Quantum refresh & intro

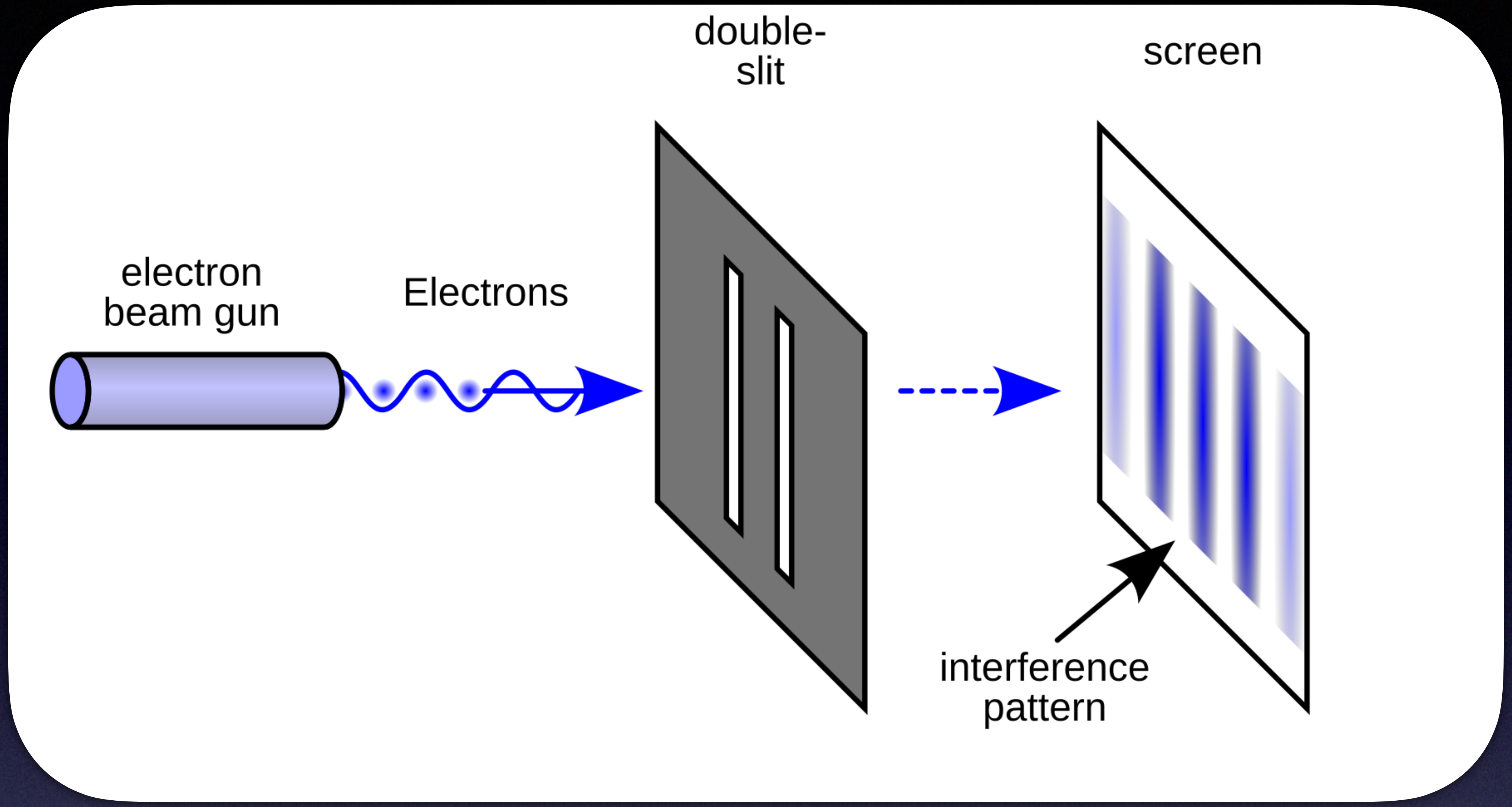
a short intro/reminder of properties and peculiarities
(hopefully) useful to understand the Quantum Computing

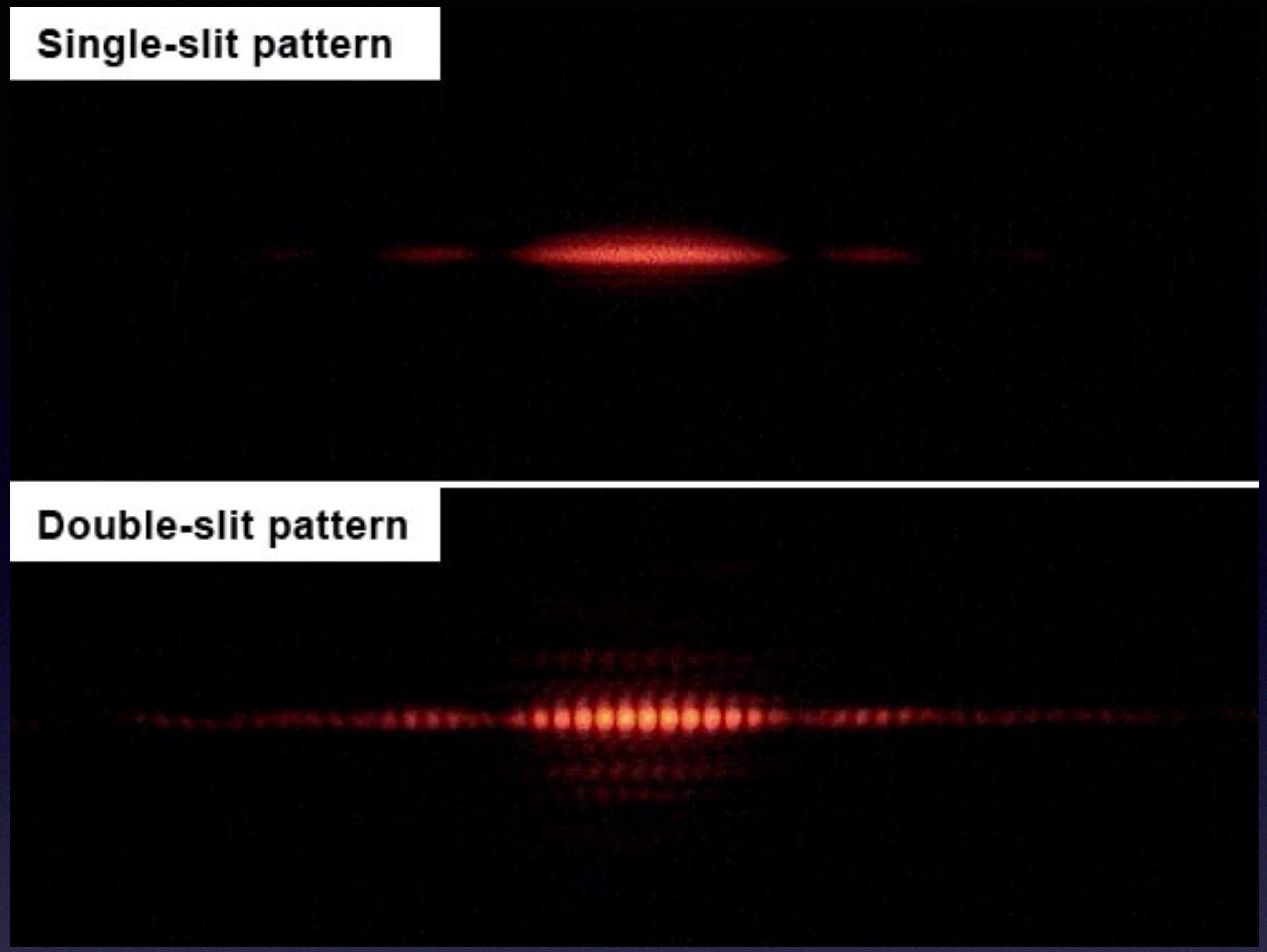
R. Scaramella - Trieste March 2026 - INAF USC-C

Overview

- Quantum: why and how
- wave/particle behaviour
- interference
- wave function, probabilistic interpretation
- superposition, Qbit, entanglement, EPR & Bell inequalities
- quantum computing: notation and circuits vs hardware
- list of some applications in astronomy/cosmology

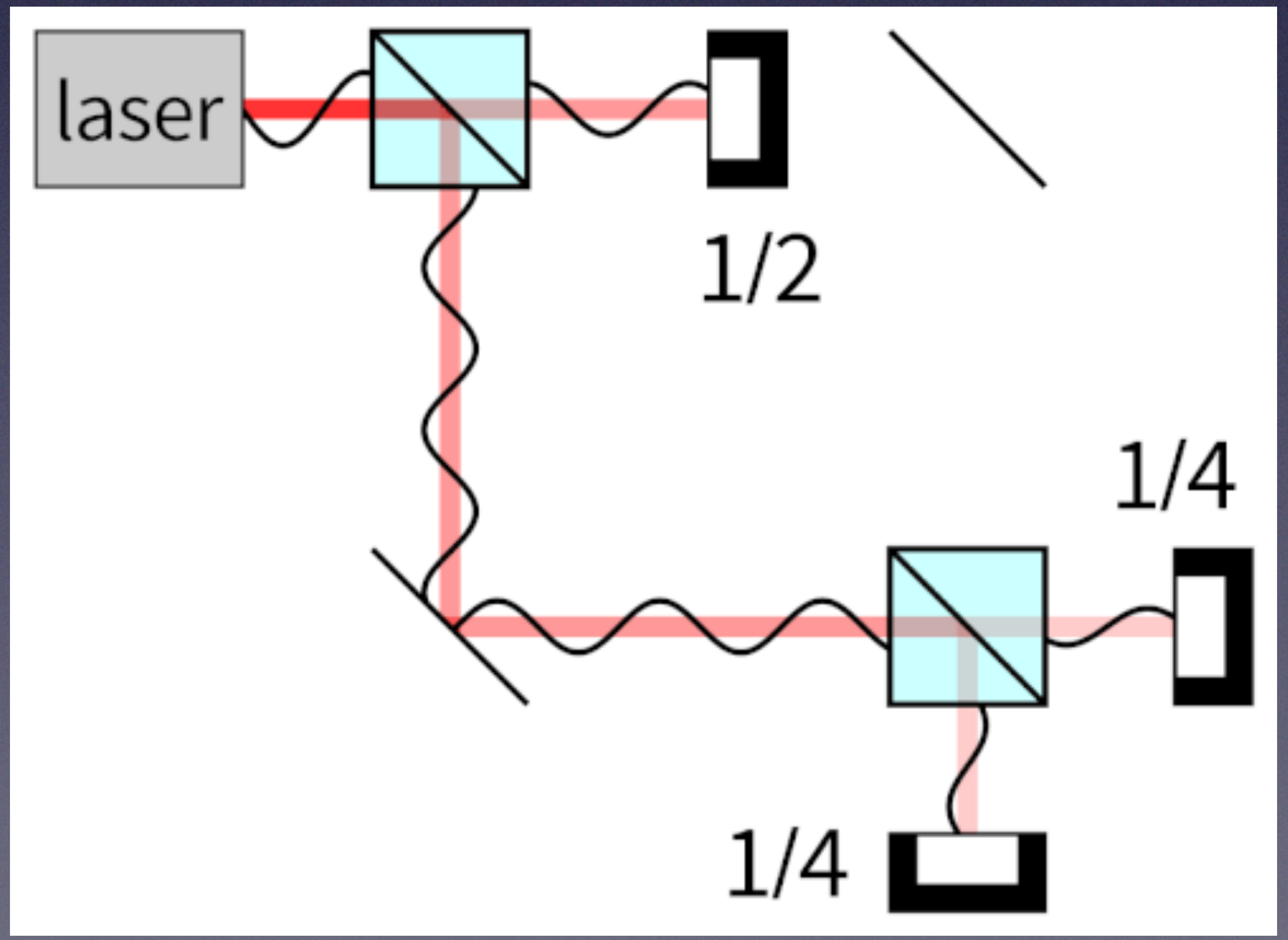
Famous double slit experiment





This happens also for single particles! (one at a time)

Light in Mach–Zehnder interferometer produces interference (wave-like behavior) even when being detected one photon at a time (particle-like behavior).



Copenhagen probabilistic interpretation

[relational interpretation, many worlds, De Broglie--Bohm]

Quantum states, represented by Dirac's ket, $|\psi\rangle$, evolve in time according to the Schrödinger equation:

$$\frac{d|\psi\rangle}{dt} = -\left(\frac{i}{\hbar}\right) \hat{H}(|\psi\rangle)$$

This implies that time evolution is described by unitary transformations: $|\psi\rangle \to \hat{U}|\psi\rangle$, with $\hat{U} = \hat{U}^{\dagger}$ is an unitary operator (matrix), $\hat{U}^{\dagger} = \left(\hat{U}\right)^{-1}$ where $|\psi\rangle$ is the quantum state (wavefunction) and H is Hamiltonian. $\hat{U}^{\dagger}$ is the hermitian conjugate (array is transposed and complex conjugated), $\hat{U}^{\dagger} = \left(\hat{U}^{T}\right)^{*} = \left(\hat{U}^{*}\right)^{T}$

$$\frac{d\hat{U}(t)}{dt} = -\frac{i}{\hbar}\hat{H}(t)\,\hat{U}(t)$$

This theory, which has been extensively tested by experiments, **is probabilistic in nature.**
The outcomes of measurements on quantum systems are not deterministic.
Between measurements, quantum systems evolve according to linear equations (the Schrödinger equation).
This means that solutions to the equations obey a superposition principle: **linear combinations of solutions are still solutions**.

Quantum Bit → Qubit

- **Since quantum systems evolve according to linear equations (the Schrödinger equation), linear combinations of solutions are also solutions.**
- **So, for the state of a qubit $|0\rangle$ and $|1\rangle$, its superposition also describes a state**
- **The general form of a qubit state can be represented by:** $\alpha_0|0\rangle + \alpha_1|1\rangle$

where α_0 and α_1 are complex numbers that specify the probability amplitudes of the corresponding states.

- $|\alpha_0|^2$ **gives the probability that you will find the qubit in the "off" $|0\rangle$ state;** $|\alpha_1|^2$ **gives the probability that you will find the qubit in the "on" $|1\rangle$ state.**
- **Normalization condition:** $|\alpha_0|^2 + |\alpha_1|^2 = 1$

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

So electrons with spin 1/2 have two states. However, recall that the photon has 1 spin but only two states of polarisation (helicity) because it moves at c.

Typical notation

Two level system eigenstates: $|\psi\rangle = |0\rangle$ **or** $|\psi\rangle = |1\rangle$ **(spin down or up)**

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

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

$$\langle\psi|\psi\rangle = |\psi|^2 = 1$$

density operator $\rho = \dfrac{1}{2}\left(I + \vec{a}\cdot\vec{\sigma}\right)$ Pauli matrices $\vec{\sigma}$

$$\rho = \frac{1}{2}\left(I + \vec{a}\cdot\vec{\sigma}\right)$$

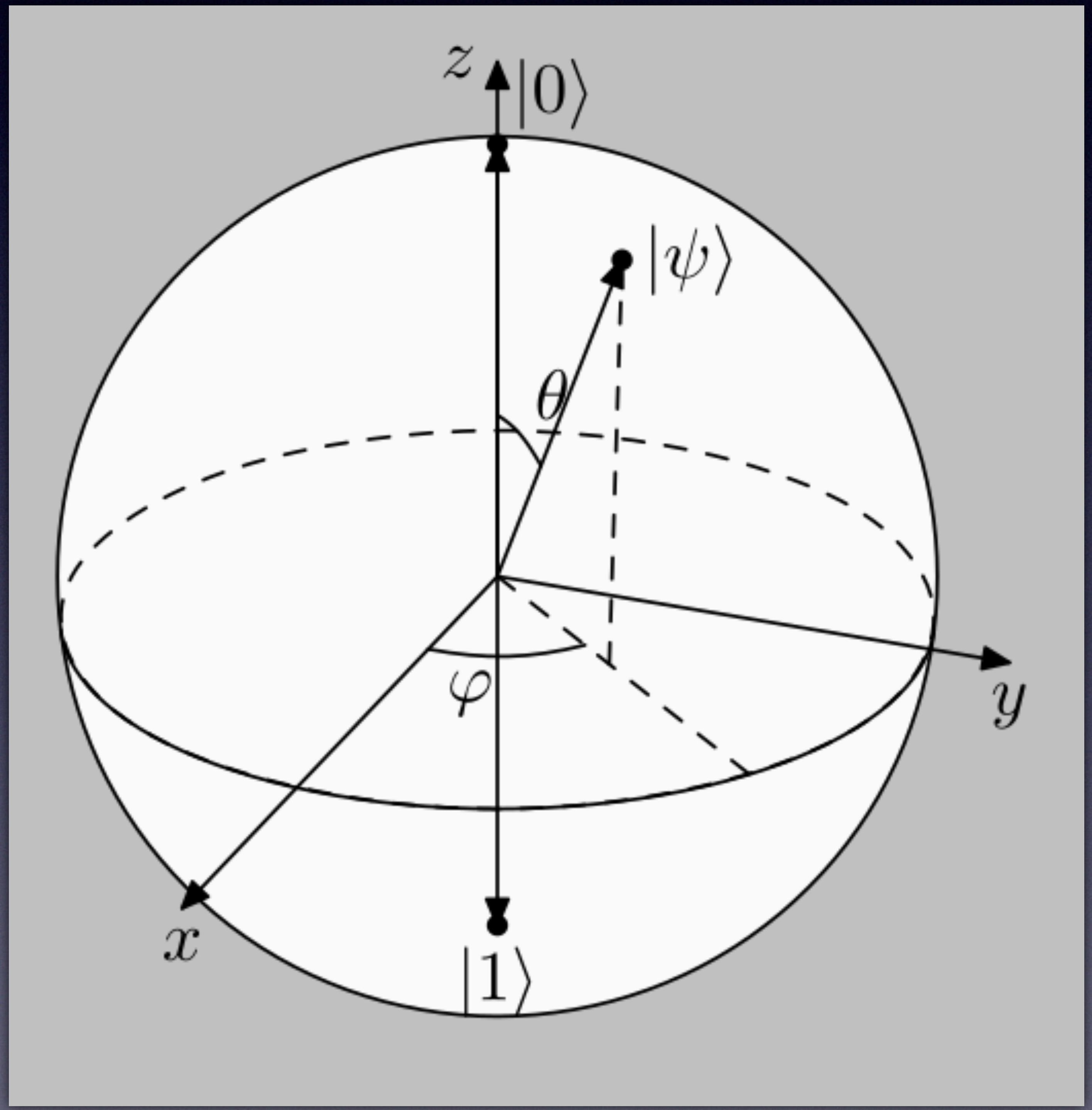
$$\rho = \frac{1}{2}\begin{pmatrix} 1 + a_z & a_x - ia_y \\ a_x + ia_y & 1 - a_z \end{pmatrix}$$

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + w & u - iv \\ u + iv & 1 - w \end{pmatrix}$$

Bloch sphere

$$\vec{a} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

$$\vec{a} = (a_x, a_y, a_z) = (u, v, w)$$



Rotation along versor $\hat{n}$ $R_{\hat{n}}(\theta) = exp\left(-i\theta\hat{n}\cdot\vec{\sigma}/2\right)$

$\langle\,|$ =bra $|\,\rangle$=ket

$\langle\,|\,\rangle$=number

$\sum_n |n\rangle\langle n|$ =basis

1 qbit

$$|0\rangle = 1|0\rangle + 0|1\rangle \rightarrow \begin{bmatrix}1\\0\end{bmatrix}$$

$$|1\rangle = 0|0\rangle + 1|1\rangle \rightarrow \begin{bmatrix}0\\1\end{bmatrix}$$

$$\langle 0| = 1\langle 0| + 0\langle 1| \rightarrow \begin{bmatrix}1 & 0\end{bmatrix}$$

$$\langle 1| = 0\langle 0| + 1\langle 1| \rightarrow \begin{bmatrix}0 & 1\end{bmatrix}$$

$$|v\rangle = v_0|0\rangle + v_1|1\rangle = v_0\begin{bmatrix}1\\0\end{bmatrix} + v_1\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}v_0\\v_1\end{bmatrix}$$

2 qbits

$$|a\rangle = \begin{bmatrix}a_0\\a_1\end{bmatrix} \quad \text{and} \quad |b\rangle = \begin{bmatrix}b_0\\b_1\end{bmatrix}$$

$$|x\rangle = |a\rangle \otimes |b\rangle = |ab\rangle$$

tensor product

$$|x\rangle = \begin{bmatrix}a_0 * \begin{bmatrix}b_0\\b_1\end{bmatrix}\\ a_1 * \begin{bmatrix}b_0\\b_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}a_0b_0\\a_0b_1\\a_1b_0\\a_1b_1\end{bmatrix} = \begin{bmatrix}x_0\\x_1\\x_2\\x_3\end{bmatrix}$$

$$|x\rangle = a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

$$|x\rangle = x_0|00\rangle + x_1|01\rangle + x_2|10\rangle + x_3|11\rangle$$

$$|a_0b_0|^2 + |a_0b_1|^2 + |a_1b_0|^2 + |a_1b_1|^2 = 1$$

3 qbits

$$|y\rangle = |ab\rangle \otimes |c\rangle = |abc\rangle$$

$$|c\rangle = \begin{bmatrix}c_0\\c_1\end{bmatrix}$$

$$|y\rangle = \begin{bmatrix}a_0b_0 * \begin{bmatrix}c0\\c1\end{bmatrix}\\ a_0b_1 * \begin{bmatrix}c0\\c1\end{bmatrix}\\ a_1b_0 * \begin{bmatrix}c0\\c1\end{bmatrix}\\ a_1b_1 * \begin{bmatrix}c0\\c1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}a_0b_oc_0\\a_0b_oc_1\\a_0b_1c_0\\a_0b_1c_1\\a_1b_oc_0\\a_1b_oc_1\\a_1b_1c_0\\a_1b_1c_1\end{bmatrix} = \begin{bmatrix}y_0\\y_1\\y_2\\y_3\\y_4\\y_5\\y_6\\y_7\end{bmatrix}$$

2^N **coordinates**

Classical Bit vs. Quantum Bit

CLASSICAL BIT:

- can be in two distinct states, 0 and 1
- can be measured completely
- are not changed by measurement
- can be copied
- can be erased

QUANTUM BIT:

- can be in state $|0\rangle$ or in state $|1\rangle$ or in any other state that is a linear combination of the two states
- can be measured partially with given probability
- are changed by measurement
- cannot be copied
- cannot be erased

What is a quantum computer?

➢ Classical Computer: a computer that uses voltages flowing through circuits and gates, which can be controlled and manipulated entirely by classical mechanics.

➢ Quantum Computer: a computer that uses laws of quantum mechanics to perform massively parallel computing through superposition, entanglement, and decoherence

Entanglement:

a physical state of two (or more) "particles" which appear to have correlated properties independently of their mutual space distance: there is a restricted space of possible outcomes such that if, e.g., one of two entangled particles is ***measured*** to have spin up ,$|0\rangle$, then the other will always have spin down, $|1\rangle$, The opposite is true: if the first is measured to have spin down, $|1\rangle$ then the other will always have spin up ,$|0\rangle$ (collapse of wave function)

Entanglement is fragile: any interactions with other particles/environment can destroy it (decoherence). A measure of any particle destroys it.

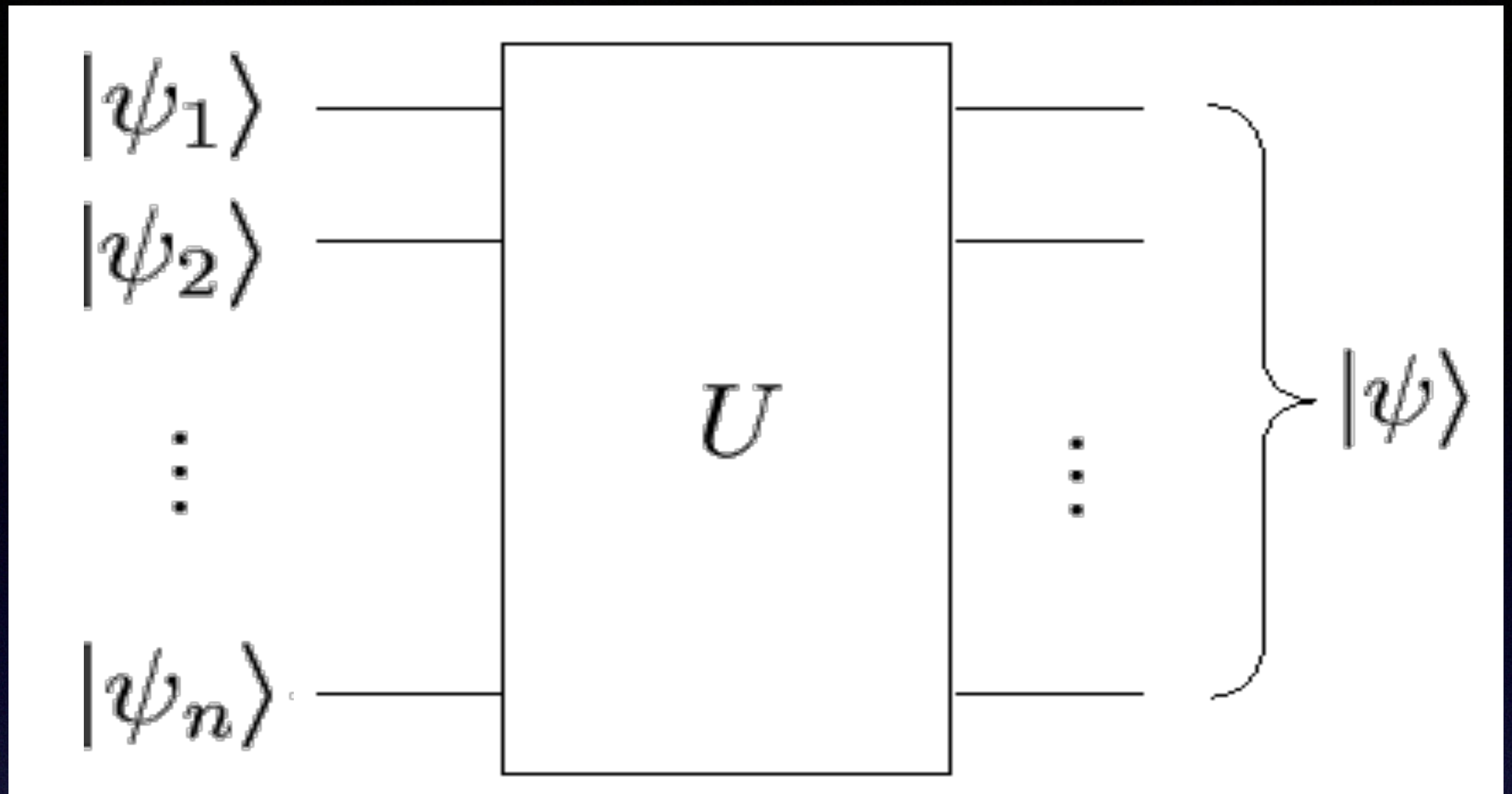
Entanglement can be shared among N particles (→ quantum computers)

Key Aspects of Quantum Entanglement:

- **Non-Separability:** Entangled particles cannot be described individually; they act as a single system.
- **Instant Correlation**: Measuring a property (e.g., spin, polarisation) of one particle instantly determines the state of the other, even if they are light-years apart.
- **Probabilistic Nature:** Before measurement, particles exist in a superposition of states.
- **No FTL Communication:** Although the connection is instantaneous, it cannot be used to transmit information faster than the speed of light.
- **Applications:** It is crucial for quantum computing (qubits), quantum teleportation, and quantum cryptography.

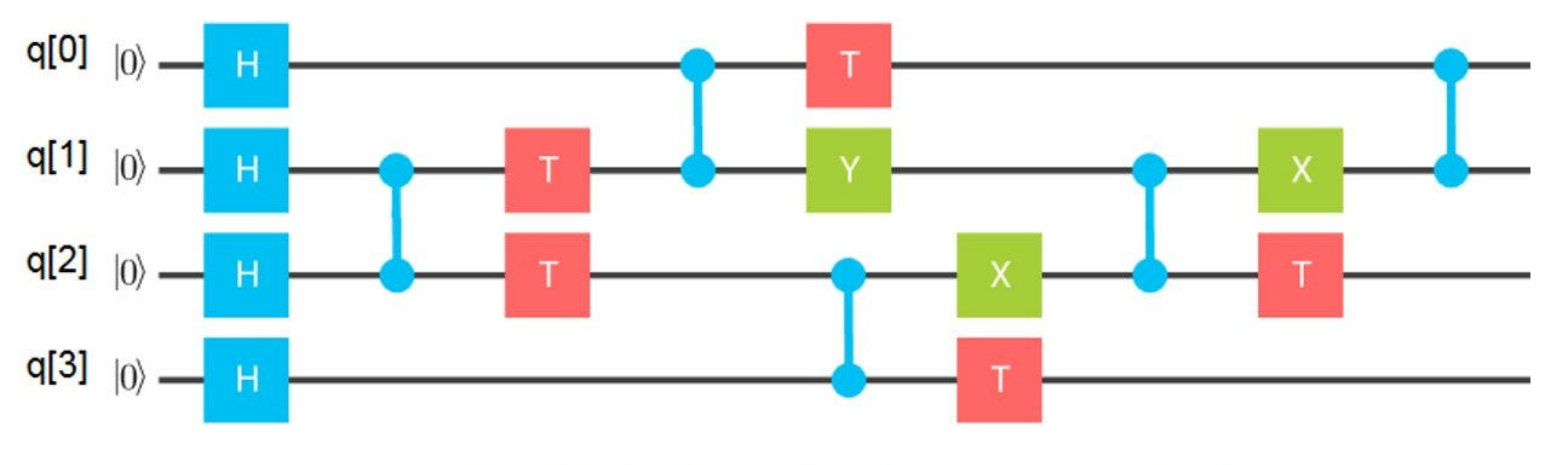
Unitary Transformation as Quantum Computing

On a quantum computer, programs are executed by unitary evolution of an input that is given by the state of the system, $|\psi_n\rangle$, which can in either 0 or 1 state.
Since all unitary operators are invertible, we can always reverse or 'uncompute' a computation on a quantum computer.



Topology of the quantum circuit is fundamental: e.g. entanglement among nearest neighbour only, a few qbits, all qbits.

Schematic of a quantum circuit



(a) A 4x1 universal random quantum circuit

$$\{|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$$

Bell states (entangled) form a 2 qbit basis

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
$$Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y,$$
$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x,$$
$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z.$$

Single qbit gates: X is the NOT operator, Y is the phase shift and Z=XY

H is Hadamard gate, S is the phase gate and T is the $\pi/8$ gate

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

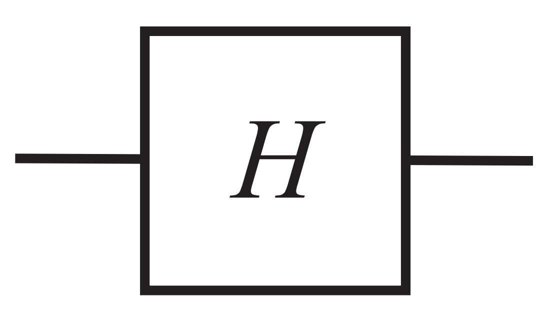
$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

Rotation operators about $\hat{x}$, $\hat{y}$, $\hat{z}$ axis

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

$$U_{\rm H}: \ |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

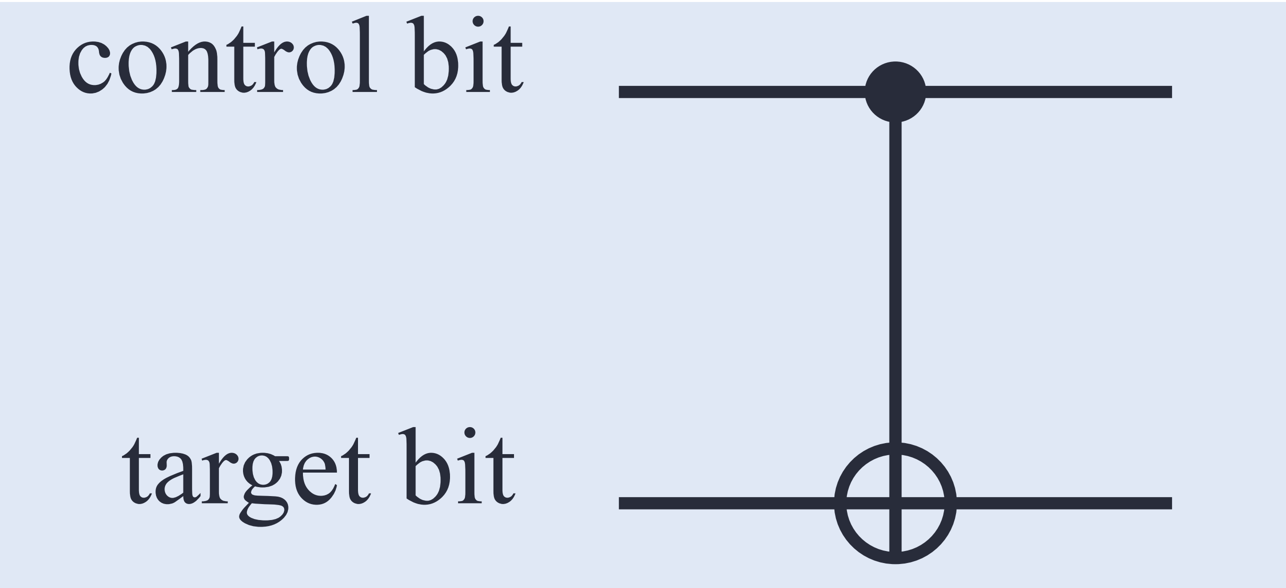
The Hadamard transformation entangles two qbits



Hadamard on N qbits

$$(H \otimes H \otimes \ldots \otimes H)|00\ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Two qbit gates: the CNOT (Controlled NOT): the first qbit is the control, the second one is the target. If the first is $|0\rangle$ then the second is unchanged, if the first is $|1\rangle$ then the second is flipped



$$U_{\rm CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$

$$U_{\rm CNOT} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}.$$

$$U_{\rm CNOT}: |00\rangle \mapsto |00\rangle, \ |01\rangle \mapsto |01\rangle, \ |10\rangle \mapsto |11\rangle, \ |11\rangle \mapsto |10\rangle.$$