Computação Quântica

Parte 2

PedroCal |IST> = 75699 |IST>

HonQ- 2015

Portas de Multiplos Qubits

- Classicamente: AND, OR, XOR, NAND e NOR

- Estas portas podem ser formadas apenas utilizando a porta NAND => **Porta Universal**

Quanticamente:

-A mais importante porta de múltiplos qubits é a porta Controlled-NOT ou C-NOT

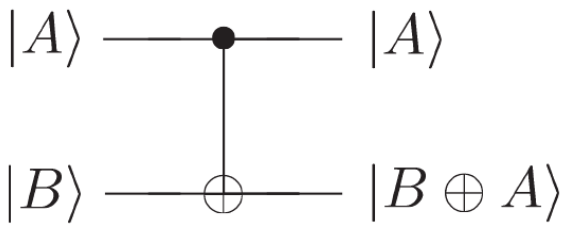
DOIS INPUT QUBITS

CONTROL QUBIT **TARGET QUBIT**

controlled-NOT

a) Se **CONTROL QUBIT** for 0, não acontece nada ao target qubit.

b) Se **CONTROL QUBIT** for 1, o valor do target bit é “flippado”.

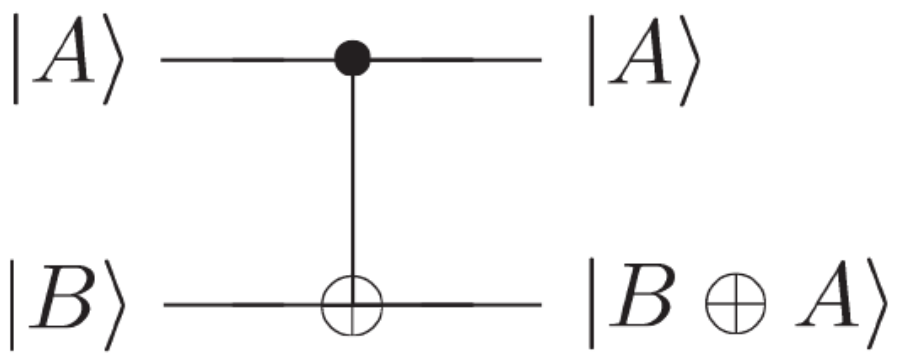


$$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle$$

- Outra maneira de ver a coisa:

$$|A, B\rangle \rightarrow |A, B \oplus A\rangle$$

controlled-NOT



-Outra ainda:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Note-se que é unitária

-Será que existem portas quânticas análogas às portas **NAND** e **XOR** clássicas, do mesmo modo que existe a porta **CNOT** como análoga da **NOT**?


NÃO

-A razão é porque as portas NAND e XOR clássicas são **IRREVERSÍVEIS**

- Se soubermos o resultado de A *XOR* B não nos é possível extrair os valores de A e de B

- Há portanto uma perda de informação.

- Como as portas quânticas são representadas por **matrizes unitárias**, e qualquer matriz unitária **tem a sua inversa** (também ela unitária), então é sempre possível inverter o efeito de uma porta quântica.

-Um teorema importante: Qualquer porta lógica de multiplos qubits pode ser decomposta em portas de um bit e portas C-NOT

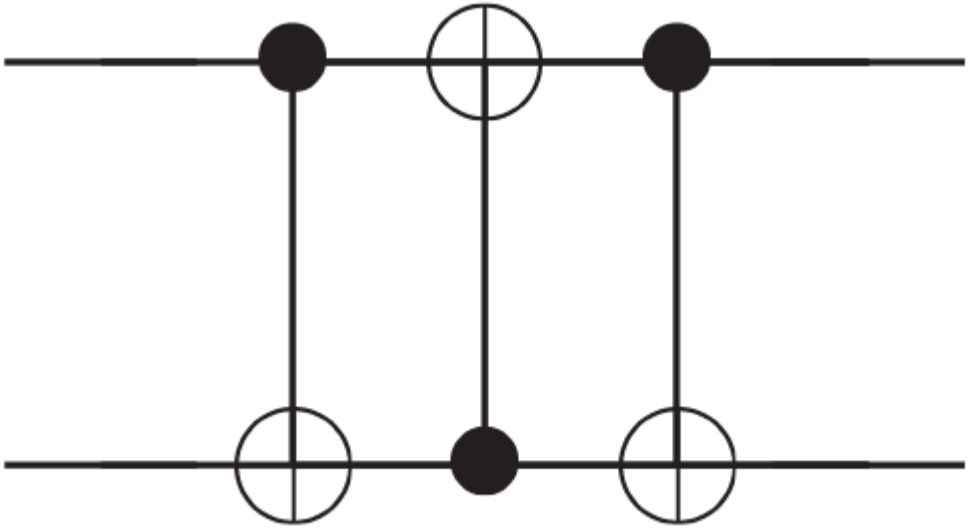
Circuitos Quânticos

-Lêem-se da esquerda para a direita

-Já podemos analisar um circuito quântico.

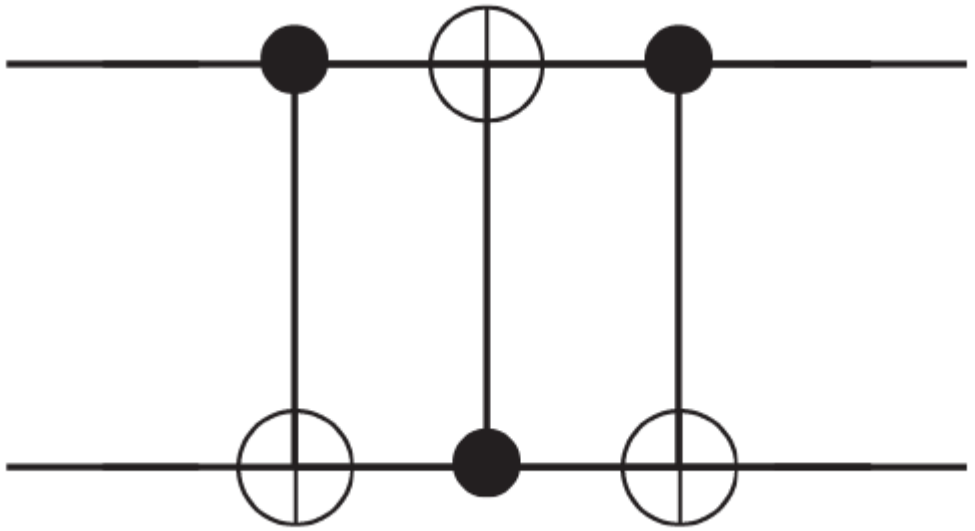
Exemplo, circuito que troca os qubits

$|a, b\rangle$



Exemplo, circuito que troca os qubits

$|a, b\rangle$



$$
\begin{aligned}
|a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\
&\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
&\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle \, ,
\end{aligned}
$$

-Há características de circuitos clássicos que **não** são permitidas em circuitos quânticos:

i) Loops

ii) FANIN

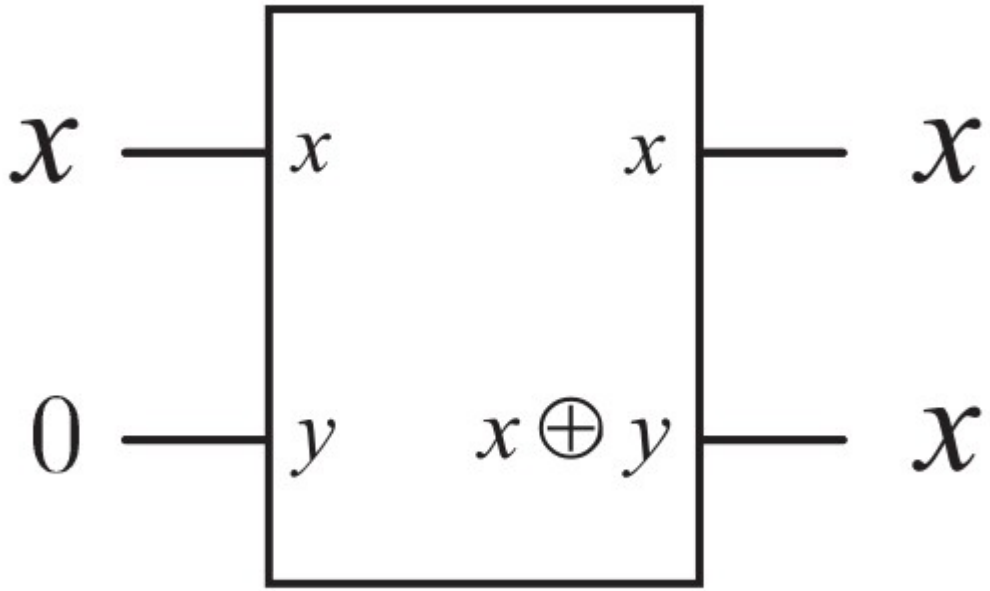
iii) FANOUT

-Vamos já ver que **copiar um qubit é expressamente proíbido** pela mecânica quântica, o que torna a operação FANOUT impossível.

Será que se pode copiar um qubit para um target qubit?

Não.

-Classicamente como é que se copia um bit?



Agora quanticamente:

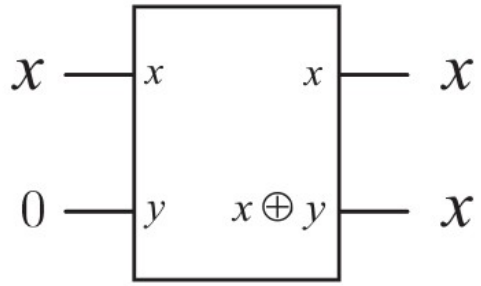
Se queremos copiar o qubit:

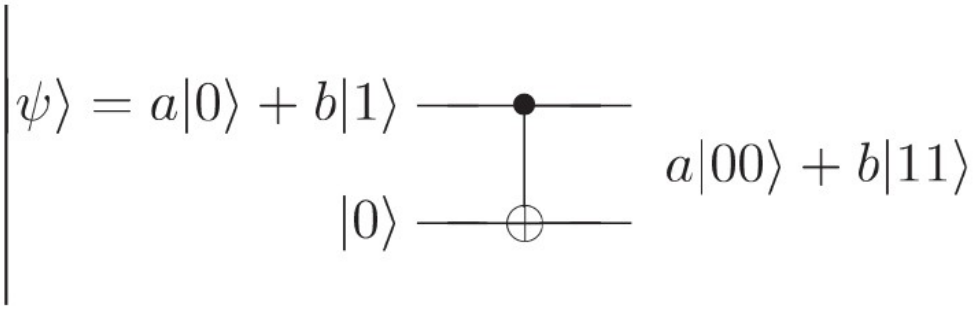
$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Então queremos que o estado final total dos dois qubits seja:

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

-Vamos tentar fazer quanticamente o análogo ao que se faz classicamente para copiar um bit





-Estado total inicial:

$$\left[a\,|0\rangle + b\,|1\rangle\right]|0\rangle = a\,|00\rangle + b\,|10\rangle$$

-Passando pela CNOT, o estado final total é:

$$a\,|00\rangle + b\,|11\rangle$$

-Estado final obtido:

$$a\,|00\rangle + b\,|11\rangle$$

-Estado final pretendido:

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

- A não ser que *ab=0,* o circuito não copia o qubit.

- É impossível copiar um qubit com um estado quântico desconhecido

-Note-se que copiar um qubit seria ganhar informação.