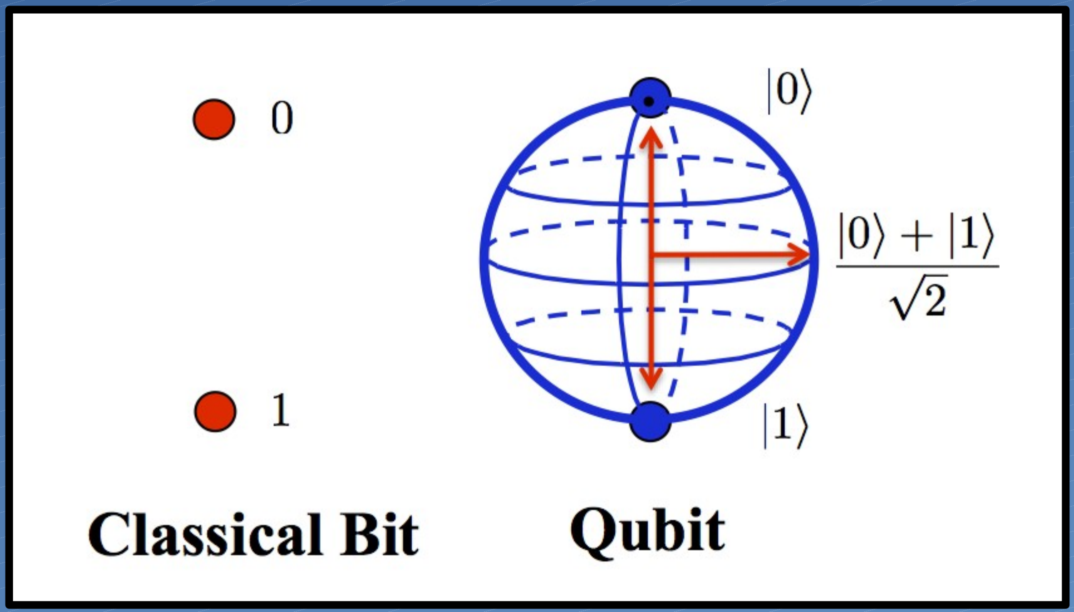
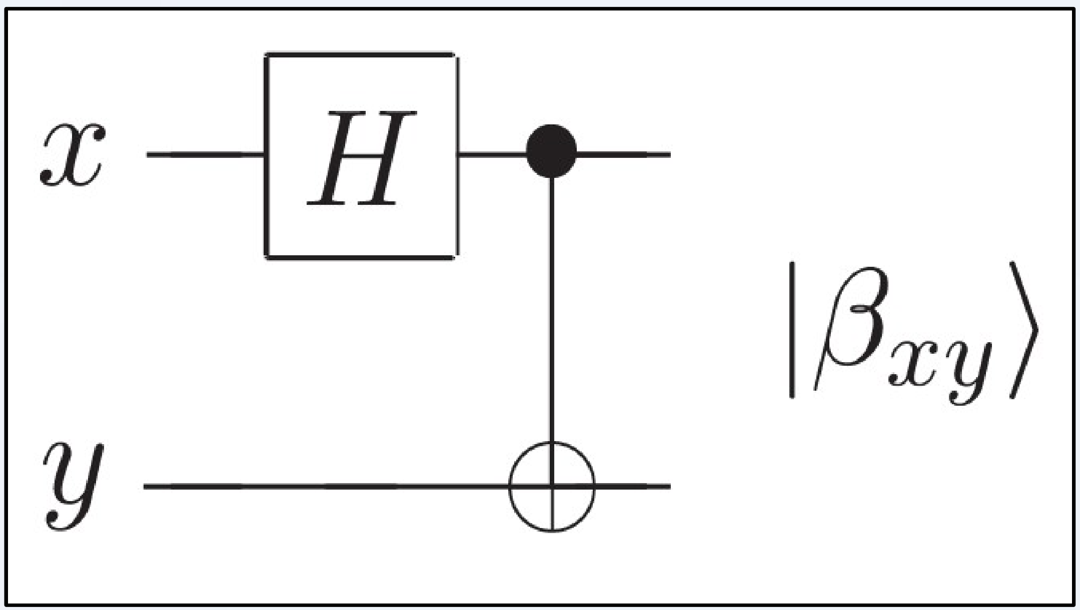
Quantum Computation



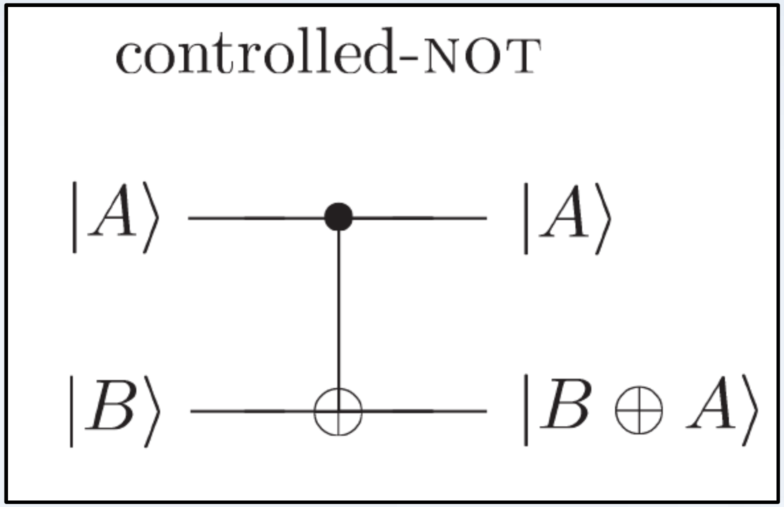
Pedro Cal - Hands on Quantum Mechanics 2015

- **Considere-se agora este circuito**



Estados de Bell

- **Recordar que o efeito de uma porta *C-NOT* é**



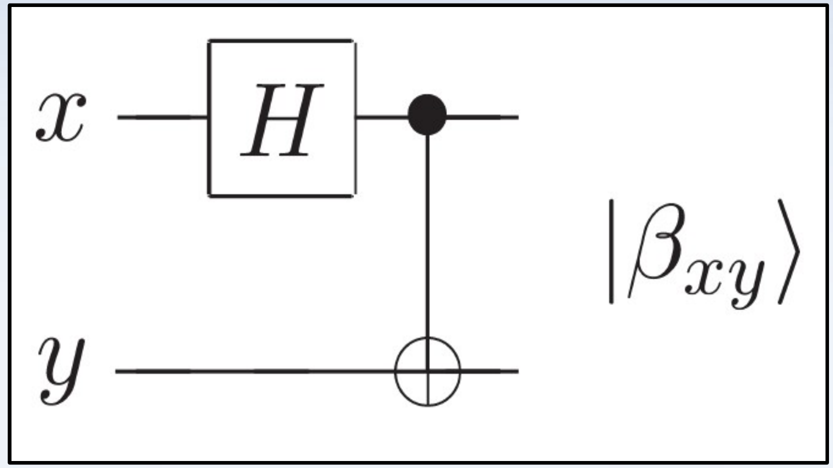
$$|00\rangle \rightarrow |00\rangle;\ \ |01\rangle \rightarrow |01\rangle;\ \ |10\rangle \rightarrow |11\rangle;\ \ |11\rangle \rightarrow |10\rangle$$

- **E que o efeito de uma porta *Hadamard* é**

$$\alpha\,|0\rangle + \beta\,|1\rangle \;\text{———}\boxed{H}\text{———}\; \alpha\,\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Estados de Bell

- **Voltemos ao circuito**



- **Se por exemplo o input for**

$$|00\rangle$$

- **Então ao passar o primeiro qubit pela porta Hadamard**

$$(|0\rangle + |1\rangle)|0\rangle/\sqrt{2}$$

- **E depois ao passar pela porta C-NOT**

$$(|00\rangle + |11\rangle)/\sqrt{2}$$

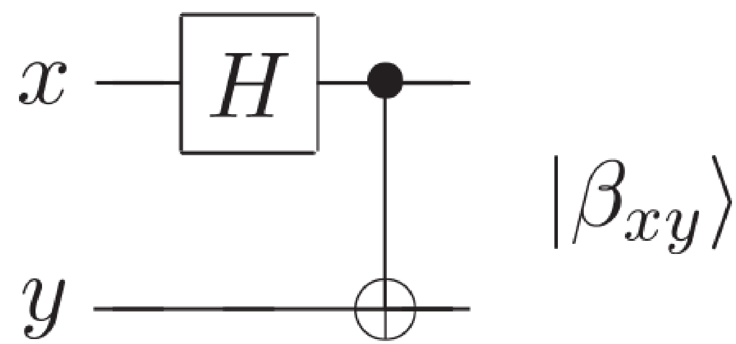
Estados de Bell

- **Este estado é um dos denominados *pares EPR***

$$(|00\rangle + |11\rangle)/\sqrt{2}$$

- **Fazendo o mesmo para os outros inputs possíveis, obtemos os restantes pares EPR**

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$



Quantum Teleportation

- **A Alice e o Bob conhecem-se há muito tempo, juntos criaram um par EPR, do qual cada um deles ficou com um qubit**

- **Muitos anos depois, o Bob está escondido numa cave num país estrangeiro**

- **A missão da Alice é enviar-lhe um novo qubit**

$$\boxed{|\psi\rangle}$$

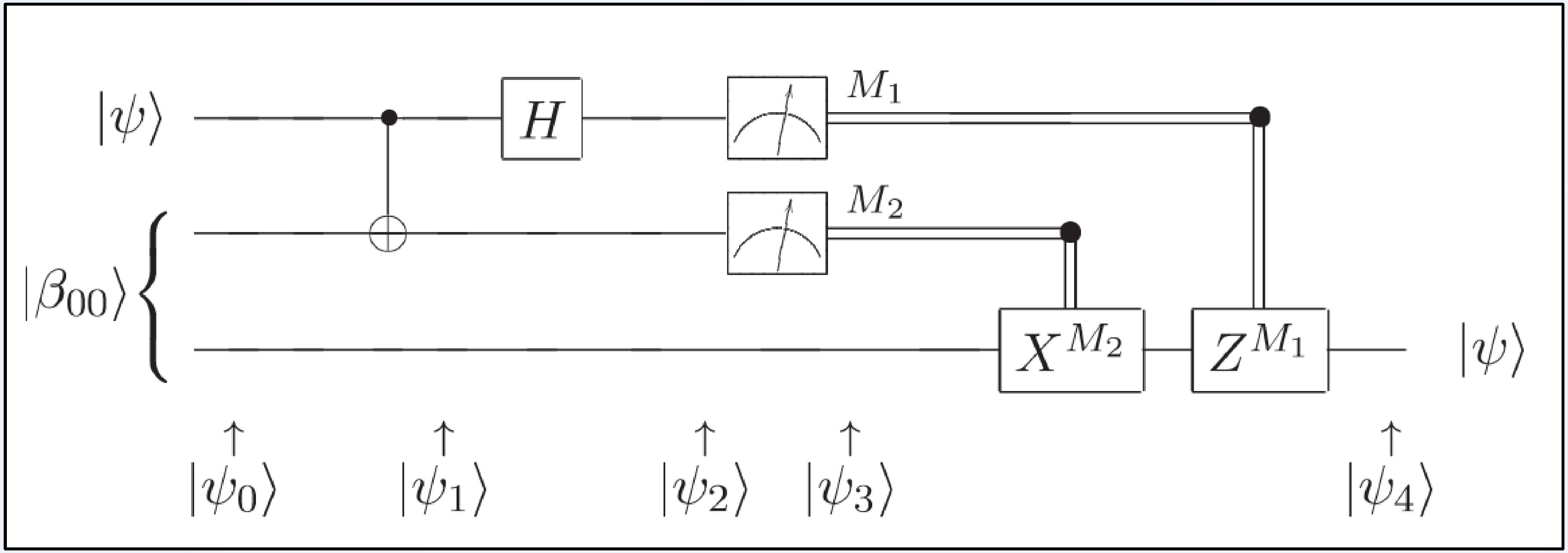
A Alice não sabe o estado deste qubit

- **A Alice só pode enviar ao Bob informação clássica!**

Quantum Teleportation

- **Como é que a Alice consegue fazer isto? Parece impossível**
- **Mas não é**

- **O circuito que consegue fazer isto é**

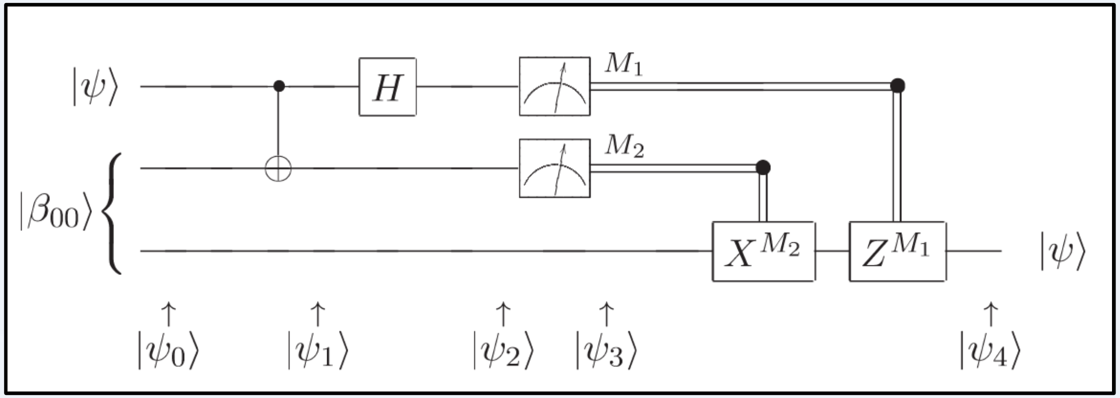


- **Os 2 qubits de cima são da Alice, e o de baixo é do Bob**

Quantum Teleportation

- **Analisemos em detalhe, é mais simples do que parece**
- **O qubit a transportar é**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

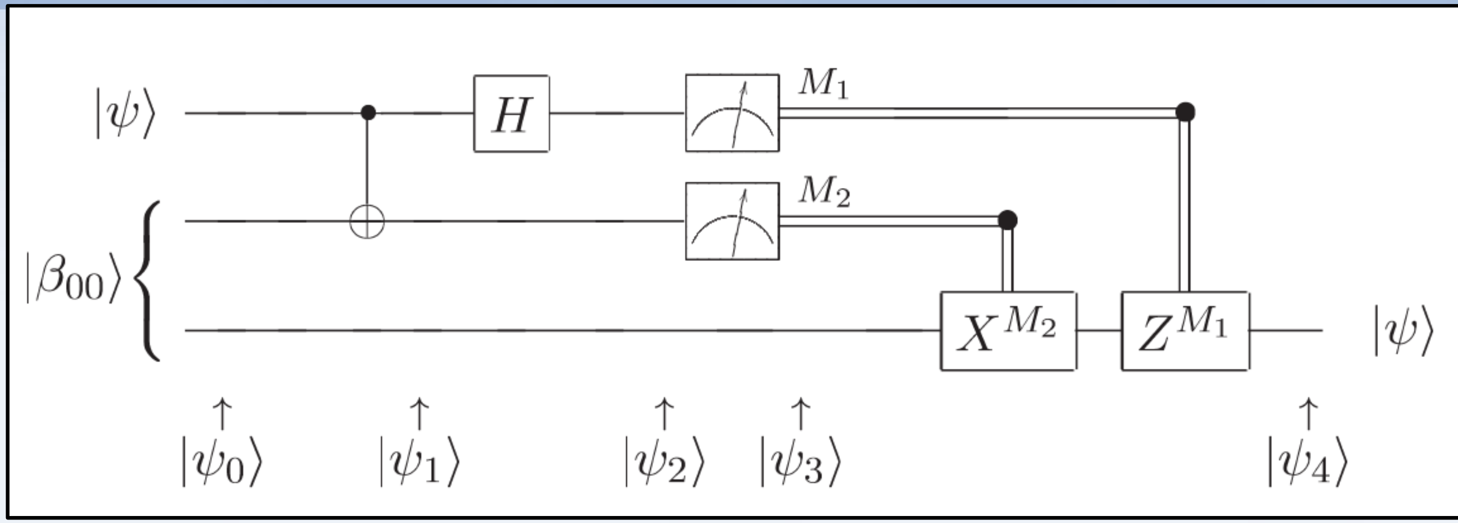


- **Então o estado inicial total do sistema é**

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]$$

Quantum Teleportation



- **Passando pela porta C-NOT temos**

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

- **Passando pela porta Hadamard**

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

Quantum Teleportation

- **Rearrajando-se simplesmente os termos temos**

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\Big]$$

- **Em que os dois qubits da esquerda são os da Alice, e o qubit da direita é o do Bob**
- **O que é que acontece se a Alice medir os seus qubits?**
- **Consoante o que ela medir, atira o qubit do Bob para o estado associado a essa medição**

Quantum Teleportation

- **Sistematizando**

Se Alice medir	**O qubit do Bob é**

$$
\begin{aligned}
00 &\longmapsto |\psi_3(00)\rangle \equiv \Big[\alpha|0\rangle + \beta|1\rangle\Big] \\
01 &\longmapsto |\psi_3(01)\rangle \equiv \Big[\alpha|1\rangle + \beta|0\rangle\Big] \\
10 &\longmapsto |\psi_3(10)\rangle \equiv \Big[\alpha|0\rangle - \beta|1\rangle\Big] \\
11 &\longmapsto |\psi_3(11)\rangle \equiv \Big[\alpha|1\rangle - \beta|0\rangle\Big] .
\end{aligned}
$$

- **Se a Alice disser ao Bob o que é que mediu (informação clássica), o Bob pode fazer a operação necessária para recuperar o qubit original**

Quantum Teleportation

- **Então mas...**

- **Não houve transmissão de informação mais rápida que a velocidade da luz?**

- **Não. Bob teve de receber informação classica da Alice, cuja velocidade é inferior a *c***

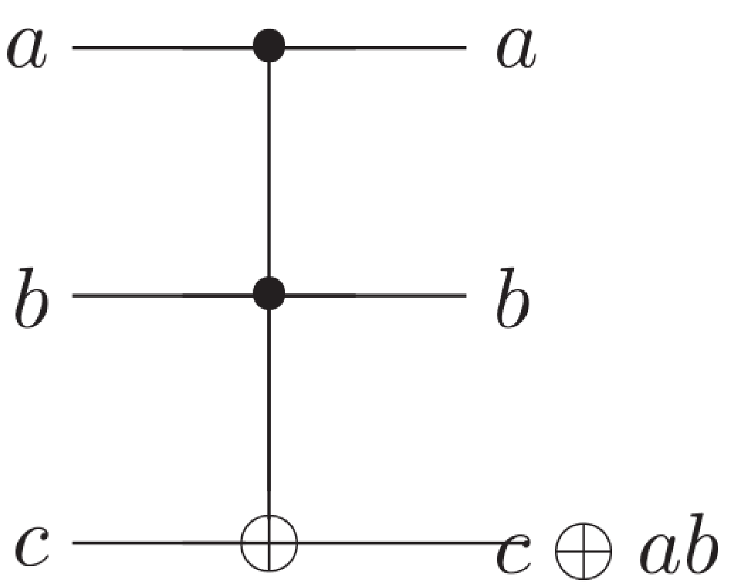
- **A Alice não copiou o qubit quando o enviou para o Bob, algo que é proíbido?**

- **Não. Quando a Alice mediu o seu qubit, colapsou-o. O qubit foi apenas transferido.**

Algoritmos Quânticos

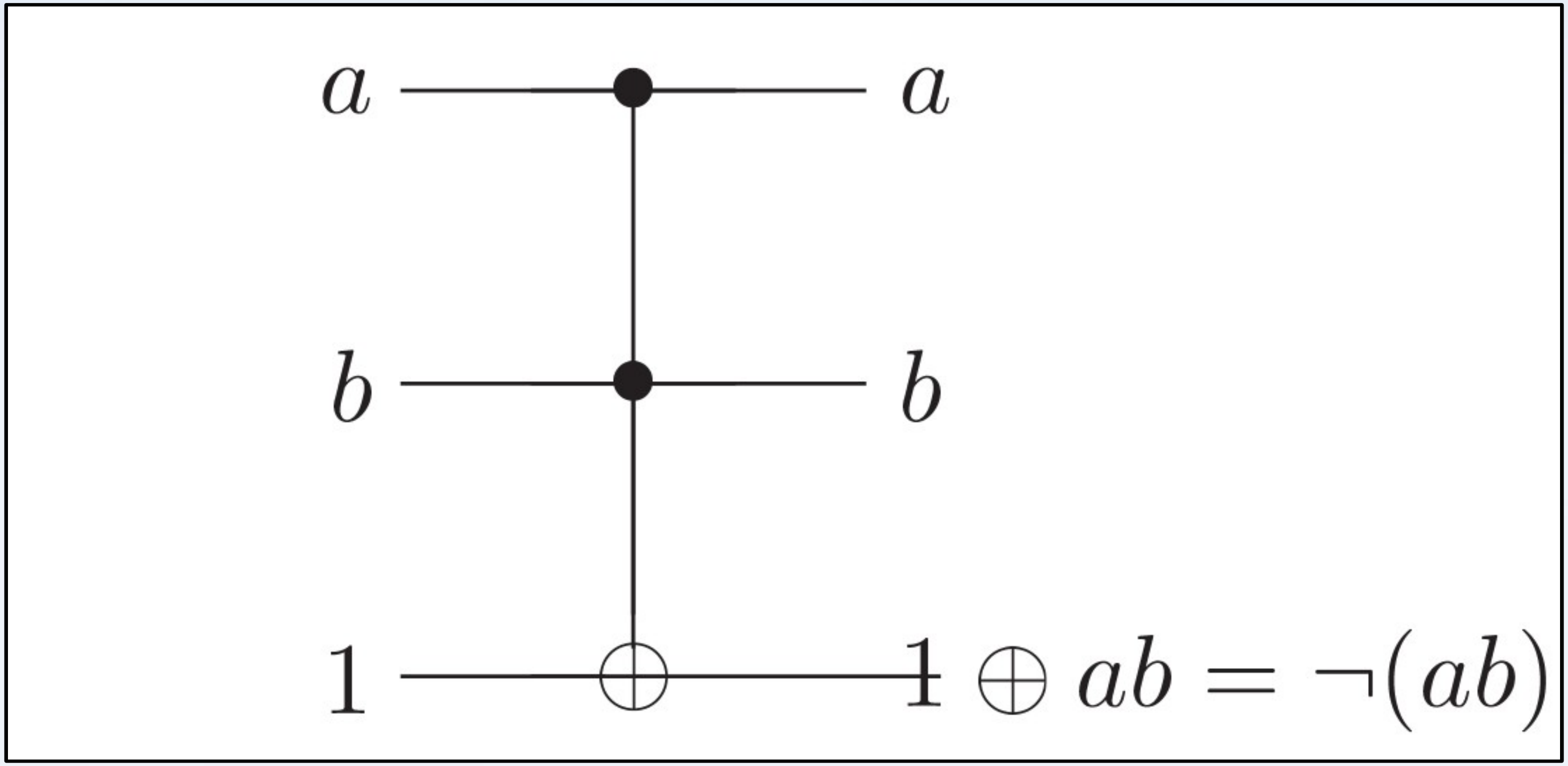
- **Veremos agora como fazer cálculos clássicos num computador quântico**
- **Introduzimos a Toffoli-Gate**

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Algoritmos Quânticos

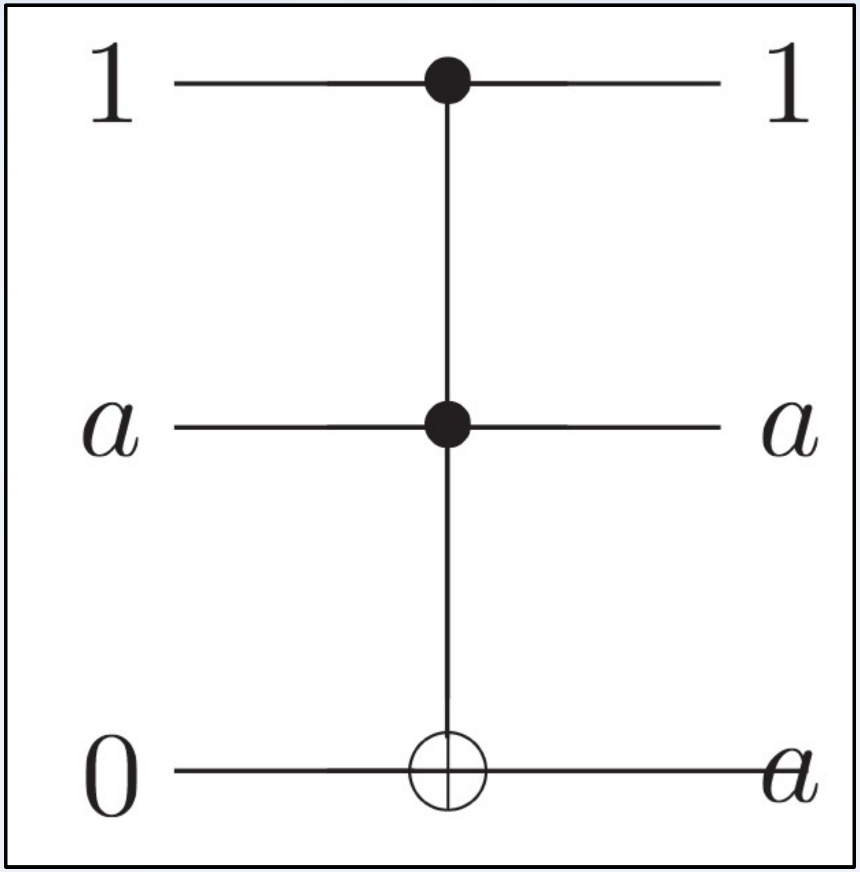
- **Como é que simulamos uma porta NAND clássica utilizando a porta Toffoli?**



- **Note-se que estes inputs, a e b, são inputs clássicos, i.e. 0 ou 1, e não sobreposições de estados**

Algoritmos Quânticos

- E como é que simulamos o Fan-Out?



- Então mas, não se copiou um qubit?
- Copiou-se um um qubit 'clássico' e cujo estado era conhecido, só não se pode copiar qubits de estado quântico desconhecido

Algoritmos Quânticos

- **Comprovámos que um computador quântico consegue fazer qualquer cálculo que um computador clássico consegue fazer!**

- **Mas será que há vantagens?**

Paralelismo Quântico

- **Imagine-se uma função**

$$\boxed{f(x) : \{0,1\} \rightarrow \{0,1\}}$$

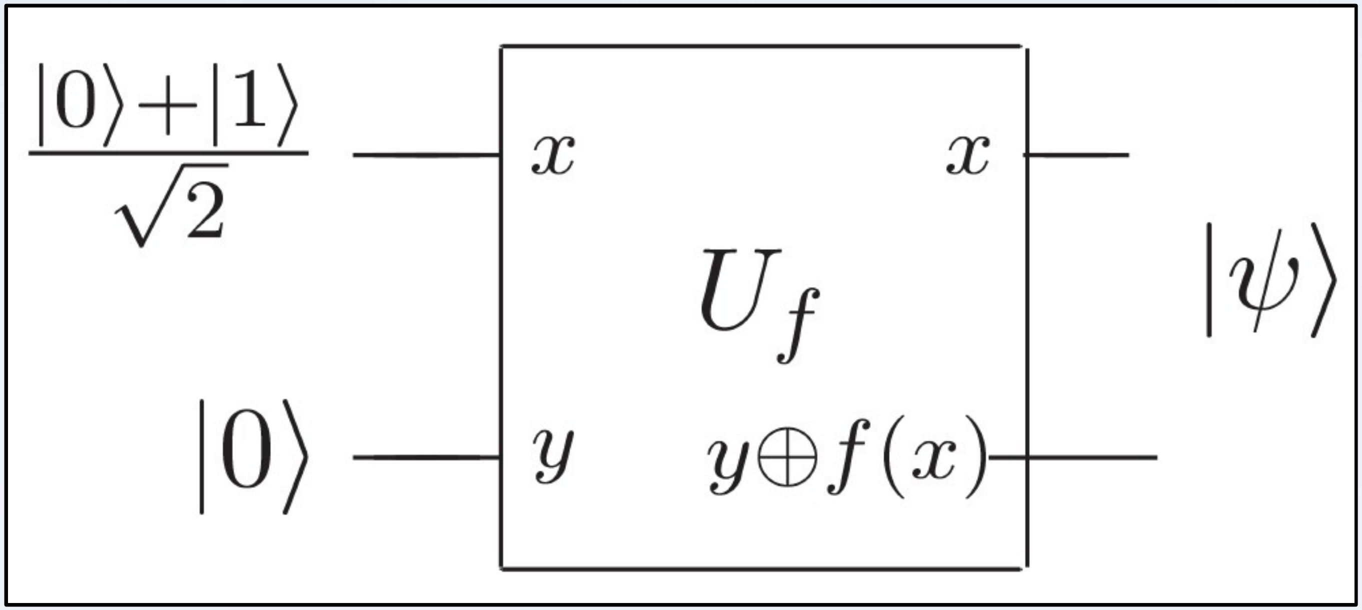
- **Vamos agora considerar um circuito que começa no estado** $|x, y\rangle$

- **E cujo estado final é** $|x, y \oplus f(x)\rangle$

- **Se y=0, o estado final do segundo qubit será f(x)**

- **Concretizemos...**

- **Se tivermos o circuito com as seguintes entradas**



- **O estado final é então**

$$\boxed{\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}}$$

Paralelismo Quântico

$$\boxed{\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}}$$

!

- **Conseguimos avaliar a função em dois valores simultâneamente, apenas com uma aplicação do circuito!**
- **Podemos levar isto ao extremo e ver o que é que acontece**

Paralelismo Quântico

- **Uma transformada de Hadamard não é nada mais que n portas Hadamard a actuarem em paralelo em n qubits.**

- **Para dois qubits que tenham começado no estado |0>, temos por exemplo**

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

- **Então para n qubits temos**

- **Em que a soma é feita para todos os valores possíveis de x**

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

Paralelismo Quântico

- Isto dá que o estado final é uma sobreposição de 2^n estados próprios

- Aplicando o circuito que avalia f(x) no resultado de uma transformada Hadamard temos

$$\boxed{\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle}$$

- Com apenas n bits, conseguimos avaliar a função simultaneamente em 2^n valores!