the operator must be an *endomorphism*, mapping elements from an Hilbert space to elements to the same Hilbert space. Note that, for these reason, a measurement cannot be considered a quantum transformation.

A quantum state is a linear combination of base states, therefore a quantum transformation, in order to return a quantum state, must be linear. In other words, given a state $a_1 |\varphi_1\rangle + \dots + a_n |\varphi_n\rangle$ and a quantum transformation U , the following must hold:

$$U(a_1 |\varphi_1\rangle + \dots + a_n |\varphi_n\rangle) = U(a_1 |\varphi_1\rangle) + \dots + U(a_n |\varphi_n\rangle) = a_1 U(|\varphi_1\rangle) + \dots + a_n U(|\varphi_n\rangle)$$

This way, applying a quantum transformation to a superposition of states is the same as applying the transformation to each component of the superposition.

A quantum state is a unit vector, therefore a quantum transformation must return a state that is also a unit vector. Also, the subspaces associated to the basis in which the vector is a linear combination of must be orthogonal, therefore the resulting state must also be a linear combination of orthogonal vectors.

These requirements ensure that measuring a state in the original basis and then applying a transformation to the outcome gives the same result as applying the transformation first and then measuring the resulting state in the transformed basis. For these properties to be true, a quantum transformation must preserve the inner product. That is, the inner product of two quantum states $|\Psi_1\rangle$ and $|\Psi_2\rangle$ and the inner product of $U |\Psi_1\rangle$ and $U |\Psi_2\rangle$, the result of applying the transformation to said states, must be the same:

$$\langle |\Psi_1\rangle, |\Psi_2\rangle \rangle = \langle U |\Psi_1\rangle, U |\Psi_2\rangle \rangle \Rightarrow \langle \Psi_1 | \Psi_2 \rangle = \langle \Psi_1 | U^\dagger U | \Psi_2 \rangle = \langle \Psi_1 | U^\dagger U | \Psi_2 \rangle$$

For this condition to be true, the operator in matrix form U and its adjoint U^\dagger must be one the inverse of the other, that is $U^\dagger U = I$. In other words, the matrix U must be unitary.

It can be proven that this condition is not only necessary, but also sufficient. Therefore, the set of unitary matrices that map an element of the Hilbert space to other elements of the same space and the set of valid quantum transformations are the same set. Since unitary operators preserve the inner product, they map orthonormal bases to orthonormal bases. In fact, the converse is true: any linear transformation that maps an orthonormal basis to an orthonormal basis is unitary.

Recall that, from Lemma 1.3.2, the product of two unitary matrices is also a unitary matrix. Therefore, applying more than one quantum transformation to a quantum state will still result in a valid quantum state. The tensor product $U_1 \otimes U_2$ is a unitary transformation of the space $X_1 \otimes X_2$ if U_1 and U_2 are unitary transformations of X_1 and X_2 respectively.

Any quantum state transformation that acts on only a small number of qubits a **quantum gate**. Sequences of quantum gates are called **quantum gate arrays** or **quantum circuits**. Given a basic set of quantum gates, it is possible to combine them to construct elaborate transformations of varying complexity.

³In quantum physics, these labels are often chosen to represent a shared property, such as the energy, of the eigenstates in the corresponding eigenspace.

The term “gate” is used to suggest a similarity with the classical logical gates, but does not necessarily entail that the physical implementation of a quantum transformation has to be a gate in the literal sense. Conceiving a quantum transformation as gates has the added advantage of abstracting the need to specify a basis when talking about operators.

Drawing quantum transformations as gates is obiquitous. Transformations are represented graphically by boxes, labeled by the transformation performed, that are to be read left-to-right. Boxes are connected with a line that represents the state of the qubit “flowing” through the circuit.

$$|\Psi\rangle \text{---} \boxed{U_1} \text{---} \boxed{U_2} \text{---} \dots \text{---} \boxed{U_n} \text{---} |\Psi'\rangle \qquad |\Psi'\rangle = U_n \dots U_2 U_1 |\Psi\rangle$$

Figure 2: On the left, a generic circuit acting on a state $|\Psi\rangle$ that returns a state $|\Psi'\rangle$. On the right, its analogous representation with matrix products.

The simplest operator is the **identity operator**, denoted as I , leaves the state unchanged. With respect to the standard basis, the operator has this following form:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{---} \boxed{I} \text{---}$$

Three matrices, called **Pauli matrices**⁴, are also obiquitous:

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = -|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\text{---} \boxed{X} \text{---} \qquad \text{---} \boxed{Y} \text{---} \qquad \text{---} \boxed{Z} \text{---}$$

Note how:

- X is equivalent to a classical NOT gate, since it changes $|0\rangle$ into $|1\rangle$ and vice versa. X has no effect on $|+\rangle$ and $|-\rangle$, therefore those states are its eigenvectors;
- Z changes the relative phase of a superposition in the standard basis. Z has no effect on $|0\rangle$ and $|1\rangle$, therefore those states are its eigenvectors;
- $Y = ZX$ is a combination of negation and phase change. Y has no effect on $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$, therefore those states are its eigenvectors.

Another useful operator is the **Hadamard operator**, denoted as H :

$$H = \frac{\sqrt{2}}{2}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|) = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{---} \boxed{H} \text{---}$$

Which produces an even superposition of $|0\rangle$ and $|1\rangle$ from either of the standard basis elements:

$$H|0\rangle = |+\rangle \qquad H|1\rangle = |-\rangle \qquad H|+\rangle = |0\rangle \qquad H|-\rangle = |1\rangle$$

Extending quantum transformations that act on single qubits from an n qubit system is trivial. As a matter of fact, applying a transformation U to the i -th qubit from an n qubit system is equivalent to applying $I \otimes \dots \otimes I \otimes U \otimes I \otimes \dots \otimes I$ to the entire system, that is applying U to the i -th qubit and applying the identity operator to each of the other qubits of the system.

In general, the simplest quantum transformations that acts on more than a single qubit at a time are those that can be reduced to the application of a transformation to each qubit separately. For example, given the transformation $U \otimes V$ that acts on two qubits at the same time can be broken down into first applying $U \otimes I$ and then applying $I \otimes V$.

Since it's not possible to conceive an entangled state simply as the sum of its parts, transformations that act on single qubits cannot influence (create or destroy) the entanglement of states. Just as entangled states cannot be factorized into single qubit states, transformations that act on entangled states cannot be factorized into a tensor product between single-qubit transformations.

⁴Other sources refer to the Pauli matrices respectively as $\sigma_x, \sigma_y, \sigma_z$

A qubit transformation such as these is the **controlled not gate**, or C_{not} for short. The gate acts on two qubits as follows:

$$C_{\text{not}} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



If the state of the single qubits are thought of as the values of classical bits, the C_{not} gate can be conceived as “flipping” the second bit (the state of the second qubit) if the first bit is 1 (if the first qubit is in state $|1\rangle$) and leave it unchanged otherwise.

Exercise 2.4.1: What is the effect of applying the C_{not} gate to the two-qubit state $\frac{\sqrt{2}}{2}(|00\rangle + |10\rangle)$?

Solution:

$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|) \frac{\sqrt{2}}{2}(|00\rangle + |10\rangle) = \frac{\sqrt{2}}{2}(|00\rangle + |11\rangle)$$

The starting state is not entangled; the final state is. □

For its analogy with classical control gates, the state of the first qubit (the first bit) is also referred to as the **control bit**, whereas the state of the second qubit (the second bit) is also referred to as the **target bit**. However, this terminology might be misleading, since states expressed in different bases than the standard basis might result in the control bit becoming the target bit and viceversa, or having both bits changed.

Exercise 2.4.2: What happens when a C_{not} gate is applied to the state $|+-\rangle$?

Solution: Converting $|+-\rangle$ to the standard basis gives:

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \otimes \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Applying C_{not} to this state gives:

$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|) \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

Converting it back:

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

Which means that, in the Hadamard basis, the control bit and the target bit are in reversed! □

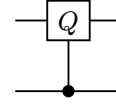
Another transformation that acts on two-qubit systems is the **swap gate**, that changes the state of the first qubit to be equal to the state of the second qubit and vice versa:

$$\text{SWAP} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



The controlled not gate and the swap gate are examples of a more general class of two-qubit controlled gates, where the gate performs a certain transformation Q on the second qubit when the first qubit is in state $|1\rangle$ and does nothing when the first qubit is in state $|0\rangle$. Any gate in this form can be written as $\wedge Q$:

$$\bigwedge Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q = \begin{pmatrix} I & 0 \\ 0 & Q \end{pmatrix}$$



For example, the controlled not gate is equivalent to $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$. Another example is the **controlled phase shift**, that changes the phase of the second qubit if the first qubit is in state $|1\rangle$ and does nothing otherwise:

$$\bigwedge e^{i\varphi} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Ie^{i\varphi} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\varphi} & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}$$

This gate is interesting because it employs a phase shift that when applied to single-qubit systems it just changes the global phase, and therefore is physically meaningless, whereas when applied as part of a conditional transformation it changes the relative phase between elements of a superposition, which is physically meaningful.

Applying a transformation by means of any physical process can be modelled as a rotation along the Bloch sphere. In particular, any rotation can be broken down in two components: one zenithal and one azimuthal.

A zenithal rotation of a state $|\Psi\rangle$ changes its longitude by an angle $\theta/2$ without changing its latitude. Applied to the standard basis gives:

$$\hat{R}_\theta |0\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + \sin\left(\frac{\theta}{2}\right) |1\rangle \quad \hat{R}_\theta |1\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle - \sin\left(\frac{\theta}{2}\right) |1\rangle$$

Which is equivalent to the following matrix multiplication:

$$\hat{R}_\theta = \begin{pmatrix} \langle 0|\hat{R}_\theta|0\rangle & \langle 0|\hat{R}_\theta|1\rangle \\ \langle 1|\hat{R}_\theta|0\rangle & \langle 1|\hat{R}_\theta|1\rangle \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

An azimuthal rotation of a state $|\Psi\rangle$, also called **phase rotation**, changes its latitude by an angle θ without changing its longitude. Applied to the basis $\{|+\rangle, |-\rangle\}$ gives⁵:

$$\hat{P}_\theta |+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + e^{i\theta} |1\rangle) \quad \hat{P}_\theta |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle + e^{i(\theta+\pi)} |1\rangle)$$

Which is equivalent to the following matrix multiplication:

$$\hat{P}_\theta = \begin{pmatrix} \langle 0|\hat{P}_\theta|0\rangle & \langle 0|\hat{P}_\theta|1\rangle \\ \langle 1|\hat{P}_\theta|0\rangle & \langle 1|\hat{P}_\theta|1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Phase rotations of $\pi/2$ radians and $\pi/4$ radians are quite obiquitous, therefore they have been given proper names: \hat{S} and \hat{T} respectively:

$$\hat{P}_{\frac{\pi}{2}} = \hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \hat{P}_{\frac{\pi}{4}} = \hat{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

When a new state is reached, there's most likely interest in sampling its value. Which is why the $|\Psi'\rangle$ symbol is often replaced by $\boxed{\times}$.

⁵Applying an azimuthal rotation on the basis $\{|0\rangle, |1\rangle\}$ would make no sense, since it would be left unchanged.

3. Quantum Theory

3.1. Basics

Any quantum computer architecture that presents itself as usable must respect all of these criteria, called **DiVincenzo Criteria**⁶:

1. Possesses well isolated qubits, qubits shouldn't drift away;
2. Qubits must be initialized to a starting state that is fully under control;
3. Implements a universal set of operations;
4. Taking quantum decoherence into account: the operation time of quantum logic gates should be significantly less than the time frame in which qubits are stable;
5. There must be a way to sample the status of the qubit (readout);
6. Interconversion between qubits and flying qubits;
7. Existence of flying qubits;
8. Scalability: a technology that is not just theoretical but also usable in real applications.

Many real implementations of quantum computers include:

- **Superconducting qubits**;
- **Semiconductors**;
- **Photonic qubits**;
- **Trapped ions**;
- **Neutral atoms**.

Classical computers are based on the Von Neumann architecture, whereas quantum computers have many architecture model. Some architectures are better for some uses, whereas some are better for other uses. Most common ones are:

- **Gate model**, where gates are chained with each other in the same way as classical logic gates are combined into circuits. Supports criteria 1, 2, 4, 5;
- **Adiabatic**, arranging qubits and then applying thermodynamical processes. Supports criteria 1 and 4;
- **Measurement based**, virtualization of the gate model performing operation to condition each state. Support criteria 3;
- **Topological**, at the moment only theoretical.

Quantum noise is still problematic, but can be mitigated with **quantum error correction** introducing redundancy.

Similar to how the ISO-OSI model was formulated for classical computing, an analogous layered architecture was formulated for quantum computing. From top to bottom:

1. **Application layer**, where only algorithm live, hardware-independent;
2. **Representation layer**, where qubits are abstracted to logical qubits, hardware-independent;
3. **Quantum error correction layer**, to introduce redundancy;
4. **Virtual layer**, exploiting physical properties so that qubits are stable;
5. **Physical layer**, raw atoms and molecules.

Even though it is possible to consider qubits as the single atoms or molecules, a more reasonable approach is to go up one level of abstraction and talk about **logical qubits**, that also comprehend redundancy qubits for error correction.

Quantum systems are different from classical systems. The evolution of a classical system can be completely determined from its starting conditions, that is, a classical system is **deterministic**. Observing a classical system at a certain time and predicting the state in which the system will find itself at that same time are, as a matter of fact, indistinguishable.

Quantum systems are not entirely deterministic. When a quantum system is not observed, it evolves in a deterministic way (according to, say, the Schrodinger equation), but when it is observed the result is only partially predictable. This is because, when observed, the system must be found in any of the possible states it can be,

⁶Only the first five criteria are present in the original formulation; the remaining three were introduced later.

but until then it could be in any of those. The probability of finding the system in a certain state depends on the initial conditions.

Quantum mechanics rests on six postulates:

1. **Superposition principle.** At any given time t_0 , the state of a physical system $|\Phi(t_0)\rangle$ is described by specifying the vector ket as an appropriately normalized element of an Hilbert space H , also called **state space**.
2. **Observable quantities.** Energy, angular momentum, position, ecc... are not described by functions. Instead, they are described by operators that act on elements of H . The matrix representation of operators is required to be Hermitian (square and has real eigenvalues). Operators, in general, do not commute, therefore the order of application matters.
3. **Spectrum of measurements.** Every possible value of an observable quantity is quantized, and it is an eigenvalue of the (matrix representation of the) operator associated to such observable.
4. **Probabilistic measurement for a non-degenerate discrete spectra of an operator.** Each possible eigenvalue has a probability to be sampled. Measuring an operator A over state $|\Psi(t_0)\rangle$ has a probability of obtaining the value a_i equal to $P(a_i)$, that goes with $|\langle\mu_i, a_i\rangle|^2$, with μ_i being the eigenvector associated to a_i . The vector $|\mu_i\rangle$ is given by an operator called **projection**, that extracts a component of a vector:
5. **Irreversibility of measurements.** The measurement of an observable A on the state $|\Psi\rangle$, equivalent to applying said operator to $|\Psi\rangle$, after the measurement process the new state is given by:

$$\frac{P_i |\Psi\rangle}{\sqrt{\langle P_i | \Psi \rangle}}$$

Which means that measuring a state influences the system giving a new system, states are not reversible.

6. **Time evolution.** The evolution in time of the states $|\Psi\rangle$ are governed by the **Schroedinger equation**:

$$i \frac{\hbar}{2\pi} \frac{d}{dt} |\Psi(t)\rangle = H(t) |\Psi(t)\rangle$$

Where $H(t)$ is the **Hermitian operator**, an operator associated to the energy of the system.

Postulates 5 and 6 seem to be contradictory, but they are not. Until a measurement is performed, a state is governed smoothly by and equation, whereas when a measurement happens the state is influenced.

3.2. Complexity

A **Turing machine** is a fundamental theoretical model of computation. It can be informally conceived as a moving head with an internal state that can move along a tape of infinite length, divided into cells. The machine can perform one operation at a time, reading the symbol on the current cell, replacing it with another symbol (or with the symbol itself) and moving one cell to the left or to the right.

A Turing machine M is formally defined as the tuple:

$$M = (Q, A, b \in A, \Sigma = A \cup \{L, R\}, \delta : Q \times A \rightarrow Q \times \Sigma, q_0 \in Q, F \subseteq Q)$$

Where:

- Q is the finite control set of states;
- A is the alphabet of the tape (the symbols that can be written on it);
- b is a special symbol called *blank*;
- Σ is the symbol output alphabet;
- δ is a function that, given a state and a tape symbol, outputs a state and an output symbol;
- q_0 is a special state, called *starting state*;
- F are special states, called *final states*;

Each Turing machine can be encoded into a binary string. That is, to each tuple as defined above is possible to associate a binary string that is able to represent the machine, without any loss of information. For a Turing machine M , its binary encoding is denoted as $\langle M \rangle$.

Any string S can be expressed in different languages. The most generic way to express S is as $\langle M \rangle w$, where w is an input string and $\langle M \rangle$ is a Turing machine that accepts w as input and has S as output. This equivalent description of S with respect to $\langle M \rangle$ and w is $d(S)$.

The length of $d(S)$ is denoted as $l(s)$. Note that both $\langle M \rangle$ and w are not unique, therefore there are countably infinitely many combinations of Turing machines and inputs outputting S . A Turing machine-input combination constitutes a **program**: $P = \langle M \rangle$

Being countable, there must be (at least) one program that is *minimal*, that is, constituted by the smallest number of characters. The length of one of those minimal programs is called **Kolmogorov complexity** of the string S , denoted as $K(S)$:

$$K(S) = \min\{l(P) \mid M(P) = S\}$$

The Kolmogorov complexity of a string can be conceived as the minimum number of characters necessary to encode a string in the most generic language possible.

The Turing machine here described is, to be more precise, a **deterministic Turing machine**, because the transition relation is a function: each time the head reads a symbol on the tape, it performs a single action. It is also possible to construct a **non deterministic Turing machine**, where the transition relation is not a function: each time the head reads a symbol on the tape, it performs one or more actions. Of course, it is not possible to construct a non deterministic Turing machine in practice, but it is still possible to employ it as a theoretical model.

Other Turing machines extensions include **probabilistic Turing machines** and **bounded probabilistic Turing machines**

Computational complexity is defined by a language and a machine capable of recognizing the language. In this context, a *machine* is any classical or quantum device that executes a single algorithm of which it is possible to compute the number of steps needed to complete its operation (**time complexity**) or the number of bits needed to store information (**space complexity**). A *language* is simply any sets of strings on an alphabet. A machine *recognises* a language if it is able to stop in a finite number of steps with an affirmative answer for all strings in the language.

A set of languages recognised by a particular kind of machine within given resource bounds in terms of transition relation is called **complexity class**. For each algorithm it is possible to have a complexity class with respect to time and to space; the two might not be the same.

Note that, while Kolmogorov complexity is uncomputable, complexity class is not. That is, there is an algorithm that, given in input another algorithm, is capable of (always) determining its complexity class, whereas there is no algorithm that, given in input a string, is capable of (always) determining its Kolmogorov complexity.

All previously stated computation models are still based on classical computations. A computational model for quantum computation is given by the **quantum Turing machine**:

$$M = (H_Q, H_A, b \in H_A, \Sigma = H_A \cup \{L, R\}, \delta : H_Q \rightarrow H_Q, q_0 \in H_Q, F \subseteq H_Q)$$

Where:

- H_Q is an Hilbert space containing the states;
- H_A is an Hilbert space containing the alphabet of the tape;
- b is the null vector of H_Q ;
- Σ is the set that contains vectors of H_Q ;
- δ is an automorphism from H_Q to itself;
- q_0 is a special state, called *starting state*;
- F are special states, called *final states*;

The **quantum speedup**, that is, the improvement in algorithm speed that a quantum computer has with respect to classical computers, is not due to the raw power of the machine. It is instead due to the fact that complexity classes of quantum algorithms are not arranged in the same way as classical algorithms: