Advanced Parallel School 2022
Quantum Computing – Day 1
Quantum Algorithms

Mengoni Riccardo, PhD

14 Feb 2022

CINECA QUANTUM COMPUTING LAB

Quantum Computing @ CINECA

CINECA: Italian HPC center

CINECA Quantum Computing Lab:

- Research with Universities, Industries and QC startups

- Internship programs, Courses and Conference (HPCQC)

https://www.quantumcomputinglab.cineca.it

r.mengoni@cineca.it

QUANTUM COMPUTING LAB

Recap of Quantum Computing

Vectors

Ket: $|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}$ $\psi_i \in \mathbb{C}$

Complex Number

Bra: $\langle\psi| = (\psi_1^* \ \ \psi_2^* \ \ ... \ \ \psi_n^*)$ ψ_i^* Complex Conjugate

Scalar Product

$$\langle \phi | \psi \rangle = \begin{pmatrix} \phi_1^* & \phi_2^* & \dots & \phi_n^* \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}$$

$$\langle \phi | \psi \rangle \in \mathbb{C}$$

Complex Number

Scalar Product

$$\langle \phi | \psi \rangle = \begin{pmatrix} \phi_1^* & \phi_2^* & \cdots & \phi_n^* \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}$$

$$\langle \phi | \psi \rangle \in \mathbb{C}$$

Complex Number

The scalar product induces a **norm**

$$\| \, |\psi\rangle \, \| = \sqrt{\langle \psi | \psi \rangle}$$

Outer Product

$$|\psi\rangle\langle\phi| = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \begin{pmatrix} \phi_1^* & \phi_2^* & \dots & \phi_n^* \end{pmatrix} = \begin{pmatrix} \psi_1\phi_1^* & \psi_1\phi_2^* & \dots & \psi_1\phi_n^* \\ \psi_2\phi_1^* & \psi_2\phi_2^* & \dots & \psi_2\phi_n^* \\ \vdots & \vdots & & \vdots \\ \psi_n\phi_1^* & \psi_n\phi_2^* & \dots & \psi_n\phi_n^* \end{pmatrix}$$

Dimension = n x n

Tensor Product

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \phi_1 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \phi_2 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \vdots \\ \phi_n \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \end{pmatrix}$$

Dimension = n^2

Tensor Product

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \phi_1 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \phi_2 \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \\ \vdots \\ \phi_n \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix} \end{pmatrix}$$

Dimension = n^2

Compact form:

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle |\phi\rangle = |\psi\,\phi\rangle$$

1. Unit of Information

Classically

Unit of classical information is the bit

State of a bit:

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

Postulates of Quantum Computing (1)

Quantumly

To a closed quantum system is associated a space of states *H* which is a Hilbert space. The pure state of the system is then represented by a unit norm vector on such Hilbert space.

The unit of quantum information is the quantum bit a.k.a. Qubit

State of a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Postulates of Quantum Computing (1)

Space of states: $\mathcal{H} \simeq \mathbb{C}^2$

State of a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$\alpha, \beta \in \mathbb{C}$ $\qquad |\alpha|^2 + |\beta|^2 = 1$

Postulates of Quantum Computing (1)

Space of states: $\mathcal{H} \simeq \mathbb{C}^2$

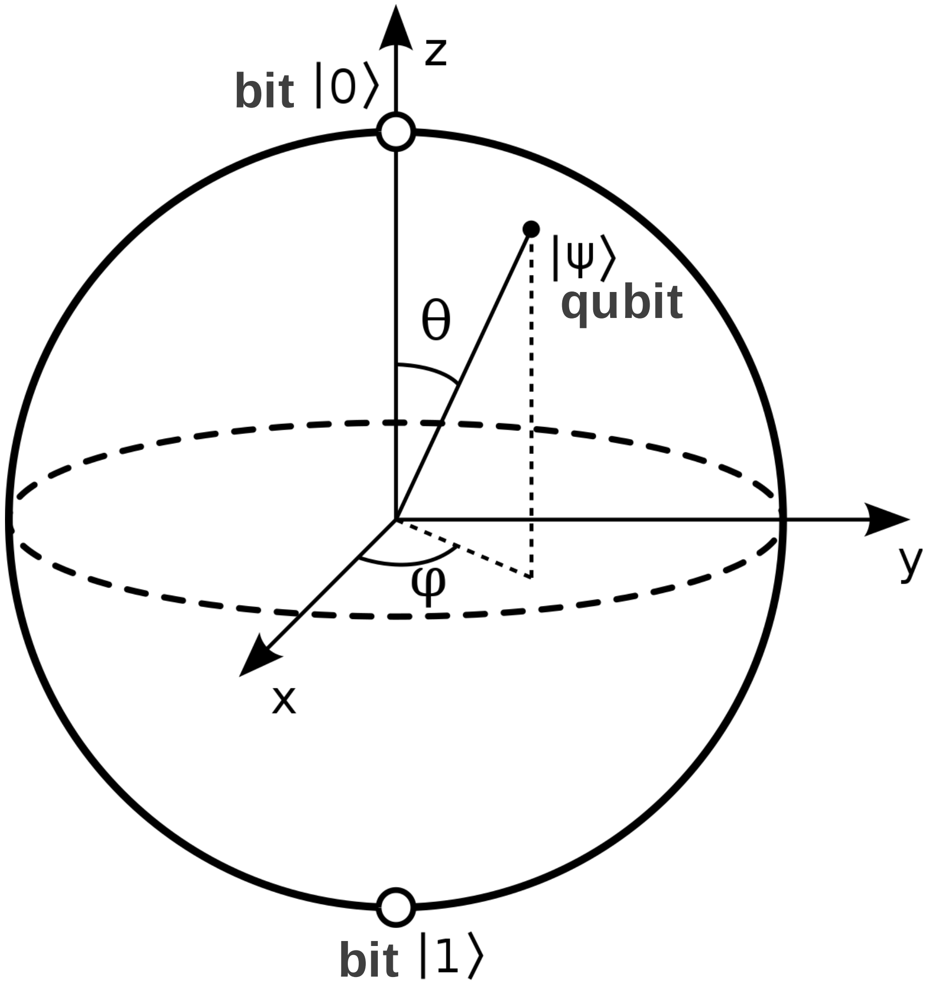
State of a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

$$\alpha, \beta \in \mathbb{C} \qquad |\alpha|^2 + |\beta|^2 = 1$$

Can be parametrized as:

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



2. Composite systems

Classically

State of N bits:

$$|000\ldots0\rangle,\ |100\ldots0\rangle,\ |010\ldots0\rangle\ \ldots\ |111\ldots1\rangle$$

Quantumly

The space of states of a composite system is the tensor product of the spaces of the subsystems

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$$

State of N qubits:

$$\alpha_1 |000..0\rangle + \alpha_2 |100..0\rangle + \alpha_3 |010..0\rangle + \ldots \alpha_n |111..1\rangle$$

$$\alpha_i \in \mathbb{C} \qquad \sum_i |\alpha_i|^2 = 1$$

Quantum Entanglement

States that can be written as tensor product

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

are called **factorable or product states**

Quantum Entanglement

States that **can NOT** be written as tensor product

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_N\rangle$$

are called **entangled states**

Postulates of Quantum Computing (2)

Quantum Entangled

Bell's states

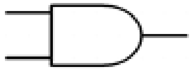
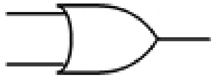
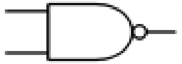
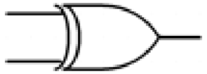
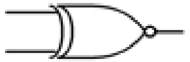
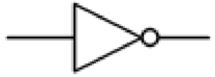
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \qquad \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

3. State Change

Postulates of Quantum Computing (3)

Classically: logic gates

Logic Gate	Symbol	Description	Boolean
AND		Output is at logic 1 when, and only when all its inputs are at logic 1,otherwise the output is at logic 0.	$X = A \cdot B$
OR		Output is at logic 1 when one or more are at logic 1.If all inputs are at logic 0,output is at logic 0.	$X = A + B$
NAND		Output is at logic 0 when,and only when all its inputs are at logic 1,otherwise the output is at logic 1	$X = \overline{A \cdot B}$
NOR		Output is at logic 0 when one or more of its inputs are at logic 1.If all the inputs are at logic 0,the output is at logic 1.	$X = \overline{A + B}$
XOR		Output is at logic 1 when one and Only one of its inputs is at logic 1. Otherwise is it logic 0.	$X = A \oplus B$
XNOR		Output is at logic 0 when one and only one of its inputs is at logic1.Otherwise it is logic 1. Similar to XOR but inverted.	$X = \overline{A \oplus B}$
NOT		Output is at logic 0 when its only input is at logic 1, and at logic 1 when its only input is at logic 0.That's why it is called and INVERTER	$X = \overline{A}$

Quantumly

The state change of a closed quantum system is described by a unitary operator

$$i \frac{d|\psi\rangle}{dt} = H|\psi\rangle \Rightarrow |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

$$U = e^{-iHt}$$

Schrodinger Equation

Quantumly: Quantum Gates

X Gate
Bit–flip, Not

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Z Gate
Phase–flip

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

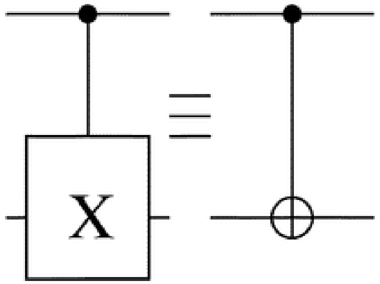
H Gate
Hadamard

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{\alpha+\beta|0\rangle + \alpha-\beta|1\rangle}{\sqrt{2}}$$

T Gate

$$T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

Controlled Not
Controlled X
CNot



$$\equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$$

4. Measurement

Postulates of Quantum Computing (4)

Classically

Measuring returns the state of a bit with certainty

$$|0\rangle \xrightarrow{\text{Measure}} \underset{}{\overset{\text{Outcome}}{|0\rangle}} \qquad |1\rangle \xrightarrow{\text{Measure}} \overset{\text{Outcome}}{|1\rangle}$$

Measurements do not affect the state of a bit

Postulates of Quantum Computing (4)

Quantumly

Measuring returns the bit state with some probability

Outcome

Measure

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \xrightarrow{\text{Measure}} \quad \begin{cases} |0\rangle \text{ with } P_r = |\alpha|^2 \\ |1\rangle \text{ with } P_r = |\beta|^2 \end{cases}$$

Measurement affects the state of a qubit

Quantumly

- To **any observable** physical quantity is associated an **hermitian operator** *O*

$$O|o_i\rangle = o_i|o_i\rangle$$

- A **measurement** outcomes are the **possibile eigenvalues** $\{o_i\}$.

- The **probability of obtaining** o_i as a result of the measurement is

$$P_r(o_i) = |\langle\psi|o_i\rangle|^2$$

- The effect of the **measure is to change the state** $|\psi\rangle$ **into the eigenvector of** *O*

$$|\psi\rangle \rightarrow |o_i\rangle$$

Quantum Algorithms

Quantum Algorithm = Quantum Circuit

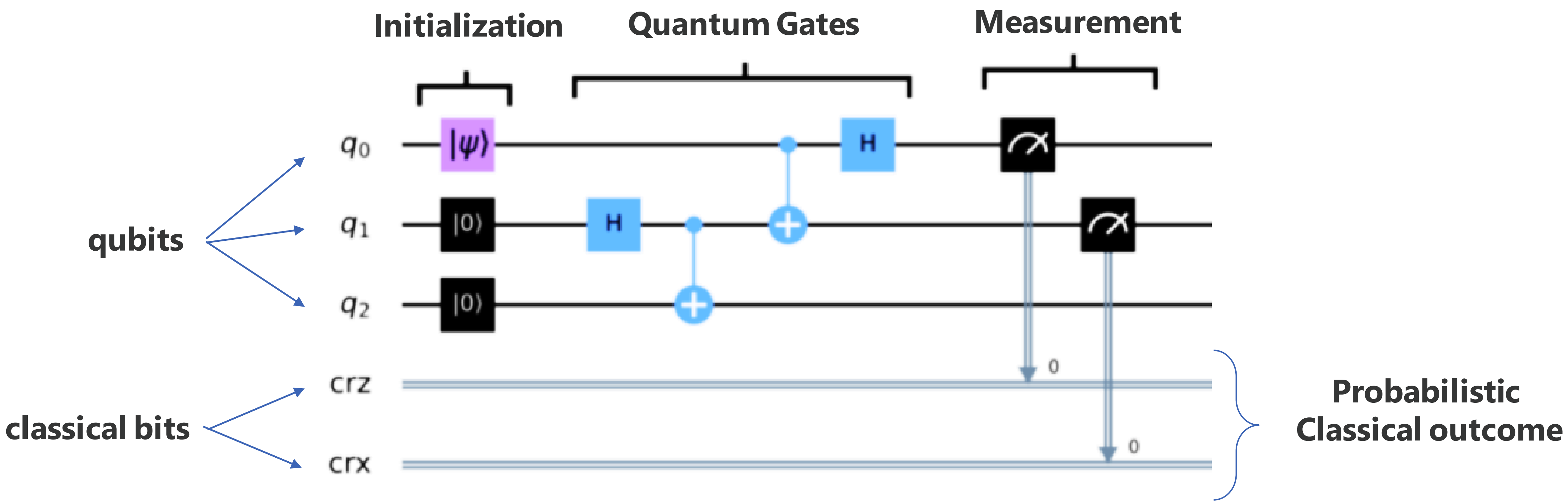
A quantum circuit with *n* input qubits and *n* output qubits is defined by a unitary transformation

$$U \in U(2^n)$$

$$U^\dagger U = UU^\dagger = I$$

$$U^{-1} = U^\dagger$$

Quantum Algorithms



Quantum Algorithms: Gates

Single Qubit Gates

Generic single qubit rotation:

$$R_{\vec{n}}(\theta) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) \vec{n}\cdot\vec{\sigma}$$

Pauli matrices:

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

Single Qubit Gates: Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H = -\boxed{H}-$$

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

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

Single Qubit Gates: Phase

$$U_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

$$U_\phi |0\rangle = |0\rangle$$

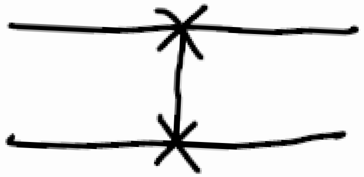
$$U_\phi |1\rangle = e^{i\phi} |1\rangle$$

Two Qubit Gates: SWAP

$$U_{SWAP} |z_1\rangle |z_2\rangle = |z_2\rangle |z_1\rangle \qquad z_1, z_2 \in \{0,1\}$$

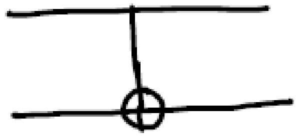
$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

SWAP =



Two Qubit Gates: Control Not

$$U_{cx} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$U_{cx} =$ 

$$U_{cx} |z_1\rangle |z_2\rangle = |z_1\rangle X^{z_1} |z_2\rangle$$

$$U_{cx} |00\rangle = |00\rangle$$

$$U_{cx} |10\rangle = |11\rangle$$

$$U_{cx} |01\rangle = |01\rangle$$

$$U_{cx} |11\rangle = |10\rangle$$

Two Qubit Gates: Control Unitary

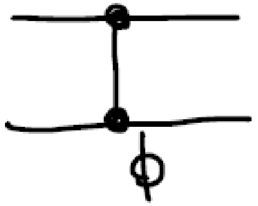
$$CU\,|z_1\rangle|z_2\rangle = |z_1\rangle\, U^{z_1}\,|z_2\rangle$$

Control Phase

$$CU_\phi\,|z_1\rangle|z_2\rangle = |z_1\rangle\, U_\phi^{z_1}\,|z_2\rangle$$

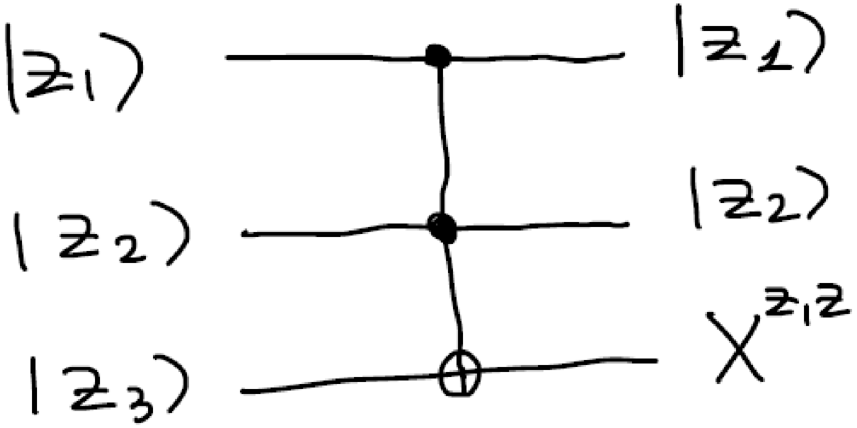
$$CU_\phi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}$$

$CU_\phi =$



Three Qubit Gates: Toffoli

$$U_{C_2X} |z_1 z_2 z_3\rangle = |z_1 z_2\rangle X^{z_1 z_2} |z_3\rangle$$



$$X^{z_1 z_2} |z_3\rangle = |z_3 \oplus z_1 \cdot z_2\rangle$$

Quantum Algorithms: Universality

Universal set of Quantum Gates

We can exactly build any unitary $U \in U(2^n)$ on n qubits

by means of single qubit gates and Control-Not

$$\mathcal{G}_{ex} = \{ U \in \mathcal{U}(2) \; ; \; U_{cx} \}$$

Universal set of Quantum Gates

We can exactly build any unitary $U \in U(2^n)$ on n qubits

by means of single qubit gates and Control-Not

$$\mathcal{G}_{ex} = \{ U \in \mathcal{U}(2) \; ; \; U_{cx} \}$$

$$R_{\vec{n}}(\theta) = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) \vec{n} \cdot \vec{\sigma}$$

$$U_{cx} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Universal set of Quantum Gates

Given $U, U' \in \mathcal{U}(2^n)$, U' approximates U within ε $(\varepsilon > 0)$ if $d(U, U') < \varepsilon$

Universal set of Quantum Gates

Given $U, U' \in \mathcal{U}(2^n)$, U' **approximates** U **within** ε $(\varepsilon > 0)$ **if** $d(U, U') < \varepsilon$

where $$d(U,U') = \max_{|\psi\rangle} \| (U - U')|\psi\rangle \|$$

and $$\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle}$$

Universal set of Quantum Gates

We can approximate any unitary $U \in U(2^n)$ on n qubits

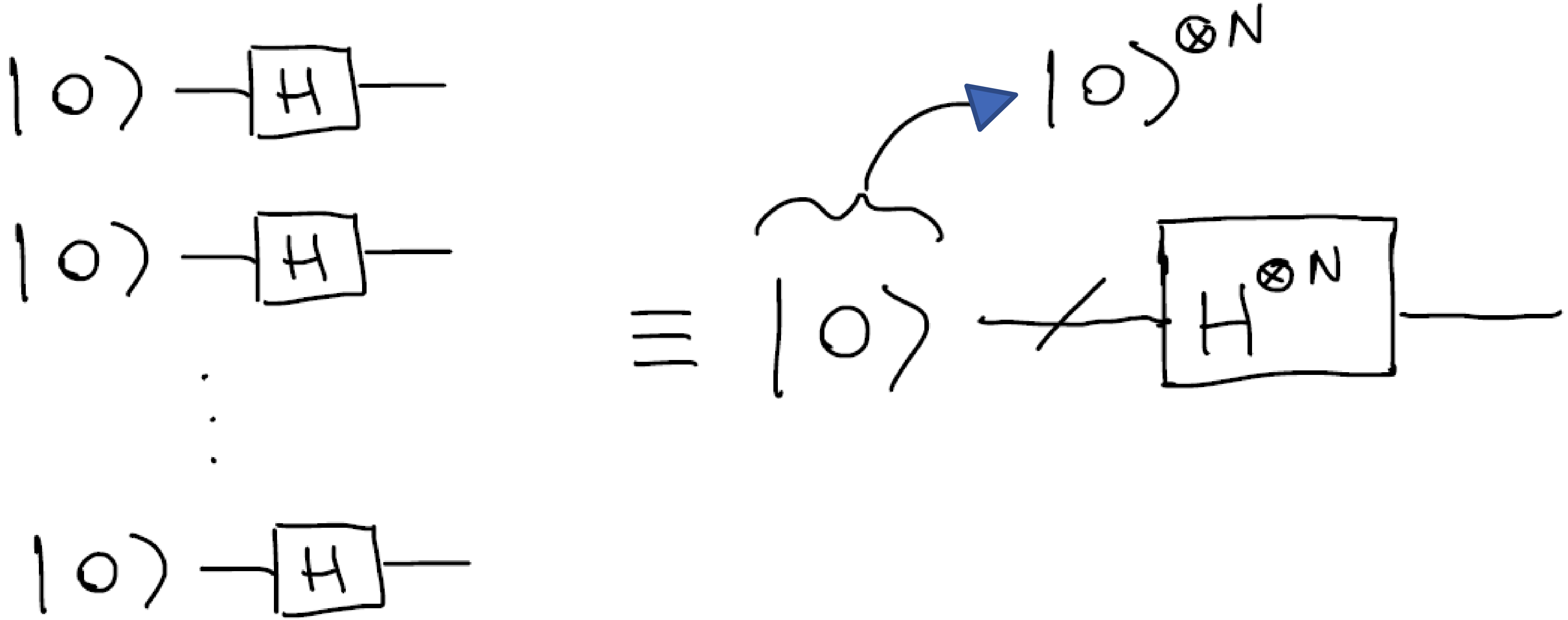
by means of the following gates

$$\{H, S, T, U_{cx}\}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Quantum Algorithms: basics

Multiple Hadamard gates



Single Qubit Gates: Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H = -\boxed{H}-$$

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

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

Multiple Hadamard gates

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

$$H^{\otimes N} = \frac{1}{\sqrt{2^N}} \sum_{x,y \in \{0,1\}^N} (-1)^{x \cdot y} |x\rangle\langle y|$$

Quantum Computing @ CINECA

CINECA: Italian HPC center

CINECA Quantum Computing Lab:

- Research with Universities, Industries and QC startups
- Internship programs, Courses and Conference (HPCQC)

https://www.quantumcomputinglab.cineca.it

r.mengoni@cineca.it

QUANTUM COMPUTING LAB