An introduction to quantum computation and information

A.y. 2023/24 — Leonardo Mazza — leonardo.mazza@universite-paris.saclay.fr

Lecture 1: The qubit

1) Introduction: Why quantum information and computation?

Key sentence: "Information is physical" — R. Landauer.

Although pronounced in a different context, this sentence is always quoted in this context to say that there is not a single and universal theory of computation / information, but one should develop a specific one depending on the specific physical platform that performs that computation.

The information theory developed by Turing, Shannon etc... is well adapted to classical systems. If one wants to manipulate information with a quantum mechanical system, then he needs another theory.

The idea is not different from the more familiar concept of Euclidean and non-Euclidean geometries. We can say, along with Landauer, that "Geometry is physical". There is not a single and universal geometry, but many geometries that depend on the system that we want to model. On a planar surface I will use Euclidean geometry, on a spherical surface I will use non-Euclidean geometries.

In a sense, quantum information theory is for classical information theory what non-Euclidean geometry is for Euclidean geometry

2) The bit

Information is surprise.

Information is 'news' or 'surprise.' If Alice tells Bob[1] something he already knows, she has not transmitted any information to him and Bob has not learned (received) any information. Suppose for example that Bob asks Alice a question that has two possible answers (yes/no or true/false, say). Further suppose that Bob does not know the answer to his own question. Alice can transmit the answer as a message to Bob by choosing one of two (agreed upon) symbols, say T or F for true or false, or y or n for yes or no. For simplicity we will assume that Alice transmits a 'binary digit,' or 'bit', either the symbol 0 or 1.

[1] In the quantum communication literature, it is traditional to refer to the two communicating parties as 'Alice' and 'Bob.' An eavesdropper listening in on the conversation is traditionally referred to as 'Eve.' Who says physicists don't have a sense of humor?

The bit is the simplest and minimal way of carrying information.

The word 'bit' is short for binary digit a number whose value can be represented by 0 or 1 in the binary numbering system (base 2 numbers). The word bit is also used to mean the amount of information contained in the answer to a yes/no or true/false question (assuming you have no prior knowledge of the answer and that the two answers are equally likely as far as you know). If Alice gives Bob either a 0 or a 1 drawn randomly with equal probability, then Bob receives one bit of information. Bits and base 2 numbers are very natural to use because information is *physical*. It is transmitted and stored using the states of physical objects, as illustrated in Fig. 1.1. For example an electrical switch can be open or closed and its state naturally encodes one 1 bit of information. Similarly a transistor in a computer chip can be in one of two electrical states, on or off. Discrete voltage levels in a computer circuit, say 0 volts and 5 volts are also used to encode the value of a bit. This discretization is convenient because it helps make the system robust against noise. Any value of voltage near 0 is interpreted as representing the symbol 0 and any value near 5 volts is interpreted as representing the symbol 1. Information can also be stored in small domains of magnetism in disk drives. Each magnetic domain acts like a small bar magnet whose magnetic moment (a vector quantity pointing in the direction running from the south pole to the north pole of the bar magnet) can only point up or down. Ordinarily a bar magnet can point in any direction in space, but the material properties of the disk drive are intentionally chosen to be anisotropic so that only two directions are possible. Information is also communicated via the states of physical objects. A light bulb can be on or off and the particles of light (photons) that it emits can be present or absent, allowing a distant observer to receive information.

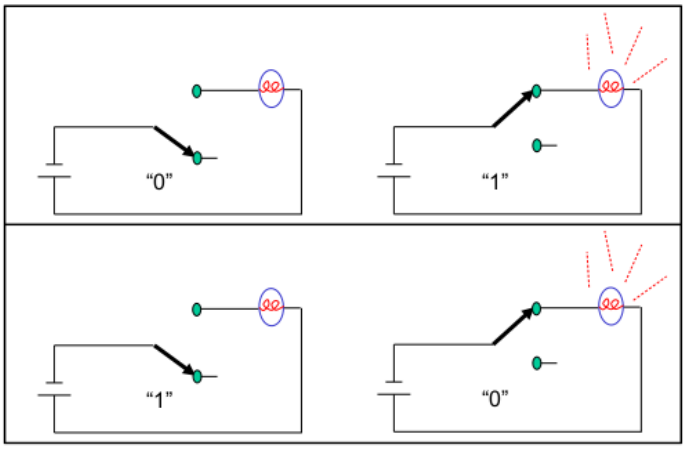


Figure 1.1: The fact that 'information is physical' is illustrated by this electrical circuit encoding one bit of information. Upper panel: Bit value 0 (1) is represented by the switch being open (closed) and the light bulb is off (on). Lower panel: There is only one other possible encoding of the classical information, namely the one in which states 0 and 1 and interchanged. A simple NOT operation transforms one encoding into the other. We will see that the quantum situation is much richer than this.

3) The qubit

A qubit (quantum bit) is information stored in a two-level quantum system.

Physical example #1: the polarisation of the photon.
(see book "Quantum mechanics" by Basdevant & Dalibard sec. 6.1 and 6.2)

Given two orthogonal polarisation states, for instance linear horizontal $|H\rangle$ or $|\rightarrow\rangle$ and linear vertical $|V\rangle$ or $|\uparrow\rangle$, the most generic polarisation state is $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, with $|\alpha|^2+|\beta|^2=1$. It is a two level system and we can make the identification $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$ so that we have a qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha|^2+|\beta|^2=1.$$

Physical example #2: Spin states of a spin-1/2 particle.

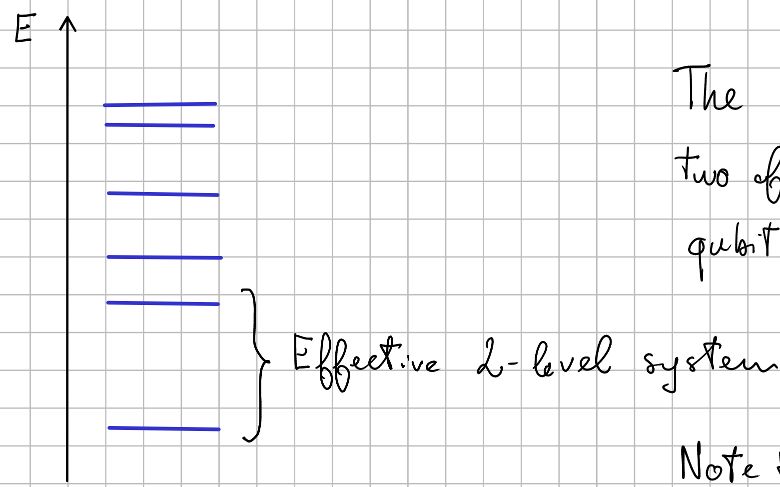
Electrons, protons, neutrons are spin-1/2 particles. Their spin is a two-level system. If I consider the eigenstates of the $\hat{S}_z$ operator, $|\uparrow\rangle$ and $|\downarrow\rangle$, with eigenvalues $\pm\frac{\hbar}{2}$ respectively, the most generic spin state is:

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \quad \text{with } |\alpha|^2+|\beta|^2=1.$$

Hence, we can use it as a physical system for implementing a qubit via the identification $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$.

Physical system #3. Energy levels of an atom.

An atom is characterised by many discrete energy levels, that are all characterised by a set of quantum numbers.



The idea is to consider just two of them and to construct a qubit using them.

Note that in the previous example we had an exact 2-level system.

4) The Bloch sphere.

We need an efficient representation of the qubit. How many and which parameters specify the state of a qubit?

We write that:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \; ; \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

Moreover, there is a gauge freedom:

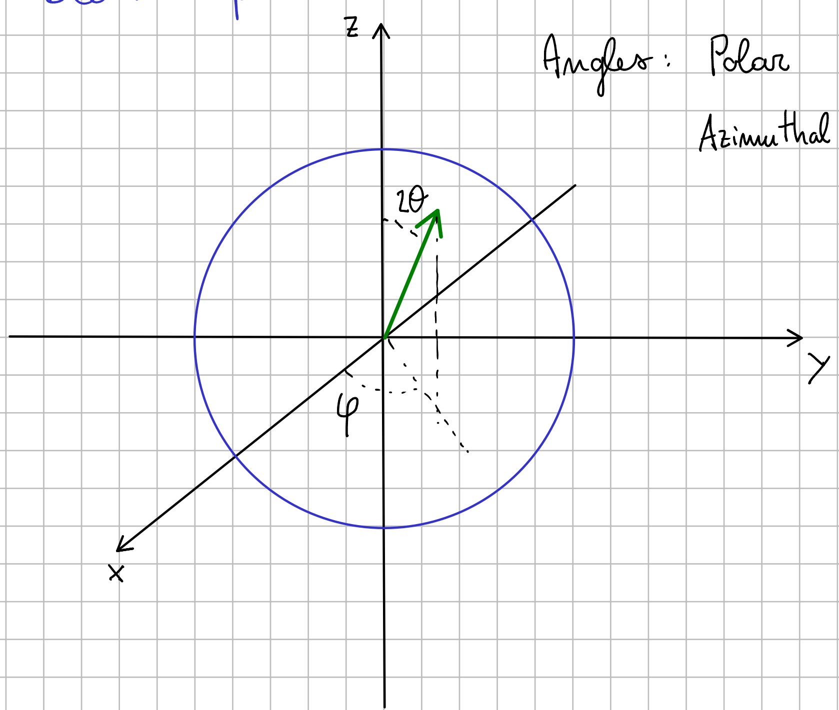
$$|\psi\rangle \quad \text{and} \quad e^{i\delta}|\psi\rangle, \text{ with } \delta \in [0, 2\pi[$$

describe exactly the same physical state. This is an additional freedom that we have. Using this freedom we decide that we take $\alpha \in \mathbb{R}^+$ and hence $|\alpha| = \alpha$. β is complex.

The normalisation condition leads to the natural parametrisation $|\alpha| = \alpha = \cos\theta$ and $|\beta| = \sin\theta$ and since $|\alpha| \geq 0$ we take $\theta \in [0, \frac{\pi}{2}]$. Thus:

$$|\psi\rangle = \cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle, \quad \theta \in [0, \tfrac{\pi}{2}]$$
$$\varphi \in [0, 2\pi]$$

This is the parametrisation of a spherical surface, also called the Bloch sphere.



Angles: Polar $2\theta \in [0, \pi]$

Azimuthal $\varphi \in [0, 2\pi]$

Correctly, as in a sphere, φ is not well-defined when $2\theta = 0$ or π.

Remark: the Bloch sphere is a useful graphical representation of the space state of a qubit. It is an abstract representation. The x, y, z axes have nothing to do with the x, y z axis of a physical real space.

Remarkable points of the Bloch sphere:

- NORTH POLE: $|\psi\rangle = |0\rangle$
- SOUTH POLE: $|\psi\rangle = |1\rangle$
- EQUATOR: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$

Exercise: Prove that states that are opposite on the Bloch sphere are orthogonal.

5) Quantum gates and circuits.

Once we have a qubit, we want to manipulate it. This manipulation is typically represented by an operator acting on $|\psi\rangle$:

$$|\psi\rangle \longrightarrow \hat{U}|\psi\rangle = |\psi'\rangle$$

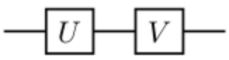
We demand that $|\psi'\rangle$ is still a well-defined qubit, and that for instance $\langle\psi'|\psi'\rangle = 1$ for any $|\psi\rangle$.
This implies that $U^{\dagger}U = \mathbb{1}$.
If we ask the same for the transformation $|\psi\rangle \rightarrow \hat{U}^{\dagger}|\psi\rangle = |\psi''\rangle$ we also get that $UU^{\dagger} = \mathbb{1}$.
Hence, $UU^{\dagger} = U^{\dagger}U = \mathbb{1}$ means that U is a unitary operator.
Rules of the game: In standard quantum information science,

We manipulate qubits ONLY with unitary transformations. Other schemes are of course possible, but the standard version is with unitaries.

> A **quantum (logic) gate** is a device which performs a fixed unitary operation on selected qubits in a fixed period of time, and a **quantum circuit** is a device consisting of quantum logic gates whose computational steps are synchronised in time.
>
> The **size** of such a circuit is the number of gates it contains. The gates in a circuit can be divided into layers, where the gates in the same layer operate at the same time, and the number of such layers is called the **depth** of a circuit.

Some unitary U acting on a single qubit is represented diagrammatically as

This diagram should be read *from left to right*. The horizontal line represents a qubit that is inertly carried from one quantum operation to another. We often call this line a **quantum wire**. The wire may describe translation in space (e.g. atoms travelling through cavities) or translation in time (e.g. a sequence of operations performed on a trapped ion). A sequence of two gates acting on the same qubit, say U followed by V, is represented by

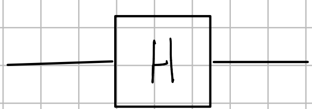


and is described by the matrix product VU (note the order in which we multiply the matrices).

Some notable single-qubit gates.

The Hadamard gate.

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



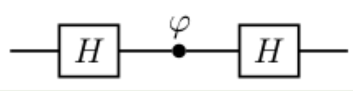
The phase shift gate

$$P_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \qquad \begin{aligned} P_\varphi|0\rangle &= |0\rangle \\ P_\varphi|1\rangle &= e^{i\varphi}|1\rangle \end{aligned}$$

Are these gates unitaries?

A simple quantum circuit. (Note that the composition of unitaries is a unitary)

$|\psi\rangle$



$|\psi'\rangle$

initial state

final state.

Matrix representation of the circuit:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & e^{i\varphi}\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = e^{i\frac{\varphi}{2}}\begin{bmatrix}\cos\varphi/2 & -i\sin\varphi/2\\ -i\sin\varphi/2 & \cos\varphi/2\end{bmatrix}$$

The phase φ determines the output.

Other notable single-qubit gate: the Pauli gates.

- Identity $\mathbb{1} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ $\quad |0\rangle \to |0\rangle$, $|1\rangle \to |1\rangle$
- Bit flip $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \sigma_x$ $\quad |0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$
- Phase flip $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \sigma_z$ $\quad |0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$ $\quad$ This is a special instance of P_φ for $\varphi = \pi$.
- Bit-phase flip $Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} = \sigma_y$ $\quad |0\rangle \to i|1\rangle$, $|1\rangle \to -i|0\rangle$

Note that $Y = -iZX$.

The phase flip is a specific instance of the P_φ. There are other notable phase flips:

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

Note the confusing names!

6) Systematic study of single qbit quantum gates.

How many single qbit quantum gates are there? Let us begin by considering the classical case.
In classical information theory there are only four single bit functions.

Identity $0 \to 0$, $1 \to 1$

Not $0 \to 1$, $1 \to 0$

Erase $0 \to 0$, $1 \to 0$

Erase Not $0 \to 1$, $1 \to 1$

In quantum information we are interested in the most generic unitary operation. It is parametrised by three angles α, β, φ, taking values in $[0, 2\pi]$.

Any unitary operation on a qubit (up to an overall multiplicative phase factor) can be implemented by a circuit containing just two Hadamards and three phase gates, with adjustable phase settings, as in Figure 2.3.

Figure 2.3: The universal circuit for unitary (2×2) matrices, exhibiting how any such matrix is uniquely determined (up to a global phase) by three real parameters.

If we multiply the matrices corresponding to each gate in the network we obtain the single matrix

$$U(\alpha, \beta, \varphi) = \begin{bmatrix} e^{-i\left(\frac{\alpha+\beta}{2}\right)} \cos \varphi/2 & -ie^{i\left(\frac{\alpha-\beta}{2}\right)} \sin \varphi/2 \\ -ie^{-i\left(\frac{\alpha-\beta}{2}\right)} \sin \varphi/2 & e^{i\left(\frac{\alpha+\beta}{2}\right)} \cos \varphi/2 \end{bmatrix}.$$

Any (2×2) unitary matrix (up to global phase) can be expressed in this form using the three independent real parameters, α, β, and φ, which take values in $[0, 2\pi]$. In order to see that this construction does what it claims, let us explore an intriguing mathematical connection between single-qubit unitaries and rotations in three dimensions.

Intuitive derivation of the result that we are going to prove

A q-gate is a mapping from the Bloch sphere to the Bloch sphere.

A q-gate is unitary, hence it preserves scalar products.

On the Bloch sphere, opposite vectors are orthogonal.

A q-gate should be represented by a rotation of the Bloch sphere that maintains opposite vectors at opposite position.

→ Hence, it is a rotation of the Bloch sphere.

It is a 3D rotation of the Bloch sphere: 3 real parameters (Euler angles or Tait-Bryan angles).

↑

$R_z(\alpha)\, R_x(\beta)\, R_z(\gamma)$

1) The phase gate is a rotation of φ around the z axis.

In a 2-level system, a rotation around the z axis is:

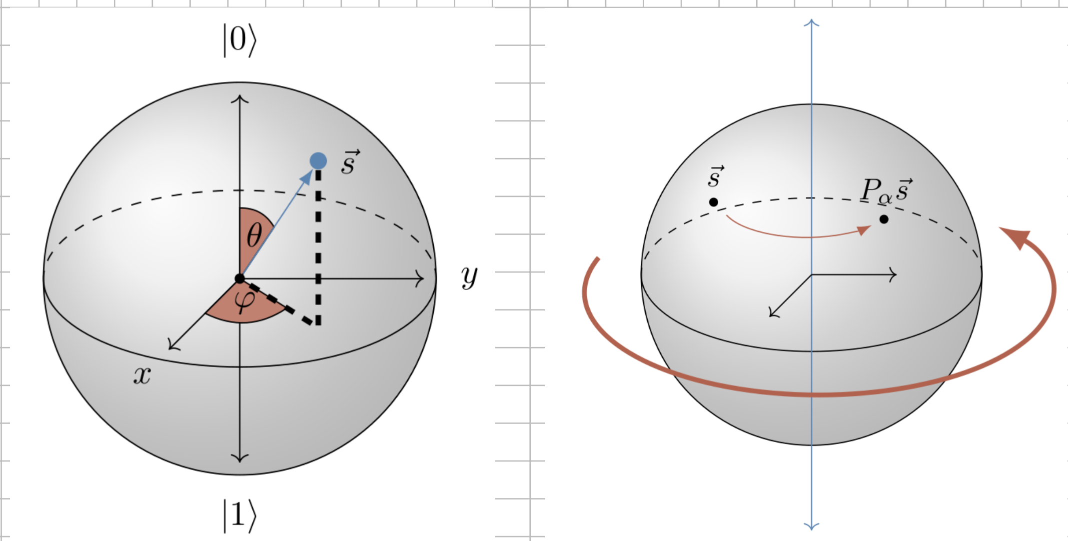
$$R_z(\varphi) = e^{-i\frac{\varphi}{2}\sigma^z} = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix} = e^{-i\varphi/2} P_\varphi$$

Remarks on the matrix exponential:

1. Defined through the series of the exponential
2. In the basis in which σ^z is diagonal, it is the exponential of the eigenvalues.

Physical interpretation: it is a rotation of φ around the z axis of the Bloch sphere.

Geometric:



Check on simple examples:

1) $R_z(\varphi)\,|0\rangle = e^{-i\varphi/2}|0\rangle$ OK 2) $R_z(\varphi)\,|1\rangle = e^{i\varphi/2}\,|1\rangle$ OK

3) $$R_z(\varphi)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{\sqrt{2}}\left(e^{-i\varphi/2}|0\rangle + e^{i\varphi/2}|1\rangle\right) =$$

$$= e^{-i\varphi/2}\,\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right) \quad \text{OK}$$

4) General: $R_z(\varphi)\left(\cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle\right) =$

$$= e^{-i\varphi/2}\left(\cos\theta\,|0\rangle + e^{i(\phi+\varphi)}\sin\theta\,|1\rangle\right) \qquad \underline{\text{OK}}$$

Important properties:

$$R_z(-\varphi) = R_z(\varphi)^{\dagger} = R_z(\varphi)^{-1}$$

2) Other rotation axes.

If $R_z(\varphi) = e^{-i\frac{\varphi}{2}\sigma^z}$ is the rotation operator around the z axis of the Bloch sphere, then

$$R_x(\varphi) = e^{-i\frac{\varphi}{2}\sigma^x} \quad \text{and} \quad R_y(\varphi) = e^{-i\frac{\varphi}{2}\sigma^y}$$

are the rotation operators around the x and y axes.

We may want to consider a generic axis:

$$\hat{n} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix} \quad \text{with} \quad \|\hat{n}\| = 1$$

then:

$$R_{\hat{n}}(\varphi) = e^{-i\frac{\varphi}{2}(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)}$$

$$= e^{-i\frac{\varphi}{2}(\hat{n}\cdot\vec{\sigma})}$$

3) $-\boxed{H}-\underset{\varphi}{\bullet}-\boxed{H}-$ is a rotation around the x axis.

We need to study $\quad H \cdot \sum_{k=0}^{\infty} \frac{(-i\varphi/2)^k}{k!}\,\sigma_z^{\,k} \cdot H.$

Useful properties: • $H^2 = \mathbb{1}$. By explicit calculation.

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \mathbb{1}$$

- $H\sigma_z H = \sigma_x$. By explicit calculation:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x .$$

Now:

$$H \sum_{k=0}^{\infty} \frac{(-i\varphi/2)^k}{k!} \sigma_z^k H = \sum_{k=0}^{\infty} \frac{(-i\varphi/2)^k}{k!} (H\sigma_z H)^k = \sum_{k=0}^{\infty} \frac{(-i\varphi/2)^k}{k!} \sigma_x^k = e^{-i\frac{\varphi}{2}\sigma_x}$$

4) Any rotation in 3D can be represented as:

$$R_{\hat{n}}(\chi) = R_z(\alpha) R_x(\beta) R_z(\gamma)$$

Euler!

5) Any unitary transformation is a rotation of the Bloch sphere.

Consider a unitary transformation: $\mathcal{U}\mathcal{U}^+ = \mathcal{U}^+\mathcal{U} = \mathbb{1}$.
A unitary transformation can be put in diagonal form (because $[\mathcal{U}, \mathcal{U}^+] = 0$). The eigenvalues are $|\lambda| = 1$, $\lambda = e^{i\delta}$.

$$\mathcal{U} = e^{i\delta_1} |u_1\rangle\langle u_1| + e^{i\delta_2} |u_2\rangle\langle u_2|$$

$$\mathcal{U}^+ = e^{-i\delta_1} |u_1\rangle\langle u_1| + e^{-i\delta_2} |u_2\rangle\langle u_2|$$

$$\langle u_1|u_2\rangle = 0.$$

Write $\mathcal{U} = e^{i\frac{\delta_1+\delta_2}{2}} \left(e^{i\frac{\delta_1-\delta_2}{2}} |u_1\rangle\langle u_1| + e^{-i\frac{\delta_1-\delta_2}{2}} |u_2\rangle\langle u_2| \right)$

$\log \mathcal{U} = i\delta_1 |u_1\rangle\langle u_1| + i\delta_2 |u_2\rangle\langle u_2| = i h$

with $h = \delta_1 |u_1\rangle\langle u_1| + \delta_2 |u_2\rangle\langle u_2|$, with $h = h^+$ Hermitian.

Result: any unitary is the exponential of a antihermitian operator,

i × hermitian.

$$\mathcal{U} = e^{ih}$$

What is the most generic hermitian operator acting on a qubit? Easy to prove that we need 4 real parameters: and that we can write:

$$h = \alpha_0 \mathbb{1} + \alpha_x \sigma_x + \alpha_y \sigma_y + \alpha_z \sigma_z$$

$$\mathcal{U} = e^{i(\alpha_0 \mathbb{1} + \alpha_x \sigma_x + \alpha_y \sigma_y + \alpha_z \sigma_z)}$$

$[\alpha_0 \mathbb{1}, \alpha_x \sigma_x + \alpha_y \sigma_y + \alpha_z \sigma_z] = 0$ and hence I can split the exponential:

$$\mathcal{U} = \underbrace{e^{i\alpha_0 \mathbb{1}}}_{e^{i\alpha_0}\ \text{just a global phase}} \cdot \underbrace{e^{+i(\alpha_x \sigma_x + \alpha_y \sigma_y + \alpha_z \sigma_z)}}_{\text{Rotation operator.}}$$

Conclusion: A single q-bit gate is a rotation of the Bloch sphere. A rotation is parametrised by three real parameters, which are angles.

A single qu-bit gate is parametrised by 3 real parameters.

Do I need to be able to implement all possible rotations?
No! Rotations around 2 perpendicular axes will be enough.
For instance x and z.

Do I need to be able to implement rotations of any angle for a given axis? NO! a rotation of an angle χ that is not commensurate with 2π is enough. Then, apply repeatedly until you approximate your angle with the desired accuracy.

7) Retrieving information on the quantum computation.

After a series of gates (a quantum circuit) has been executed, the information about the quantum computation performed is retrieved by performing a measurement. Assume that at the end of the q-computation we have the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
It is customary to measure the observable σ_z, which has eigenvalues / eigenvectors

$$\{+1, |0\rangle\} \quad \text{and} \quad \{-1, |1\rangle\}$$ ← be careful it's strange!

Result of the measurement:

- $+1$ and projection to $|\psi'\rangle = |0\rangle$ with probability $p_1 = |\alpha|^2$
- -1 and projection to $|\psi'\rangle = |1\rangle$ with probability $p_{-1} = |\beta|^2$

Important difference with classical computing: the final result is probabilistic. (Although there are quantum algorithms that give deterministic answers, in general they are probabilistic algorithms).