A computação do futuro

Miguel Afonso Oliveira

Laboratório de Instrumentação e Física Experimental de Partículas

Computadores do futuro???

- Porque é que vamos falar de computadores numa sessão de física?
- E os computadores do passado?
- E já agora o que é um computador?

O que é um computador?

- Computer (inglês) = o que faz cálculos.
- Ordinateur (françês) = o que ordena (processa) informação

Computador é um sistema programável que processa informação.

- Porque é que vamos falar de computadores numa sessão de física?
- E os computadores do passado?

Vejamos a história da Física e da Computação...

Física

séc. XVI | séc. XVII | séc. XVIII | séc. XIX | séc. XX

Astronomia Descritiva e de Previsão

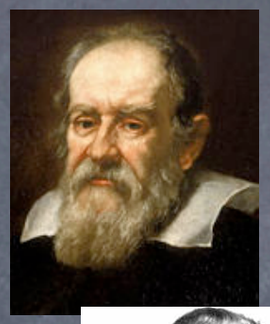
Copernico

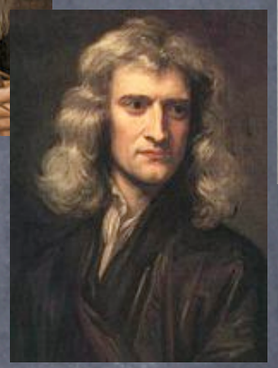
Galileo
Pascal

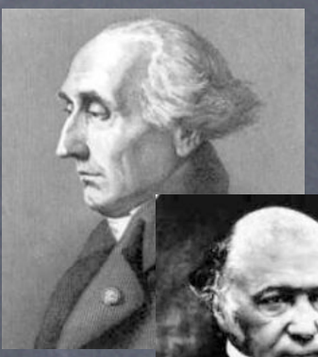
Kepler

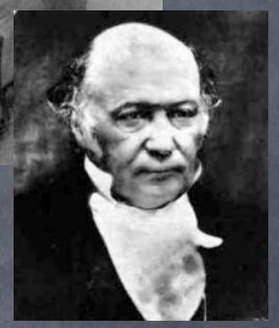
Newton

Lagrange
Hamilton

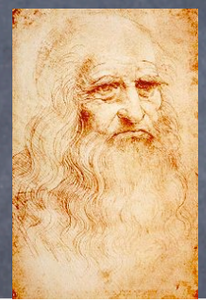








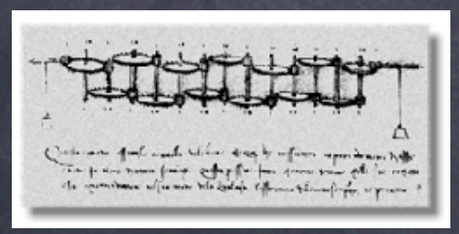
Abaco



da Vinci

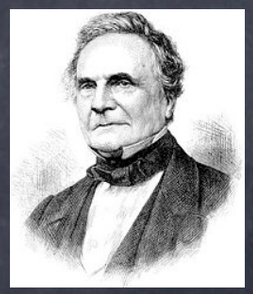
Computação

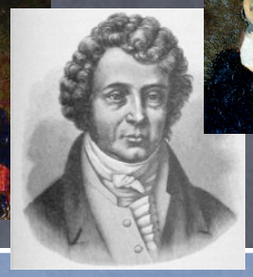
Antikythera
100 AC



Pascal

Babbage



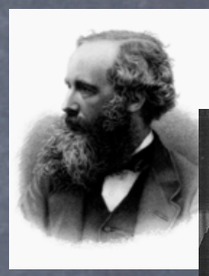


16 de Dezembro
1946

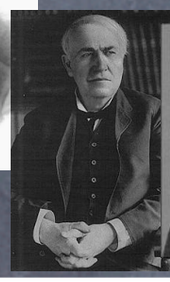
séc. XVIII

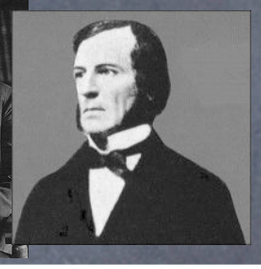
Coulomb
Ampère
Gauss

séc. XIX



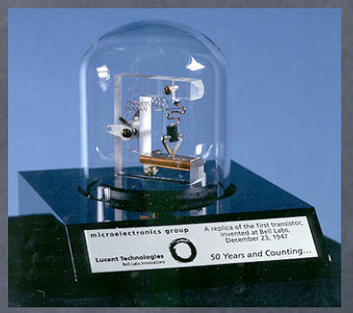
Maxwell
Edison
Boole

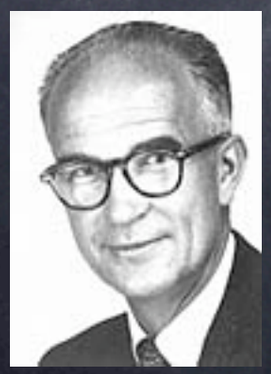


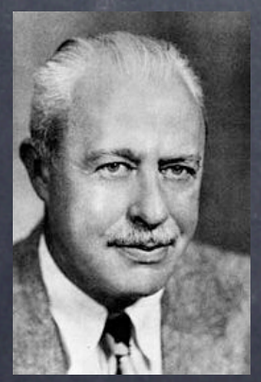


séc. XX

Transistor



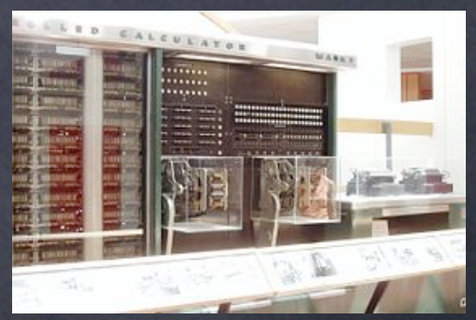




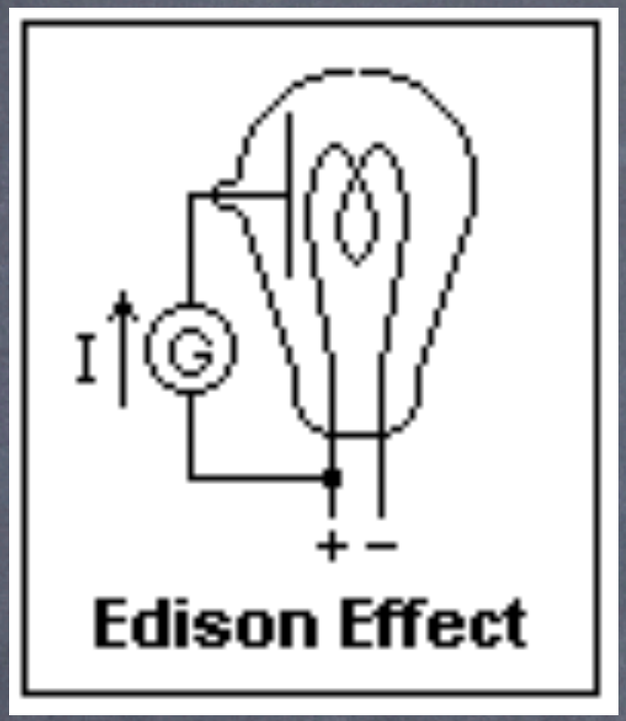
William Shockley, John Bardeen, Walter Brattain
Prémio Nobel em 1956

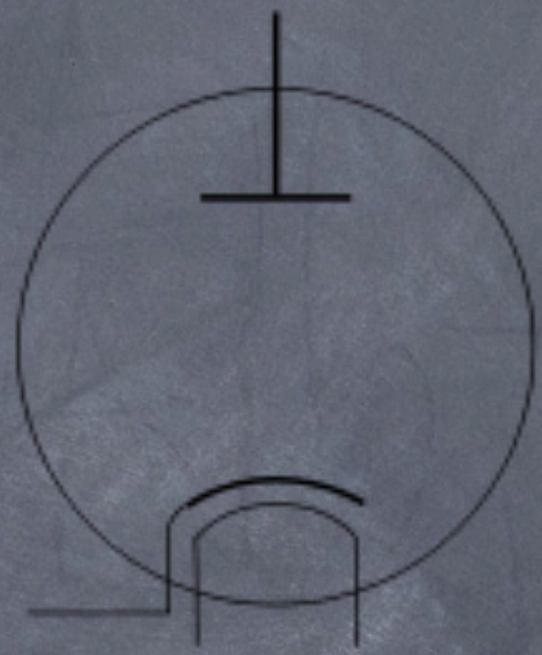
séc. XX

Harvard Mark I
ENIAC
SSEM
EDVAC
WIRLWIND
UNIVAC



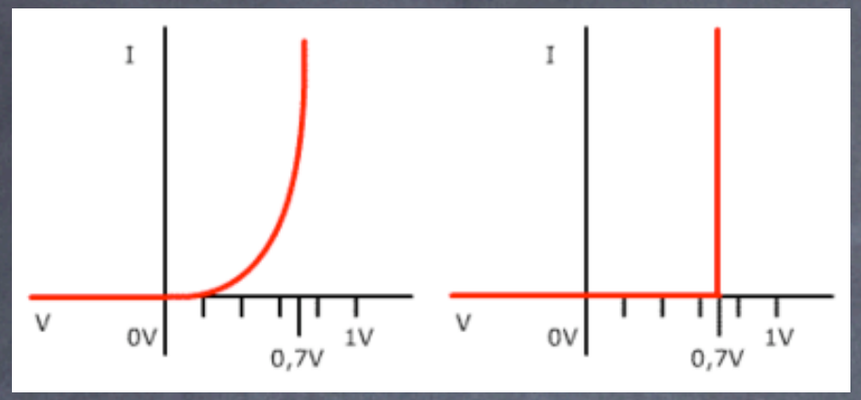
Efeito de Edison



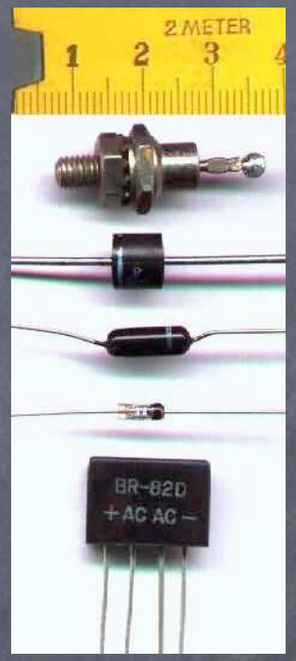


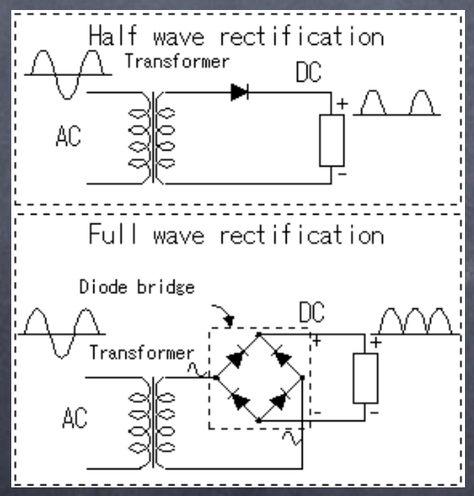
Efeito termoiónico

Díodo

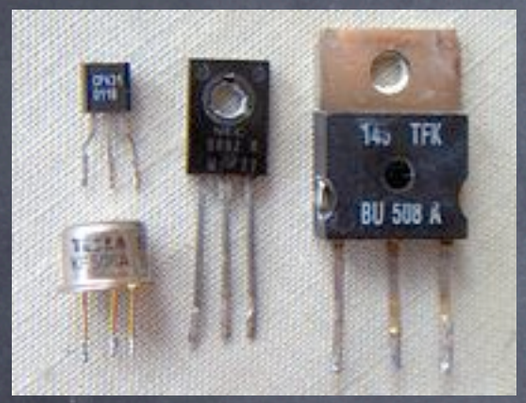

I
V
0V
0,7V
1V
I
V
0V
0,7V
1V

Eimac
2-50A


2 METER
1
2
3
BR-82D
+AC AC-


Half wave rectification
Transformer
DC
AC
+
-
Full wave rectification
Diode bridge
DC
Transformer
AC
+
-

Transístor



Um transístor é um dispositivo que permite controlar com uma pequena corrente ou voltagem uma outra usualmente muito maior.

Mas para que servem os díodos e os transístores em computação?

Servem para construir os circuitos lógicos e implementar a lógica boolena que é a formalização matemática para as operações com bits.

Lógica boolena??? Bits???

Bit, ou digito binário, é a unidade de informação digital e só pode ter valores de 0 e 1.

A representação de bit pode ser feita de várias formas. Nos circuitos digitais é representado pela existência ou não de voltagem.

Os bits servem para codificar:

- os números.
- os estados lógicos (1=Verdade,0=Falso).

Numeração binária

$$2573 = 2\times10^{3} + 5\times10^{2} + 7\times10^{1} + 3\times10^{0}$$

$$1101 = 1\times2^{3} + 1\times2^{2} + 0\times2^{1} + 1\times2^{0}$$

$$1101_{2} = 13_{10}$$

Estados lógicos, operações lógicas: lógica booleana

NOT

Logical Negation

p	¬p
F	T
T	F

AND

Logical Conjunction

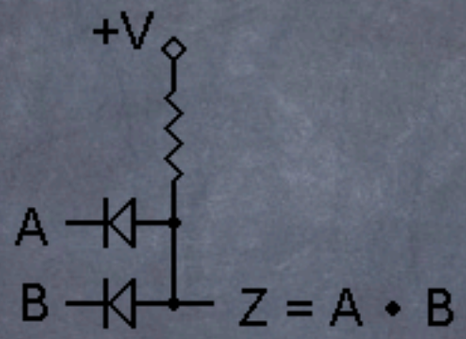
p	q	p ∧ q
T	T	T
T	F	F
F	T	F
F	F	F

OR

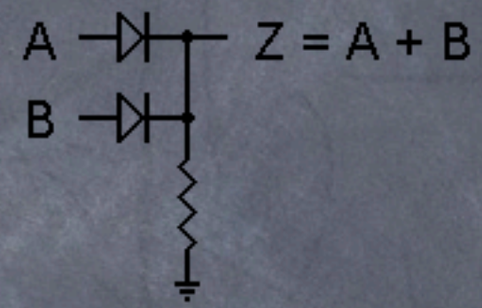
Logical Disjunction

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

E como se implementam os circuitos?



AND



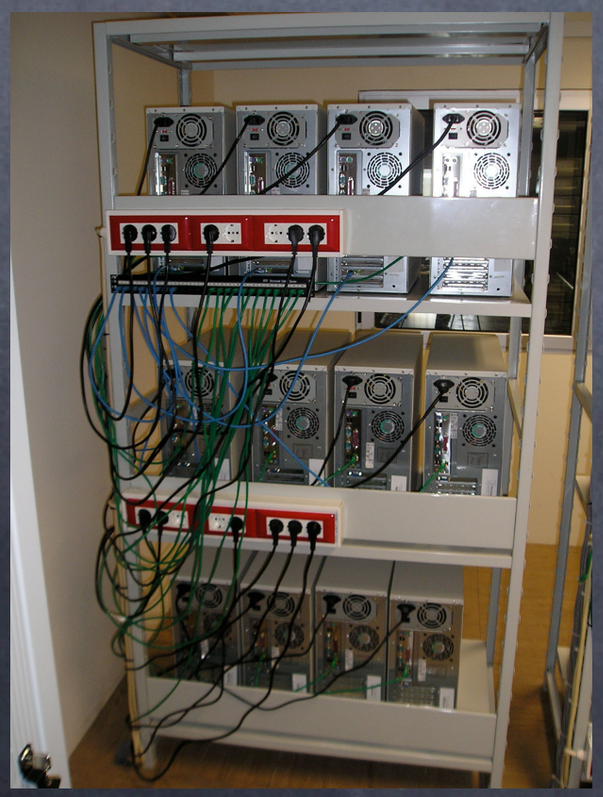
OR

As gerações da computação

1943 - 1959 -> 1ª geração: válvulas.
1959 - 1964 -> 2ª geração: transístores e circuitos impressos.
1964 - 1972 -> 3ª geração: circuitos integrados.
1972 -   -> 4ª geração: LSI, VLSI.

Computação hoje

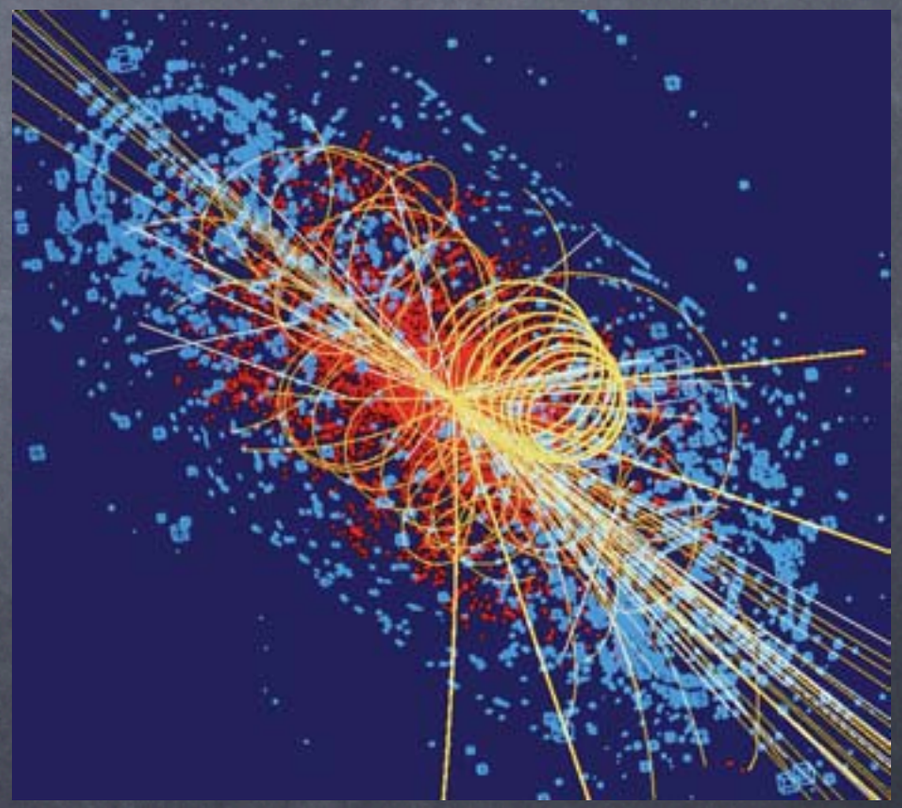
HPC: Milipeia



GRID: Centopeia

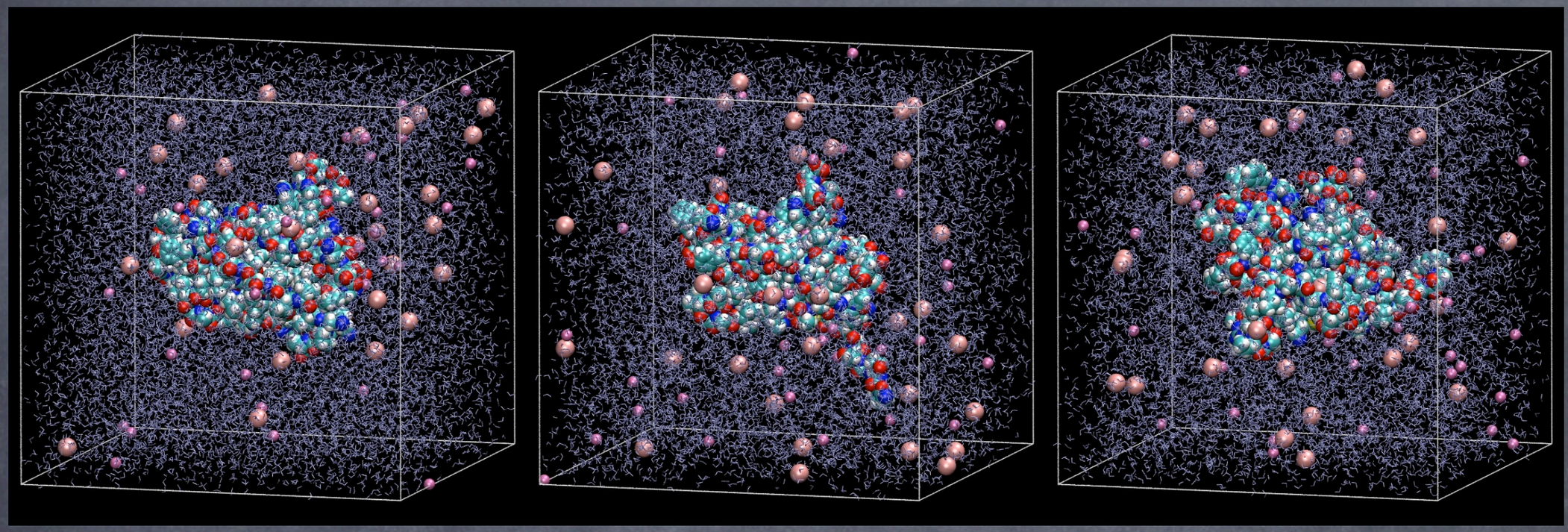
A Física e os computadores

Do muito grande
(astrofísica)...



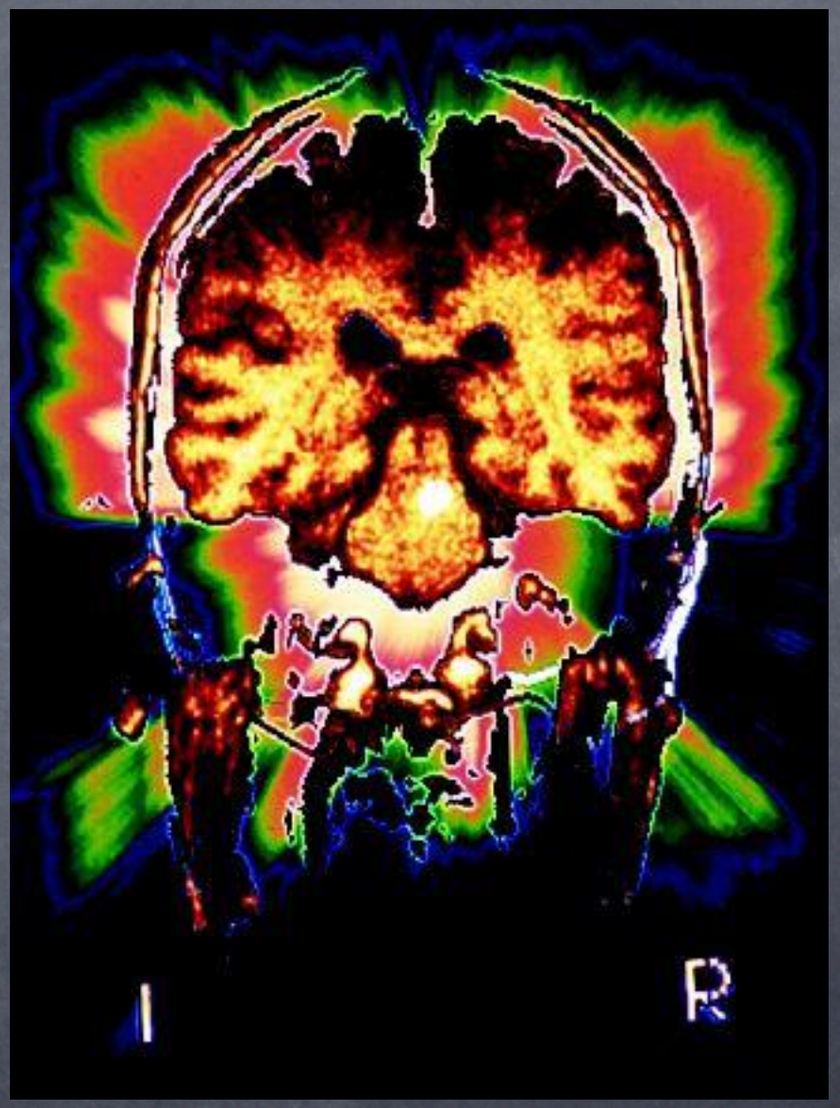
ao muito pequeno
(física de partículas)

A Biologia e os computadores



Usados para estudar as interacções entre as moléculas biológicas

A Medicina e os computadores

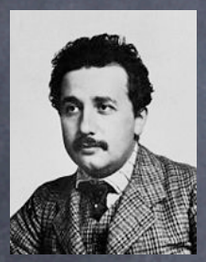


O poder computacional é fundamental para a imagiologia médica

A computação é hoje essencial em todos os domínios da Ciência.

Voltemos à história...

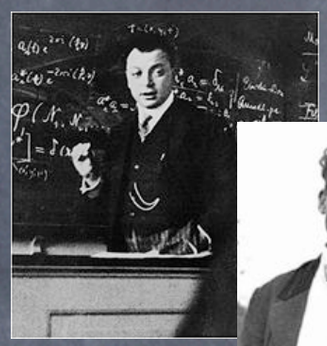
1905/1915
Teoria da Relatividade

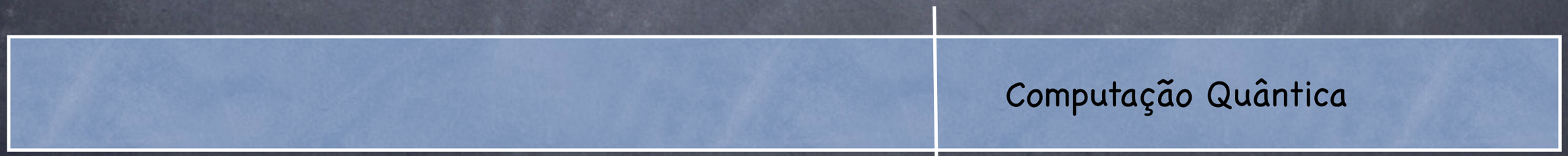


1920

Pauli
Schroedinger
Heisenberg

1930

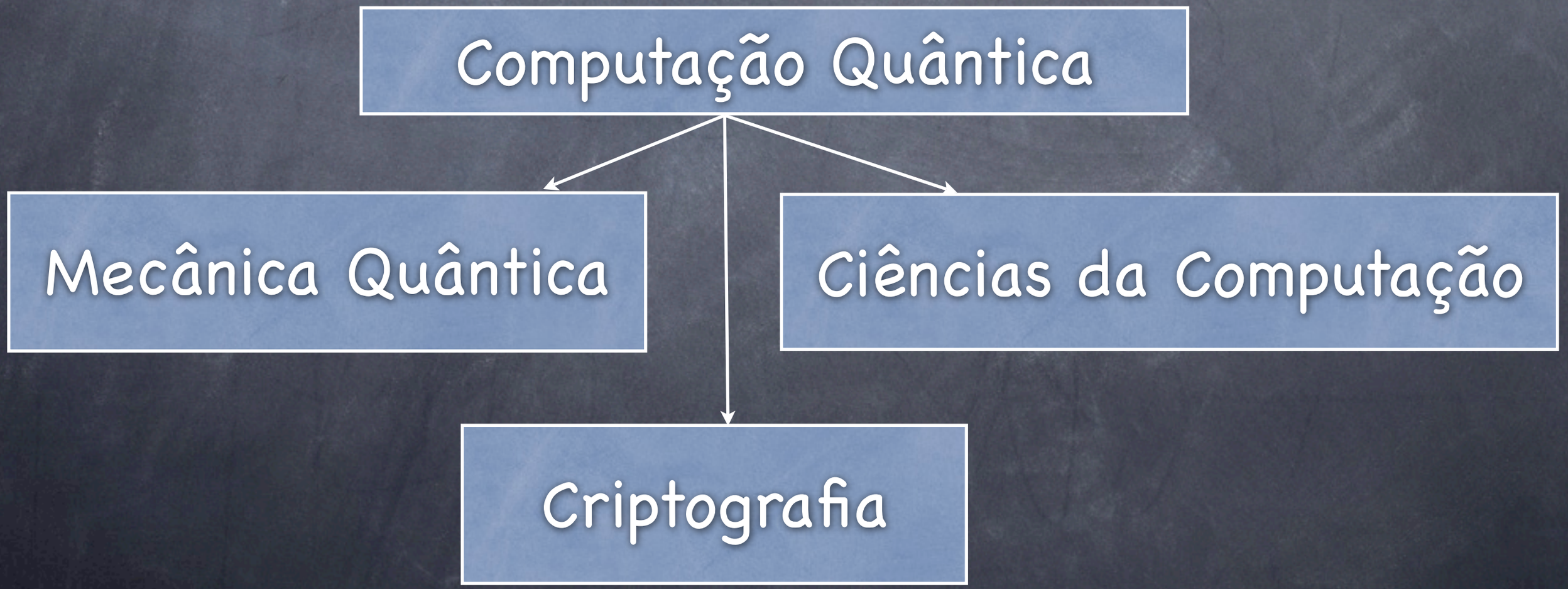




??? Será este o futuro???

Computação Quântica

Computação Quântica é o estudo do processamento que é feito com sistemas quânticos.



Bit quântico ou qubit

É uma abstracção matemática com certas propriedades relativas aos seus estados:

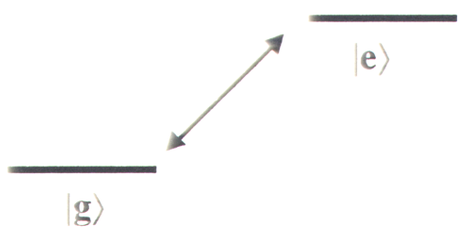
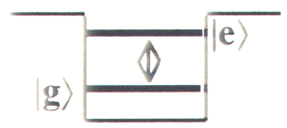
- os estados lógicos $|0\rangle$ e $|1\rangle$ que correspondem aos estados 0 e 1 dos bits clássicos.
- têm também todos os estados de combinação em $|0\rangle$ e $|1\rangle$:

$$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle \text{ (Sobreposição de estados).}$$

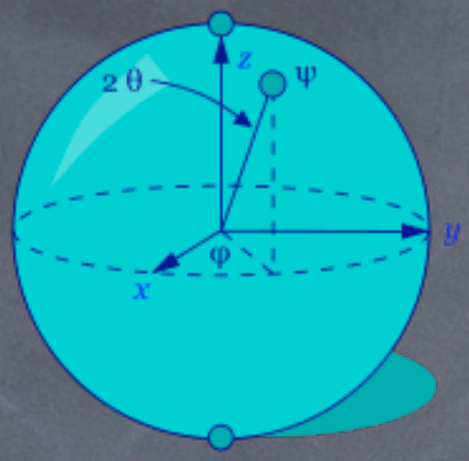
Em termos físicos o qubit é um sistema quântico que tem duas soluções que podem ser medidas com probabilidades $|\alpha|^2$ para a solução $|0\rangle$ e $|\beta|^2$ para o estado $|1\rangle$. Teremos que ter:

$$|\alpha|^2+|\beta|^2=1.$$

Mas afinal o que são qubits?

'0'	'1'	Qubit
		Photon: linear polarization
		Photon: circular polarization
		Electron, Neutron: Spin
		Atom: Energy levels
		Quantum Dot

Posso representar um qubit?



Esfera de Bloch

Quanta informação pode ser representada num qubit?

Há um número infinito de pontos sobre a superfície da esfera pelo que se podia codificar infinita informação num qubit mas cuidado:

Apenas podemos medir |0> e |1>.

Porquê?

Ninguém sabe. É um princípio básico da mecânica quântico.

Um só qubit?

Não. Podemos usar tantos quantos quisermos, ou melhor, tantos quantos formos tecnicamente capazes.

Número de qubits	Soluções	Número de soluções
1	$\|0\rangle,\|1\rangle$	2
2	$\|00\rangle,\|01\rangle,\|10\rangle,\|11\rangle$	4
3	$\|000\rangle,\|001\rangle,\ldots$	8
...		
n	$\|0\ldots0\rangle,\ldots$	2^n

O que significa isto?

Por exemplo para dois qubits teremos:

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

ou seja, poderemos medir qualquer um dos resultados $|ab\rangle$ com probabilidade $|\alpha|^2_{ab}$ desde que:

$$|\alpha|^2_{00}+|\alpha|^2_{01}+|\alpha|^2_{10}+|\alpha|^2_{11}=1$$

Sim e depois???

Qbits	Número de soluções
1	2
2	4
3	8
…	…
10	$2^{10}=1024$
…	…
500	$2^{500}\approx10^{150}$
…	…

Número de partículas no universo: entre 10^{72} e 10^{87}.

Tentar guardar isto num computador clássico é impossível!!!

Para além da sobreposição os qubits têm mais algum comportamento estranho?

Os qubits só têm comportamentos estranhos!!!

Consideremos o estado:

$$\frac{|00> + |11>}{\sqrt{2}}$$

Estados correlacionados.

É a base da teleportação quântica.

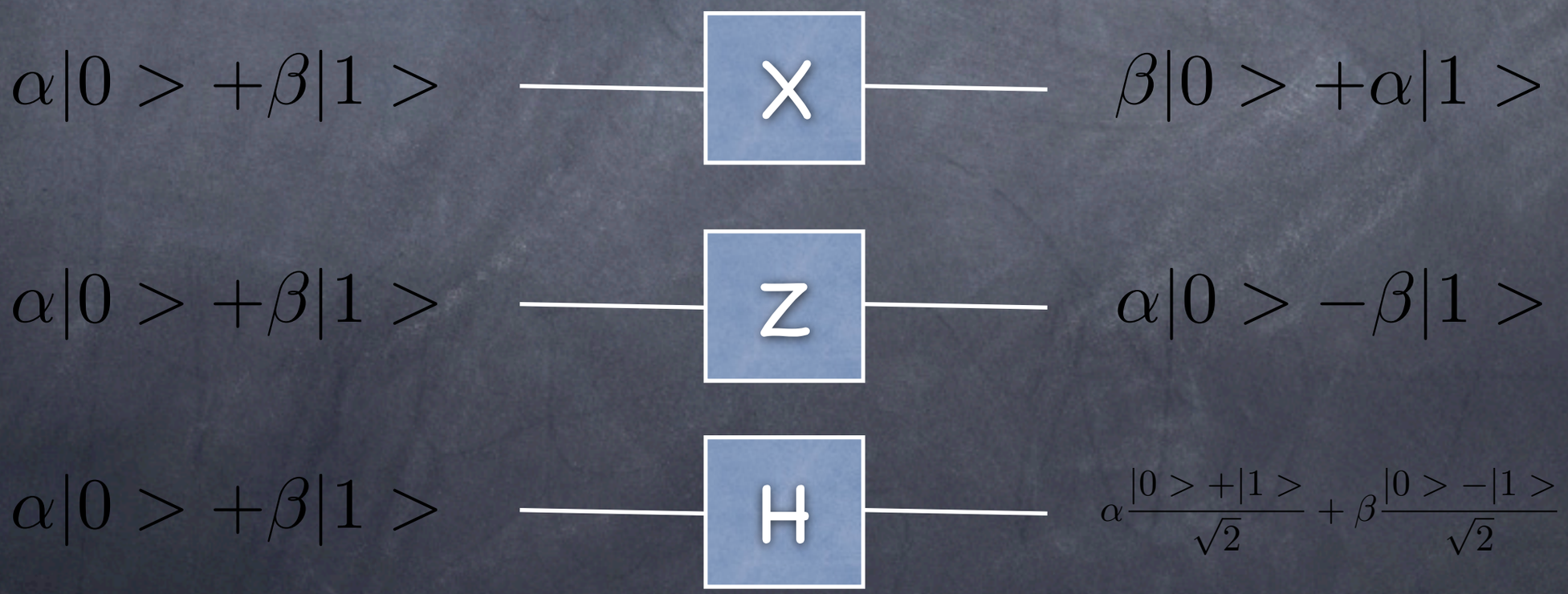
Portas lógicas em computação quântica

Cada porta lógica corresponde a um processo físico executado sobre os qubits.

Portas lógicas de um só qubit

Em computação clássica só existe uma porta lógica de um só qubit: a negação.

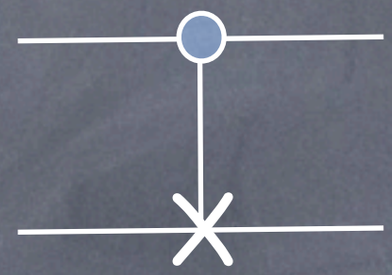
Mas em computação quântica existem 3:



Portas lógicas de múltiplos qubits

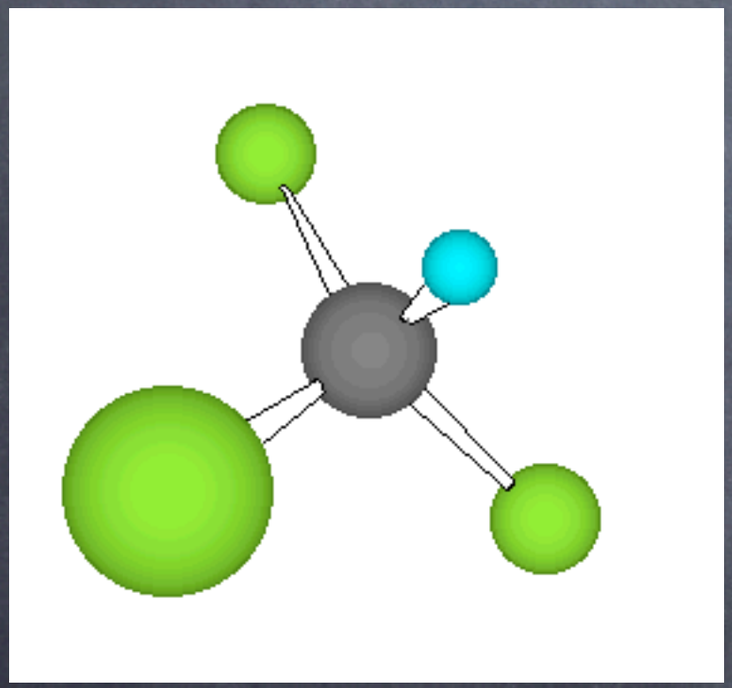
Controlled NOT

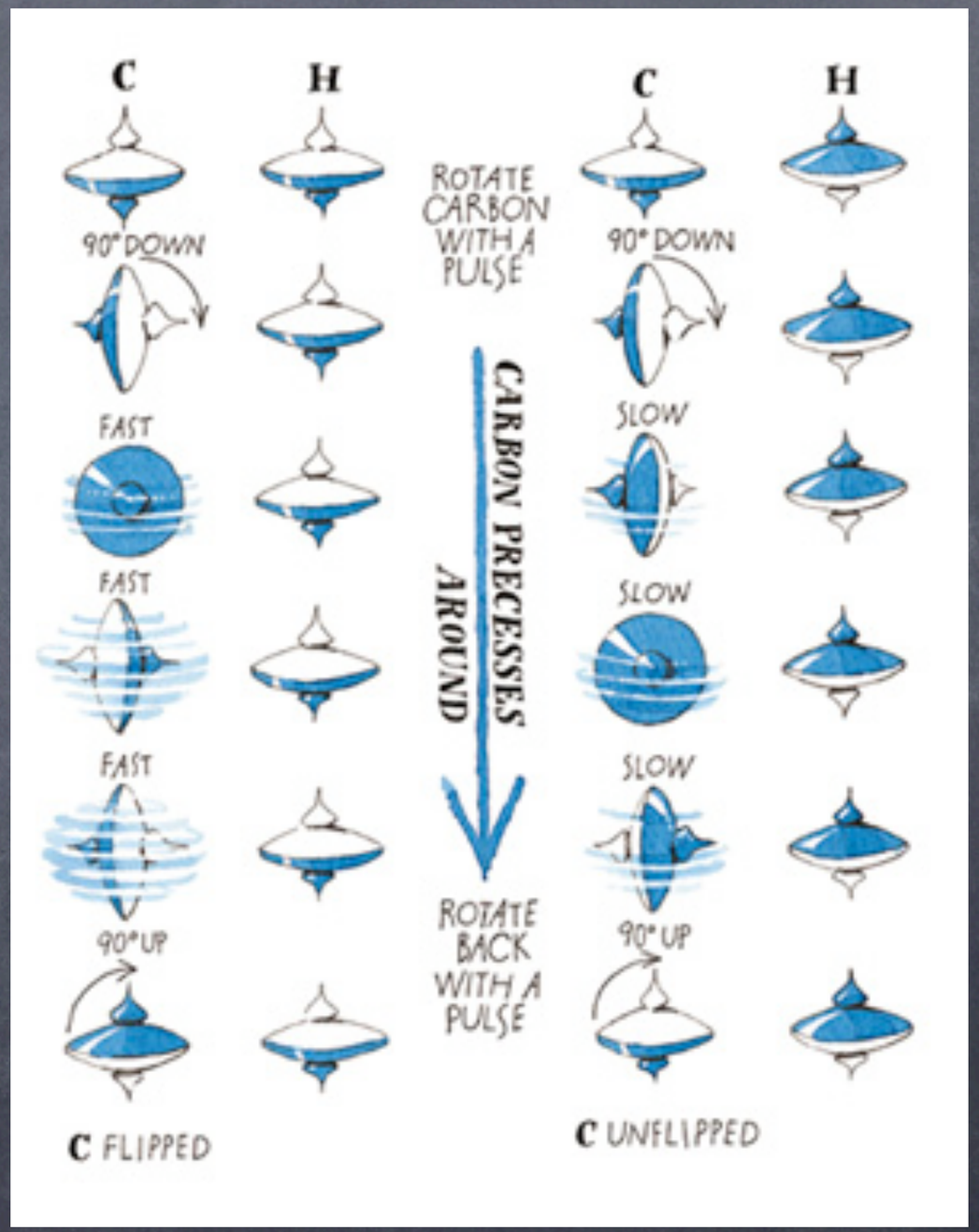
CNOT



|00>	|00>
|01>	|01>
|10>	|11>
|11>	|10>

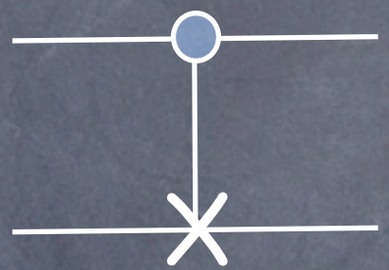
CNOT with $CHCl_3$





Circuitos quânticos

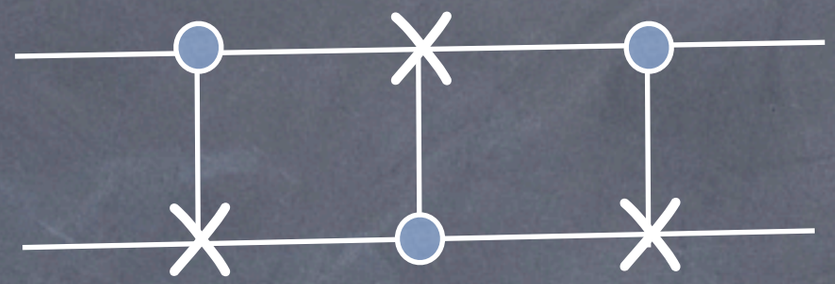
Um circuito quântico é uma representação da evolução do sistema de qubits.



Lê-se da esquerda para a direita.

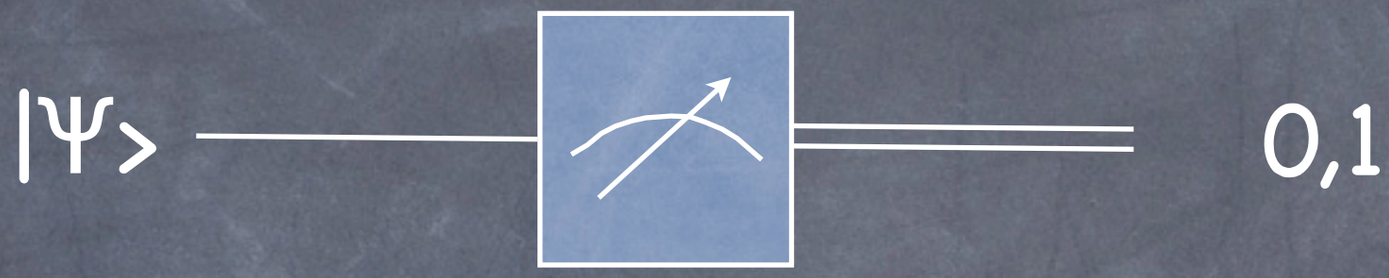
Cada linha usualmente representa a evolução do tempo.

Circuito de troca



|00>	|00>	|00>	|00>
|01>	|01>	|11>	|10>
|10>	|11>	|01>	|01>
|11>	|10>	|10>	|11>

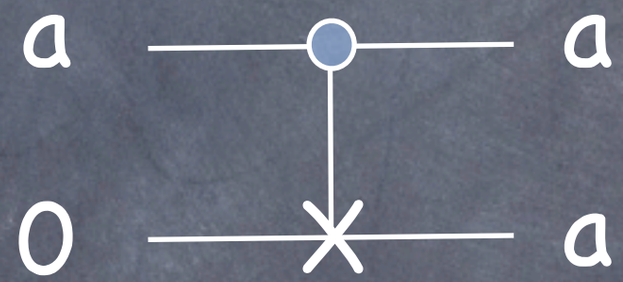
Circuito medida



Circuitos quânticos

Será possível copiar um qubit?

Classicamente

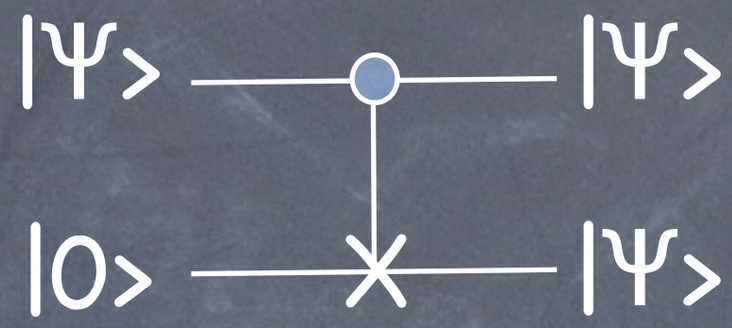


|00>	|00>
|10>	|11>

Circuitos quânticos

Quanticamente

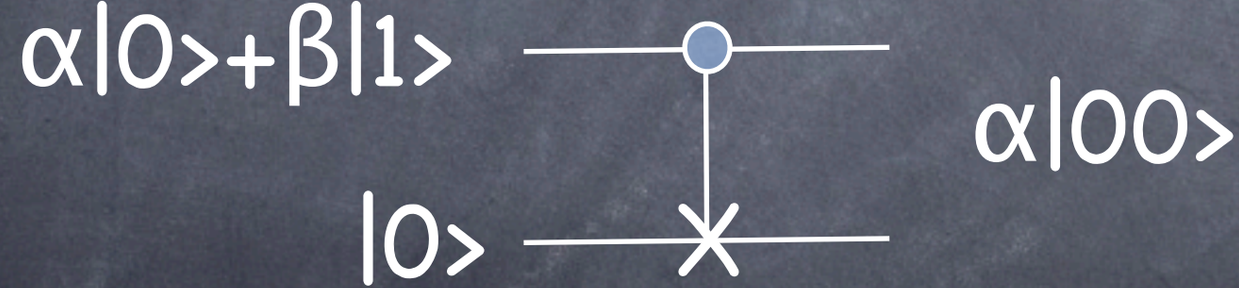
Funcionaria se:



$$|\Psi > |\Psi > \quad = \quad (\alpha|0 > +\beta|1 >)(\alpha|0 > +\beta|1 >) =$$

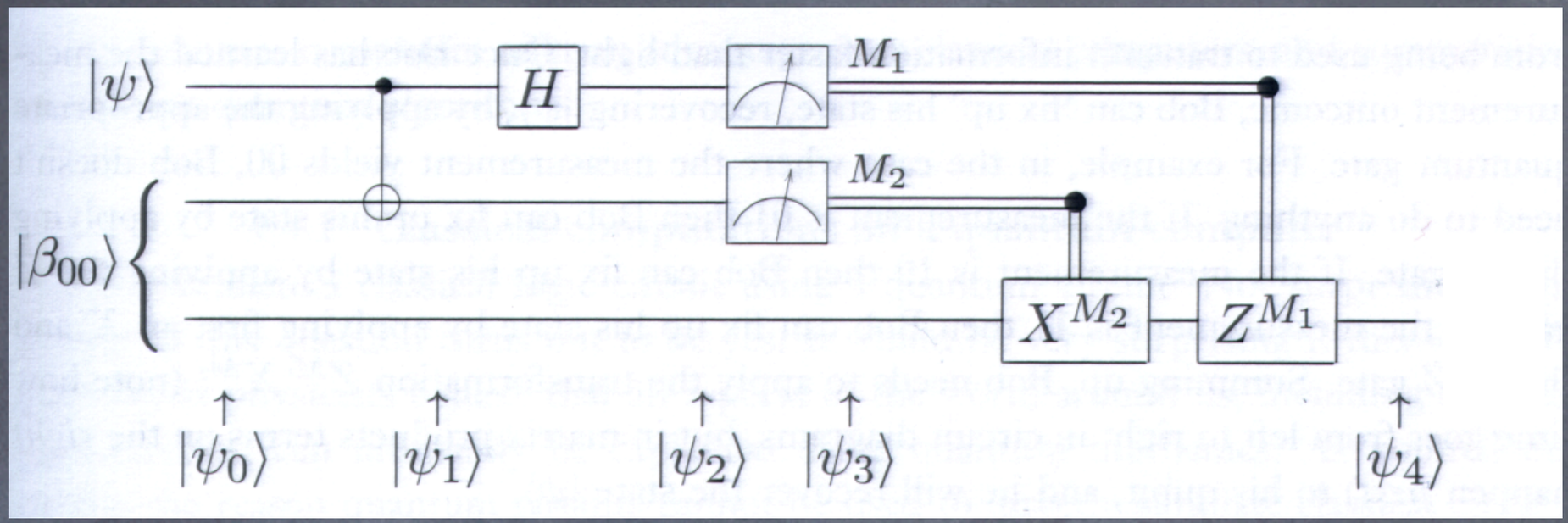
$$= \quad \alpha^2|00 > +\alpha\beta|01 > +\alpha\beta|10 > +\beta^2|11 >$$

Mas:



É impossível copiar um qubit
(Teorema da não clonagem)

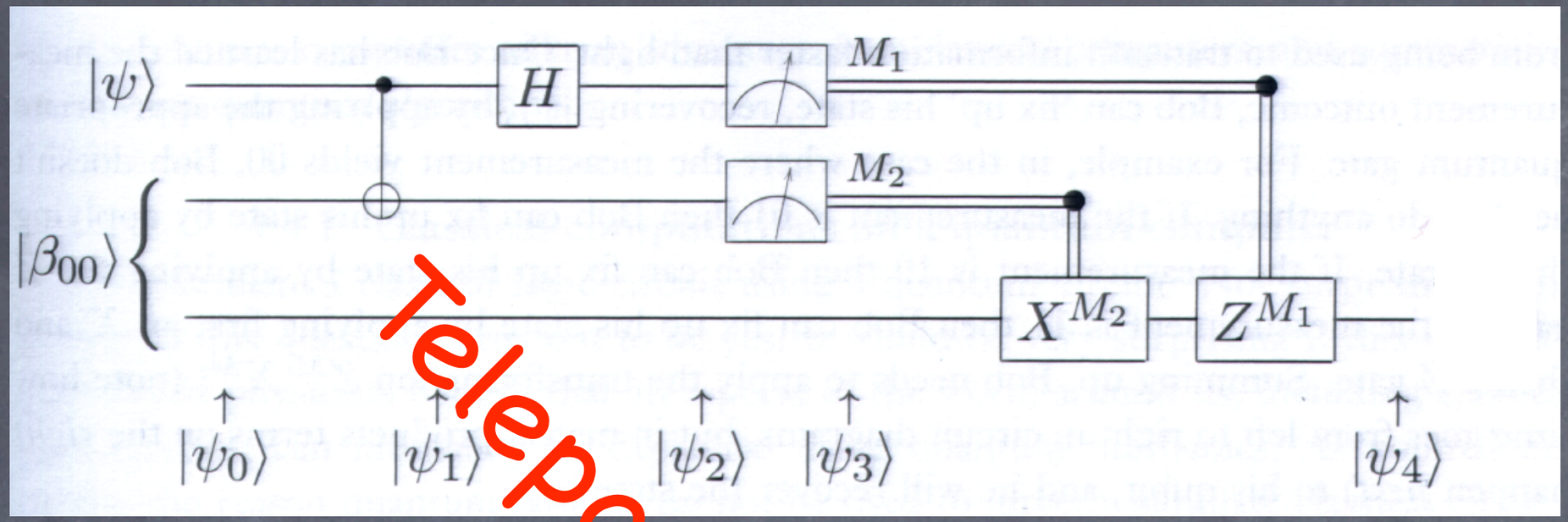
O meu primeiro circuito quântico



$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]$$

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

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



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

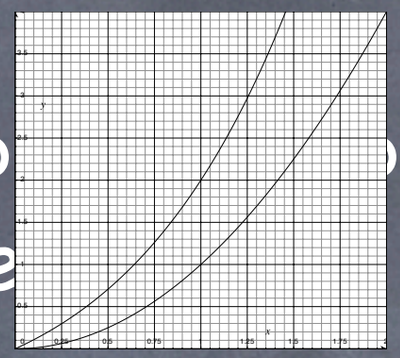
$$\begin{aligned}
00 &\longmapsto |\psi_3(00)\rangle \equiv \Big[\alpha|0\rangle + \beta|1\rangle\Big] \\
01 &\longmapsto |\psi_3(01)\rangle \equiv \Big[\alpha|1\rangle + \beta|0\rangle\Big] \\
10 &\longmapsto |\psi_3(10)\rangle \equiv \Big[\alpha|0\rangle - \beta|1\rangle\Big] \\
11 &\longmapsto |\psi_3(11)\rangle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

Teleportação quântica

Algoritmos quânticos

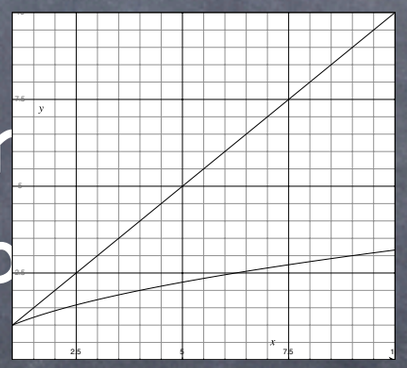
Algoritmos baseados em Transformadas de Fourier:

- Deutsch-Jozsa
- Shor (factorização)
  - Clássico - cerca de $n2^n$ op… para 2^n números.
  - Quântico - cerca de n^2 ope…



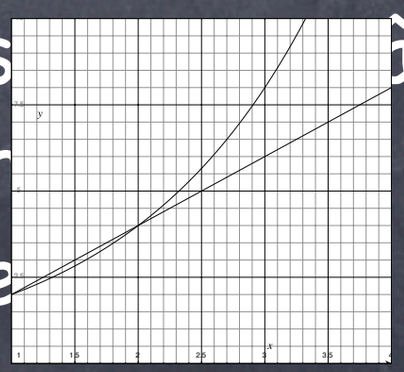
Algoritmos de pesquisa:

- Clássico - cerca de n oper…
- Quântico - cerca de $\sqrt{N}$ op…



Algoritmos de simulação de sis…ânticos:

- Clássico - para n componer… cerca de c^n.
- Quântico - para n compone…



Serão os computadores quânticos melhores que os clássicos?

Ninguém sabe. Parece que sim...

Criptografia

Criptografia é a ciência que estuda o problema de enviar mensagens entre dois ou mais parceiros que podem não confiar entre si.

Há dois tipos de criptografia:

A de chave privada
A de chave pública

Criptografia de chave privada

A Alice e o Roberto têm uma chave que só eles conhecem e que serve para encriptar e desencriptar as mensagens transmitidas entre ambos.

Problema: Como se distribuem as chaves?

Classicamente não há soluções óptimas...
Quanticamente há!!!

A chave pode ser transmitida sem problema. Se alguém a escutar (corresponde a medir) a chave chega alterada...

Criptografia de pública privada

Cada parceiro tem uma chave pública e uma chave privada. Para enviar uma mensagem bastar ir buscar a chave pública do destinatário, encriptar e enviar. O destinatário pode usar a sua chave pública para fácilmente desencriptar a mensagem.

A chave pública pode também ser usada para desencriptar a mensagem mas isto é um problema que os computadores clássicos ainda não conseguem resolver em tempo útil.

Criptografia de pública privada

O problema de usar a chave pública e privada na tarefa de encriptar e desencriptar corresponde ao problema de factorizar números inteiros.

Cuidado: os computadores quânticos conseguem factorizar rapidamente....