Introdução à computação quântica

Ernesto F. Galvão
Instituto de Física
Universidade Federal Fluminense (UFF)

Panorama da Física – 2010

Linha do tempo – computação

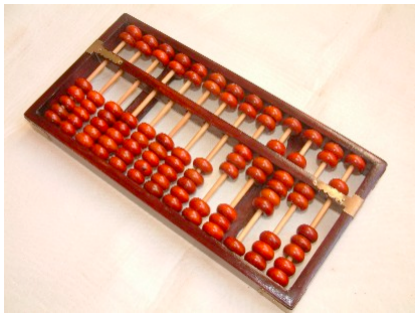
Pré-história — c. 3000 A.C. — c. 2400 A.C. — c. 100 A.C.

Pedrinhas, contabilidade do gado

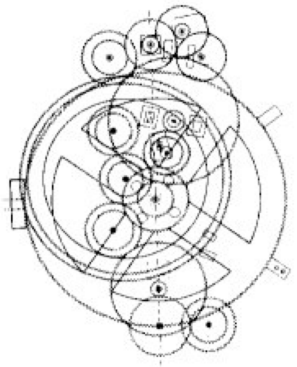
Escrita, contabilidade (Mesopotâmia)

Escrita suméria (c. 2500 A.C.)

Ábaco (Babilônia)

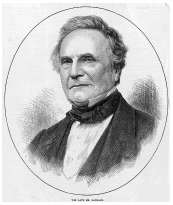


Máquina de Anticítera: cálculos astronômicos



Reconstituição

Linha do tempo – computação



Séc. XVII — 1801 — 1837-1871

Schickard (1623)
Pascal (1642)
Leibniz (1671)

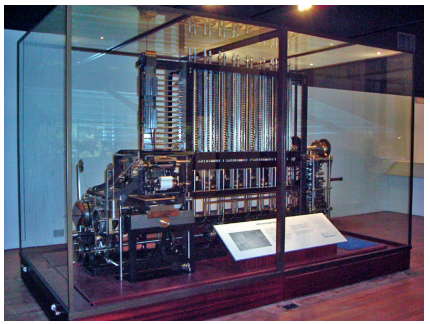
Calculadoras mecânicas para certas tarefas

Leibniz

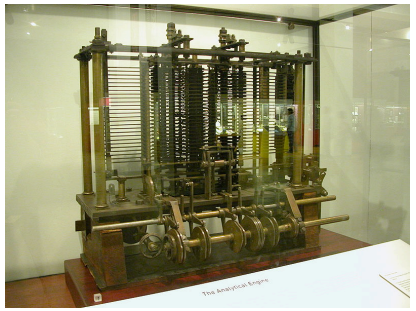
Dispositivos "programáveis

Tear de Jacquard (1801)

Charles Babbage: primeiro projeto de computador programável – Engenho Analítico



Engenho Diferencial (1822/1991)



Engenho Analítico (parte)(1837-1991) - 10m x 30m, movido a vapor!

Linha do tempo – computação

1936-1937

Alonzo Church e Alan Turing lançam os fundamentos da Ciência da Computação

- Problemas indecidíveis
- Máquina de Turing universal

Turing

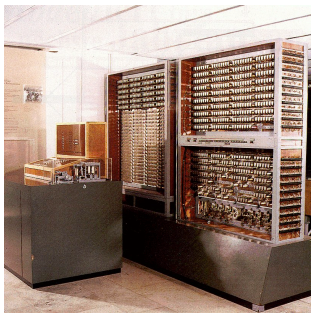
Church

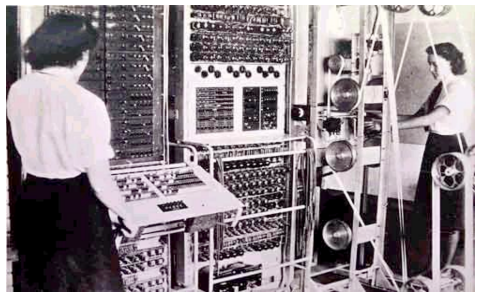
1939-1945
(2ª Guerra Mundial)

Primeiros computadores elétricos ou eletromecânicos programáveis

- Quebra de códigos secretos
- Otimização, balística etc

Z3 – Alemanha
(1941)



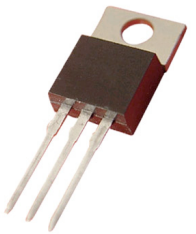


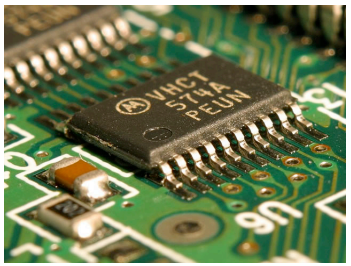
Colossus
Reino Unido
(1943)

1947

Invenção do transístor – versão miniaturizada das válvulas

- Início da indústria eletrônica





Linha do tempo – computação e Física

1961

Formulação do **Princípio de Landauer**:

-Mínimo de energia dissipada por operação lógica irreversível

1973

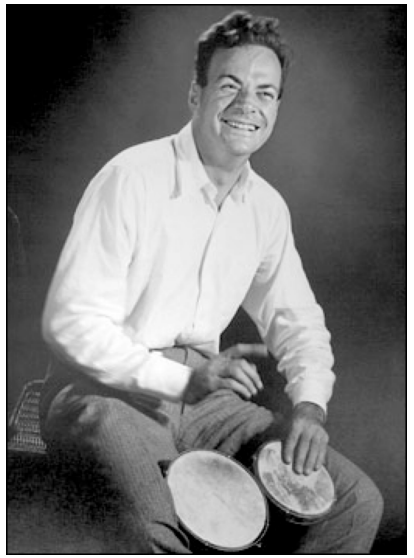
Charles Bennett

- Como fazer computação reversível, em princípio sem gasto de energia

1982

Richard Feynman

-Sistema quântico bem controlado para simular outros sist. quânticos

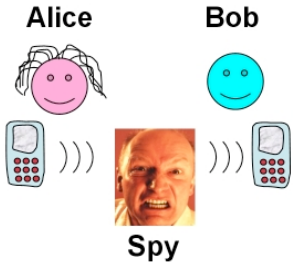


Linha do tempo – computação e Física

1984 — 1985 — 1991

Bennett/Brassard

- Primeiro artigo descrevendo um protocolo de **criptografia quântica**, que ficou conhecido como BB84

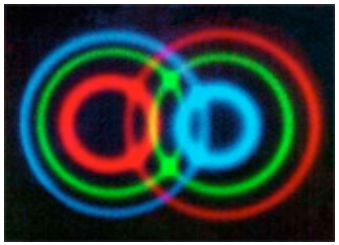


David Deutsch

- Descreveu **uma máquina de Turing quântica**, e mostrou que ela poderia resolver alguns problemas mais rapidamente que um computador clássico

Artur Ekert

- Criptografia quântica baseada em emaranhamento – E91



Linha do tempo – computação e Física

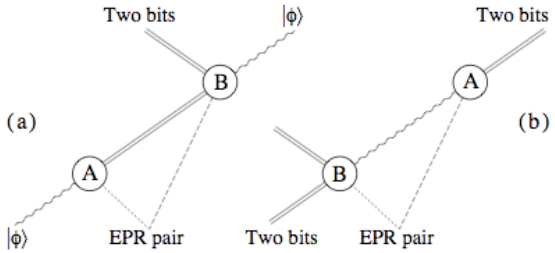
1992 — 1993 — 1994

Bennett *et al*.

- Demonstração experimental do protocolo de criptografia quântica BB84

Bennett, Brassrd, Crépeau, Jozsa, Peres, Wootters

-Teletransporte quântico



Peter Shor

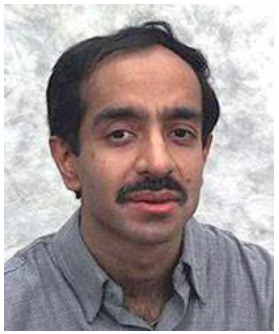
- Algoritmo quântico **de fatoração de inteiros exponencialmente mais rápido** que o melhor algoritmo clássico
- quebra de RSA por computador quântico

Linha do tempo – computação e Física

1996 — 1997 — 2001

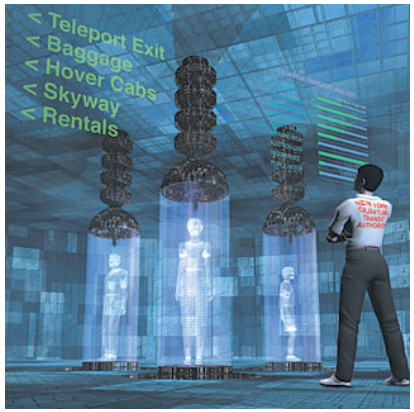
Lov Grover

- Algoritmo quântico de busca: vantagem quadrática sobre computador clássico



Bouwmeester et al.

- teletransporte quântico experimental



Vandersypen *et al.*

- fatoração quântica experimental

(15= 3 x 5)

História

Mecânica = movimento de corpos

- Aristóteles, Galileu, … Isaac Newton (1643-1727):

  - Leis do movimento: sistema de partículas é descrito por posição e velocidade de cada uma.

  - A dinâmica é calculada a partir das forças sobre o sistema.

Fins do séc. XIX: crise

- Espectro da luz, efeito fotoelétrico, … problemas sem explicações usando a física *clássica* (= pré-quântica)

Espaço para surgimento da Mecânica Quântica

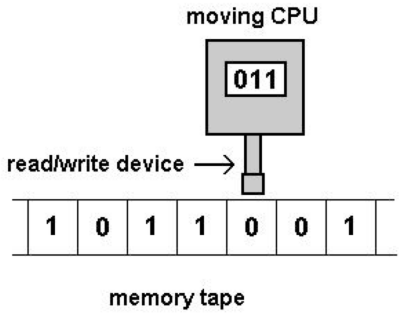
Ciência da Computação

- **Alan Turing** (1935) - Formalização matemática dos conceitos de:

  - procedimento preciso para calcular algo - *algoritmo*
  - um tipo simples de computador

- **Máquina de Turing**

CPU se movimenta de acordo com programa, lendo e apagando dados



- simples, mas capaz de *qualquer* computação:

Tese de Church-Turing

<u>Resultados:</u>

- existem problemas incomputáveis - à la Gödel

- problemas computacionais podem ser divididos, grosso modo, entre ***tratáveis*** e ***intratáveis***.

Intratabilidade computacional

- Imagine problema computacional com entrada de *n* dígitos

- Problema tratável: número *N* de passos computacionais é proporcional a polinômio de *n*.
  - exemplo: multiplicação de dois números de *n* dígitos.

$N \sim n^2$

- Problema intratável: número de passos cresce mais rápido do que qualquer polinômio.
  - exemplo: fatoração de inteiro de *n* dígitos.
  - Melhor algoritmo conhecido: $N \sim 2^n$
  - ➡ resultado: fatorar um número de 400 dígitos levaria **bilhões de anos** neste computador!!

- Problemas intratáveis são importantes:

- Fatoração: chave para quebrar códigos de segurança bancária
- Otimização: aumento de rendimento na indústria
- Problemas científicos em geral

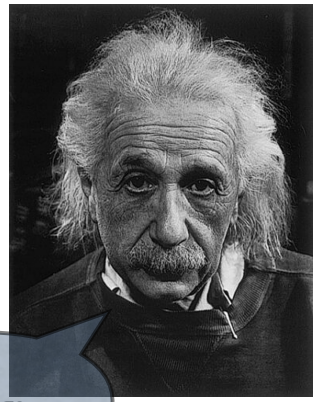
Mas...

- A ciência da computação não levava em conta que a **computação é um processo físico!**

- Leis físicas determinam os limites dos computadores…

Física quântica

- Desenvolvida na década de 1920 para descrever sistemas microscópicos: fótons (luz), elétrons, átomos, etc.



- Muito diferente das teorias físicas anteriores ("clássicas"):

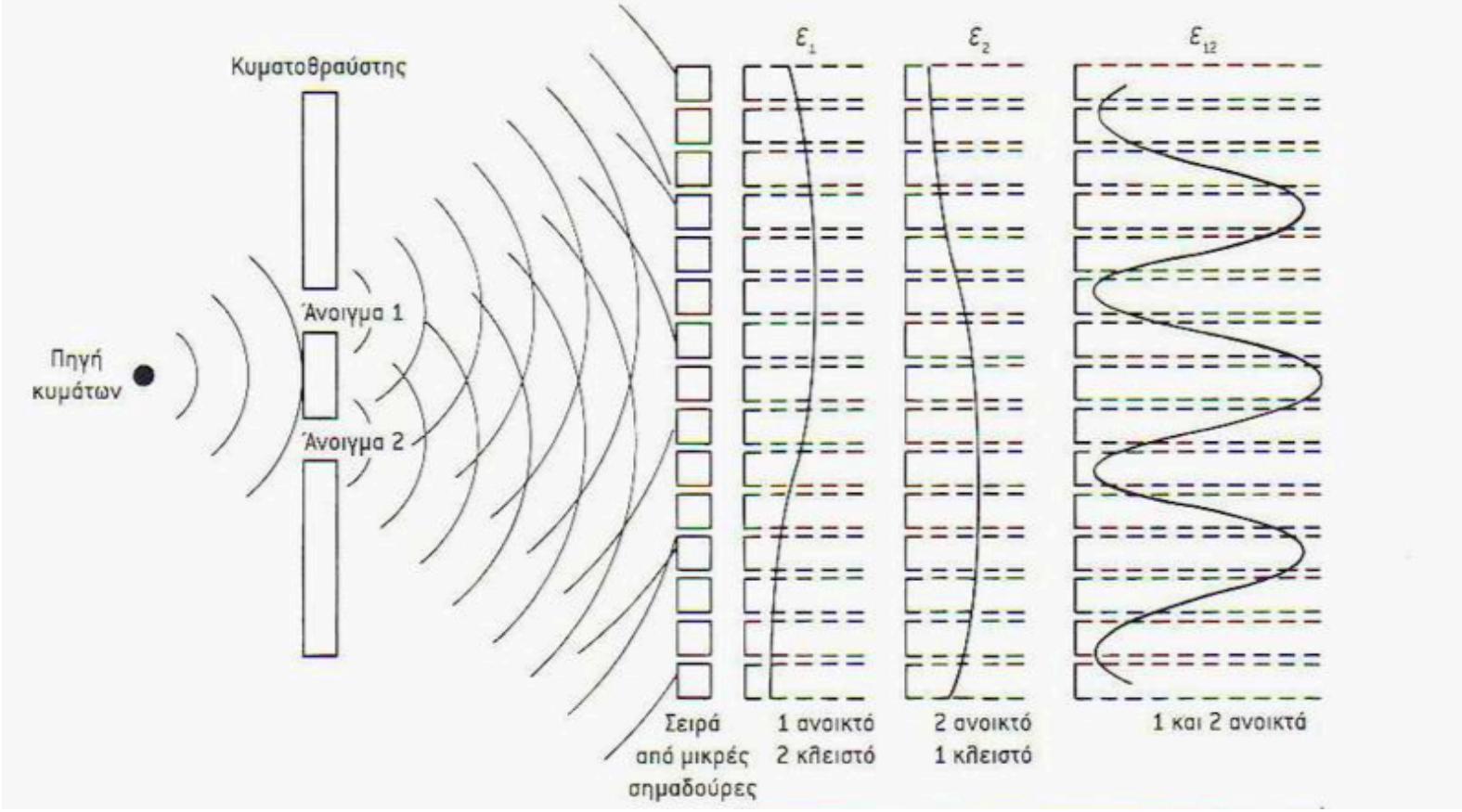
  - Descrição probabilística – a teoria só descreve as probabilidades de qualquer evento ocorrer.

  - Possibilidade de "superposição quântica" – combinação estranha de propriedades contraditórias (como estar em dois lugares ao mesmo tempo)

  - Emaranhamento quântico - correlações fortes entre
  - propriedades de partículas separadas

Fenda dupla – ondas

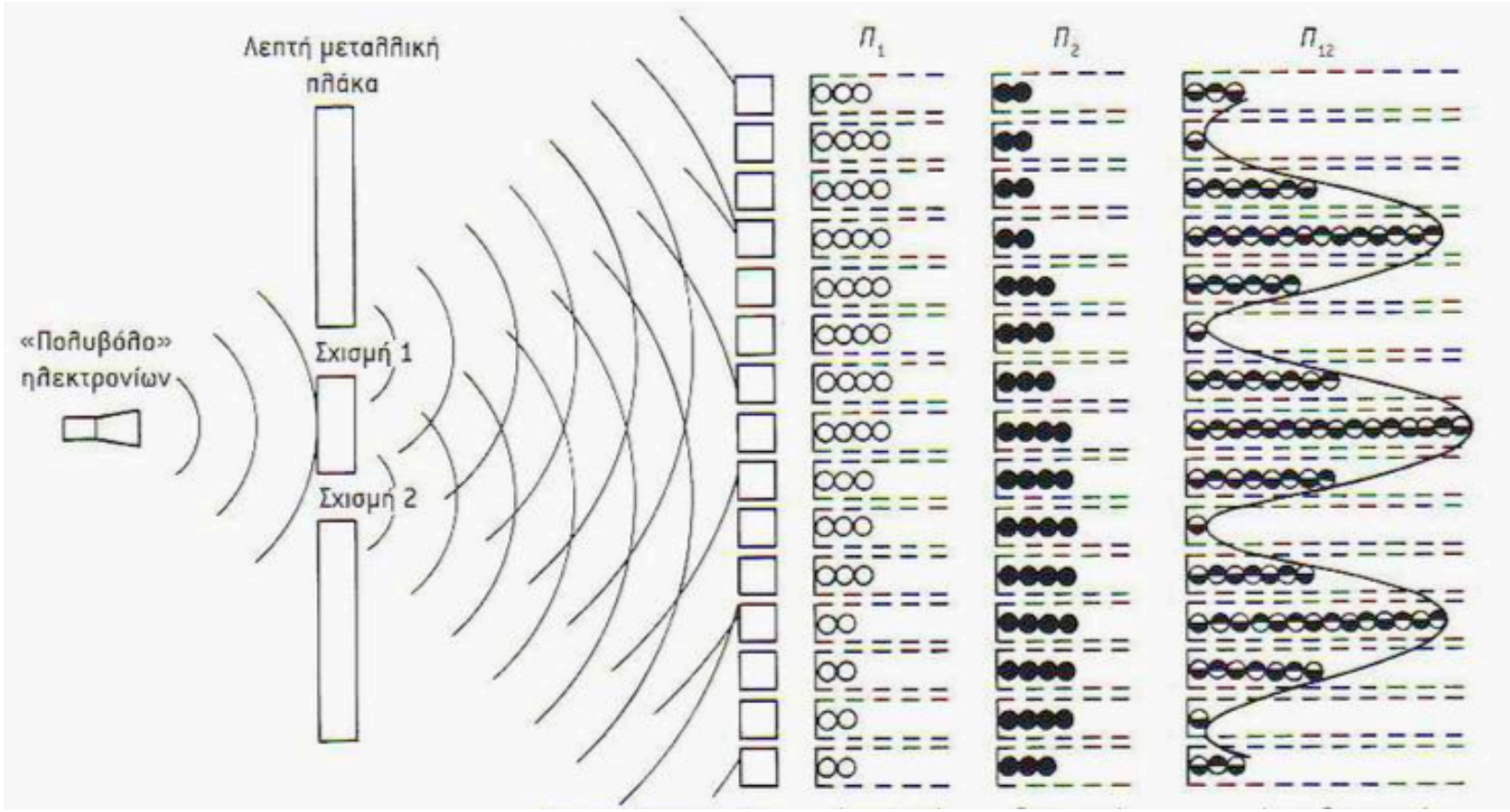
Experiência da fenda dupla com ondas d'água:



Fenda dupla Bóias I_1 I_2 I_{12} = intensidade com as duas fendas abertas

Fenda dupla – luz

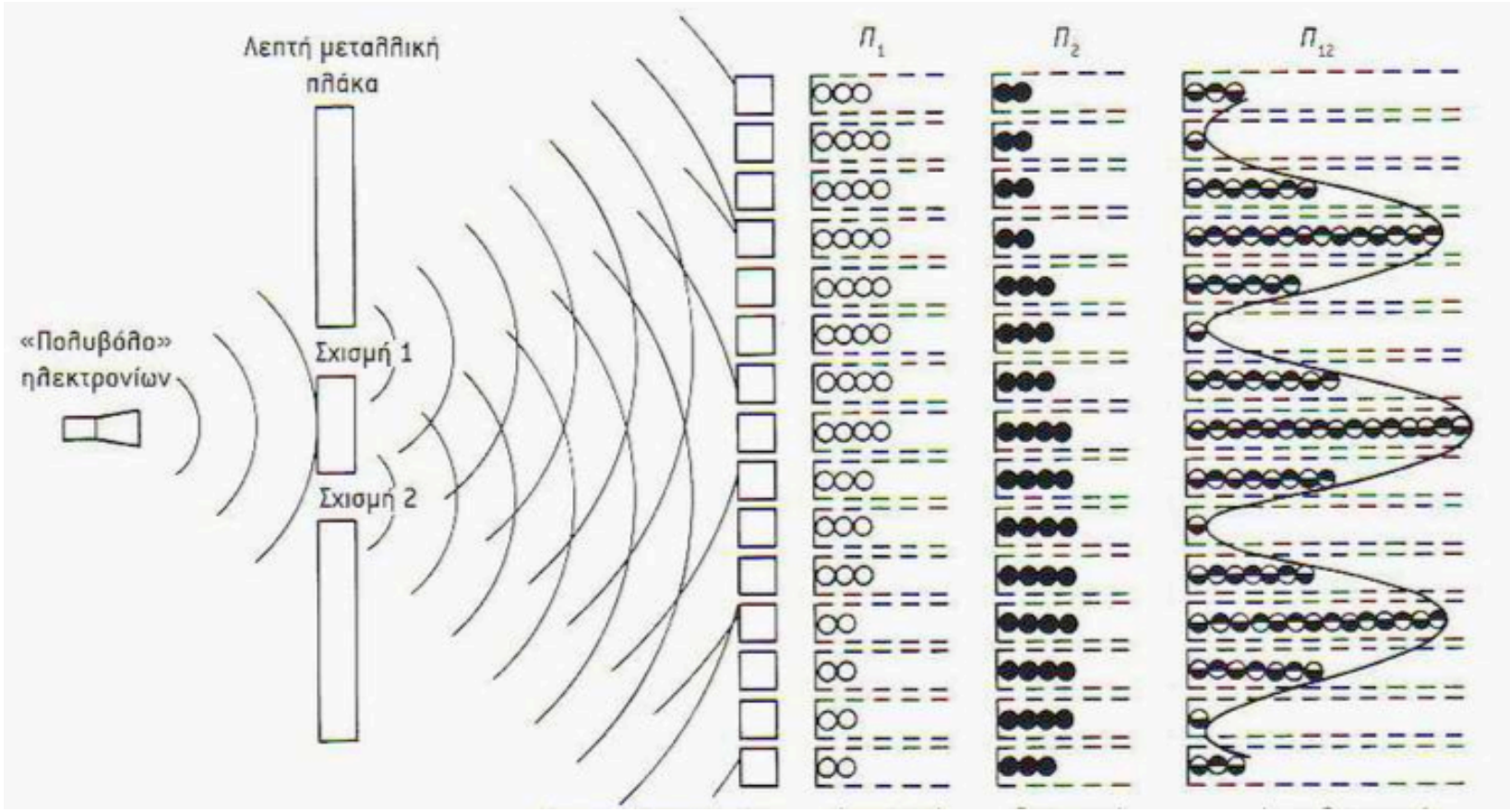
Experiência da fenda dupla com fótons:



Fenda dupla | Foto-detetores | P_1 | P_2 | P_{12} = detecções com as duas fendas abertas.

Fenda dupla – elétrons

Experiência da fenda dupla com elétrons:



Fenda dupla Tela P_1 P_2 P_{12} = detecções com as duas fendas abertas.

Elétrons se comportam da mesma forma que fótons!

O papel do observador na dinâmica

Sistemas quânticos seguem duas dinâmicas diferentes:

• Dinâmica de onda: $\psi(x,t)$ evolui como onda, de acordo com a equação de Schrodinger, desde que não haja observação.

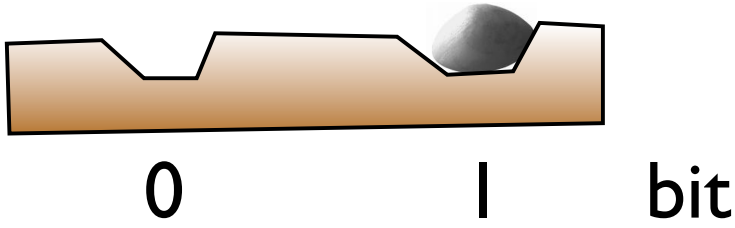
• Colapso: Interação com observador reduz a função de onda, de forma probabilística ($p = |\psi(x,t)|^2$), a uma função de onda específica, associada ao valor observado.

• Papel do observador é novidade em física, introduzida pela MQ. Manifestações disso:

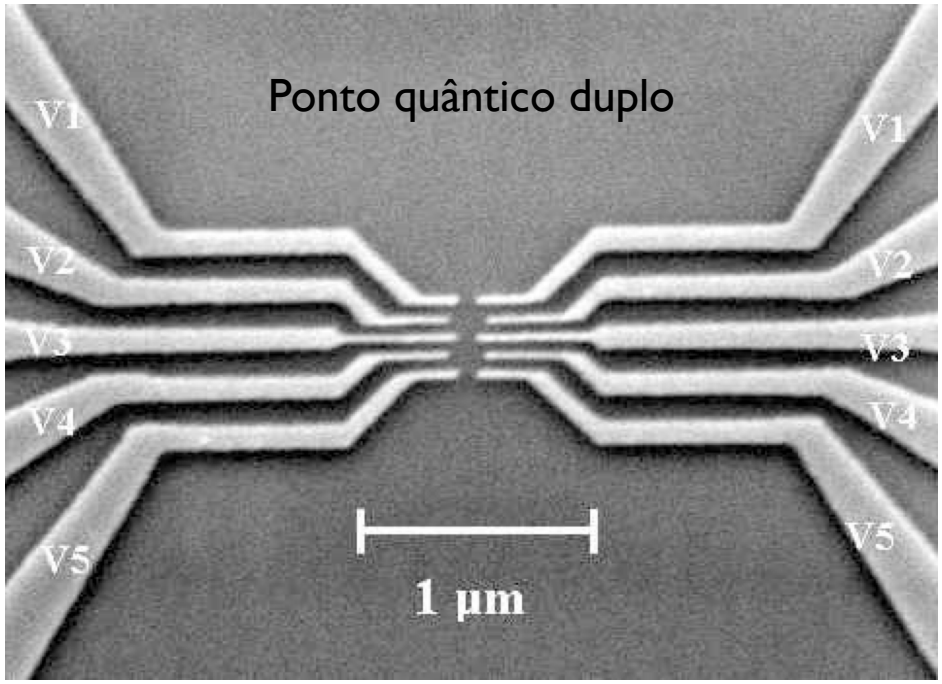
- Princípio da incerteza de Heisenberg
- Efeito Zenão

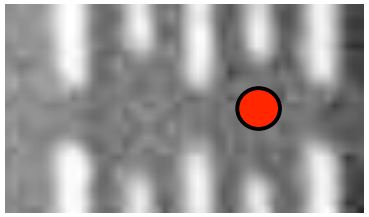
Superposições

- Física clássica: objeto tem posição bem-definida
- (2 posições codificam 1 bit)



- Física quântica: elétron pode estar numa situação de superposição de 2 posições





1

Superposições

•A física quântica permite novas operações sobre o elétron:
-estado inicial: 0
-Operação especial com eletrodos cria superposição

Medida da posição revela
-50% das vezes em 0
-50% das vezes em 1

qbit

p=1/2 0

p=1/2 1

• A superposição é sensível ao que fizermos nas duas posições!
Pulsos lasers nas duas posições afetam o elétron

Medida da posição revela mudanças nas probabilidades
de encontrar o elétron em cada ponto.

P=3/4 0

p=1/4 1

➡ um pouco como se o elétron estivesse nos dois lugares ao mesmo tempo!

Não-localidade quântica

Computando com qbits

- Escolhemos sistema quântico para codificar zeros e uns.

Ex: níveis de energia eletrônicos de íons presos em armadilha

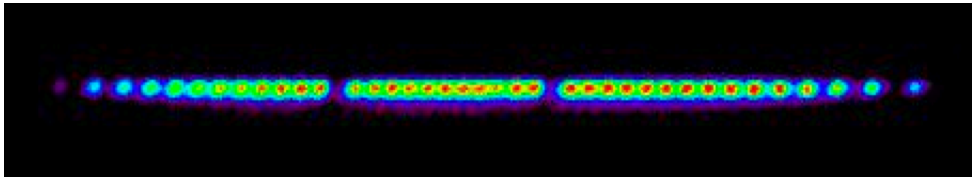
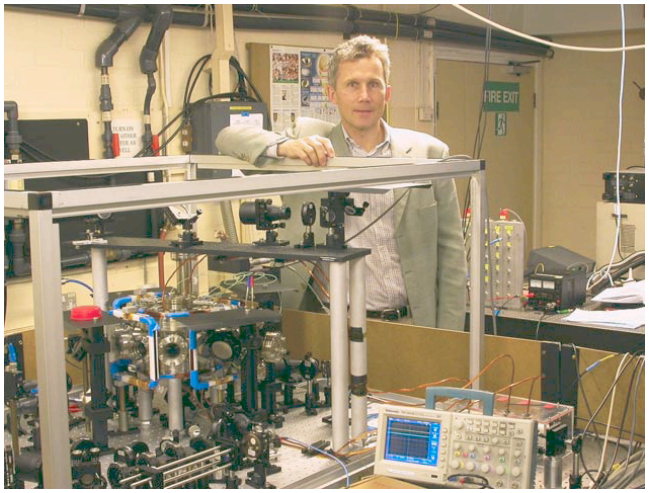
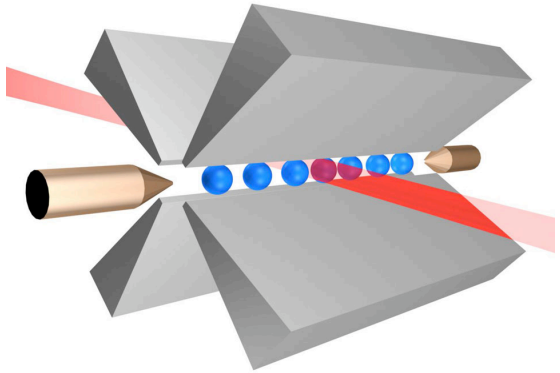


Foto de íons armadilhados



- Modificamos as superposições quânticas de maneira controlada.

Ex: pulsos laser em conjuntos de íons



- Medimos o sistema ao final das manipulações.

Ex: pulsos laser especiais para identificar os níveis de energia.

Só que há muitas dificuldades experimentais…

Computando com qbits

- Dificuldades:

  - acesso experimental x isolamento

  - fragilidade das superposições (*descoerência*)

  - controle preciso dos sistemas usados

- Situação experimental atual:

  - criptografia quântica comercial

  - demonstração do algoritmo de fatoração em RNM (15 = 3 x 5)

  - criação de superposições e controle de poucos qbits em diversos sistemas

- Ainda à procura de um sistema que possibilite um computador quântico útil...

Construindo um computador quântico: possibilidades

•Armadilhas de íons

-correntes e cargas elétricas prendem íons individuais no vácuo
-qbits codificados no estado eletrônico
-interações entre qbits são feitas com lasers e através do balanço conjunto dos íons

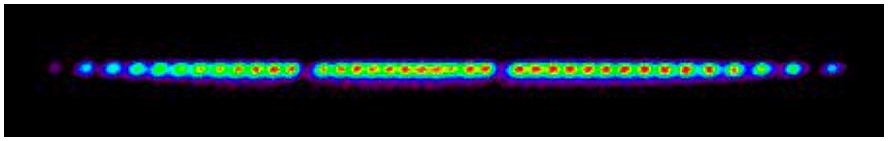
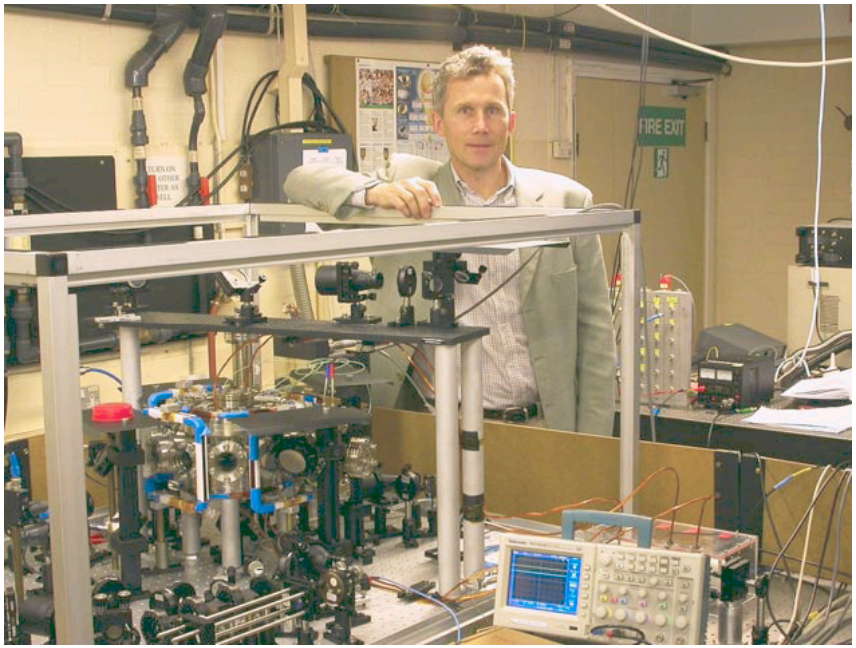
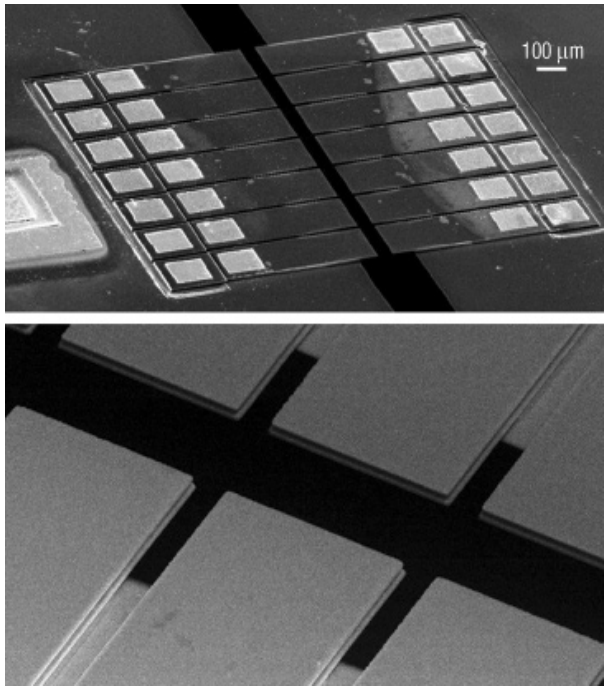


Foto de íons armadilhados



Laboratório (Chris Foot - Oxford)

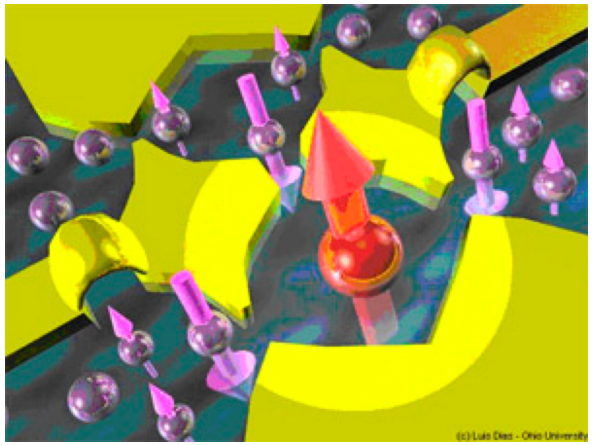


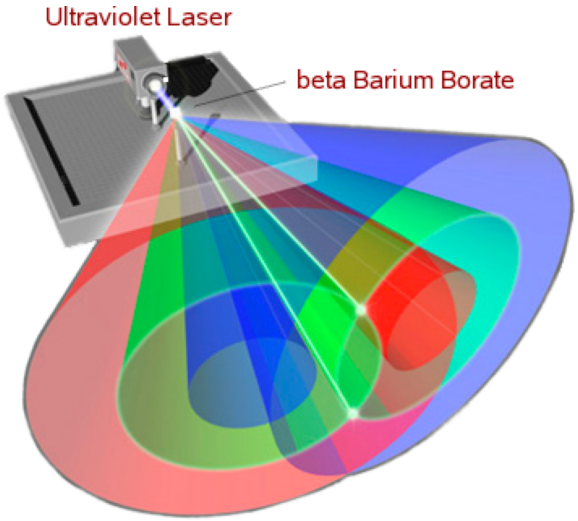
micro-armadilha de íons

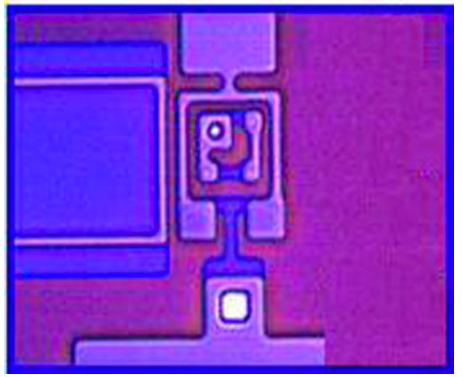
Construindo um computador quântico: possibilidades

•Outras alternativas:

-elétrons presos em pontos quânticos
-ressonância nuclear em líquidos
-luz laser (ótica quântica)
-circuitos supercondutores
-[??????]





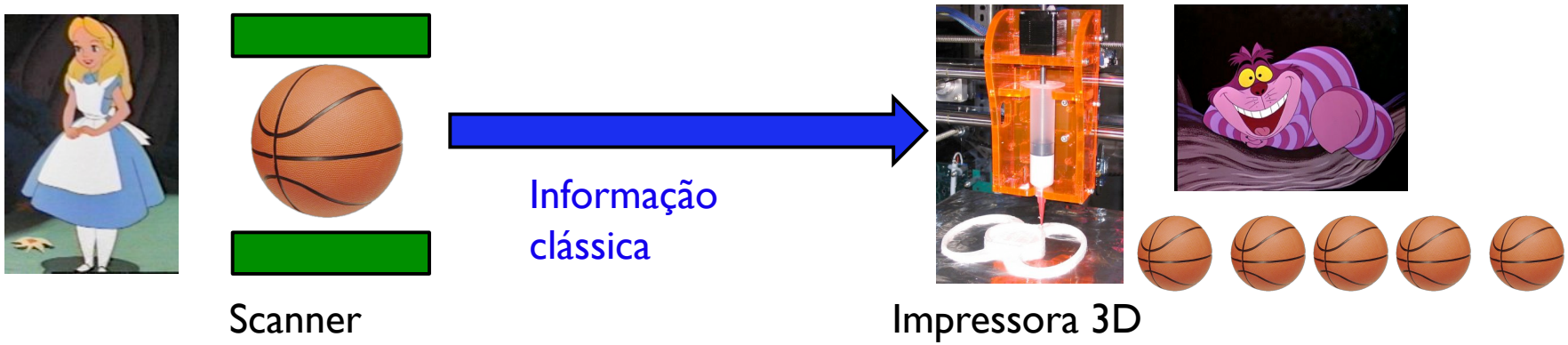


??????????

Outras aplicações de informação quântica

Teletransporte

Teletransporte: equivale a conjunto perfeito de scanner/impressora.

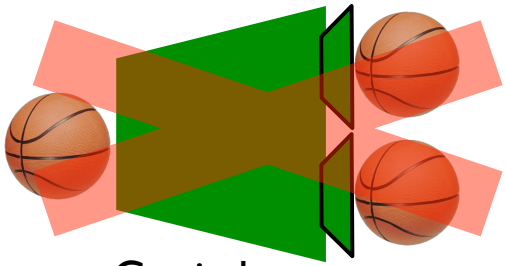


Problema: não dá para obter toda a informação de uma única cópia de sistema quântico – (Princípio da Incerteza de Heisenberg)

Redefinindo a tarefa: eu só quero fazer uma copiadora quântica perfeita, sem tentar obter/transmitir informação sobre o original.

Copiadoras quânticas

Copiadora quântica: usa evolução quântica (unitária) para criar cópias de um sistema quântico.



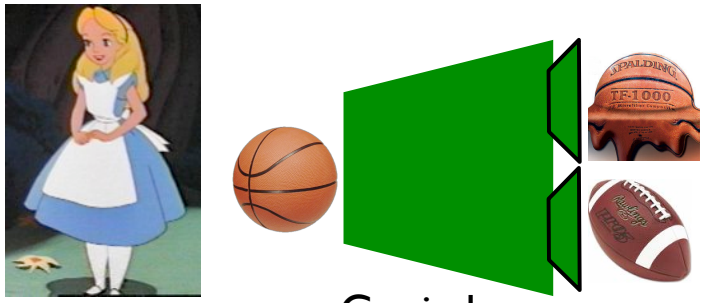
Copiadora

Problema: não dá!

Teorema da não clonagem – Wootters/Zurek (1982).

Copiadoras quânticas

Copiadora quântica *(quantum cloning machine):* usa evolução quântica para criar cópias imperfeitas de um sistema quântico.



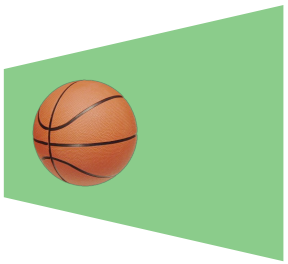
Copiadora imperfeita

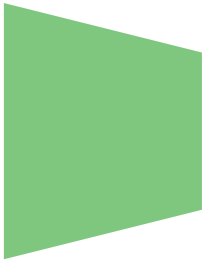
Copiadoras imperfeitas são possíveis – os limites são impostos pela MQ

Teletransporte quântico

Precisamos recriar à distância estado original, destruindo-o e sem obter nenhuma informação sobre ele.

Impossível classicamente, mas possível se usarmos efeitos quânticos.

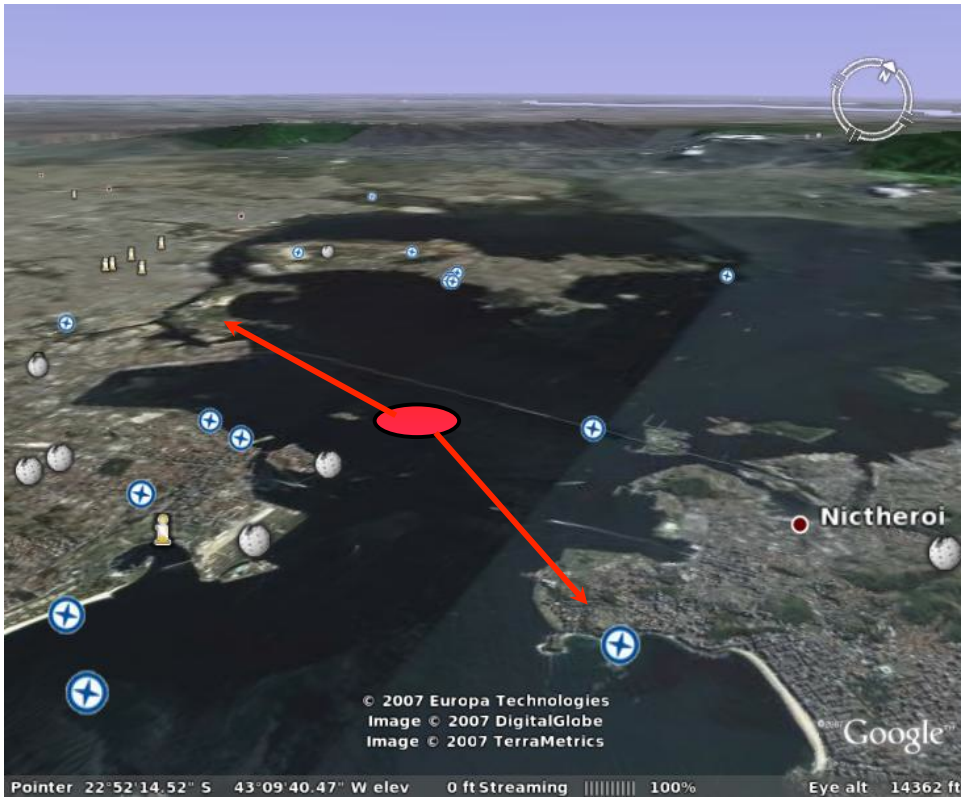




Emaranhamento

•Podemos criar pares de partículas para explorar a não-localidade quântica em aplicações

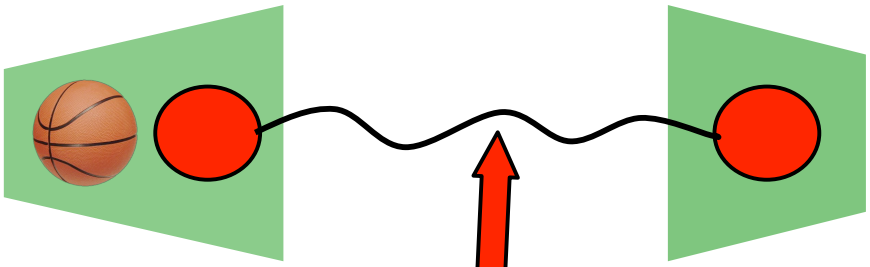
•Pares de partículas assim são ditas "emaranhadas"
-medidas separadas têm resultados fortemente correlacionados
-correlações úteis em tarefas envolvendo telecomunicação



Teletransporte quântico

Precisamos recriar à distância estado original, destruindo-o e sem obter nenhuma informação sobre ele.

Impossível classicamente, mas possível se usarmos efeitos quânticos.



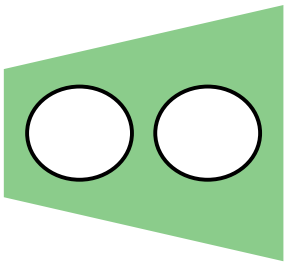
Protocolo de teletransporte: (Bennett et al., 1993)

1- A e B dispõem de par de partículas emaranhadas.

Teletransporte quântico

Precisamos recriar à distância estado original, destruindo-o e sem obter nenhuma informação sobre ele.

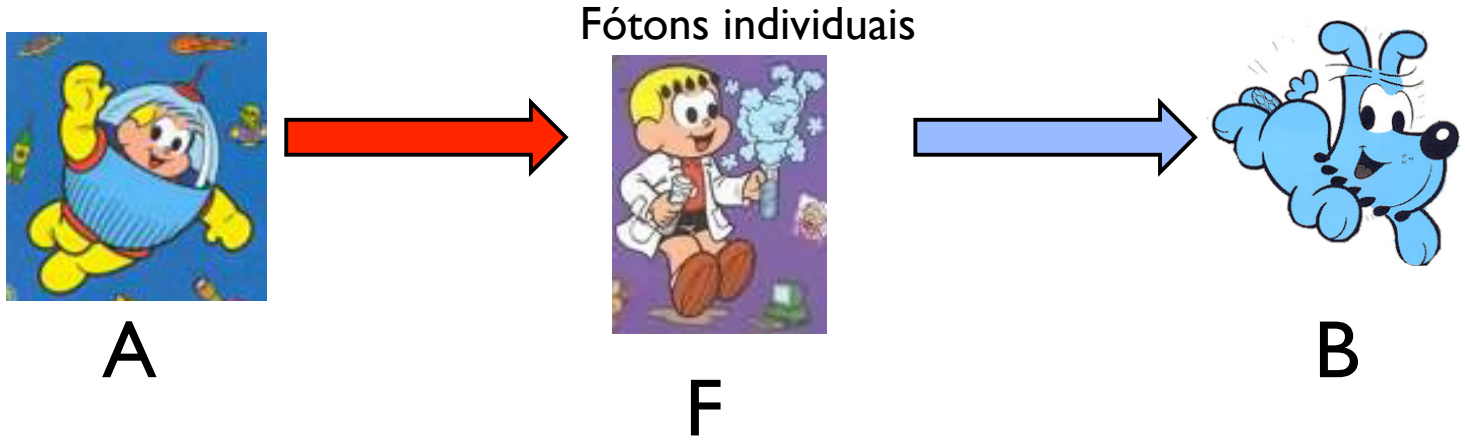
Impossível classicamente, mas possível se usarmos efeitos quânticos.



Protocolo de teletransporte: (Bennett et al., 1993)

1- A e B dispõem de par de partículas emaranhadas.
2- A faz medida conjunta em [original + uma perna do par].
3- A diz a B o resultado da medida, que B usa para aplicar unitário que faz seu sistema assumir o estado do original.

Criptografia quântica



- A se comunica com B através de canal quântico (ex: polarização de fótons)
- Interceptação pelo espião (F) resulta em perturbação inevitável do fóton

medida quântica

Garantia de segurança absoluta na troca de mensagens

Criptografia quântica comercial

- Já há pelo menos 4 companhias que já comercializam sistemas de criptografia quântica:

- IdQuantique (Suíça)

- Smartquantum (França)

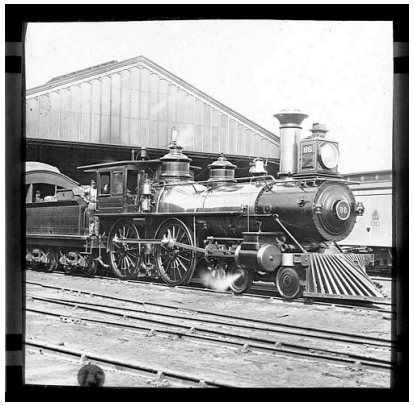
- QuintessenceLabs (Austrália)

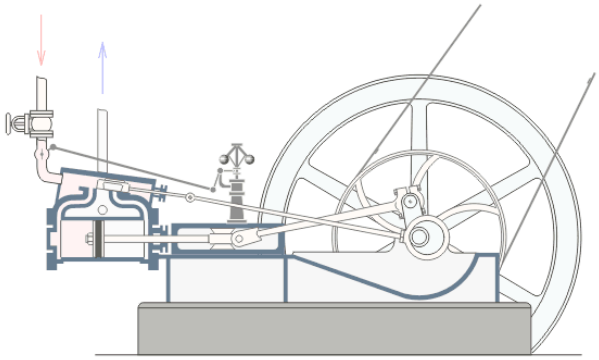
- MagiQ Technologies (EUA)

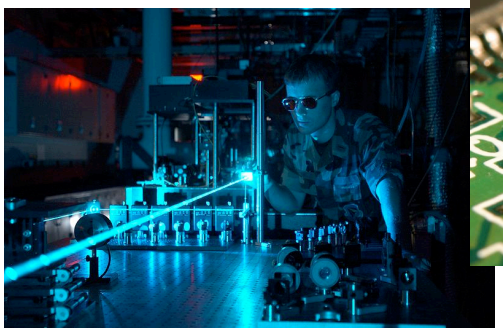
Importância estratégica

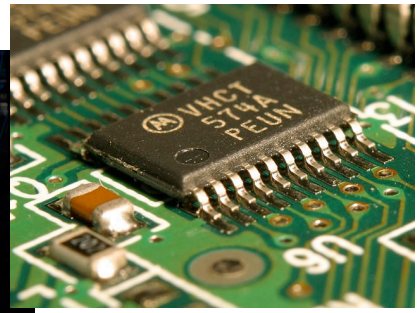
Séc. XIX:

tecnologias limitadas pela
termodinâmica e mecânica clássica









Séc. XX:

tecnologias limitadas pela mecânica
quântica

Séc. XXI:

tecnologias usando os efeitos mais sutis da mecânica quântica:
Informação quântica, spintrônica, ... ?

Novas tecnologias usando informação quântica

Computação

- Tratabilidade/intratabilidade com computadores quânticos
- Que problemas tratáveis (classicamente) admitem aceleração polinomial com CQ?
- Simulação de sistemas quânticos (novos materiais, etc)
- Códigos quânticos de correção de erros

Criptografia

- fatoração rápida = quebra da criptografia RSA
- desenvolvimento de protocolos seguros mesmo contra CQs
- criptografia quântica com segurança absoluta

Protocolos interativos com comunicação quântica/emaranhamento

- vantagem quântica (até exponencial) em complexidade de comunicação e outras tarefas

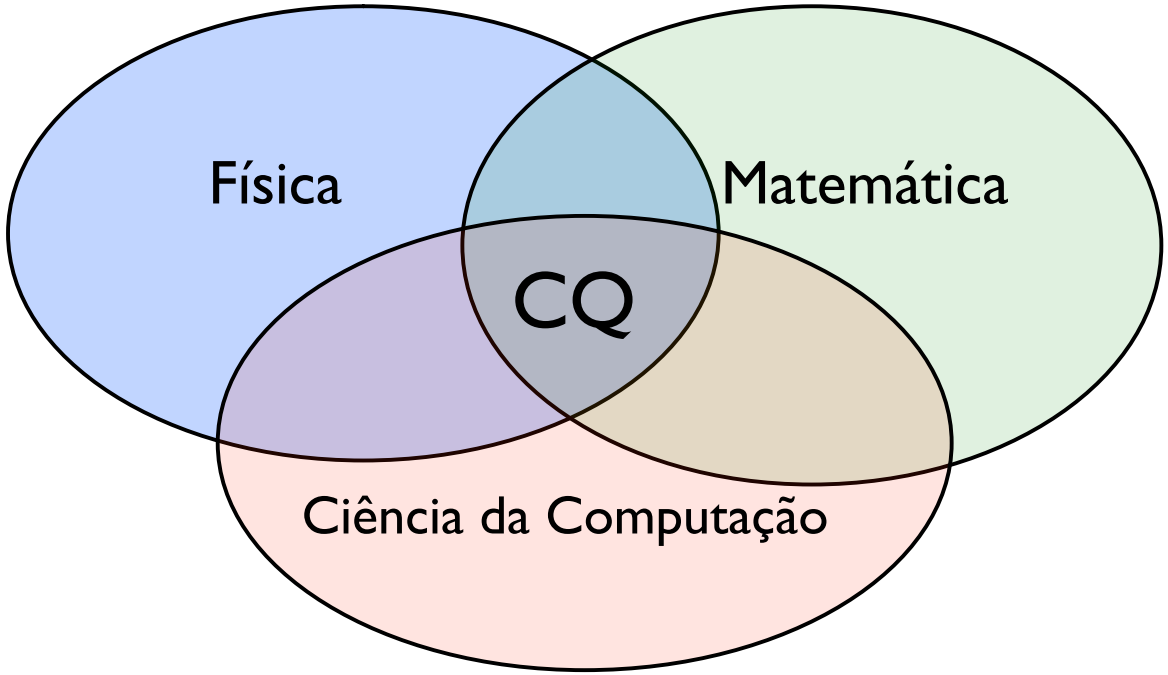
Metrologia

- vantagem em medidas de precisão usando estados emaranhados da luz

Design de células solares, cálculos de química quântica, …

[ver *A Federal Vision for Quantum Information Science* (Janeiro 2009) – relatório do Conselho Nacional de Ciência e Tecnologia – E.U.A.]

Perspectivas – Computação Quântica



No Brasil:

Instituto Nacional de Ciência e Tecnologia (INCT) de Informação Quântica - CNPq
- 20 grupos de pesquisa em 7 estados, predominância de físicos

Fora:

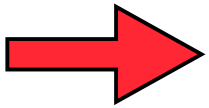
IQC & Perimeter (Waterloo, Canadá), Caltech, MIT, CQCT (Austrália), Cambridge, Viena, …

Perspectivas – Computação Quântica

- Área interdisciplinar em pleno desenvolvimento

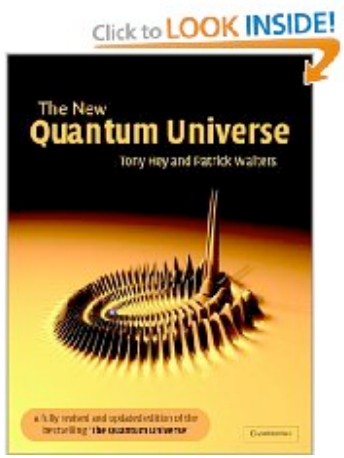
- Computação quântica em grande escala pode levar décadas, mas antes:
  - criptografia quântica
  - simulações de sistemas quânticos
  - outras novas tecnologias

- Por volta de 2020 já não conseguiremos mais miniaturizar os transístores...



Melhor aprender desde já como processar informação quanticamente!

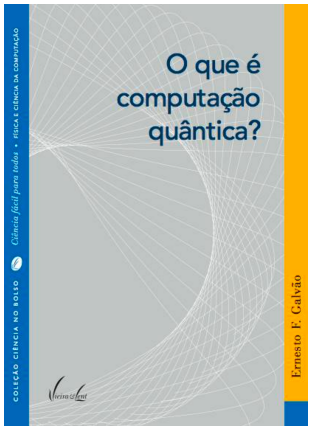
Sugestões de leitura



"The new quantum universe", Tony Hey and Patrick Walters (Cambridge University Press, 2003)

•"A face oculta da Natureza: o novo mundo da física quântica", Anton Zeilinger (Ed. Globo)

•"O que é computação quântica?", Ernesto F. Galvão (Ed. Vieira&Lent - 2007).



•"A essência da realidade", David Deutsch (Ed. Makron Books)

•Vejam o site do meu livro para mais dicas de leitura na web:

•http://profs.if.uff.br/ernesto/

- Mini-curso de introdução à MQ;
- Palestras sobre computação quântica.