Quantum computation : lecture 2

- Axioms of quantum mechanics:
  1. state of a quantum system
  2. evolution of a quantum system
  3. measurement postulate
  4. combination of quantum systems

- Quantum circuits - Barenco & al's theorem

Axiom 1: State of a quantum system

The state of a quantum system (isolated from the environment) is represented by a unit vector $|\varphi\rangle$ in a Hilbert space $\mathcal{H}$.

In particular, the state of a system of n qubits is represented by a unit vector in

$$\mathcal{H} = \mathbb{C}^{2^n} \sim \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}}.$$

⚠ $\| |\varphi\rangle \|^2 \neq n$ for n qubits!

Computational basis: $\{ |x_1,\dots,x_n>, \ x_i \in \{0,1\}, 1 \leq i \leq n \}$

$$<x_1',\dots,x_n'|x_1,\dots,x_n> = \delta_{x_1' x_1} \cdots \delta_{x_n' x_n}$$

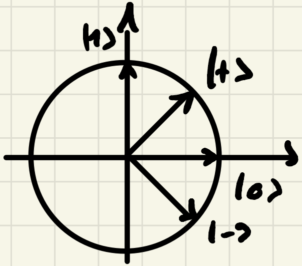
$$|\varphi> = \sum_{x_1..x_n \in \{0,1\}} \alpha_{x_1,\dots,x_n} |x_1,\dots,x_n>$$

$$1 = <\varphi|\varphi> = \sum_{x_1..x_n \in \{0,1\}} |\alpha_{x_1,\dots,x_n}|^2$$

$\underline{n=1}$: $|\varphi> = (\cos\theta)|0> + (\sin\theta)|1>$, $(\cos\theta)^2 + (\sin\theta)^2 = 1$

Two particular cases: $(\theta = +45° \ \& \ -45°)$

$$\begin{cases} |+> = \frac{1}{\sqrt{2}}(|0> + |1>) \\ |-> = \frac{1}{\sqrt{2}}(|0> - |1>) \end{cases}$$



⚠ Various notations here!

$$\left\{\begin{array}{l} |0\rangle + |1\rangle : \text{addition of 2 vectors} \\ \\ 0 \oplus 1 \; : \text{XOR of 2 bits} \\ \\ |0\rangle \otimes |1\rangle : \text{tensor product of 2 vectors} \end{array}\right.$$

Axiom 2: Time evolution

An isolated quantum system evolves in time via unitary linear transformations:

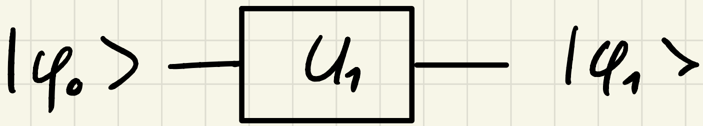
$$\underset{\text{time } t=0}{|\varphi\rangle} \longrightarrow \underset{\text{time } t>0}{U|\varphi\rangle}$$

where $U = 2^n \times 2^n$ unitary matrix:

$UU^+ = U^+U = I$ with $U^+ =$ adjoint of U

$($so $U^{-1} = U^+)$ (= complex-conjugate transpose)

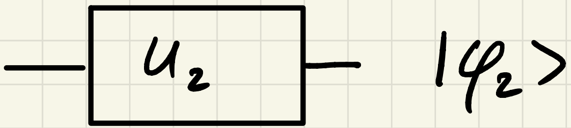
Quantum circuit:



$$|\varphi_1\rangle = U_1 |\varphi_0\rangle$$

($\Rightarrow$ reversibility!)

Another quantum circuit:



$$|\varphi_2\rangle = U_2 |\varphi_1\rangle$$

$$= U_2 U_1 |\varphi_0\rangle$$

(⚠ order ⚠)

Norm conservation:

$$\langle\varphi_1|\varphi_1\rangle = \langle\varphi_0|U_1^+ U_1|\varphi_0\rangle$$

$$= \langle\varphi_0|I|\varphi_0\rangle = \langle\varphi_0|\varphi_0\rangle = 1$$

Observe that similarly:

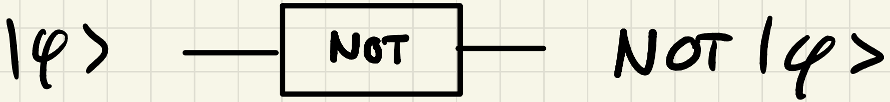
$$\langle \varphi_2 | \varphi_2 \rangle = \langle \varphi_1 | \underbrace{U_2^\dagger U_2}_{=I} | \varphi_1 \rangle = \langle \varphi_1 | \varphi_1 \rangle = 1$$

i.e. $U = U_2 U_1$ is also a unitary transformation (more formally, one can check that $UU^\dagger = U_2 U_1 U_1^\dagger U_2^\dagger = U_2 U_2^\dagger = I$)

and more generally, any quantum circuit can always be represented by a <u>single</u> unitary transformation U.

Examples of quantum circuits (elementary gates)

1) **NOT gate:** acts on a single qubit in $\mathbb{C}^2$



$$\text{NOT}\,|0\rangle = |1\rangle \ , \quad \text{NOT}\,|1\rangle = |0\rangle$$

$$\Rightarrow \text{NOT}\left(\alpha_0\,|0\rangle + \alpha_1\,|1\rangle\right) = \alpha_0\,|1\rangle + \alpha_1\,|0\rangle$$

(= reflection w.r.t. to the axis with angle 45°)

Matrix representation in $\mathbb{C}^2$:

$\langle 0 | NOT | 0 \rangle = \langle 0 | 1 \rangle = 0$ $\quad$ $\langle 0 | NOT | 1 \rangle = \langle 0 | 0 \rangle = 1$

$\langle 1 | NOT | 0 \rangle = \langle 1 | 1 \rangle = 1$ $\quad$ $\langle 1 | NOT | 1 \rangle = \langle 1 | 0 \rangle = 0$

$$\Longrightarrow NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = NOT^{\dagger} \quad \text{Hermitian}$$

and $NOT \cdot NOT^{\dagger} = NOT^{\dagger} \cdot NOT = I$ unitary

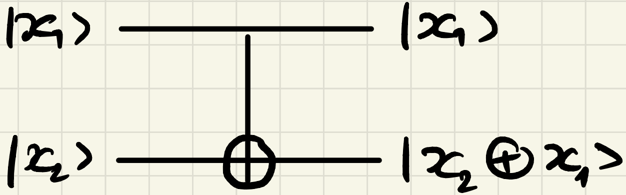
Also: $NOT\,|+\rangle = |+\rangle$, $NOT\,|-\rangle = (-1)\,|-\rangle$

2) **C-NOT gate:** acts on 2 qubits in $\mathbb{C}^2 \otimes \mathbb{C}^2 \sim \mathbb{C}^4$

$\text{CNOT}\,|00\rangle = |00\rangle$ $\qquad$ $\text{CNOT}\,|01\rangle = |01\rangle$

$\text{CNOT}\,|10\rangle = |11\rangle$ $\qquad$ $\text{CNOT}\,|11\rangle = |10\rangle$

said otherwise : $\text{CNOT}\,|x_1, x_2\rangle = |x_1, x_2 \oplus x_1\rangle$



Matrix representation in $\mathbb{C}^4$: $\text{CNOT} = \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle\downarrow & |10\rangle & |11\rangle\downarrow \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$

$CNOT^{\dagger} = CNOT$ Hermitian

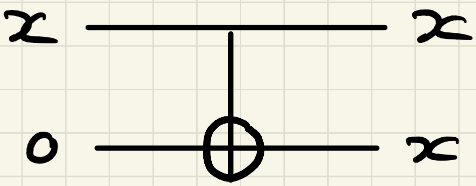
$CNOT \cdot CNOT^{\dagger} = CNOT^{\dagger} \cdot CNOT = I$ unitary

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

$\Rightarrow CNOT\ |\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$

Parenthesis

Classically, a CNOT gate can emulate a COPY gate:



But in the quantum world, copying a quantum state is impossible (no cloning thm).

Let us solve this apparent contradiction...

Consider $|\varphi\rangle \otimes |0\rangle$ as input state to the CNOT gate, with $|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$:

$$\mathrm{CNOT}\,(|\varphi\rangle \otimes |0\rangle) = \mathrm{CNOT}\,((\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes |0\rangle)$$

$$= \alpha_0 \,\mathrm{CNOT}\, |0,0\rangle + \alpha_1 \,\mathrm{CNOT}\, |1,0\rangle$$

$$= \alpha_0 |0,0\rangle + \alpha_1 |1,1\rangle = \text{Bell state}$$

$$\neq |\varphi\rangle \otimes |\varphi\rangle$$

(only states in the computational basis can be copied)

Axian 3: Measurement postulate

If an isdated quantum system is in state $|\psi\rangle \in \mathcal{H} = \mathbb{C}^{2^n}$ and one obseves the system through a measure apparatus, described by an orthonormal basis $\{|\varphi_0\rangle, |\varphi_1\rangle \dots |\varphi_{2^n-1}\rangle\}$ of $\mathcal{H}$ (note that in this course, we will always consider the computational basis), then the outcome of the measurement is given by $|\varphi_i\rangle$ $(0 \leq i \leq 2^n-1)$ with probability

$$\text{prob}(i) = |\langle \varphi_i | \psi \rangle|^2$$

Note that

$$\sum_{i=0}^{2^n-1} \text{prob}(i) = \sum_{i=0}^{2^n-1} \overline{\langle \varphi_i | \psi \rangle} \langle \varphi_i | \psi \rangle$$

$$= \sum_{i=0}^{2^n-1} \langle \psi | \varphi_i \rangle \langle \varphi_i | \psi \rangle = \langle \psi | \underbrace{\left(\sum_{i=0}^{2^n-1} |\varphi_i\rangle\langle\varphi_i| \right)}_{=I} |\psi\rangle$$

$$= \langle \psi | I | \psi \rangle = \langle \psi | \psi \rangle = 1$$

Observe that

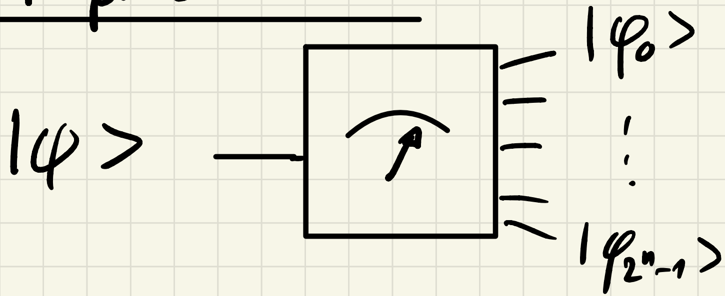
$$|\varphi_i\rangle\langle\varphi_i| = \begin{array}{c} \begin{pmatrix} 0 & & & & \\ & \ddots & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 0 \end{pmatrix} \begin{array}{l} \\ \\ \leftarrow i\text{th row} \\ \\ \\ \end{array} \\ \uparrow \\ i\text{th column} \end{array}$$

is a <u>rank-one</u> matrix

which is also a <u>projector</u> matrix (on $|\varphi_i\rangle$)

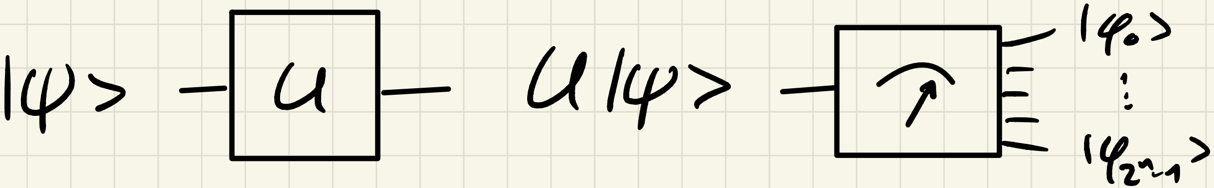
(Later in the course, we will see a more general definition of measurement with projectors.)

Graphical representation :



$$\text{prob}(i) = |\langle \varphi_i | \psi \rangle|^2$$

and with the addition of a quantum circuit U:



$$\text{prob}(i) = |\langle \varphi_i | U | \psi \rangle|^2$$

Axiom 4: Composition of quantum systems

system 1 : n_1 qubits $\mathcal{H}_1 = (\mathbb{C}^2)^{\otimes n_1}$ (dimension 2^{n_1})

system 2 : n_2 qubits $\mathcal{H}_2 = (\mathbb{C}^2)^{\otimes n_2}$ (dimension 2^{n_2})

$\longrightarrow$ n_1+n_2 qubits $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = (\mathbb{C}^2)^{\otimes(n_1+n_2)}$ (dim. $2^{n_1+n_2}$)

Product states and entangled states

Not all states in $\mathcal{H}$ can be written as

$|\varphi_1\rangle \otimes |\varphi_2\rangle$: these are <u>product states</u>

Examples in $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$: (2 qubits)

$$|0,0\rangle = |0\rangle \otimes |0\rangle$$

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

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

Counter-examples are entangled states:

$$\frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,1\rangle\right) \quad \text{Bell state} \quad \neq |\varphi_1\rangle \otimes |\varphi_2\rangle$$

Easy criterion: $\alpha_{00}|0,0\rangle + \alpha_{01}|0,1\rangle + \alpha_{10}|1,0\rangle + \alpha_{11}|1,1\rangle$

is a product state iff $\det\begin{pmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{pmatrix} = 0$

Quantum circuits (David Deutsch)

Remember that a quantum circuit operating on n qubits can always be represented by a $2^n \times 2^n$ unitary matrix $\mathcal{U}$.

1) 1-qubit gates ($\mathcal{H} = \mathbb{C}^2$)

- NOT gate: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

  ↑ we will keep this notation from now on

- **Hadamard gate**: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\begin{cases} H\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle \\ H\,|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle \end{cases}$$

$$|\varphi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$$

$$\Rightarrow\ H\,|\varphi\rangle = \alpha_0\,|+\rangle + \alpha_1\,|-\rangle$$

$$= \frac{\alpha_0 + \alpha_1}{\sqrt{2}}\,|0\rangle + \frac{\alpha_0 - \alpha_1}{\sqrt{2}}\,|1\rangle$$

Observe that $H = H^{\dagger}$ and $HH^{\dagger} = I$ (unitary matrix)

- Phase gates Z, S and T : (= unitary matrices also!)

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & \underbrace{e^{i\pi}}_{=-1} \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & \underbrace{e^{i\pi/2}}_{=i} \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = (-1)|1\rangle$$

$$|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \implies Z|\varphi\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle$$

(same for S and T)

Observe that $Z = S^2 = T^4$ and $S = T^2$

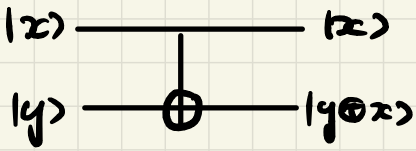
Theorem (without proof)

Any 2×2 unitary matrix U can be approximated by a product of gates H, S, T in the following sense: $\forall \delta > 0$, $\exists V$ a product of $O(\frac{1}{\delta})$ matrices H, S, T such that $\| U - V \| < \delta$

(where $\|\cdot\|$ is some matrix norm)

2) 2-qubit gates ($\mathcal{H} = \mathbb{C}^4$)

- **CNOT gate** : $\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$



$\text{CNOT}\,|00\rangle = |00\rangle \qquad \text{CNOT}\,|01\rangle = |01\rangle$

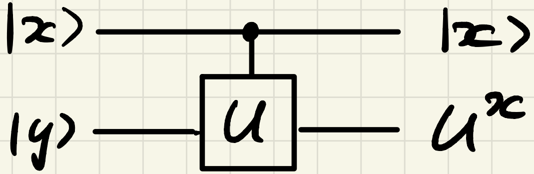
$\text{CNOT}\,|10\rangle = |11\rangle \qquad \text{CNOT}\,|11\rangle = |10\rangle$

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

$$\Longrightarrow \text{CNOT}|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle$$

⚠ input & output states ≠ product states in general!

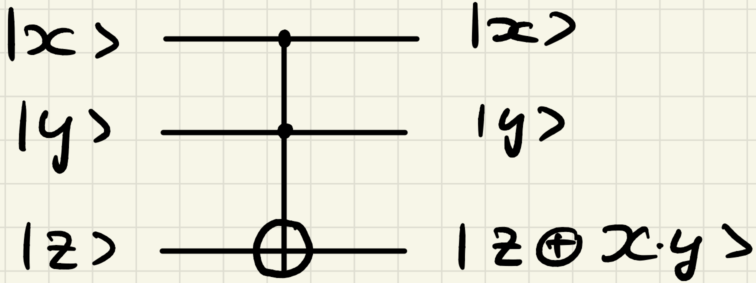
- **Controlled-U gate**: (where U = 2x2 unitary matrix)



$$U^x|y\rangle = \begin{cases} |y\rangle & \text{if } x=0 \\ U|y\rangle & \text{if } x=1 \end{cases}$$

3) Multiple qubit gates

- **Toffoli gate** (CCNOT) $\mathcal{H}=\mathbb{C}^8$ (⚠ not $\mathbb{C}^6$)



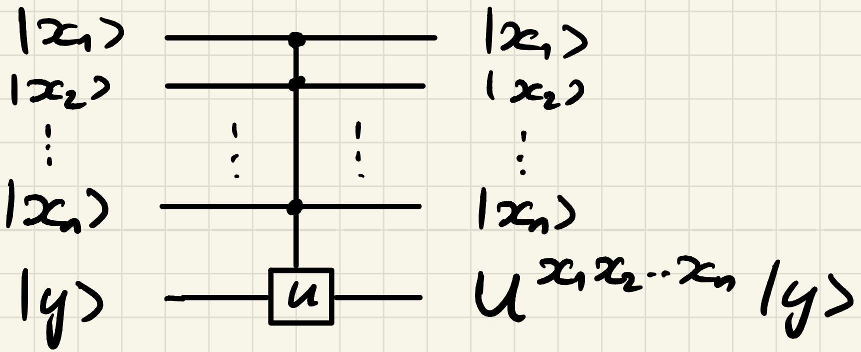
Matrix representation → exercises!

Remark

- Classically, it is not possible to create a Toffoli gate from CNOT & 1-bit gates.
- In the quantum world, this is possible (using more precisely CNOT, H, T & S gates)

→ exercises!

• Multicontrol gates $\quad \mathcal{H} = \mathbb{C}^{2^{n+1}}$



U acts on $|y\rangle$ only if $x_1 = x_2 = \dots = x_n = 1$

realization with $n=3$ → exercises!

Theorem (A. Barenco & al.) (without proof)

Any $2^n \times 2^n$ unitary matrix U can be approximated (with arbitrary precision) by a circuit made only of gates T, S, H & CNOT.

The number of gates needed for this approximation depends on the unitary matrix U (may be exp. in n).

Remark: Without the T gate, it can be shown that no quantum advantage can be obtained over classical circuits. (= Gottesman-Knill thm)