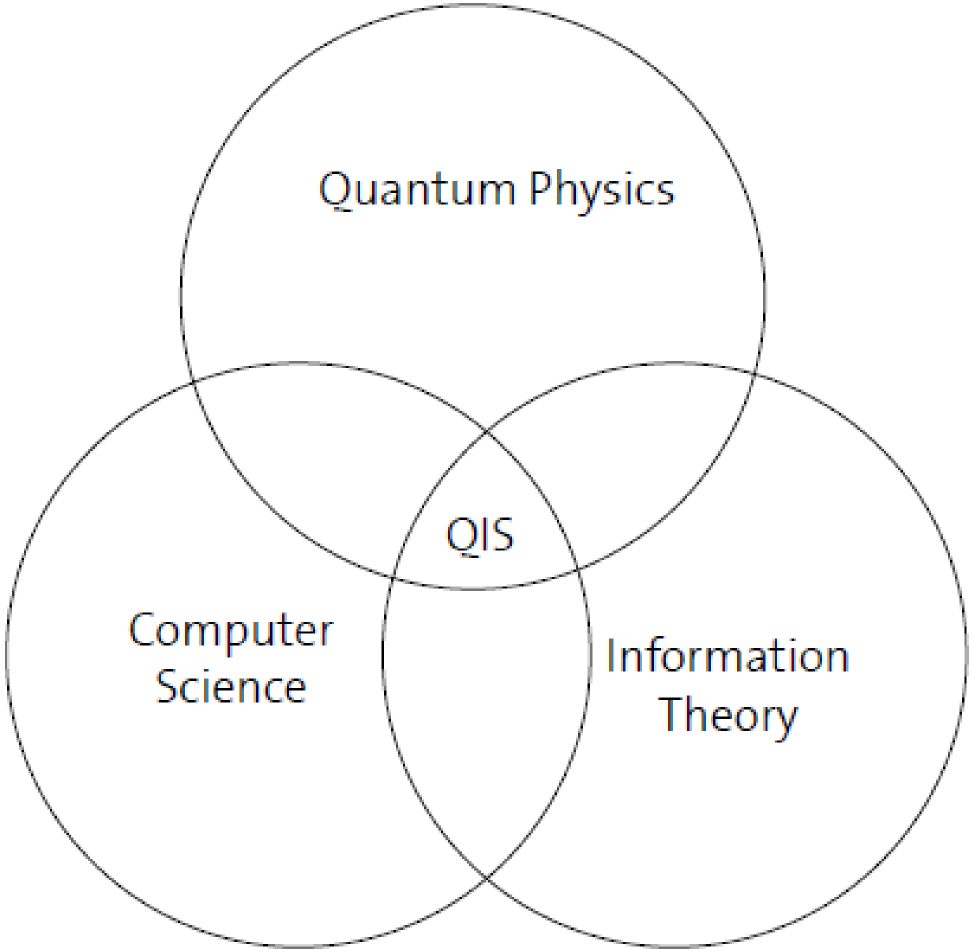
Summary of Quantum Information Science



Why is Quantum Computing Interesting?

A quantum computer is a device that leverages specific properties described and ruled out by Quantum Mechanics to perform computational tasks.

Quantum Computing:

- Represents a new paradigm of computing
- Uses theory of quantum mechanics for performing computational task
- Provides an efficiency (advantages) that cannot be overcome by any conceivable classical computing scheme
- Can be simulated, till a certain extent, on a classical computer BUT NOT EFFICIENTLY

<u>EFFICIENT</u>: computer running in time polynomial in the size of the problem

<u>INEFFICIENT</u>: computer running in time super-polynomial (typically exponential) in the size of the problem.

Challenges: *Building a gate based quantum computer requires control over individual quantum degrees of freedom!*

Classical Logic Gates: electronic circuits

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

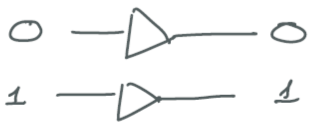
1 OR MORE BOOLEAN VALUES ('0'/'1') → SINGLE BOOLEN

↳ SINGLE-BIT GATE ↳ TWO-BIT GATE

NOT REVERSIBLE!

(1.) SET THE VALUE OF THE BIT: "SINGLE-BIT GATE"

IDENTITY GATE ("DO NOTHING") "BUFFER"



INPUT	OUTPUT
0	0
1	1

$$\begin{bmatrix}'0'\\'1'\end{bmatrix}$$

$$\underbrace{\begin{bmatrix}1&0\\0&1\end{bmatrix}}_{\sigma_0}\begin{bmatrix}'0'\\'1'\end{bmatrix}$$

$\sigma_0 \times [\text{bit}]$

QUANTUM - VERSION: FREE - EVOLUTION

ERASE GATE (IRREVERSIBLE)

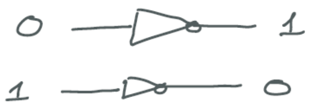
INPUT	OUTPUT
0	0
1	0

$$\begin{bmatrix}'0'\\'1'\end{bmatrix}$$

$$\begin{bmatrix}1&0\\1&0\end{bmatrix}\begin{bmatrix}'0'\\'0'\end{bmatrix}$$

QUANTUM VERSION: "RELAXATION"

NOT GATE (INVERTER)



INPUT	OUTPUT
0	1
1	0

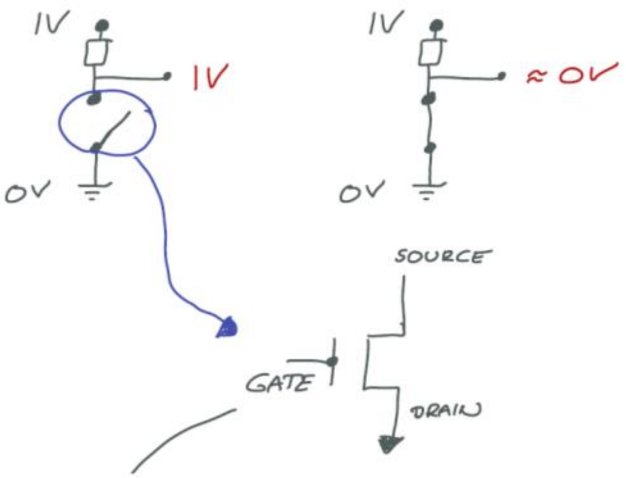
$$\begin{bmatrix}'0'\\'1'\end{bmatrix}$$

$$\underbrace{\begin{bmatrix}0&1\\1&0\end{bmatrix}}_{\sigma_x}\begin{bmatrix}'1'\\'0'\end{bmatrix}$$

$\boxed{\text{QUANTUM VERSION: X GATE}}$

THESE ARE THE MOST COMMON SINGLE-BIT GATES

Physical Realization:
“controllable switch”: TRANSISTOR



- *information is represented (and stored) in a physical system:*
  for example, as a voltage level at the input of a transistor in a digital circuit
- *in Transistor-Transistor-Logic (TTL)*
  "low" = logical 0 = 0 - 0.8 V
  "high" = logical 1 = 2.2 - 5 V

Classical Logic Gates

- IRREVERSIBLE TWO-BIT GATES : AND / OR

AND

a\b	0	1
0	0	0
1	0	1

OR

a\b	0	1
0	0	1
1	1	1

CAN NOT DETERMINE UNIQUE INPUTS FOR ALL OUTPUTS

XOR

a\b	0	1
0	0	1
1	1	0

"QUANTUM VERSION"
CX (CNOT) GATE

THERE ARE REVERSIBLE GATES AS WELL

UNIQUE INPUT ASSOCIATED WITH UNIQUE OUTPUT.

NOT

a	a'
0	1
1	0

SWAP

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

CNOT

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

UNIVERSAL GATE FOR CLASSICAL REVERSIBLE COMPUTING {TOFFOLI}

3 INPUT / 3 OUTPUT

NO TWO INPUTS ARE ALLOWED TO MAP TO THE SAME OUTPUT → PERMUTATION MATRIX

The quantum information paradigm

In **quantum information**, the element of information is the **quantum bit** or **qubit**

A qubit is a physical object governed by the laws of quantum physics: if 0 and 1 are possible "states" then, because of the linear superposition principle, possible states are also

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$a,\ b \in \mathbb{C} \qquad |a|^2 + |b|^2 = 1$$

A quantum register made of several qubits can be in the states $|0,\ 1,\ 1,\ 0, \ldots\rangle$. These states form a basis in the vector space of all possible states, called the "computational basis".

The most general state build for N qubits, according to the laws of quantum mechanics, is

$$|\psi\rangle = a_0|00\ldots0\rangle + a_1|00\ldots1\rangle + \ldots + a_N|11\ldots1\rangle \qquad \sum_j^N |a_j|^2 = 1$$

There are 2^N complex coefficients.

What are the main differences with respect to a classical bit?

1) **Phase** between the qubits **matter**! That is why the decoherence is an issue.
2) **Parallelism**: operations (gates) act on qubits in both $|0\rangle$ and $|1\rangle$ states.
3) In extended to N qubits register, **a gate operation acts in parallel** on 2^N states.

Circuit Model of Quantum Computation:

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

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

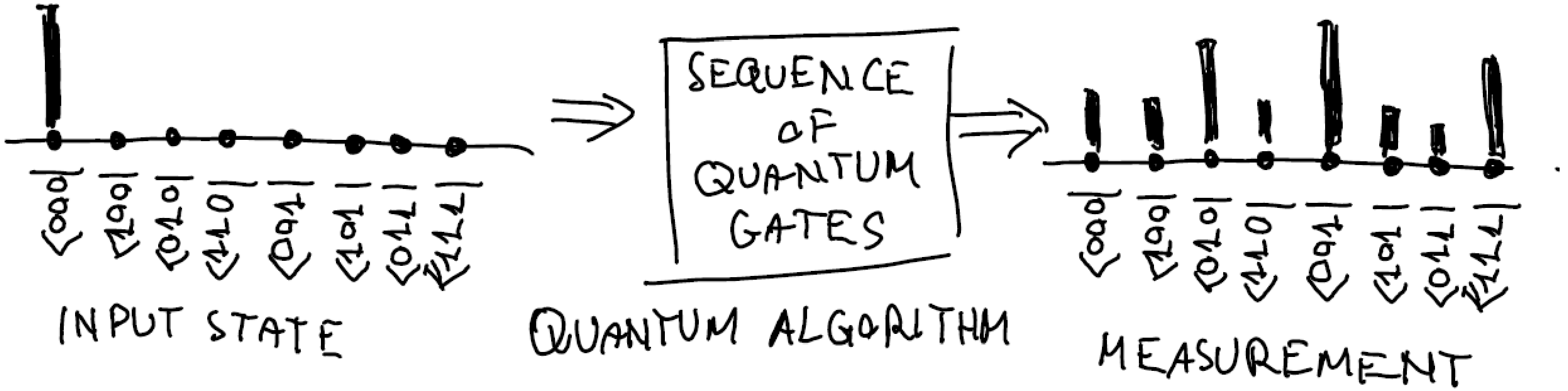
U → unitary operator

$|\psi_{IN}\rangle$ → register of qubits → n qubits

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

[2^n components to one state
quantum parallelisms]

Decomposition of any U gate the n-qubit register into single-qubit gates and controlled-NOT gates is possible.



Definition of a Quantum Bit

Quantum Mechanics Reminder:
QM postulate I:
The quantum state of an isolated physical system is completely described by its state vector in a complex vector space with a inner product (a **Hilbert Space**).The state vector is a unit vector in that space.

Note: This mathematical representation of a qubit allows us to consider its abstract properties independent of its actual physical realization.

Quantum **bits** (qubits) are quantum mechanical systems with **two distinct quantum mechanical states**.

- Qubits can be realized in a wide variety of physical systems displaying quantum mechanical properties:
  - atoms, ions, molecules
  - electronic and nuclear magnetic moments
  - charges in semiconductor quantum dots
  - charges and fluxes in superconducting circuits
  - and many more ...

A suitable realization of a qubit should fulfil the so called **DiVincenzo criteria**.

What requirements have to be fulfilled to build a Quantum Computer?

Di Vincenzo Criteria :

For implementing a quantum computer in the standard (circuit approach) to quantum information processing (QIP)

#1. A **scalable** physical system with well-characterized qubits.
#2. The ability to **initialize** the state of the qubits to a simple fiducial state.
#3. **Long** (relative) **decoherence times**, much longer than the gate-operation time.
#4. A **universal set** of quantum gates.
#5. A qubit-specific **measurement** capability.

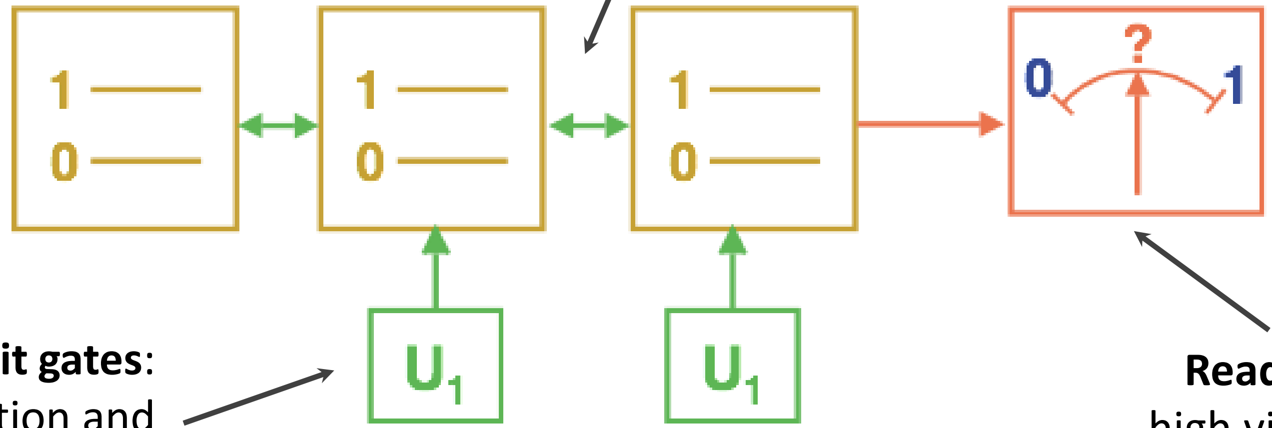
Plus two criteria requiring the possibility to transmit information:

#6. The ability to **interconvert** stationary and mobile (or flying) qubits.
#7. The ability to faithfully **transmit** flying qubits between specified locations.

Components of a Generic Quantum Information Processor

qubits: two-level systems with long coherence time

2-qubit gates: controlled interactions



Need to find a suitable physical systems

single-bit gates: Initialization and accurate control

Readout: high visibility single-shot joint read-out

The challenges:

- excellent qubits, excellent gates, excellent readout required
- perfect isolation from environment while maintaining perfect addressability
- lack of intrinsic protection from errors due to analog nature of information carriers
- requires error correction

M. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge, 2000)

Qubits and Superposition

Quantum Mechanical Description of a Qubit:

A **quantum bit** can take values (quantum mechanical states) $|\psi\rangle$

$$|0\rangle, \quad |1\rangle$$

or both of them at the same time in which case the qubit is in a **superposition of states**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \alpha, \beta \in \mathbb{C}$$

possible states are ***continuous***

- when the state of a qubit is measured one will find

$$\begin{array}{lll} |0\rangle & \text{with probability} & |\alpha|^2 = \alpha\alpha^* \\ |1\rangle & \quad " & |\beta|^2 = \beta\beta^* \end{array}$$

- where the normalization condition is

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

$$\text{with} \quad \langle\psi| = |\psi\rangle^\dagger = \alpha^*\langle 0| + \beta^*\langle 1| = (\alpha^*, \beta^*)$$

This just means that the sum over the probabilities of finding the qubit in any state must be unity.

Example: $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ equal superposition state

Bloch Sphere representation

alternative representation of qubit state vector useful for interpretation of qubit dynamics

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

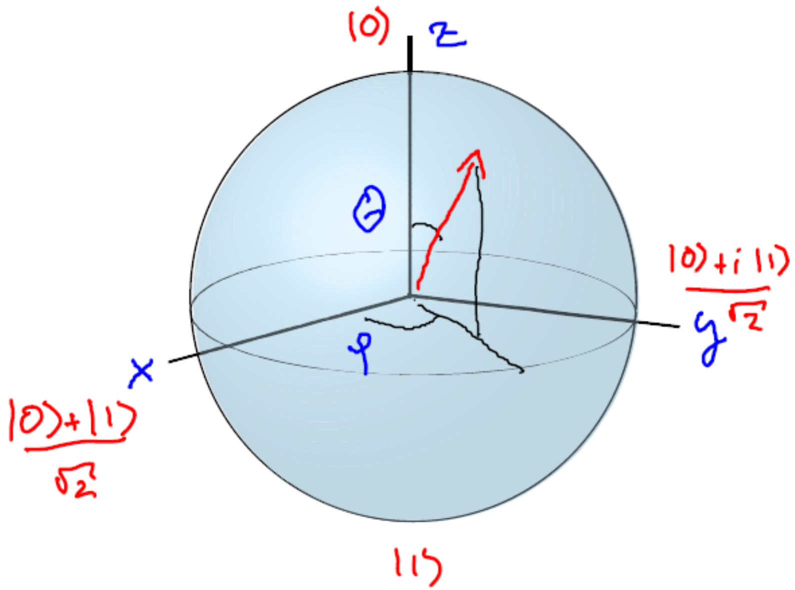
γ global phase factor

θ polar angle

φ azimuth angle

unit vector pointing at the surface of a sphere:

$$\vec{v} = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$$



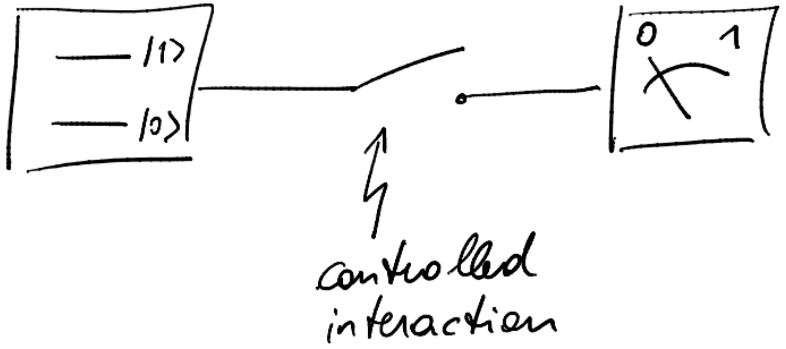
- ground state **|0>** corresponds to a vector pointing to the north pole
- excited state **|1>** corresponds to a vector pointing to the south pole
- equal superposition state **$(|0\rangle + e^{i\phi}|1\rangle)/2^{1/2}$** is a vector pointing to the equator

Quantum Measurement- Read Out

generic measurement setup

closed Quantum System (QS)

Measurement Apparatus (MA)



Goal: ***faithful reconstruction of qubit state***

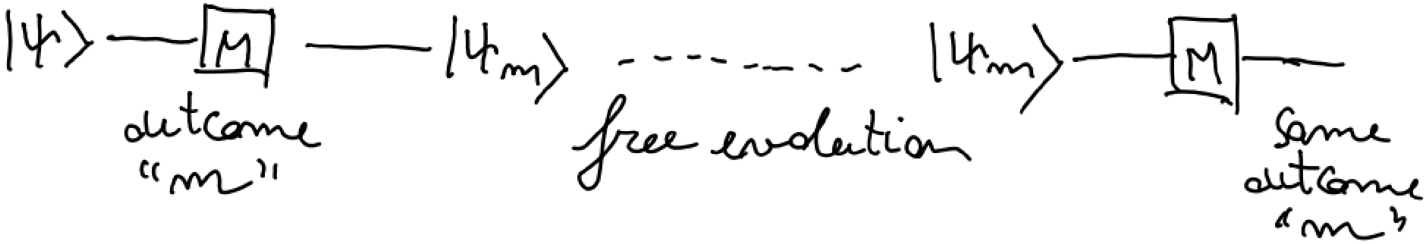
What properties should an ideal measurement apparatus have ?

- **High ON/OFF ratio**: no interaction between MA and QS when OFF, strong interaction when ON

- **High fidelity** of mapping of QS to MA state (no misidentification)

- **Fast MA** in comparison to decoherence/relaxation of the QS

- Quantum Non-Demolition (**QND**): repeatability of measurement with the same outcome.



Information readout

The readout process is a measurement process $|\psi\rangle = a|0\rangle + b|1\rangle$

Suppose to measure whether the qubit is in state 0 or 1, by measuring an observable diagonal on the basis $\{|0\rangle, |1\rangle\}$

The measurement returns 0 or 1 randomly, with probabilities

$$P(0) = |a|^2 \qquad P(1) = |b|^2$$

After the measurement, the state "collapses". It becomes $|0\rangle$ or $|1\rangle$ according to the outcome

For several qubits: $|\psi\rangle = \sum_j a_j |j\rangle$

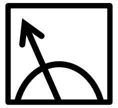
The value *j* is measured with probability $|a_j|^2$ and the register collapses on state $|j\rangle$

Read out a qubit: measure an observable which is diagonal in the computational basis $|0\rangle$,$|1\rangle$

$$M = \begin{pmatrix} m_0 & 0 \\ 0 & m_1 \end{pmatrix}$$

Measuring on a different basis can be done by first applying a rotation

Circuit notation



Information readout

What does “random” actually mean?

After the measurement, **the collapse ensures that a second measurement of the same kind will return the same result**.

“Random” means that, if one prepares many qubits in the same state, then the same measurement will give in general different values

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{measure} \longrightarrow |0\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{measure} \longrightarrow |1\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{measure} \longrightarrow |1\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{measure} \longrightarrow |0\rangle$$
$$\vdots$$

In general, **the output of a quantum computation has a probabilistic (i.e. random) nature**.

$$P(0) = |a|^2 \qquad P(1) = |b|^2$$

Dynamics of a Quantum System

QM postulate: The time evolution of a state $|\psi>$ of a closed quantum system is described by the **Schrödinger equation**

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

where H is the hermitian operator known as the **Hamiltonian** describing the closed system.

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

General solution for a time independent Hamiltonian H:

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

The **Hamiltonian**:

- **H** is hermitian and has a spectral decomposition
- with eigenvalues **E**
- and eigenvector **|E>**
- the smallest value of E_0 is the ground state energy with the eigenstate $|E_0>$

$$H = \sum_E E |E\rangle\langle E|$$

Quantum operations

A **quantum operation (gate)** is the change that the state of the system undergoes over time

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle \qquad (\hbar = 1)$$

It corresponds to an operator $U = e^{-iHt}$ (**time evolution operator**) which is unitary, i.e.

Unitary operators are linear and reversible. $U^\dagger = U^{-1}$

They preserve the norms of the vectors in the Hilbert space.

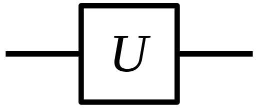
H is the Hamiltonian of the system and represents the total energy of the system.

Performing **quantum gates** on the qubits is translated in **engineering controllable** (in magnitude and time) **energy terms in the Hamiltonian**.
Those terms will represent the interaction between single qubits and the control environment and between some couples of qubits, which will be turned-ON for a certain time and then switched-OFF.

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

Quantum circuit notation

one qubit



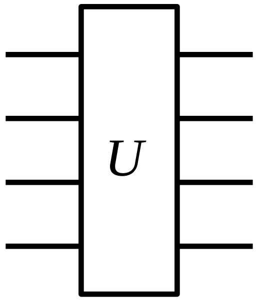
a quantum gate

A quantum gate is defined by its action on the computational basis

in	out
$\|0\rangle$	$\|\psi_0\rangle$
$\|1\rangle$	$\|\psi_1\rangle$

input $\quad |\psi\rangle = a|0\rangle + b|1\rangle$

output $\quad |\psi'\rangle = a|\psi_0\rangle + b|\psi_1\rangle$



Many-qubit gate

Defined by its action on the computational basis

$$|00\ldots0\rangle,\ |00\ldots1\rangle,\ \ldots,\ |11\ldots1\rangle$$

Some elementary one-qubit gates

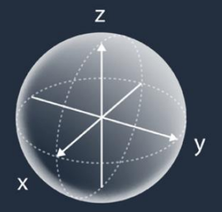
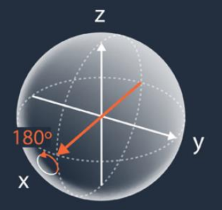
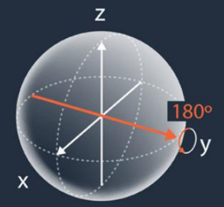
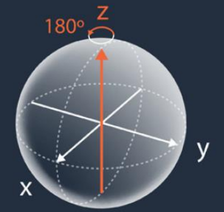
X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	NOT, bit flip
Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Conjugate bit flip
Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Phase-flip
H	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	Hadamard gate (superposition gate)
S	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	Phase gate
T	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$	π/8 gate

Pauli gates: these gates creates only 0 and 1 states from the 0

$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$
$$H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$

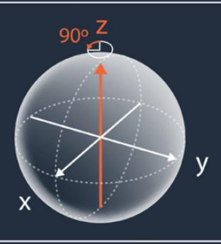
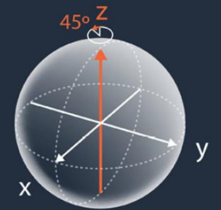
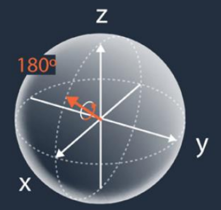
In classical computing we have just 2 reversible single-qubit gates. In Quantum Mechanics we have many more options. Hadamard gate is used in many quantum algorithms to prepare a superposition state from the basis states.

Single Qubit Gate

GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE	BLOCH SPHERE
I Identity-gate: no rotation is performed.	$-\boxed{I}-$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Input / Output $\|0\rangle$ → $\|0\rangle$ $\|1\rangle$ → $\|1\rangle$	
X gate: rotates the qubit state by π radians (180°) about the x-axis.	$-\boxed{X}-$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Input / Output $\|0\rangle$ → $\|1\rangle$ $\|1\rangle$ → $\|0\rangle$	
Y gate: rotates the qubit state by π radians (180°) about the y-axis.	$-\boxed{Y}-$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Input / Output $\|0\rangle$ → $i\|1\rangle$ $\|1\rangle$ → $-i\|0\rangle$	
Z gate: rotates the qubit state by π radians (180°) about the z-axis.	$-\boxed{Z}-$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Input / Output $\|0\rangle$ → $\|0\rangle$ $\|1\rangle$ → $-\|1\rangle$	

$|\psi\rangle_{IN}$ —$\boxed{}$— $|\psi\rangle_{OUT}$

$\longrightarrow$ time

GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE	BLOCH SPHERE
S gate: rotates the qubit state by $\frac{\pi}{2}$ radians (90°) about the z-axis.	$-\boxed{S}-$	$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$	Input / Output $\|0\rangle$ → $\|0\rangle$ $\|1\rangle$ → $e^{i\frac{\pi}{2}}\|1\rangle$	
T gate: rotates the qubit state by $\frac{\pi}{4}$ radians (45°) about the z-axis.	$-\boxed{T}-$	$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$	Input / Output $\|0\rangle$ → $\|0\rangle$ $\|1\rangle$ → $e^{i\frac{\pi}{4}}\|1\rangle$	
H gate: rotates the qubit state by π radians (180°) about an axis diagonal in the x-z plane. This is equivalent to an X-gate followed by a $\frac{\pi}{2}$ rotation about the y-axis.	$-\boxed{H}-$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	Input / Output $\|0\rangle$ → $\frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$ $\|1\rangle$ → $\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	

Philip Krantz et al., A Quantum Engineer's Guide to Superconducting Qubits, *Applied Physics Reviews* **6**, 021318 (2019).

Example: single electron spin in a magnetic Bz field

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

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

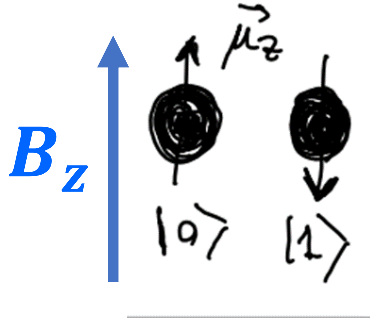
$$H = -\frac{\hbar}{2}\Omega_z \left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)$$

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

$$+\frac{\hbar}{2}\Omega_z = \frac{g\mu_B B_z}{2} = E_1 \qquad |1\rangle$$

$$0$$

$$-\frac{\hbar}{2}\Omega_z = -\frac{g\mu_B B_z}{2} = E_0 \qquad |0\rangle$$

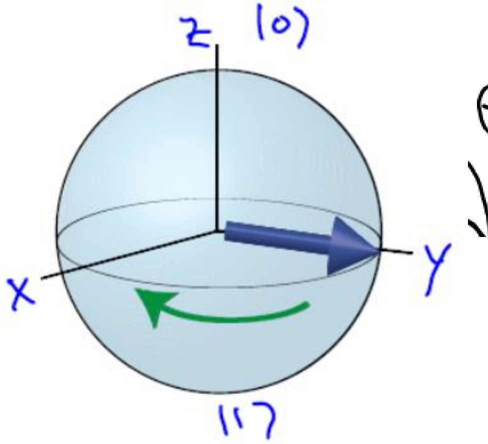


if $|\psi(0)\rangle = |0\rangle \longrightarrow |\psi(t)\rangle = e^{+i\frac{\Omega_z t}{2}}|0\rangle$

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

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

On the Bloch sphere:



$\theta = \pi/2, \quad \varphi = -\Omega_z t$
↳ equatorial plane

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

This is a rotation around the equator with **Larmor precession frequency** $\Omega_z = g\mu_B B_z$

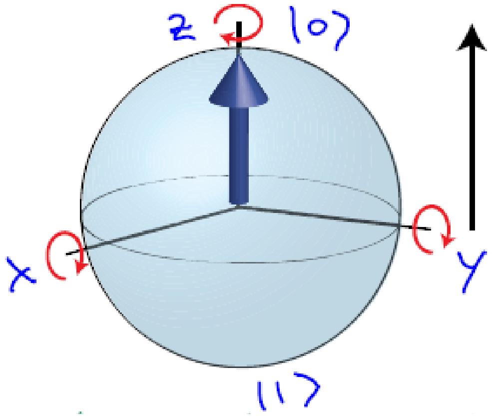
Rotation Operators

When exponentiated, the Pauli matrices give rise to rotation matrices around the three orthogonal axis in 3-dimensional space.

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

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

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

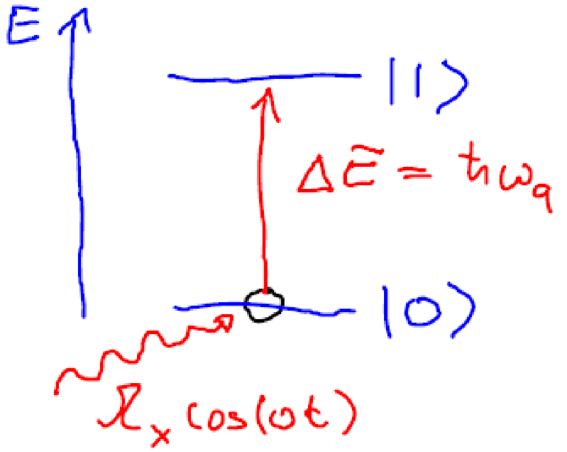


If the Pauli matrices **X**, **Y,** or **Z** are present in the Hamiltonian of a system, they will give rise to rotations of the qubit state vector around the respective axis.

exercise: convince yourself that the operators Rx,y,z do perform rotations on the qubit state written in the Bloch sphere representation.

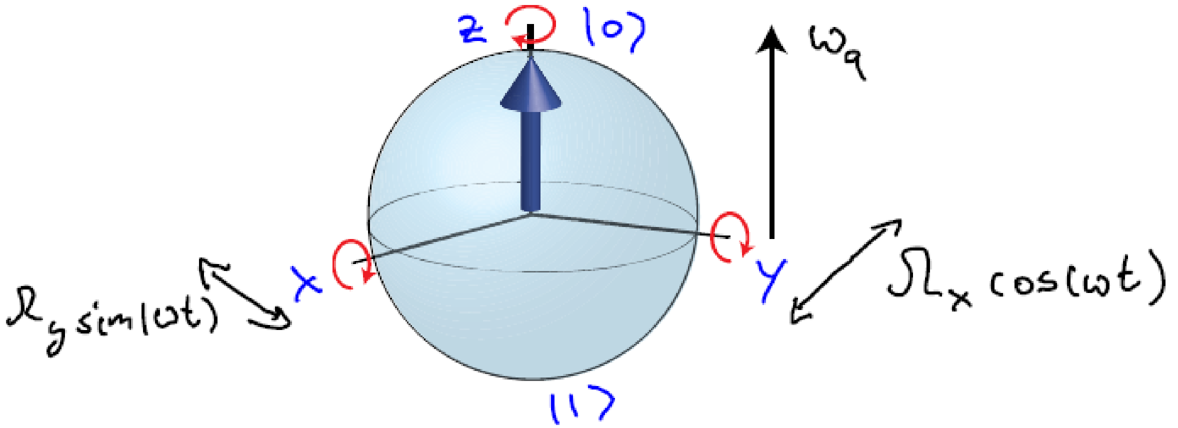
Control of Single Qubit States

By resonant irradiation:



Qubit Hamiltonian with ac-drive:

$$H = \hbar\left[\frac{\omega_q}{2}\hat{Z} + \overbrace{\Omega_x\cos(\omega t)\,\hat{X} + \Omega_y\sin(\omega t)\,\hat{Y}}^{\text{light-spin interaction}}\right]$$



ac-fields applied along the x and y components of the qubit state

Rotating Wave Approximation (RWA)

Unitary transformation:

Frame that rotates around z-axis with the free precession frequency ω

$$H' = U H U^{+} - i U \dot{U}^{-1}$$

with $U = e^{-i\frac{\omega}{2}t\hat{z}}$

What does light-spin interaction do to the qubit state on the Bloch sphere? Move to **rotating frame** to visualize it better!

Results:

$$H' = \hbar\left[\frac{\omega_a-\omega}{2}\hat{z} + \frac{\Omega_x}{2}\hat{x}\left(1+e^{2i\omega t}\right) + \frac{\Omega_y}{2}\hat{y}\left(1-e^{-2i\omega t}\right)\right]$$

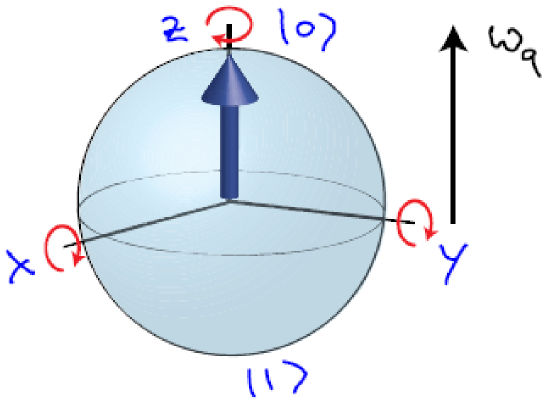
Drop fast-rotating terms (RWA):
Rotating Wave Approximation

$$H' \approx \frac{\hbar}{2}\left[\Delta\hat{z} + \Omega_x\hat{x} + \Omega_y\hat{y}\right]$$

with detuning: $\Delta = \omega_a - \omega$

i.e. irradiating the qubit with an ac-field with controlled amplitude and phase allows to realize arbitrary single qubit rotations.

Preparation of qubit states:



initial state **|0>**:

prepare excited state by rotating around x or y axis:

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

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

Preparation of a superposition state:

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

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

In fact, such a pulse of chosen length and phase can prepare **any single qubit state**, i.e. any point on the Bloch sphere can be reached.

Z-Y Decomposition

Any single qubit gate **U** can be written as:

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

TWO AXES are ENOUGH!

For example:

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

$$\left\{R_x(\theta),\, R_y(\theta),\, R_z(\theta),\, \text{CNOT}\right\}$$ is an **UNIVERSAL SET**!

- This discrete gate set can approximate any unitary operation to an arbitrary accuracy.
- Any arbitrary gate U can be decomposed into 3 consecutive qubit rotations around 2 orthogonal axes.
- This implies that we need only 2 non-parallel switchable fields in the single qubit Hamiltonian.

TWO QUBITS

2 **classical bits** with states:

bit 1	bit 2
0	0
0	1
1	0
1	1

- 2^n different states (here n=2)
- but **only one** is realized **at any** given **time**

2 **qubits** with quantum states:

qubit 1 qubit 2

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

- 2^n basis states (n=2)
- can be realized **simultaneously**
- **quantum parallelism**

2^n complex coefficients describe quantum state

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

normalization condition

$$\sum_{ij} |\alpha_{ij}|^2 = 1$$

Composite Quantum Systems

QM postulate: The state space of a composite systems is the **tensor product** of the state spaces of the component physical systems. If the component systems have states **|ψi >** the composite system state is

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_m\rangle$$

This is a tensor product state of states of the individual systems.

example:

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$$
$$|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

$$\longrightarrow \quad |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$$
$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

exercise: Write down the state vector (matrix representation) of two qubits, i.e. the tensor product, in the computational basis. Write down the basis vectors of the composite system.

There is no generalization of the Bloch Sphere to many qubits.

Quantum entanglement

A **"separable"** state of two qubits is one that is expressed as a **single product of one-qubit states**

$$\begin{aligned}|\psi_s\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + bc|10\rangle + ad|01\rangle + bd|11\rangle \\ &= |\psi_1\rangle \otimes |\psi_2\rangle\end{aligned}$$

Its property is that each qubit is in a well-defined state

In general, states of several qubits are not separable: they are **entangled**

$$|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

Entangled states are the large majority of all possible states of several qubits

Entanglement is a resource for the quantum computation paradigm. However, its role in advantageous quantum computations is subtle.

Quantum entanglement

Definition: An **entangled state** of a composite system is a state that cannot be written as a product state of the component systems.

example: an entangled 2-qubit state (one of the Bell states)

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

What is special about this state? Try to write it as a product state!

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \;;\; |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

$$|\psi_1\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$$|\psi\rangle = |\psi_1\psi_2\rangle \text{ for } \alpha_1\alpha_2 = 1/\sqrt{2} \wedge \beta_1\beta_2 = 1/\sqrt{2}$$

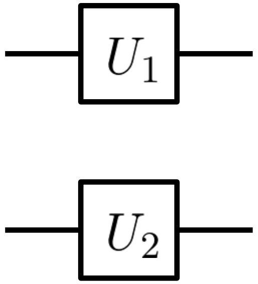
but this implies $\alpha_1\beta_2 \neq 0 \wedge \alpha_2\beta_1 \neq 0$

It is not possible! This state is special, it is entangled!

*Use this property as a **resource** in quantum information processing.*

Separable gates

$|\psi\rangle$

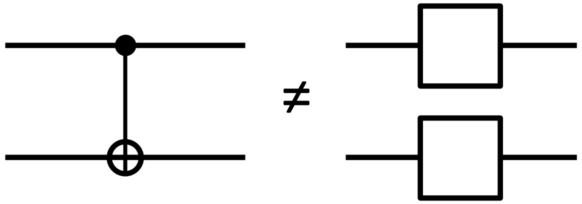


$|\psi'\rangle$

If $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ then $|\psi'\rangle = |\psi'_1\rangle \otimes |\psi'_2\rangle$

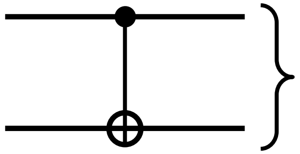
A separable two-qubit operation $U = U_1 \otimes U_2$ **can't generate entanglement**

CNOT and C-Z gates are not separable



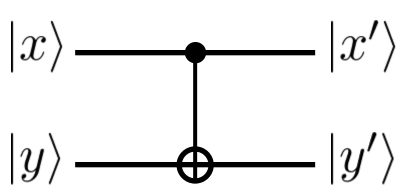
$|\psi_1\rangle = a|0\rangle + b|1\rangle$

$|\psi_2\rangle = |0\rangle$



$$|\psi'\rangle = a|00\rangle + b|11\rangle$$
$$\neq |\psi'_1\rangle \otimes |\psi'_2\rangle$$

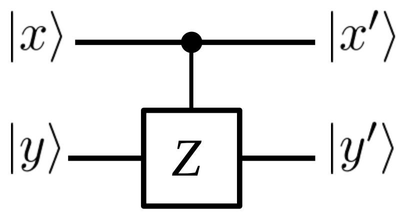
Some elementary two-qubit gates



$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

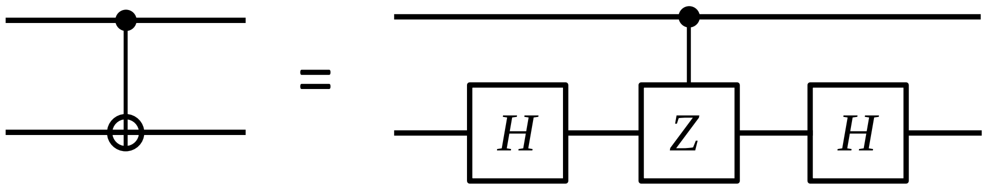
x	*y*	*x'*	*y'*
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

The CNOT gate acts on the computational basis by **flipping qubit 2 if qubit 1 is in state 1**



$$\text{C-Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

The C-Z gate acts on the computational basis by **applying Z to qubit 2 if qubit 1 is in state 1**



Two qubits gates: the Controlled NOT gate (CNOT)

- controlled-gate: "if-then-else" type
  - CNOT GATE [CX] (addition MOD 2)

if qubit A (control) is in $|0\rangle \longrightarrow$ DO NOTHING I on the TARGET

if qubit A (control) is in $|1\rangle \longrightarrow$ DO $\hat{X}$ GATE on the TARGET

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

C T

$|00\rangle \longrightarrow |00\rangle$

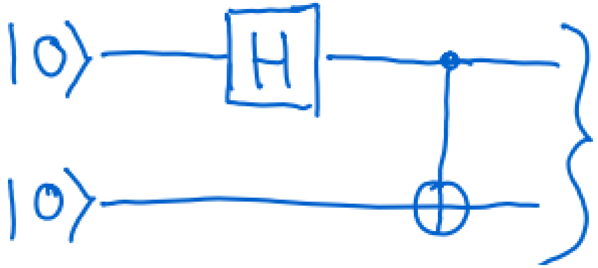
$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \longrightarrow |11\rangle$

$|11\rangle \longrightarrow |10\rangle$

N.B. CNOT is a powerful entangling gate

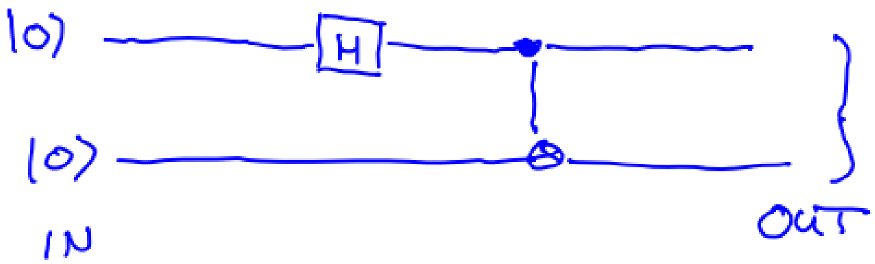
1 single qubit gate + CNOT create a fully entangled 2 qubit state



BELL STATE $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

- CNOT is reversible (unitary).
- " " universal.
- " can be realized using any 2-qubit interaction combined with single qubit manipulation.

Application of CNOT: generation of entangled states (Bell states)



$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|00\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|01\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|10\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|00\rangle - |10\rangle\right) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|11\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|01\rangle - |11\rangle\right) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

exercise: Write down the unitary matrix representations of the CNOT in the computational basis with qubit 1 being the control qubit. Write down the matrix in the same basis with qubit 2 being the control bit.

Implementation of CNOT

Ising interaction: $H = -\sum_{ij} J_{ij} \hat{Z}_i \hat{Z}_j$ pair wise spin interaction

generic two-qubit interaction: $= -J \hat{Z}_1 \hat{Z}_2$

J > 0: ferromagnetic coupling

E

$+J$ —— $|\uparrow\downarrow\rangle$ or $|\downarrow\uparrow\rangle$

$-J$ —— $|\downarrow\downarrow\rangle$ or $|\uparrow\uparrow\rangle$

J < 0: anti-ferrom. coupling

E

$+J$ —— $|\uparrow\uparrow\rangle$ or $|\downarrow\downarrow\rangle$

$-J$ —— $|\uparrow\downarrow\rangle$ or $|\downarrow\uparrow\rangle$

2-qubit unitary evolution: $C(\gamma) = e^{-i \frac{\gamma}{2} \hat{Z}_1 \hat{Z}_2}$

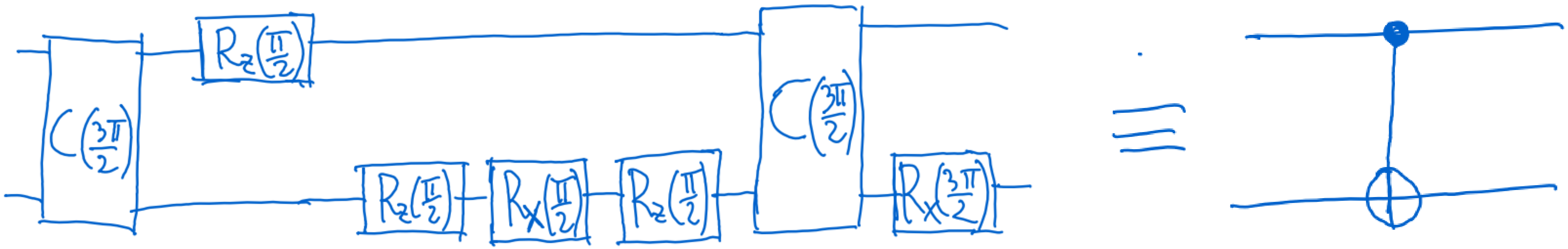
BUT this does not realize a CNOT gate yet.
Additional single qubit operations on each of the qubits are required to realize a CNOT gate.

CNOT realization with the Ising-type interaction

CNOT - unitary

$$C_{NOT} = e^{-i\frac{3\pi}{4}} R_{x_2}\left(\frac{3\pi}{2}\right) C\left(\frac{3\pi}{2}\right) R_{z_2}\left(\frac{\pi}{2}\right) R_{x_2}\left(\frac{\pi}{2}\right) R_{z_2}\left(\frac{\pi}{2}\right) R_{z_1}\left(\frac{\pi}{2}\right) C\left(\frac{3\pi}{2}\right)$$

circuit representation



Any physical two-qubit interaction that can produce entanglement can be turned into a universal two-qubit gate (such as the CNOT gate) when it is augmented by arbitrary single qubit operations.

Bremner et al., *Phys. Rev. Lett.* **89**, 247902 (2002)

Two-qubit gates

- C PHASE GATE [CZ]

if qubit A (control) is in $|0\rangle \longrightarrow$ DO NOTHING $\mathbb{I}$ on the TARGET

if qubit A (control) is in $|1\rangle \longrightarrow$ DO $\hat{Z}$ GATE on the TARGET

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

C T

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \longrightarrow |10\rangle$

$|11\rangle \longrightarrow -|11\rangle$

- SWAP GATE

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

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |10\rangle$

$|10\rangle \longrightarrow |01\rangle$

$|11\rangle \longrightarrow |11\rangle$

EXCHANGE excitations

It does not create entanglement

They create entanglement!

- $iSWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ $\quad i\sqrt{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & \frac{1+i}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Universal set of quantum gates

The set of gates **$\{H, T, S, CNOT\}$ is universal. Any unitary operation U on n qubits can be approximated to accuracy ε by finite sequence of universal gates.**

Alas, the approximation is not efficient. For an arbitrary U, it takes $O(2^n \log(1/\varepsilon)/\log(n))$ elementary gates

The goal of quantum computing is to devise efficient quantum algorithms, i.e. circuits with O(poly(n)) elementary gates to carry out useful computational tasks.

Notice that $T^2 = S$. The gate S is included in the universal set for reasons related to quantum error correction

The gates **$\{H, S, CNOT\}$** are the generators of the **Clifford group**. They are **not universal**.

Theorem (Gottesman-Knill): Any quantum circuit made only of Clifford gates can be simulated efficiently on a classical computer.
The Gottesman–Knill theorem shows that even some highly entangled states (generated by gates in te Clifford group) can be simulated efficiently.