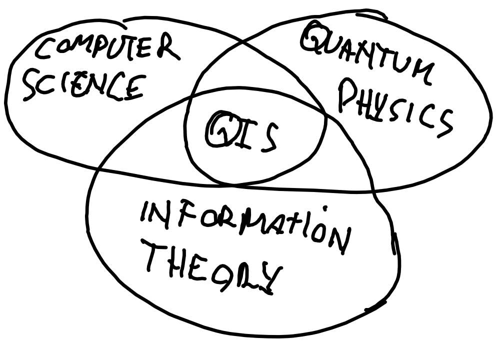
Brief Historical Background:

· How did Quantum Information Science (QIS) developed?

QIS is an offspring of 3 different fields:



Quantum Computing

- represents a new paradigm of computing
- uses theory of quantum mechanics for performing computational tasks.

- has speed (efficiency) advantages that cannot be overcome by any conceived classical computing scheme.
- can be simulated, till a certain extent, on a classical computer BUT NOT EFFICIENTLY.

EFFICIENCY:

EFFICIENT	INEFFICIENT
Computer running in time polynomial in the size of the problem	Computer running in time super-polynomial (typically exponential) in the size of the problem

- A quantum computer is a device that leverages specific properties described by Q.M to perform computational tasks.
- of course, any classical computer can be described by Q.M. However, a classical computer does not take advantages of the specific quantum properties!

Why is Quantum Computing (Q.C.) Interesting?

1. Q.C. could efficiently simulate quantum many-body systems
2. No known classical algorithm can efficiently simulate a quantum computer.
3. Known quantum algorithms (Shor, Grover, ...) which offers exponential advantages compared to the best known classical algorithms [for specific tasks]
4. Theory of quantum error corrections exists for Q.C. $\Rightarrow$ we can deal with noisy and faulty operations!
5. Building Q.C. offers rewarding scientific discoveries and stimulates advances in engineering and instrumentations.

Basic Element of Q.C.

- Key question: which components (or features) does a generic quantum computer have?
- How are those different from a classical computer?

- Let's build an "hardware independent" knoledge about quantum computers to evaluate different physical realizations.

OUTLINE:

1 Aspects of classical Info Processing → 2 Structure of a Q.C. → 3 Features of Components

<u>Challenges</u>: Requires control over individual quantum degrees of freedom.

1920's : Theoretical foundation of Quantum Physics to explain phenomena like photoelectric effect, atom level structures, Stern-Gerlach experiment, ...

1970's : Gain experimental control over single trapped atoms. Development of theory of quantum information processing (Q.I.P.)

Since 2009: Significative progresses in developing quantum hardware using varieties of physical realizations:

(trapped ions, Rydberg atoms, Quantum Dots, Superconducting qubits)

Classical Information processing:

- carrier of information in binar representation BIT { possible values 0, 1 }

Physical Representation

- voltage level in a circuit
- magnetization in hard disks
- flip-flop circuits for RAMs

- modification of information in BIT by operating with a physical process on the BITs

- any logical operations on bits can be decomposed in single and 2-bits operations (if we do not request the reversibility).

Classical Logic. (Boolean)

- 1 or more Boolean values ⟶ single Boolean
  - 1 → single bit gate
  - more → Two-bits gates
  - single → usually not reversible

Single bit operations:

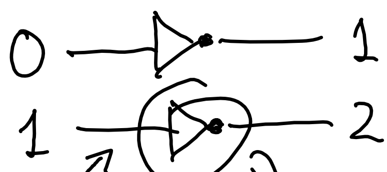
$\xrightarrow{\text{time}}$

input bit ———————— output bit

$0 \longrightarrow 0$

$1 \longrightarrow 1$

Identity $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$



NOT operation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

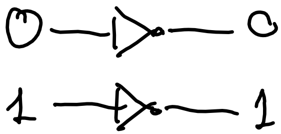
wires represent bit and preserve states

Symbols represent gates / operations so they change the bit states

- Some representation of information in <u>circuit model</u> for quantum computation.

Classical logic gates

IDENTITY GATE ("DO NOTHING") "BUFFER"



IN	OUT
0	0
1	1

$$\sigma_0$$

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

"quantum version = free evolution"

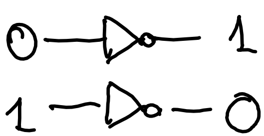
ERASE GATE (irreversible)

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

IN	OUT
0	0
1	0

"quantum version = relaxation"

NOT GATE (inverter)



IN	OUT
0	1
1	0

$$\sigma_x$$

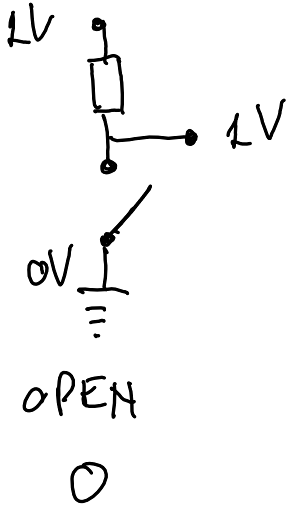
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

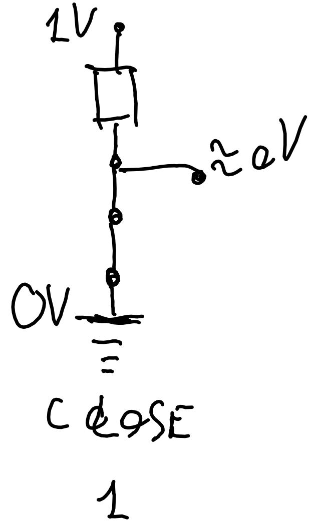
"q. version $\Rightarrow$ X gate"

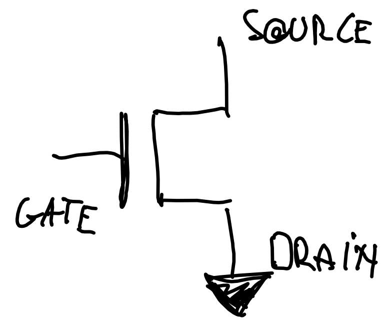
These are the most common single-bit gates.

Physical realizations: "controllable switches" (4)

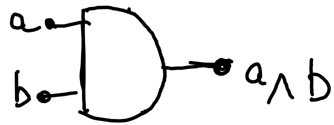
TRANSISTORS





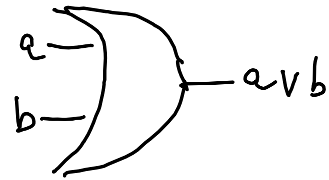


Two bits gates:



a\b	0	1
0	0	0
1	0	1

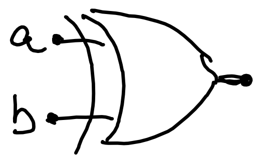
OR



a\b	0	1
0	0	1
1	1	1

They are <u>irreversible</u>: cannot determine unique inputs for all outputs

XOR



a\b	0	1
0	0	1
1	1	0

<u>reversible</u>

"quantum version" $\Longrightarrow$ CX or CNOT gate

6

Universal logic gate: a set of gates that can implement any boolean function

{AND, NOT} ; {OR; NOT} ; {NAND} ;

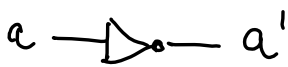
NAND is the most economical ; manufactures can focus and optimize a single gate.

- The majority of these gates are irreversible

When a bit of info is erased it takes $k_B \ln 2 \sim 10^{-21}$ J of energy $\Rightarrow$ Loss of INFO $\Rightarrow$ Heat

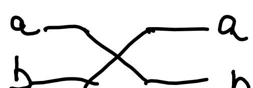
- In classical info. tech. there are also some reversible gates : UNIQUE INPUT associated with UNIQUE OUTPUT

NOT



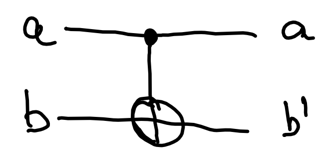
a	a'
0	1
1	0

SWAP



+ TOFFOLI (3 input 3 output) are a UNIVERSAL GATE SET

CNOT



a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Any computable function can be represented as a circuit composed of logic universal gates acting on a set of input bits generating a set of output bits.

NO CLONING THEOREM

Circuit properties: • - bits can be copied (FAN OUT)

• - additional working bits are allowed (ANCILLA BITS)

• - values of bits can be interchanged (CROSSOVER)

• - number of output bits can be lower than # of input bits (IRREVERSIBLE) REVERSIBLE

• - loops are not allowed

• Valid also for Q.C.

• forbidden for Q.C.

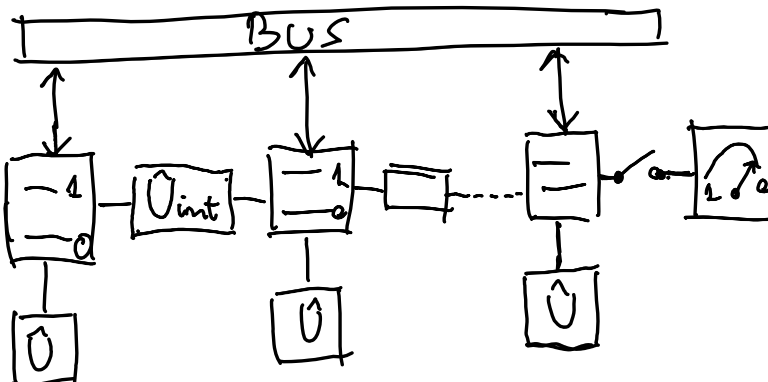
A generic Quantum processor | Features: ①

1. quantum bits [well defined two-level system] + [scalable]
2. initialization of the qubit register
3. coherence (>> gate time)
4. sets of universal gates
5. Readout

[DiVincenzo criteria]

6. Interconvert stationary and flying qubits
7. Faithfully transmit flying qubits between specific locations

→ NETWORKABILITY



Circuit model of quantum computation:

$$|\psi_{OUT}\rangle = U\,|\psi_{IN}\rangle$$

→ register of qubits → n qubits

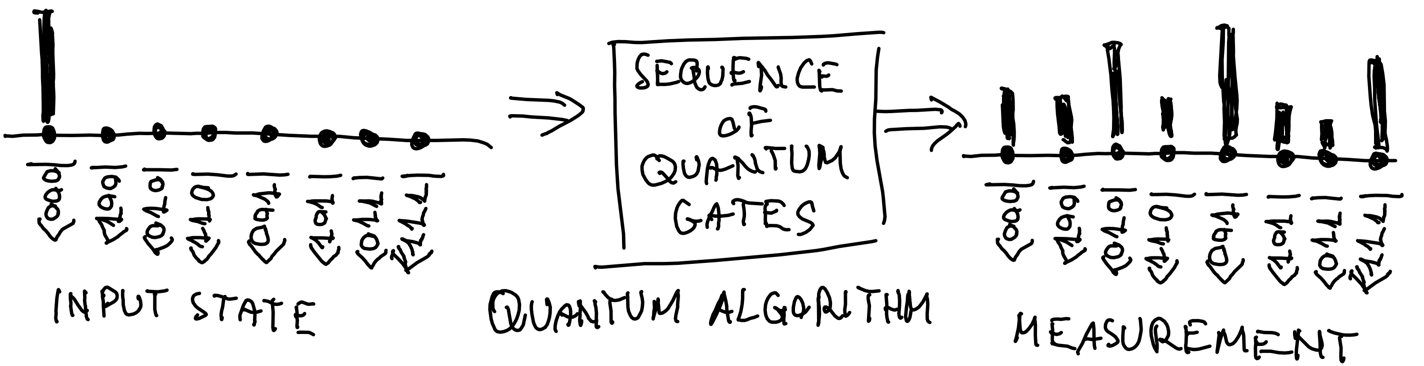
e.g. in state $|00\ldots0\rangle$

[2^n components to one state
quantum parallelisms]

$|\psi_{OUT}\rangle$ → output of the algorithm

U → unitary operator

Decomposition of any U into single-qubit gates and controlled NOT gate possible



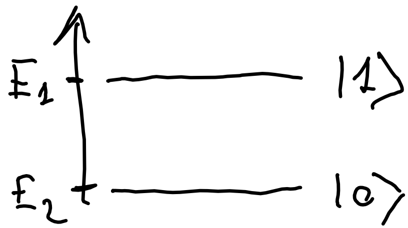
OBSERVATIONS: what are quantum operations?

In quantum mechanics a quantum operator (gate) is the time evolution of the system. You take a system, implement a series of controlled interactions with the environment (it can be, for instance, a driving MW pulse or a fast/slow sweep of the system parameters) and, as a result, the system (qubit ensamble) will evolve.

In quantum mechanics the evolution of a system is dictated by Hamiltonian operators, through this object called "time evolution operator" $U = \exp\{-i\hat{H}t\}$, which is unitary $U^{-1} = U^{\dagger}$ [so it can be inverted]. It preserves lengths of the vectors in the Hilbert space, that means that the norms of the vectors are preserved.

- The spirit of quantum computers is to design systems that evolve according to specific Hamiltonians in order to produce specific transformations of the states.

The quantum bit: • a quantum mechanical two-level system with 2 distinct states



It represents a vector in a 2D Hilbert space $\mathcal{H}$ (1^{st} postulate of Q.M.)

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

• a general qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ with basis states $\{|0\rangle, |1\rangle\}$.

properties: • qubits can be in superpositions of states $|0\rangle$ and $|1\rangle$ with $P_0 + P_1 = 1$

$P_0 = |\alpha|^2$
$P_1 = |\beta|^2$

• Measurements project into either one of the 2 states

What is the main difference with respect to classical bits? 5

1) phase matters! That is why the decoherence is an issue

2) parallelism: operations (gates) act on qubits in both $|0\rangle$ AND $|1\rangle$ states

Extention to many qubits: 2 qubits 4 states

3 " 8 states

N " 2^N "

And a gate operation acts in parallel on 2^N states!

Bloch Sphere: representing qubit states

⑥

$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$, c_0, c_1 complex numbers

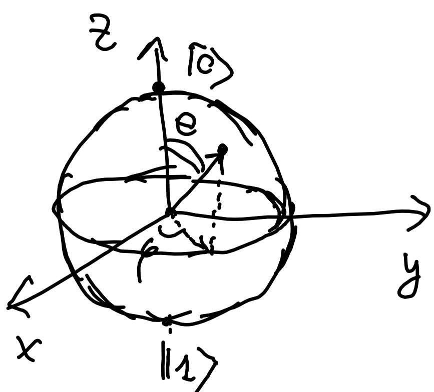
$c_0 = \alpha_0 + \beta_0 i$; $c_1 = \alpha_1 + \beta_1 i$

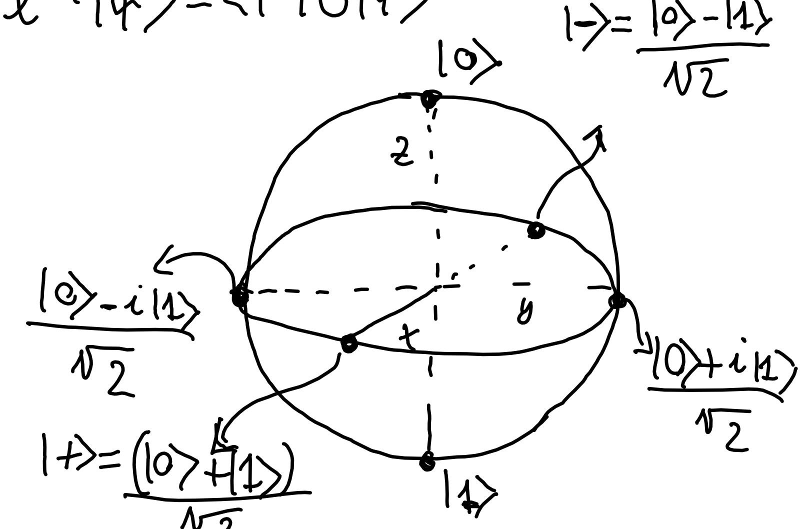
4 numbers describe the states BUT ONLY 2 ARE INDEPENDENT

1) wavefunction should be normalized $|c_0|^2 + |c_1|^2 = 1$

2) the global phase is not measurable

$$\langle\psi|\hat{O}|\psi\rangle = \langle\psi'| e^{-i\varphi} \hat{O} e^{i\varphi} |\psi'\rangle = \langle\psi'|\hat{O}|\psi'\rangle$$





In general we can write, using spherical coordinate (7)

$$|\psi\rangle = e^{i\gamma}\left[\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right]$$

with γ: global phase factor

θ: polar angle

φ: azimutal angle

This represents a vector on the surface of the Bloch sphere. (Mixed states are inside the sphere)

- Why $\frac{\theta}{2}$ and not θ? for spin $\frac{1}{2}$ (2-level system) we have a 4π-symmetry

The state returns to itself only for $\theta + 4\pi$

For 2π rotation we get an additional "$-$" sign (observable in interference experiments)

$$|\psi\rangle_{\theta=0} = -|\psi\rangle_{\theta=2\pi} = |\psi\rangle_{\theta=4\pi}$$

Physical realization of a qubit: SPIN $\frac{1}{2}$

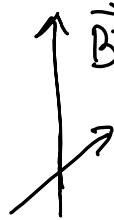
- Quantum mechanical systems are characterized by an energy level diagram, represented by the eigenstates of the system Hamiltonian $E_i|i\rangle = \hat{H}|i\rangle$
- Most physical systems have more than 2 states.

Single qubit dynamics: spin $\frac{1}{2}$ particle in an external magnetic field.

g: giromagnetic ratio

μ_B: Bohr magneton

$$H = -\vec{\mu}\cdot\vec{B}$$



$\vec{B}(0,0,B_z)$

$\vec{\mu} \rightarrow$ magnetic moment

$$\hat{H} = -g\frac{\mu_B B_z}{2}\hat{z}$$

Dynamic of Quantum systems:

Q.M. Postulate: The time evolution of a state $|\psi\rangle$ of a closed quantum system is described by the Schrödinger equation: $i\hbar \frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle$

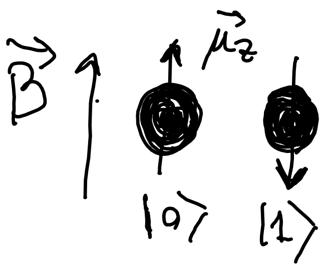
↳ Hamiltonian

Reminder: A closed quantum system is one which does not interact with any other system.

For a time-independent Hamiltonian:

$\hat{H}|\psi_i\rangle = E_i|\psi_i\rangle$. Eigenstate of $\hat{H}$ are $|0\rangle$ and $|1\rangle$

Example: electron spin in a $\vec{B}$ field

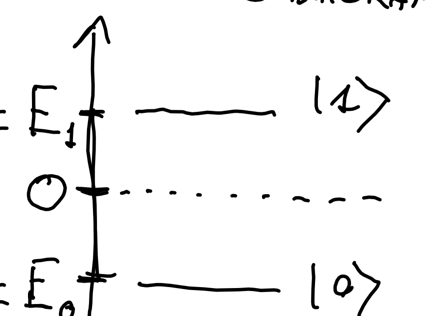


$$\Delta E = g\mu_B B_z = \hbar\Omega_z = E_1 - E_0$$

$$+\frac{\hbar}{2}\Omega_z = \frac{g\mu_B B_z}{2} = E_1$$

$$-\frac{\hbar}{2}\Omega_z = -\frac{g\mu_B B_z}{2} = E_0$$

ENERGY LEVEL DIAGRAM



- Time dependent Schrödinger Equation

$$i\hbar \frac{d}{dt}|\psi\rangle = \hat{H}|\psi\rangle$$

- general solution for time independent $\hat{H}$

$$|\psi(t)\rangle = \exp\left[-\frac{i}{\hbar}\hat{H}t\right]|\psi(0)\rangle$$

with $\exp(i\theta\hat{O}) = \cos\theta\,\hat{I} + i\sin\theta\,\hat{O}$

for operators with $\hat{O}^2 = \hat{I}$ and $\theta \in \mathbb{R}$

e.g. for all Pauli matrices

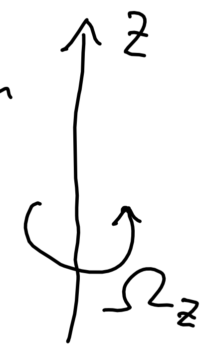
- For our spin $\frac{1}{2}$ example: $\hat{H} = -\frac{\hbar}{2}\Omega_z\hat{Z}$

$$|\psi(t)\rangle = \exp\left(-\frac{i}{\hbar}\hat{H}t\right)|\psi(0)\rangle$$

$$= \left(\cos\frac{\theta_z}{2}\,\hat{I} + i\sin\frac{\theta_z}{2}\,\hat{Z}\right)|\psi(0)\rangle$$

$$= R_z(\theta_z)|\psi(0)\rangle \text{ with } \theta_z = \Omega_z t$$

rotation about z-axis on Bloch sphere!



11

Hamiltonian for a spin-$\frac{1}{2}$ in a magnetic field

$$H = -\frac{\hbar}{2}\Omega_z \hat{Z}$$

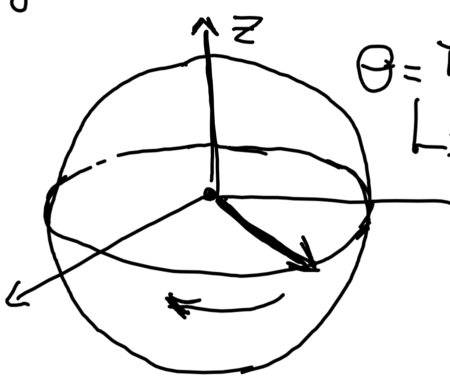
$$H = -\frac{\hbar}{2}\Omega_z \big(|0\rangle\langle 0| - |1\rangle\langle 1|\big)$$

if $|\psi(0)\rangle = |0\rangle \longrightarrow |\psi(t)\rangle = e^{+i\frac{\Omega_z t}{2}}|0\rangle$

if $|\psi(0)\rangle = |1\rangle \longrightarrow |\psi(t)\rangle = e^{-i\frac{\Omega_z t}{2}}|1\rangle$

if $|\psi(0)\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \longrightarrow |\psi(t)\rangle = \frac{1}{\sqrt{2}} e^{+i\frac{\Omega_z t}{2}}\big(|0\rangle + e^{-i\Omega_z t}|1\rangle\big)$

remember in general for a state on the Bloch sphere $|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$



$\theta = \pi/2$, $\varphi = -\Omega_z t$

$\hookrightarrow$ equatorial plane

This represents a rotation around the z-axis on the Bloch sphere with Larmor precession frequency Ω_z

Rotation of qubit state vectors and rotation operators

When exponentiated the Pauli matrices give rise to rotation matrices around the 3 orthogonal axis in 3-dimentional space

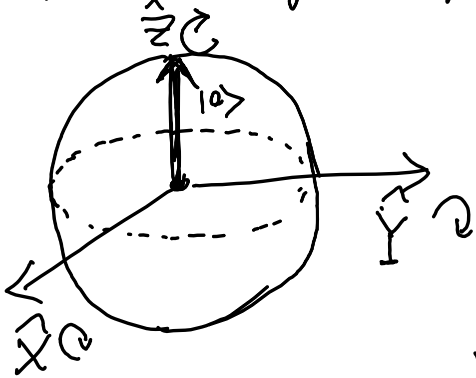
$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

N.B. If the Pauli matrices $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ are present in the Hamiltonian of a system they will give rise to rotations of the qubit state vector around the respective axis.

Preparation of specific qubit states:



- initial state $|0\rangle$
- prepare excited states by rotating around x or y axis:

X_π pulse: $\Omega_x t = \pi$; $|0\rangle - \boxed{X_\pi} - |1\rangle$

Y_π pulse: $\Omega_y t = \pi$; $|0\rangle - \boxed{Y_\pi} - i|1\rangle$

- prepare a superposition state:

$X_{\pi/2}$ pulse: $\Omega_x t = \pi/2$ $\quad |0\rangle - \boxed{X_{\pi/2}} - \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

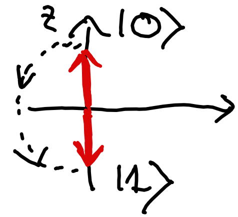
$Y_{\pi/2}$ pulse: $\Omega_y t = \pi/2$ $\quad |0\rangle - \boxed{Y_{\pi/2}} - \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$

- In fact, such a pulse of chosen length and phase can prepare any single qubit state; i.e. any point of the Bloch sphere can be reached.
- The dynamics of a two-level system can be always mapped onto the problem of a spin-½ particle in a time-dependent $\vec{B}$ field.

Single qubit gates | circuit representation

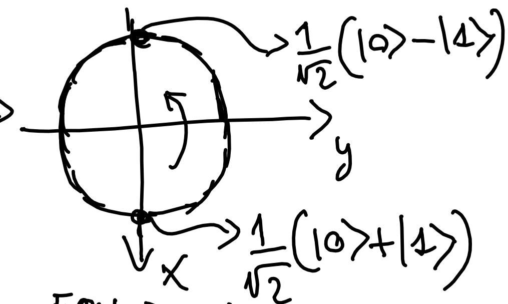
$$|\psi\rangle_{IN} \longrightarrow \boxed{\hat{O}} \longrightarrow |\psi\rangle_{OUT}$$

- $\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ identity
- $\hat{X} = \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ bit flip



- $\hat{Y} = \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ conjugate bit flip $\rightarrow$ $|0\rangle \longrightarrow -i|1\rangle$

  $|1\rangle \longrightarrow i|0\rangle$
- $\hat{Z} = \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ phase flip



EQUATORIAL PLANE OF THE BLOCH SPHERE

Pauli gates: these gates create only $|0\rangle$ and $|1\rangle$ states from the $|0\rangle$.

- In classical computing we have just 2 reversible single-bit gates.
- In quantum computing we have many more options.

A general qubit state can be written as

$$|\psi(\theta,\phi)\rangle = e^{-i\chi}\left(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle\right)$$

generic state on the surface of the Bloch sphere

$e^{-i\chi}$ → undetectable on a single qubit so it has not a physical meaning

The remaining angles can be visualized looking at the expectation values of $\hat{\sigma}_i$, that have the form of projection operators on the i-axis of the Bloch sphere:

$$\langle\psi(\theta,\phi)|\hat{\sigma}_x|\psi(\theta,\phi)\rangle = \frac{e^{i\phi}+e^{-i\phi}}{2}\, 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \cos\phi\sin\theta$$

$$\text{"} \quad \hat{\sigma}_y \quad \text{"} = -i\,\frac{e^{i\phi}-e^{-i\phi}}{2}\, 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \sin\phi\sin\theta$$

$$\text{"} \quad \hat{\sigma}_z \quad \text{"} = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta$$

Superposition gate: Hadamard ("quarter-turn")

- HADAMARD $-\boxed{H}-$

$$\hat{H} = \frac{1}{\sqrt{2}}\left(\hat{X} + \hat{Z}\right)$$

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

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

This gate is used in many quantum algorithms to prepare superpositions states from basis states.

- PHASE gate $-\boxed{S}-$ $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

These gates belong to the Clifford group (with CNOT)

They map the x, y, z axis into each other $\Rightarrow$ They do NOT cover the full Bloch sphere

$\Big\{$ Clifford gates are not universal: we cannot build arbitrary qubit rotation with just $\mathbb{I}, \vec{\sigma}$.

$\{H, S, CNOT\}$ can be simulated efficiently on a classical computer [GOTTESMAN-KILL THEOREM]

- We need also a "non-clifford" gate : T-gate —[T]—

$\{H, S, CNOT\} + T$ are universal $\begin{bmatrix} 1 & 0 \\ 0 & e^{+i\pi/4} \end{bmatrix}$

Note 1 : Z, S, T are part of "phase shift" gate

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \qquad |0\rangle \longrightarrow |0\rangle$$
$$|1\rangle \longrightarrow e^{i\varphi}|1\rangle$$

Note 2 : X is not a NOT gate for every qubit

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

$$X|\psi\rangle = |\tilde{\psi}\rangle = e^{i\phi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$$

$$|\langle\psi|\tilde{\psi}\rangle| = \left|2\cos\frac{\theta}{2}\sin\frac{\theta}{2}\right| = |\sin\theta| \begin{cases} = 0 \text{ only if} \\ \theta = 0, \pi \end{cases} \left(\begin{matrix}\text{so for} \\ |0\rangle \text{ and } |1\rangle\end{matrix}\right)$$

ROTATIONAL GATES:

exponential operator

$$\exp(i \underline{\underline{A}} x) = \cos x \, \mathbb{I} + i \sin x \, \underline{\underline{A}}$$

$$R_x(\theta) = e^{-i\theta\sigma_x/2} = \cos\frac{\theta}{2}\,\mathbb{I} - i\sin\frac{\theta}{2}\,\sigma_x$$

$$R_y(\theta) = e^{-i\theta\sigma_y/2} = \cos\frac{\theta}{2}\,\mathbb{I} - i\sin\frac{\theta}{2}\,\sigma_y$$

$$R_z(\theta) = e^{-i\theta\sigma_z/2} = \cos\frac{\theta}{2}\,\mathbb{I} - i\sin\frac{\theta}{2}\,\sigma_z$$

$$R_x(\theta) = \begin{bmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{bmatrix} ; \quad R_y(\theta) = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Z-Y decomposition: Any single qubit gate U can be written as

TWO AXIS ARE ENOUGH !

$$U = e^{i\alpha} R_z(\beta)\, R_y(\gamma)\, R_z(\delta)$$

For example: $R_x(\theta) = R_y\left(\frac{\pi}{2}\right) R_z(\theta)\, R_y\left(-\frac{\pi}{2}\right)$

$$\left\{ R_x(\theta),\ R_y(\theta),\ R_z(\theta),\ \text{CNOT} \right\}$$ are an universal set !

This discrete gate set can approximate any unitary operation to an arbitrary accuracy.

Any arbitrary single-qubit gate U can be decomposed into 3 consecutive qubit rotations around 2 ortogonal axes.

This implies that we need only 2 non-parallel switchable fields in the single qubit Hamiltonian.