

# Quantum computation: lecture 1

- General introduction
- Classical circuits - Post's theorem
- Reversible gates

~~• Linear algebra in Dirac's notation~~

# Introduction: Chronology

80's: - Feynman: idea that using quantum properties of matter at a microscopic level could help compute more efficiently

- Bennett, Wiesner, Deutsch: quantum circuits

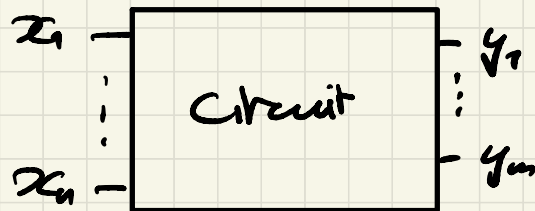
90's: - quantum algorithms (Deutsch-Josza, Simon, Bernstein-Vazirani, Shor, Grover)

2000's: realization of quantum computers ...

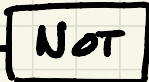
## Classical circuits


Let  $f: \{0,1\}^n \rightarrow \{0,1\}^m$  be a Boolean function.  
 $(x_1 \dots x_n) \mapsto (y_1 \dots y_m) = f(x_1 \dots x_n)$

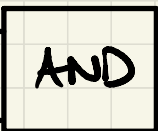
Does there exist a classical circuit computing  
in an automated manner the value of  $f$  for  
every input  $(x_1 \dots x_n)$ ?

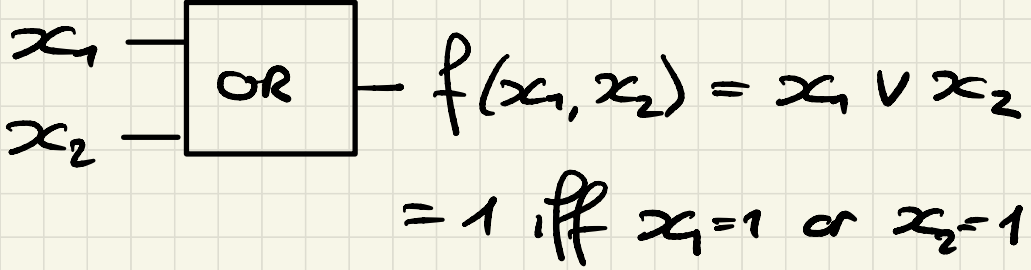


# Examples of simple circuits (= elementary gates) and associated Boolean functions

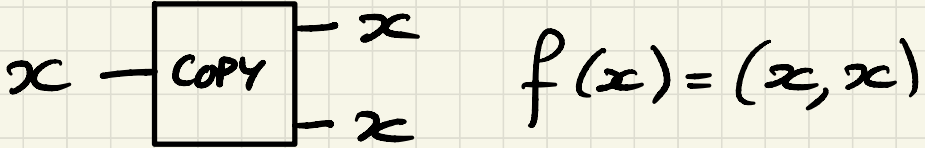
a) NOT gate:  $x$  —  —  $f(x) = \bar{x} = \begin{cases} 1 & \text{if } x=0 \\ 0 & \text{if } \bar{x}=1 \end{cases}$

(equivalent to:  $x$  —  —  $f(x) = x \oplus 1 = \bar{x}$ )

b) AND gate:  $x_1$  —  —  $f(x_1, x_2) = x_1 \wedge x_2$   
 $= 1$  iff  $x_1=1$  and  $x_2=1$

c) OR gate:   $f(x_1, x_2) = x_1 \vee x_2$   
 $= 1$  iff  $x_1=1$  or  $x_2=1$

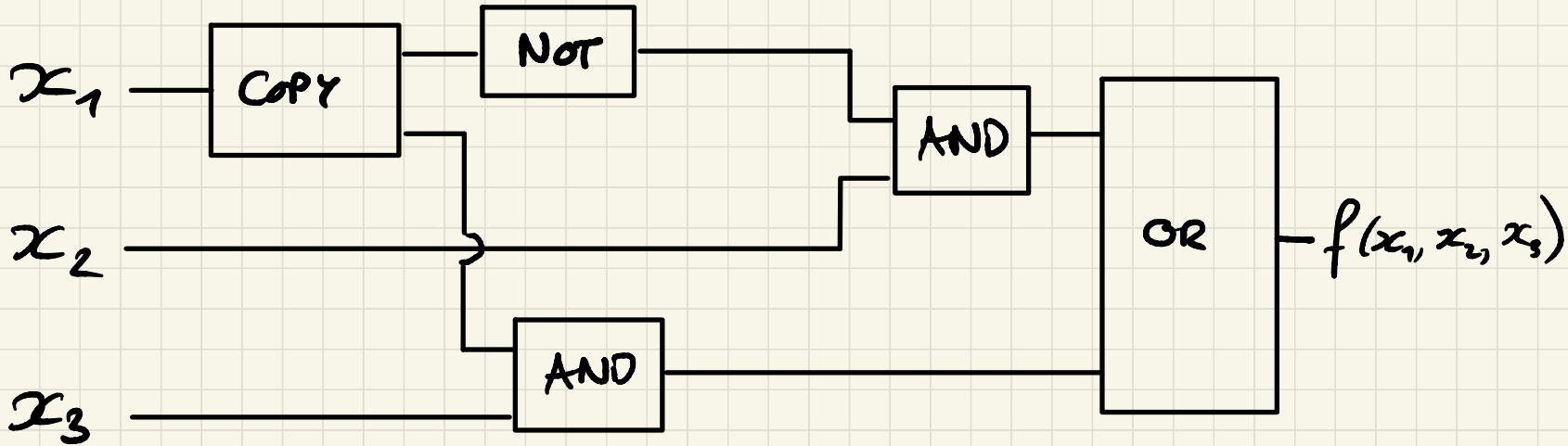
NB: this is the non-exclusive OR

d) COPY gate:   $f(x) = (x, x)$

NB: not really a gate, as it can be realized physically by joining two wires together

Example of a circuit for

$$f(x_1, x_2, x_3) = (\bar{x}_1 \wedge x_2) \vee (x_1 \wedge x_3)$$



## Formal definition of a Boolean circuit

A Boolean circuit is a directed, acyclic graph (DAG) with  $n$ -~~q~~bits input and  $m$ -~~q~~bits output, whose vertices are logic gates and edges are wires.

Theorem (Emil Post, 1921)

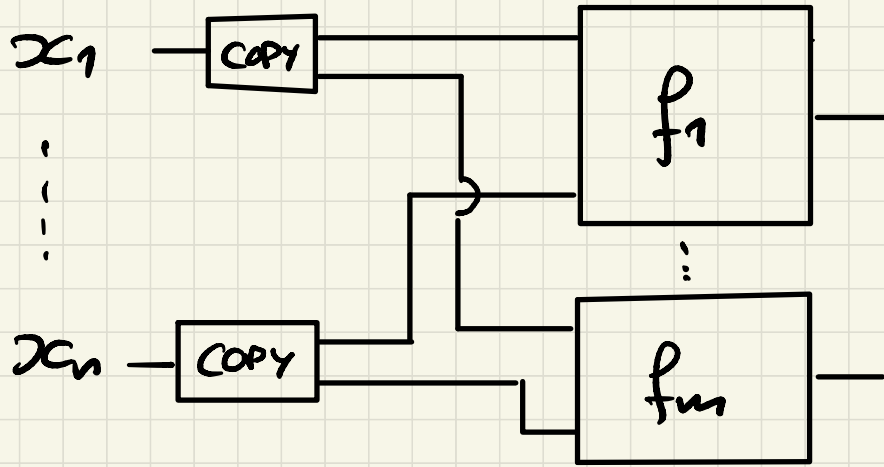
Every Boolean function  $f$  can be realized by a Boolean circuit made only of the elementary gates AND, OR, NOT and COPY.

This theorem therefore implies that this set of 4 gates is universal.

# Proof

Let  $f: \{0,1\}^n \rightarrow \{0,1\}^m$  be a Boolean function

1)  $f = (f_1, \dots, f_m)$  in general, but the theorem needs only to be proven for  $m=1$  because:





3) Observe now that for  $a \in \{0,1\}^n$ :

$$C_a(x) = \phi_{a_1}(x_1) \wedge \dots \wedge \phi_{a_n}(x_n)$$

↑                      ↑  
AND's

where  $\phi_{a_j}(x_j) = 1_{\{x_j = a_j\}} = \begin{cases} x_j & \text{if } a_j = 1 \\ \bar{x}_j & \text{if } a_j = 0 \end{cases}$

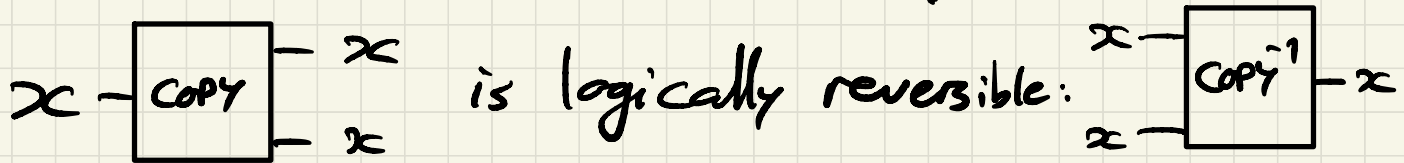
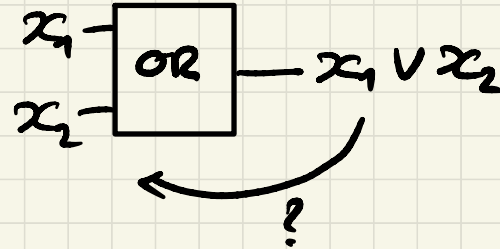
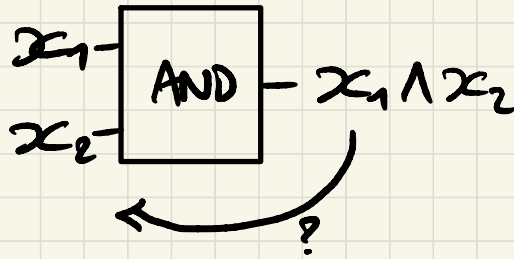
↑  
NOT

So the computation of  $f(x_1 \dots x_n)$  can be realized exclusively with COPY, OR, AND & NOT gates.

#

# Irreversibility

The gates AND, OR & COPY are irreversible:



but its inverse deletes a bit: physically,  
it dissipates heat = irreversible process!

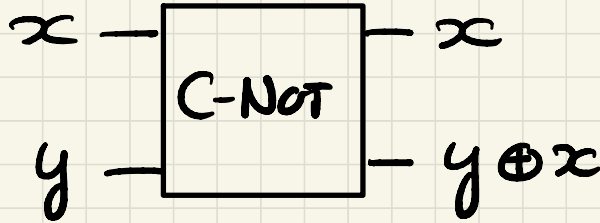
## Reversible gates

In quantum circuits, irreversible gates are forbidden. Fortunately, the previous gates can be emulated by reversible gates:

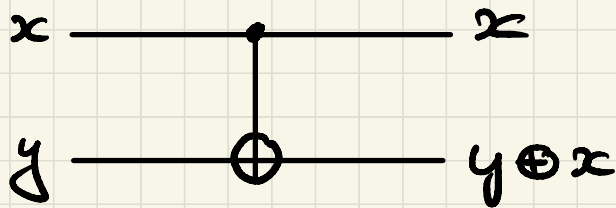
1) NOT gate:  $x \text{ --- } \boxed{\text{NOT}} \text{ --- } f(x) = x \oplus 1 = \bar{x}$

is obviously reversible (apply it twice to recover the initial state)

## 2) Controlled-NOT (C-NOT) gate



Equivalent symbol:

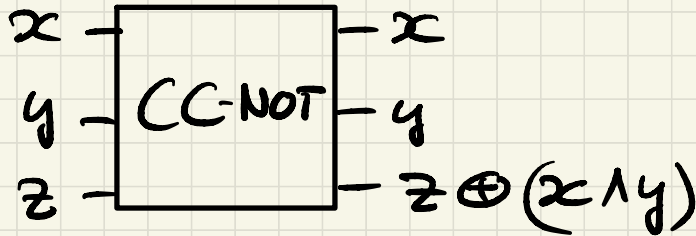


$$f(x, y) = (x, y \overset{\text{XOR}}{\oplus} x)$$

$$\begin{cases} f(0, y) = (0, y) \\ f(1, y) = (0, y \oplus 1) = (1, \bar{y}) \end{cases}$$

This gate is also reversible  
(again, apply it twice)

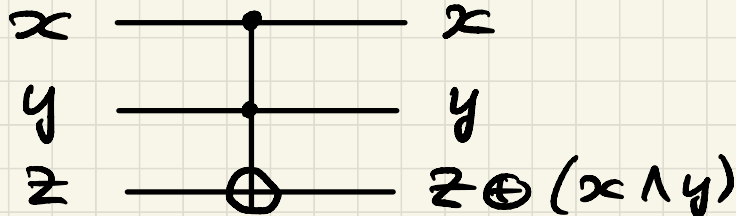
### 3) Toffoli gate (or CC-NOT gate)



$$f(x, y, z) = (x, y, z \oplus (x \wedge y))$$

$$\begin{cases} f(x, y, z) = (x, y, z) & \text{as long as } x=0 \text{ or } y=0 \\ f(1, 1, z) = (x, y, z \oplus 1) = (x, y, \bar{z}) \end{cases}$$

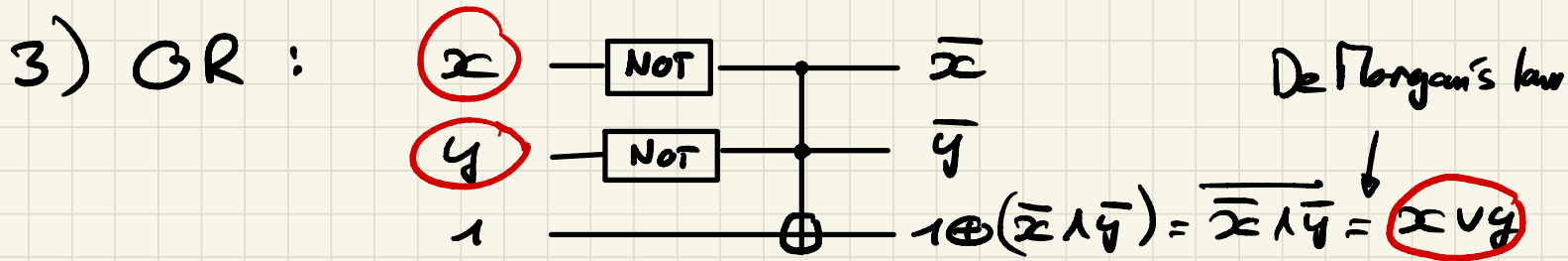
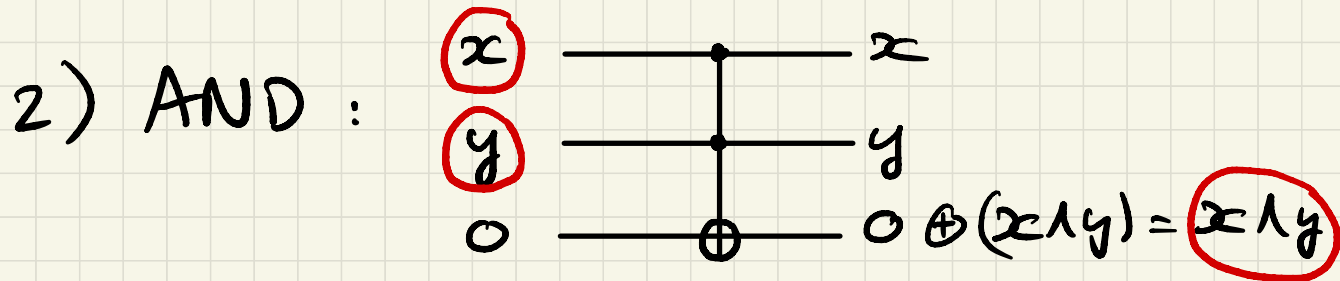
Equivalent symbol:

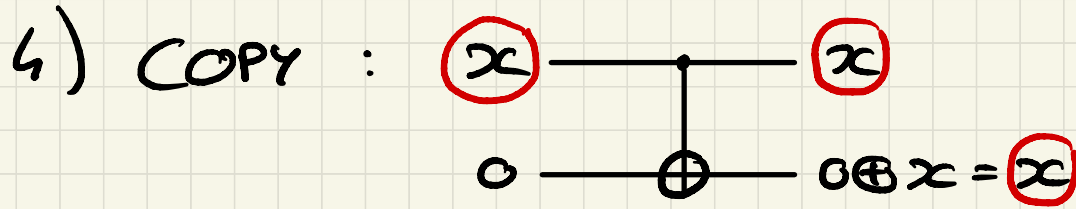


Again a reversible gate  
(apply it twice)

All previously seen gates can be retrieved from these 3 reversible gates: (use red input/output)

1) NOT : obviously...





So the set of 3 gates NOT, C-NOT, CC-NOT is also universal, according to Post's Thm.


Note that actually, the NOT & C-NOT gates can themselves be retrieved from CC-NOT gates; but the reciprocal statement is wrong.

# 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  $|\psi\rangle$  in a Hilbert space  $\mathcal{H}$ .

In particular, the state of a system of  $n$  qubits is represented by a unit vector in  $\mathcal{H} = \mathbb{C}^{2^n} \sim \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}}$ .   $\|\psi\rangle\|^2 \neq n$  for  $n$  qubits!

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

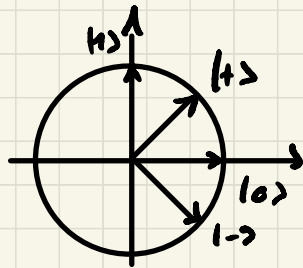
$$\langle x'_1, \dots, x'_n | x_1, \dots, x_n \rangle = \delta_{x'_1 x_1} \dots \delta_{x'_n x_n}$$

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

$$1 = \langle \varphi | \varphi \rangle = \sum_{x_1 \dots x_n \in \{0, 1\}} |\alpha_{x_1, \dots, x_n}|^2$$

$n=1$ :  $|\varphi\rangle = (\cos\theta)|0\rangle + (\sin\theta)|1\rangle, (\cos\theta)^2 + (\sin\theta)^2 = 1$

Two particular cases:  $\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$   
( $\theta = +45^\circ$  &  $-45^\circ$ )



⚠ Various notations here!

{  $|0\rangle + |1\rangle$  : addition of 2 vectors  
 $0 \oplus 1$  : XOR of 2 bits  
 $|0\rangle \otimes |1\rangle$  : tensor product of 2 vectors

## Axiom 2: Time evolution

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

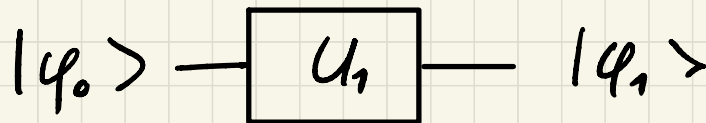
$$\begin{array}{ccc} |\varphi\rangle & \longrightarrow & U|\varphi\rangle \\ \text{time } t=0 & & \text{time } t>0 \end{array}$$

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

$$UU^\dagger = U^\dagger U = I \quad \text{with } U^\dagger = \text{adjoint of } U$$

$$\left( \text{so } U^{-1} = U^\dagger \right) \quad \left( = \text{complex-conjugate transpose} \right)$$

Quantum circuit:



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

( $\Rightarrow$  reversibility!)

Norm conservation:

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

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

Another quantum circuit:



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

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

( $\Delta$  order  $\Delta$ )

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  $U U^\dagger = U_2 U_1 U_1^\dagger U_2^\dagger = U_2 (U_1 U_1^\dagger) U_2^\dagger = U_2 (U_2^\dagger = I)$ )

and more generally, any quantum circuit  
can always be represented by a single  
unitary transformation  $U$ .

## Examples of quantum circuits (elementary gates)

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

$$|\varphi\rangle \text{ --- } \boxed{\text{NOT}} \text{ --- } \text{NOT } |\varphi\rangle$$

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

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

(= reflection w.r.t. to the axis with angle  $45^\circ$ )

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

$$\langle 0 | \text{NOT} | 0 \rangle = \langle 0 | 1 \rangle = 0$$

$$\langle 0 | \text{NOT} | 1 \rangle = \langle 0 | 0 \rangle = 1$$

$$\langle 1 | \text{NOT} | 0 \rangle = \langle 1 | 1 \rangle = 1$$

$$\langle 1 | \text{NOT} | 1 \rangle = \langle 1 | 0 \rangle = 0$$

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

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

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

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

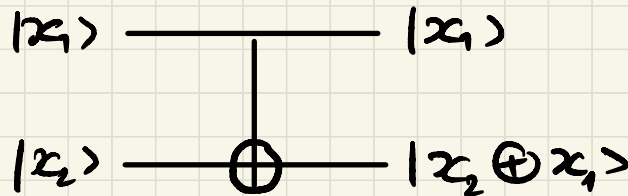
$$\text{CNOT } |00\rangle = |00\rangle$$

$$\text{CNOT } |01\rangle = |01\rangle$$

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

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

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



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

$$CNOT^\dagger = CNOT \quad \text{Hermitian}$$

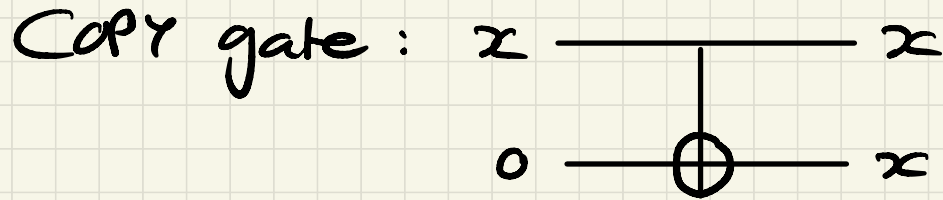
$$CNOT \cdot CNOT^\dagger = CNOT^\dagger \cdot CNOT = I \quad \text{Unitary}$$

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

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

# Parenthesis

Classically, a CNOT gate can emulate a



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

Let us solve this apparent contradiction...

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

$$\begin{aligned} \text{CNOT}(|\varphi\rangle \otimes |0\rangle) &= \text{CNOT}((\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes |0\rangle) \\ &= \alpha_0 \text{CNOT}(|0,0\rangle) + \alpha_1 \text{CNOT}(|1,0\rangle) \\ &= \alpha_0 |0,0\rangle + \alpha_1 |1,1\rangle = \text{Bell state} \\ &\neq |\varphi\rangle \otimes |\varphi\rangle \end{aligned}$$

(only states in the computational basis can be copied)

## Axiom 3: Measurement postulate

If an isolated quantum system is in state  $|\psi\rangle \in \mathcal{H} = \mathbb{C}^{2^n}$  and one observes 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

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

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

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

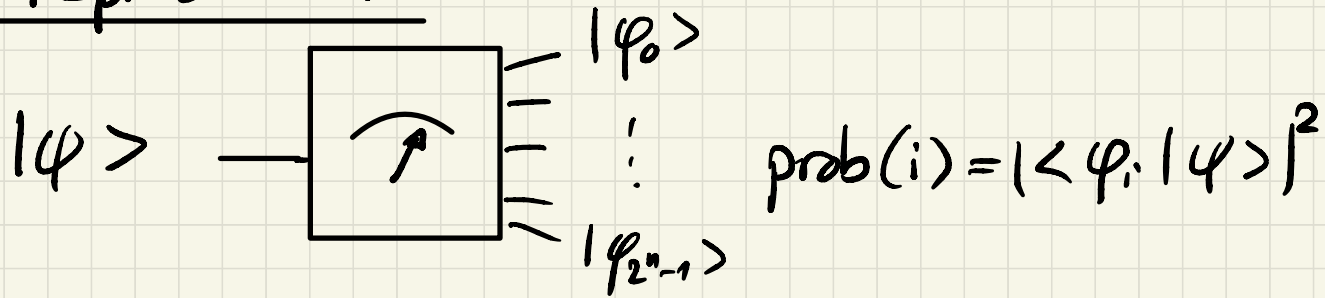
Observe that  $|\varphi_i\rangle\langle\varphi_i| = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 \\ 0 & & & & \ddots \end{pmatrix} \leftarrow \begin{matrix} \text{ith row} \\ \text{ith column} \end{matrix}$

is a rank-one matrix

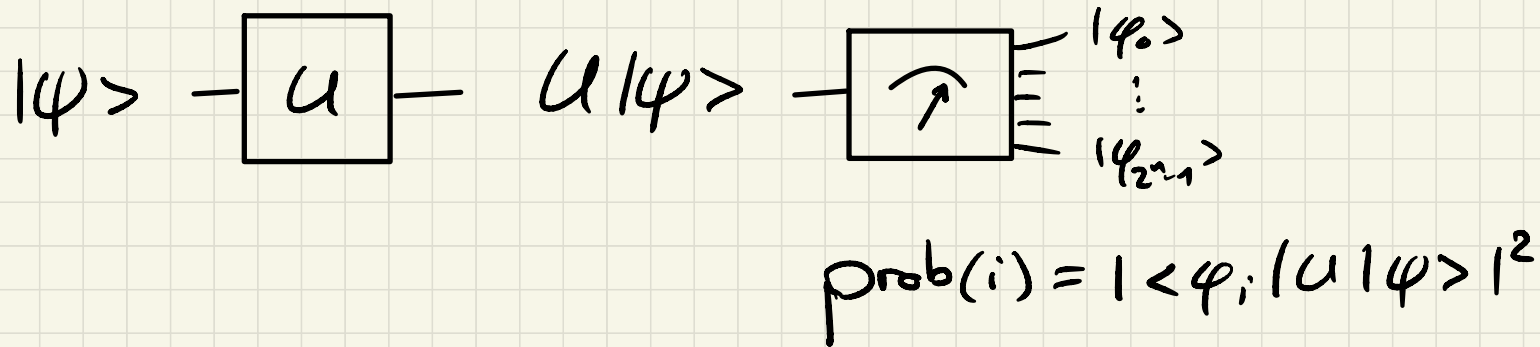
which is also a projector matrix (on  $|\varphi_i\rangle$ )

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

Graphical representation:



and with the addition of a quantum circuit  $U$ :



## 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  $2^{n_2}$ )

$\rightarrow n_1 + n_2$  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 product states

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

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

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

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

Counter-examples are entangled states:

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

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  $U$ .

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

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

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

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

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

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

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

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

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

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

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

(Same for S and T)

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

## Theorem (without proof)

Any  $2 \times 2$  unitary matrix  $U$  can be approximated by a product of gates  $H, S, T$  in the following

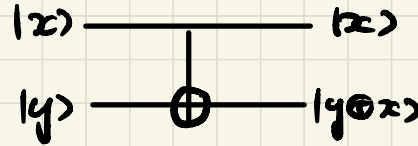
sense:  $\forall \delta > 0, \exists V$  a product of  $O(\frac{1}{\delta})$  matrices

$H, S, T$  such that  $\|U - V\| < \delta$

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

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

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



$$\text{CNOT} |00\rangle = |00\rangle \quad \text{CNOT} |01\rangle = |01\rangle$$

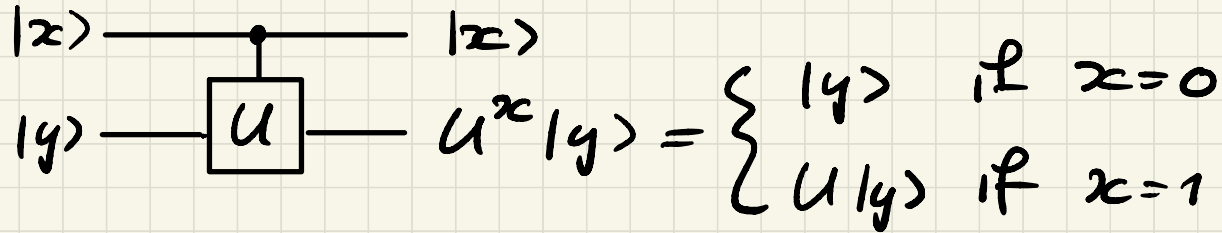
$$\text{CNOT} |10\rangle = |11\rangle \quad \text{CNOT} |11\rangle = |10\rangle$$

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

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

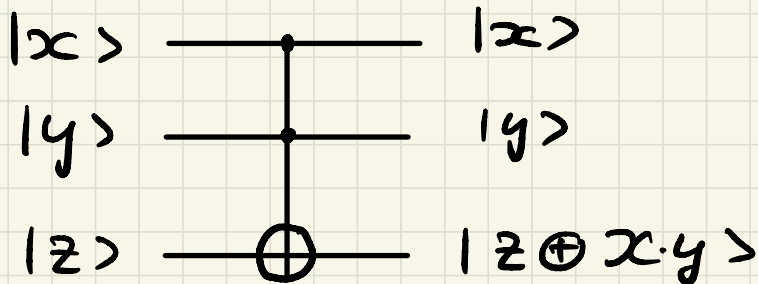
⚠ input & output states  $\neq$  product states in general!

- Controlled-U gate: (where  $U = 2 \times 2$  unitary matrix)



### 3) Multiple qubit gates

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

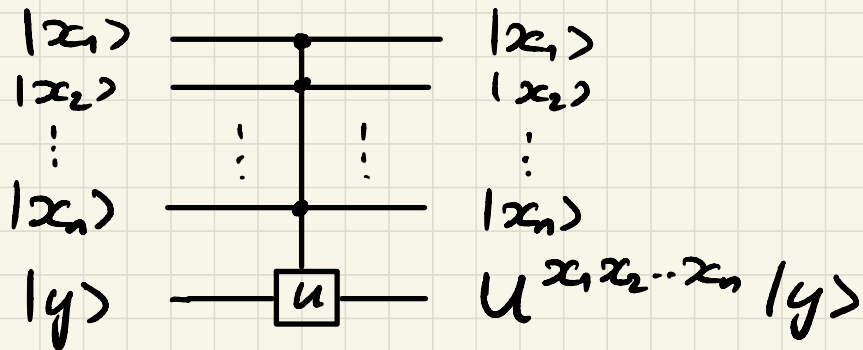


Matrix representation  $\rightarrow$  exercises!

## 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)  
 $\rightarrow$  exercises!

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



$U$  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 <sup>exponential</sup> quantum advantage can be obtained over classical circuits.  
(= Gottesman-Knill theorem)