Introduction to Quantum Computing

Paolo Cremonesi

POLITECNICO
MILANO 1863

Operations on Qubits: Single Qubit Gates

Operations on qubits

- Logic Gates
  - building blocks for a quantum circuit
  - operate on single qubits or on sets of qubits
  - change the state of the qubits
  - are “reversible”
- Measurement
  - is an irreversible operation in which information is gained about the state of a single qubit
  - collapse the state of the qubit (superposition and entanglement are lost)
- Initialization
  - to a known value, often $|0\rangle$ or $|1\rangle$ because easier
  - can be implemented as a measurement
  - collapses the quantum state (like measurement)

Quantum logic gates

- Single Qubit Gates
- Multiple Qubit Gates

Quantum logic gates

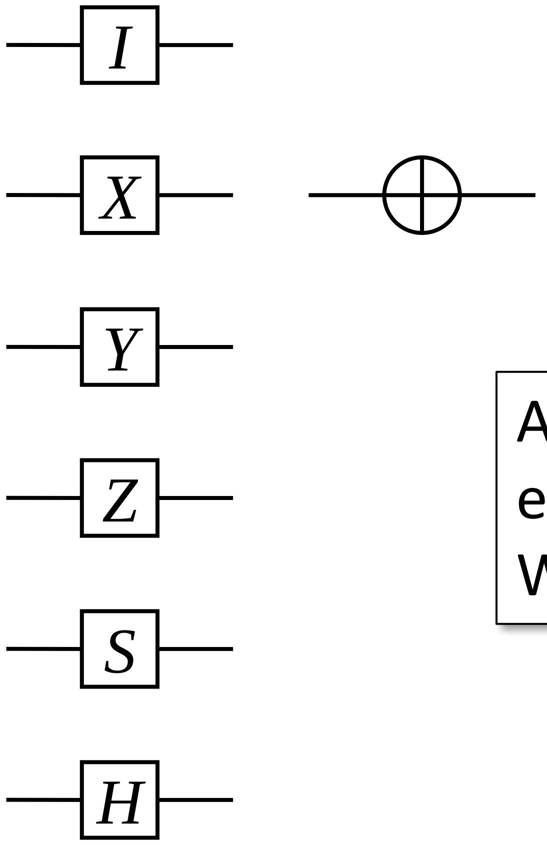
- Qubits are vectors, **gates are matrices**
- A gate that operates on a qubit is a 2×2 **unitary** matrix U that manipulates the qubit
  - **unitary** properties: $U^H U = UU^H = UU^{-1} = I$
- The action of the gate on the qubit is found by multiplying vector $|v\rangle$, which represents the state of the qubit, by matrix U representing the gate
- The result is a qubit in a new state

$$|v'\rangle = U|v\rangle$$

- Why unitary?
  - no-cloning (qubits cannot be copied)
  - no-delete (state transformation of a qubit is reversible $|v\rangle = U^H|v'\rangle$)
- Quantum gates do not necessarily correspond to physical gates

Single-qubit quantum logic gates

- Identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- Pauli-X (Not) $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- Pauli-Y $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
- Pauli-Z (Phase Flip) $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- Phase $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- Hadamard $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- … many more



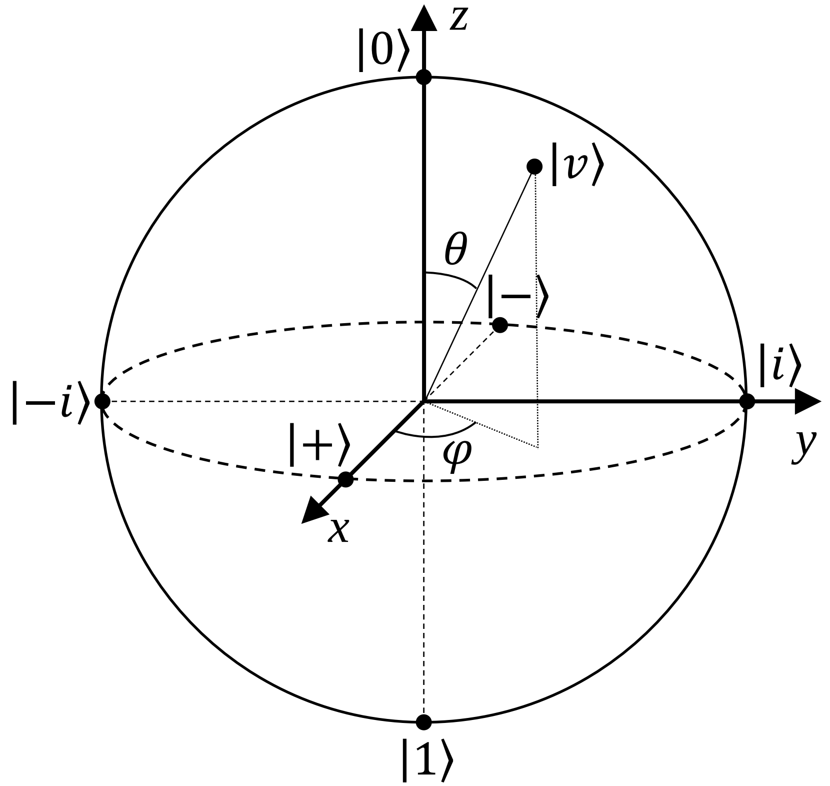
All quantum gates are equivalent to rotations. Why?

Identity gate (I)

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

- $|v\rangle = I|v\rangle$

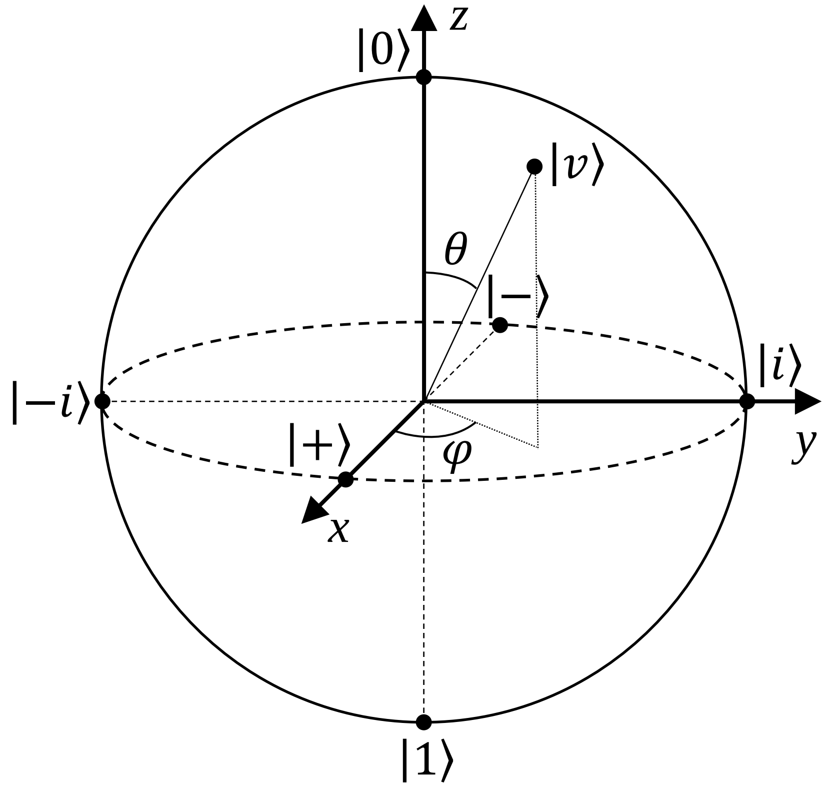
- Apparently useless, but it is not
- Useful with multiple-qubits circuits



Pauli-X gate (Not)

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

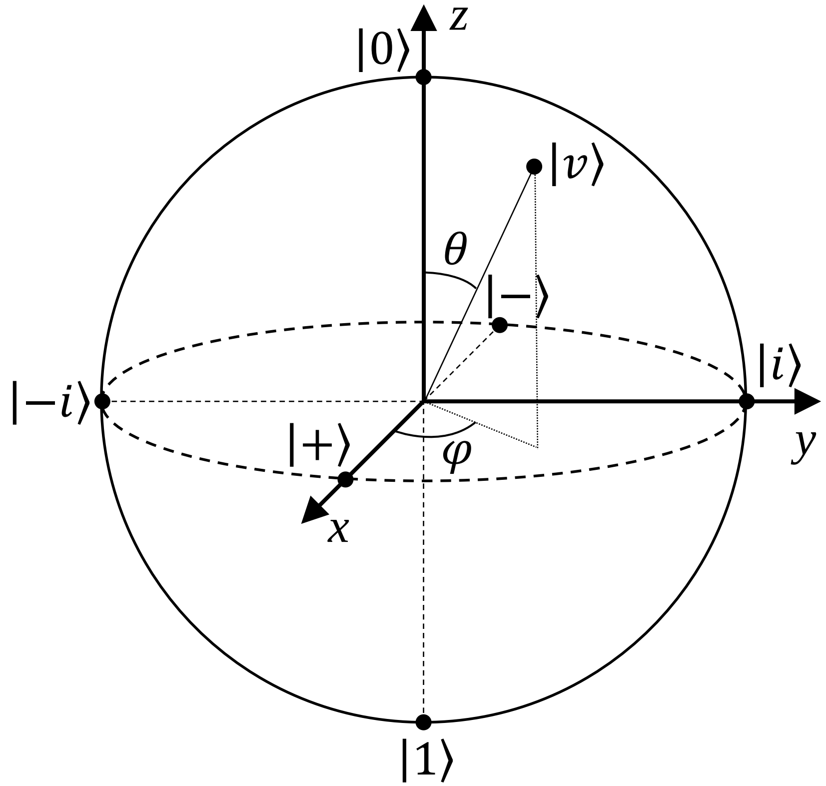
- Amplitudes a and b are **flipped** (exchanged)
  - if $|v\rangle = a|0\rangle + b|1\rangle$ we have $X|v\rangle = b|0\rangle + a|1\rangle$
  - example: $X|1\rangle = |0\rangle$ and $X|0\rangle = |1\rangle$
- Equivalent to a **rotation around the *x*-axes by π radians**
  - $|v\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - rotation requires $\theta \rightarrow \pi - \theta$ and $\varphi \rightarrow -\varphi$ (see figure)
  - substitute in $|v\rangle$ and obtain $|v'\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle + e^{-i\varphi}\cos\left(\frac{\theta}{2}\right)|1\rangle$
  - multiply $|v'\rangle$ by $e^{i\varphi}$ (unit vector, same qubit) and obtain $|v'\rangle = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle$
  - $|v'\rangle$ is the same as $|v\rangle$ with *a* and *b* swapped



Pauli-Z gate (Phase Flip)

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

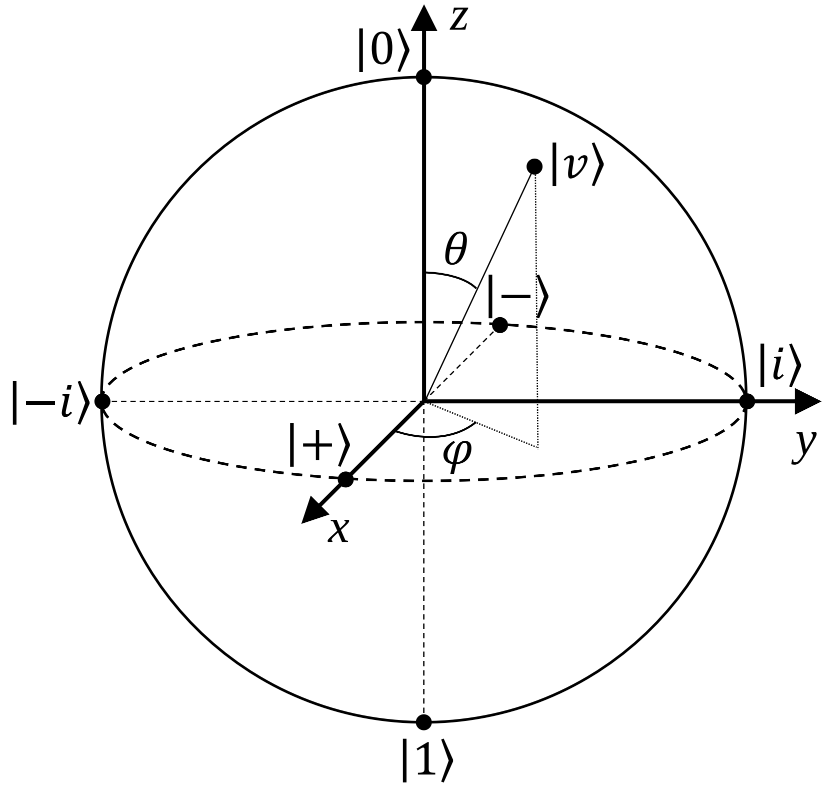
- Changes the sign of *b*
  - if $|v\rangle = a|0\rangle + b|1\rangle$ we have $X|v\rangle = a|0\rangle - b|1\rangle$
- Equivalent to a **rotation around the *z*-axes by $\boldsymbol{\pi}$ radians**
  - $|v\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - rotation requires $\varphi \rightarrow \varphi + \pi$ (see figure)
  - $e^{i(\varphi+\pi)} \rightarrow -e^{i\varphi}$
  - replace and obtain $|v'\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle - e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$
  - $|v'\rangle$ is the same as $|v\rangle$ with *b* negative



Pauli-Y gate

$$Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

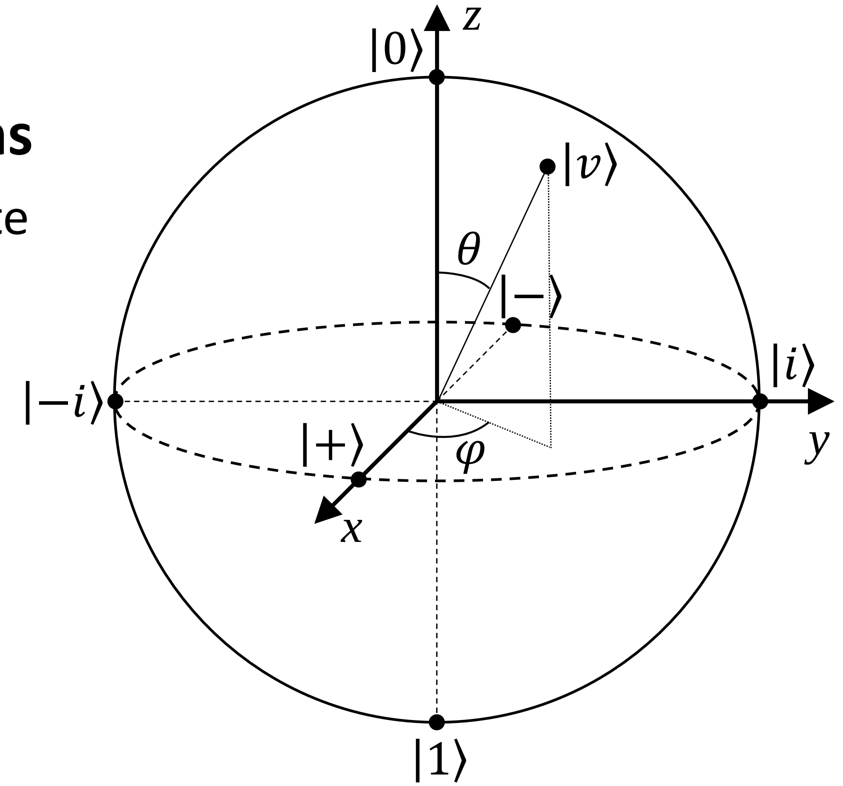
- Equivalent to a **rotation around the *y*-axes by π radians**
  - we show that $Y = iXZ$
    - i is a global phase and can be neglected
    - X and Z are two π rotations around *x*-axes and *z*-axes
    - equivalent to a π rotation around the *y*-axes (see figure)
  - $XZ = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
  - $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iXZ$
  - as we wanted to demonstrate



Phase gate (S)

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

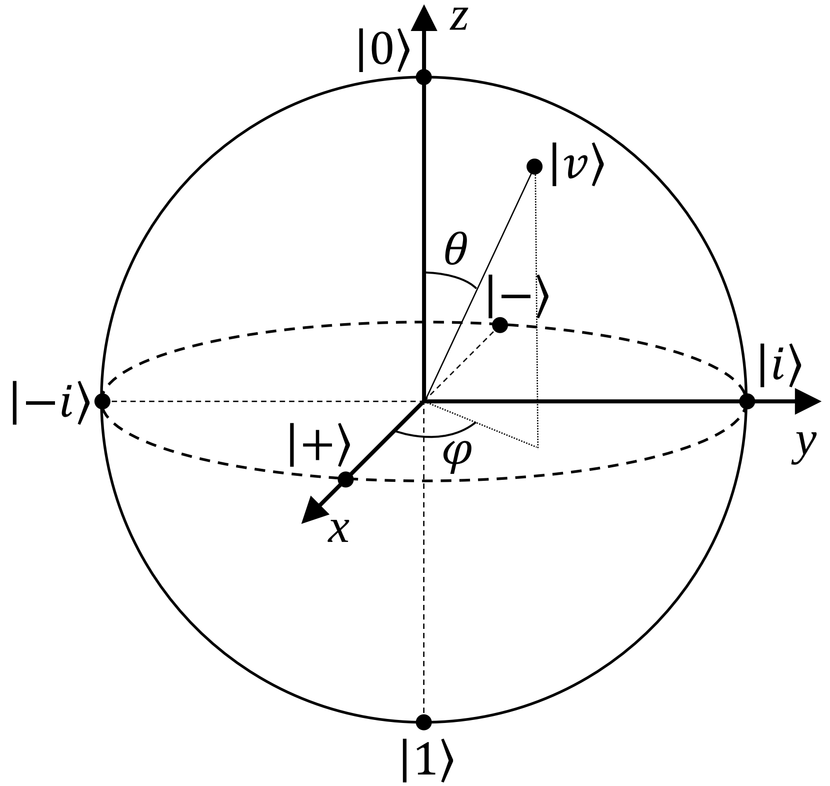
- Equivalent to a **rotation around the *z*-axes by $\pi/2$ radians**
  - we show that If you perform two consecutive rotations with gate S it is equivalent to one rotation with gate Z
  - $S \cdot S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$
  - as we wanted to demonstrate



Hadamard gate (H)

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

- Equivalent to a rotation first around the *y*-axis by $\pi/2$ radians followed by one around the *x*-axis by π radians
  - $H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$
    $H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$
- $|+\rangle$ and $|-\rangle$ are relevant states (Hadamard states)
  - for both of them $|a|^2 = |b|^2 = \frac{1}{2}$
  - **maximum superposition**
  - equal probabilities of being measured as $|0\rangle$ or $|1\rangle$
  - often used to prepare qubits in superposition states



Properties of single qubit gates

- All quantum gates are equivalent to rotations on the Bloch sphere
  - why?

- If you apply twice the same Pauli gate you go back to the initial qubit

$$X^2 = Y^2 = Z^2 = I$$

  - why? (two consecutive π rotations around the same axis …)

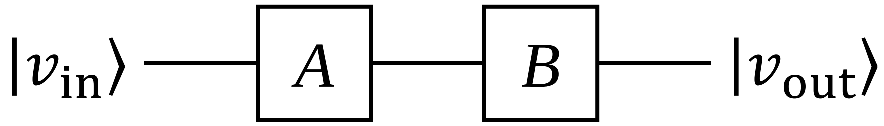
Exercise: when a gate creates superposition?

$$A = \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix}$$

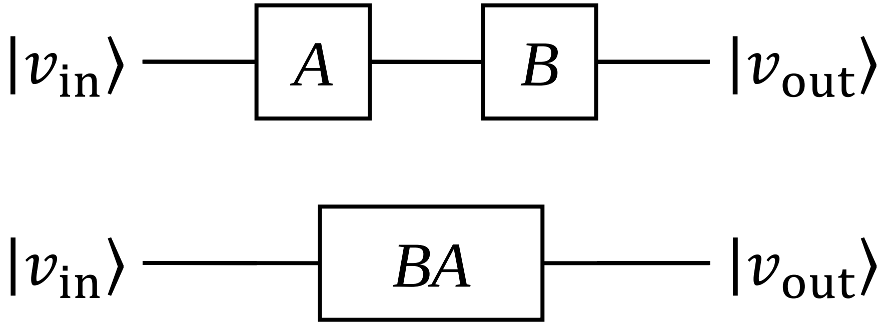
- Consider gate A and apply it to a base state $|0\rangle$ or $|1\rangle$
  - $v = A|0\rangle$ or $v = A|1\rangle$
- Show why A cannot create superposition
  - this requires that **at least in one column of *A* both elements are non-zero**
  - for A to be unitary, we must have that $A^H A = I$
  - for simplicity of discussion, we assume A to be real, so that $A^H = A^T$
  - for A to be unitary, we must have $A^H A = \begin{bmatrix} a_{11} & 0 \\ a_{12} & a_{22} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11}^2 & a_{11}a_{12} \\ a_{11}a_{12} & a_{12}^2 + a_{22}^2 \end{bmatrix} = I$
  - $a_{11} = \mp 1$, $\boldsymbol{a_{12} = 0}$, $a_{22} = \mp 1$
  - A is diagonal, the condition is not satisfied
- **To create superposition from a base state, all elements of a gate must be different from zero**

Single-qubit quantum circuits

- A model for quantum computation
- A sequence of
  - initializations of qubits to known values
  - gates
  - measurements
  - possibly other actions
- Lines define the sequence of events
  - horizontal lines are qubits
  - objects connected by lines are operations (gates, measurements) performed on qubits
  - doubled lines are classical bits
  - lines are **not** physical connections



Single-qubit quantum circuits (serial gates)



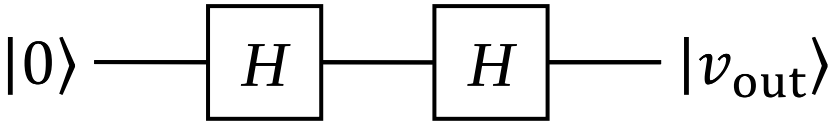
- Assume that we have two gates A and B
  - with B after A
- The effect of the two gates can be described as a single gate C

$$C = BA$$

- Multiplication is from **right to left** with respect to the order in which gates appear in the circuit

$$|v_{\text{out}}\rangle = C|v_{\text{in}}\rangle = BA|v_{\text{in}}\rangle$$

Single-qubit Quantum Circuits: Example



$$|v_{\text{out}}\rangle = HH|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = |0\rangle$$

Bra-ket notation: outer product of kets

- The **outer** product between kets $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$ and $|b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$ is a 2×2 matrix represented with the notation $|a\rangle\langle b|$ and defined as:
$$|a\rangle\langle b| = \vec{a} \otimes \vec{b}^H = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} \overline{b_1} & \overline{b_2} \end{bmatrix} = \begin{bmatrix} a_1\overline{b_1} & a_1\overline{b_2} \\ a_2\overline{b_1} & a_2\overline{b_2} \end{bmatrix}$$
- The outer product is an element-by-element product between the first vector and the Hermitian of the second vector
  - $\otimes$ is the **tensor product** operator
- The outer and scalar products have this useful property
$$(|a\rangle\langle b|)|c\rangle = |a\rangle\langle b|c\rangle = \langle b|c\rangle|a\rangle$$
  - where we should remember that $(|a\rangle\langle b|)$ is a matrix and $\langle b|c\rangle$ is a scalar
- Demonstration on the next slide

Property of outer and scalar product of kets

- We want to demonstrate that

$$(|a\rangle\langle b|)|c\rangle = |a\rangle\langle b|c\rangle = \langle b|c\rangle|a\rangle$$

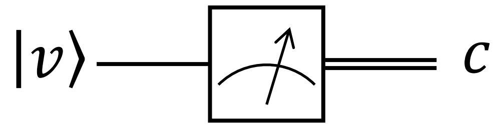
  - where $|a\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}$, $|b\rangle = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$ and $|c\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$
- Use the definition of outer product from previous slide and apply the scalar product
  - $(|a\rangle\langle b|)|c\rangle = \begin{bmatrix} a_1\overline{b_1} & a_1\overline{b_2} \\ a_2\overline{b_1} & a_2\overline{b_2} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a_1\overline{b_1}c_1 + a_1\overline{b_2}c_2 \\ a_2\overline{b_1}c_1 + a_2\overline{b_2}c_2 \end{bmatrix}$
  - observe that
  - $\begin{bmatrix} a_1\overline{b_1}c_1 + a_1\overline{b_2}c_2 \\ a_2\overline{b_1}c_1 + a_2\overline{b_2}c_2 \end{bmatrix} = \begin{bmatrix} a_1\left(\overline{b_1}c_1 + \overline{b_2}c_2\right) \\ a_2\left(\overline{b_1}c_1 + \overline{b_2}c_2\right) \end{bmatrix}$ and $\left(\overline{b_1}c_1 + \overline{b_2}c_2\right)$ is exactly the inner product $\langle b|c\rangle$
  - we can rewrite the result as
  - $(|a\rangle\langle b|)|c\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \langle b|c\rangle = |a\rangle\langle b|c\rangle$

Measurement of a qubits

- A **measurement** (or **projection**) operator is a special **non-unitary** (and **non-invertible**) two-by-two matrix M_k

$$M_k = |k\rangle\langle k|$$

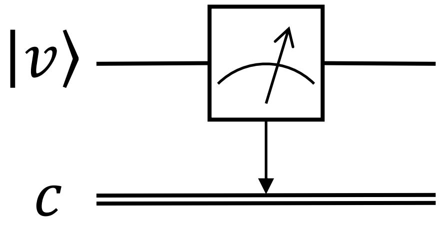
    - project a qubit $|v\rangle$ along vector $|k\rangle$ (demonstration later)



- After the projection, the resulting state **could be (probabilistic)**

$$|v_k\rangle = \frac{M_k|v\rangle}{\langle v|M_k|v\rangle}$$

    - not a rotation!!



- **Probability** of the measurement to be $|v_k\rangle$

$$p_k = \langle v|M_k|v\rangle$$

- In standard basis $M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Property of the measurement operator

- Once applied, M_k does not change the vector anymore if you apply it twice

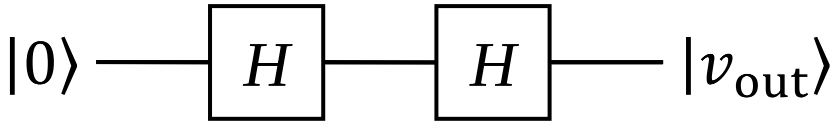
$$M_k^2 = M_k M_k = M_k$$

- Demonstration
  - define $|k\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$
  - compute $M_k = |k\rangle\langle k| = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix}$
  - compute M_k^2
  - $M_k^2 = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} = \begin{bmatrix} a^4 + a^2 b^2 & a^3\bar{b} + a\bar{b}b^2 \\ b\bar{a}a^2 + b^3\bar{a} & b^4 + a^2 b^2 \end{bmatrix} = \begin{bmatrix} a^2\left(a^2 + b^2\right) & a\bar{b}\left(a^2 + b^2\right) \\ b\bar{a}\left(a^2 + b^2\right) & b^2\left(a^2 + b^2\right) \end{bmatrix}$
  - remember that $a^2 + b^2 = 1$, thus
  - $M_k^2 = \begin{bmatrix} a^2 & a\bar{b} \\ b\bar{a} & b^2 \end{bmatrix} = M_k$

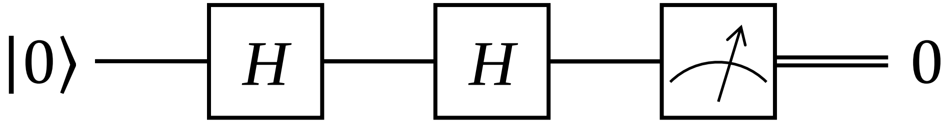
Measurement operator as a projection

- Demonstrate that the application of M_k to ket $|v\rangle$ projects $|v\rangle$ on vector $|k\rangle$
  - definition of M_k
$$M_k = |k\rangle\langle k|$$
  - application of M_k to $|v\rangle$
$$M_k|v\rangle = |k\rangle\langle k||v\rangle = \langle k|v\rangle|k\rangle$$
  - remember that $\langle k|v\rangle$ is the cosine between $|k\rangle$ and $|v\rangle$
  - the resulting vector has the same direction of $|k\rangle$ scaled by $\langle k|v\rangle$

Single-qubit Quantum Circuits: Example



$$|v_{\text{out}}\rangle = HH|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = |0\rangle$$



Thanks

Paolo Cremonesi

POLITECNICO
MILANO 1863