Contents

1. Principles of Quantum Mechanics

1.1. Bra-ket notation

An Hilbert space H is a vector space on a field (assumed to be $\mathbb{C}$) that possesses an inner product. Given two vectors $\overline{x}, \overline{y} \in H$, their inner product $\langle \overline{x}, \overline{y} \rangle$ must satisfy (at least) this three properties:

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

Given two vectors $\overline{x}$ and $\overline{y}$, their dot product is given by:

$$\langle \overline{x}, \overline{y} \rangle = \begin{pmatrix} x_1^* & \dots & x_n^* \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i=1}^{n} a_i^* b_i$$

The notion of norm can be extended to complex-valued vectors:

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

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`:

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

If a state Ψ belongs to an Hilber 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 constitued by linear functionals X over the `kets` in H: if $|\Psi\rangle \in \mathrm{H}$ then $\mathrm{X}(\Psi) \in \mathbb{C}$:

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

Denoting the dot product between two vectors Ψ_1 and Ψ_2 expressed as `kets` is particularly comfortable:

$$\langle |\ \Psi\rangle^*, |\ \Psi\rangle\rangle = \langle\langle\Psi\ |, |\ \Psi\rangle\rangle = \langle\Psi\ |\ \Psi\rangle = 0$$

By definition:

$$\langle |\ \Psi\rangle^*, |\ \Psi\rangle\rangle = \langle\langle\Psi\ |, |\ \Psi\rangle\rangle = \langle\Psi\ |\ \Psi\rangle = 0$$

A basis in quantum mechanics is required to be orthonormal, which means constituted by vectors all orthogonal to each other and whose length is 1.

1.2. 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**. 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**.

1.3. Basics

Any quantum computer architecture that presents itself as usable must respect all of these criteria, called **DiVincenzo Criteria**[1]:

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. Interconvention 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**;

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

- **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 thermodinamical 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 an talk about **logical qubits**, that also comprehend rendundancy 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 Schroedinger 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, 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 Hilber 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**:

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

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.

1.4. 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 lenght, 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:

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

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 lenght 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 affermative 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 incomputable, complexity class is not. That is, there is an algorithm that, given in input another algorithm, is capable of (always) determining its complexity class, whereis 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**:

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

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:

2. Single Qubits

2.1. Definition of a qubit

Consider any physical system that can be observed in only two possible states. Systems such as these can be constructed into 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.

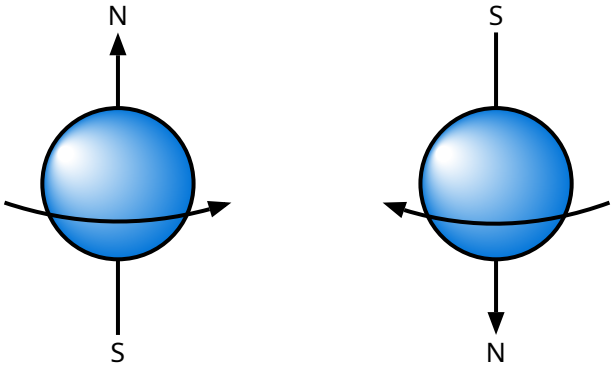


Figure 1: The spin is an intrinsic property of fundamental particles. Electrons have a value of spin that is either equal to $1/2$ or $-1/2$, also referred to as "up" and "down" respectively.

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 $|\alpha|^2$, wherease the probability of finding it in the state $|\varphi_2\rangle$ when measured is given by $|\beta|^2$.

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 performed[2].

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 $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$, commonly denoted as $|0\rangle$ and $|1\rangle$ respectively[3].

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

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

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:

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

□

This basis is used obiquitously, and is therefore reffered 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 $\{|+\rangle, |-\rangle\}$:

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

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 $\{|+\rangle, |-\rangle\}$:

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

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

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

□

Another relevant basis is $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$, defined as:

$$|\circlearrowleft\rangle = \frac{\sqrt{2}}{2}(|0\rangle + i\ |1\rangle) = \begin{pmatrix}\frac{\sqrt{2}}{2}\\i\frac{\sqrt{2}}{2}\end{pmatrix} \qquad |\circlearrowright\rangle = \frac{\sqrt{2}}{2}(|0\rangle - i\ |1\rangle) = \begin{pmatrix}\frac{\sqrt{2}}{2}\\-i\frac{\sqrt{2}}{2}\end{pmatrix}$$

Theorem 2.1.3: The set $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$ 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 $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$:

$$|0\rangle = \frac{\sqrt{2}}{2}(|\circlearrowleft\rangle + i\ |\circlearrowright\rangle) \qquad |1\rangle = \frac{\sqrt{2}}{2}(|\circlearrowleft\rangle - i\ |\circlearrowright\rangle)$$

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

$$\langle \circlearrowleft \mid \circlearrowleft \rangle = \langle \circlearrowright \mid \circlearrowright \rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \cdot i\frac{\sqrt{2}}{2} = 1 \quad \langle \circlearrowleft \mid \circlearrowright \rangle = \langle \circlearrowright \mid \circlearrowleft \rangle = \frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \cdot i\frac{\sqrt{2}}{2} = 0$$

□

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

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

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

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:

$$|\Psi\rangle = \frac{1+i}{2} \mid \circlearrowleft \rangle + \frac{1-i}{2} \mid \circlearrowright \rangle$$

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

$$P_{|\circlearrowleft\rangle} = \left|\frac{1+i}{2}\right|^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} \qquad P_{|\circlearrowright\rangle} = \left|\frac{1-i}{2}\right|^2 = \left(\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^2 = \frac{1}{2}$$

□

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 $\{|0\rangle, |1\rangle\}$?

$$|\Psi_1\rangle = \frac{\sqrt{2}}{2}(|+\rangle + |-\rangle) \qquad |\Psi_2\rangle = \frac{\sqrt{3}}{2} \mid + \rangle - \frac{1}{2} \mid - \rangle$$

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 consitutes 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 $\boldsymbol{CP}^1$:

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

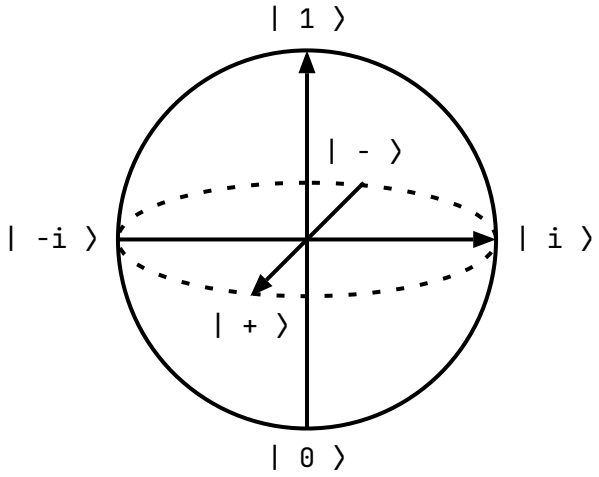
Therefore, the quantum state space for a single-qubit system is in one-to-one correspondence with the points of the complex projective space $\boldsymbol{CP}^1$.

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.

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



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 latitute. Applied to the standard basis gives:

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

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 latitute by an angle θ without changing its longitude. Applied to the basis $\{|+\rangle, |-\rangle\}$ gives[4]:

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

Which is equivalent to the following matrix multiplication:

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

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

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

Another useful operator is the **Hadamard operator**, denoted as $\hat{H}$ and given by the following matrix:

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

Note how:

$$\hat{H}\ |0\rangle = |+\rangle \qquad \hat{H}\ |0\rangle = |-\rangle \qquad \hat{H}\ |+\rangle = |0\rangle \qquad \hat{H}\ |-\rangle = |1\rangle$$

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

The identity operator, denoted as ${}^1\perp$, leaves the state unchanged:

$$ {}^1\perp = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad\qquad {}^1\perp |\Psi\rangle = |\Psi\rangle, \ \forall \Psi $$

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

$$ \hat{\sigma}_x = \hat{x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{\sigma}_y = \hat{y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \hat{\sigma}_z = \hat{z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} $$

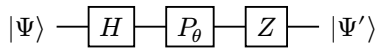
$|+\rangle$ and $|-\rangle$ are the eigenvalues of $\hat{\sigma}_x$, $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$ are the eigenvalues of $\hat{\sigma}_y$ and $|0\rangle$ and $|1\rangle$ are the eigenvalues of $\hat{\sigma}_z$:

$$ \hat{\sigma}_x \, |+\rangle = |+\rangle \qquad \hat{\sigma}_y \, |\circlearrowleft\rangle = |\circlearrowleft\rangle \qquad \hat{\sigma}_z \, |0\rangle = |0\rangle $$

$$ \hat{\sigma}_x \, |-\rangle = |-\rangle \qquad \hat{\sigma}_y \, |\circlearrowright\rangle = |\circlearrowright\rangle \qquad \hat{\sigma}_z \, |1\rangle = |1\rangle $$

$\hat{\sigma}_x$ is equivalent to a classical `NOT` gate, since it changes each 0 input into 1 and vice versa. Also note how $\hat{\sigma}_z$ corresponds to a phase rotations of π radiants.

Iterated applications of operators to a quantum state is equivalent to a gate, read in reverse order:



$$ |\Psi'\rangle = \hat{Z}\hat{P}_\theta\hat{H} \, |\Psi\rangle $$

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  .