
Introdução à Computação Quântica:

Daniel Jonathan
Instituto de Física – UFF

Baseado em slides por:
Ernesto F. Galvão



Panoramas da Física - 2012

Linha do tempo – computação

Pré-história

c. 3000 A.C.

c. 2400 A.C.

c. 100 A.C.

Pedrinhas,
contabilidade do
gado

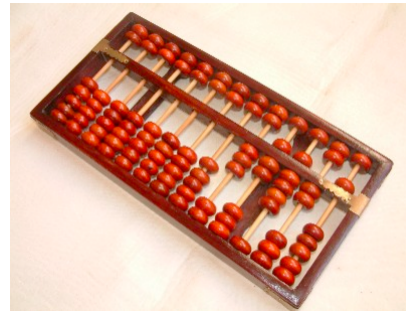


Escrita, contabilidade
(Mesopotâmia)

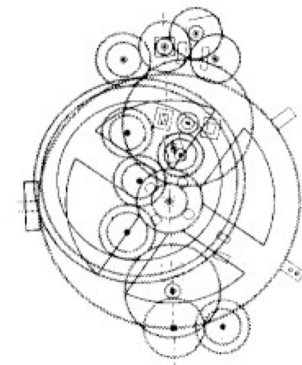


Escrita suméria (c. 2500 A.C.)

Ábaco (Babilônia)



Máquina de Anticítera:
cálculos astronômicos



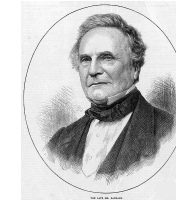
Reconstituição

Linha do tempo – computação

Séc. XVII

1801

1837-1871



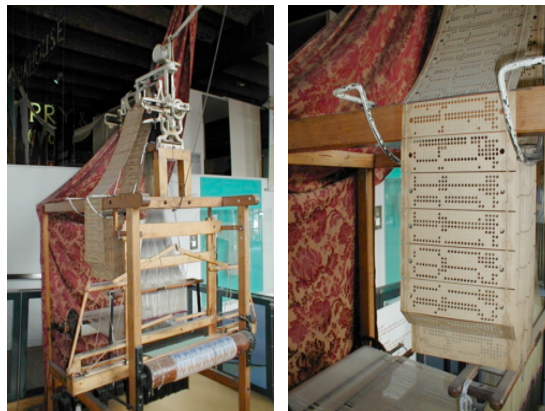
Schickard (1623)
Pascal (1642)
Leibniz (1671)

Calculadoras
mecânicas para
certas tarefas



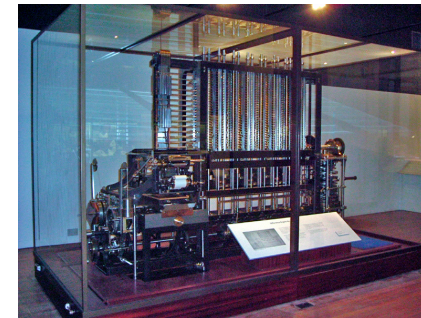
Leibniz

Dispositivos
“programáveis”

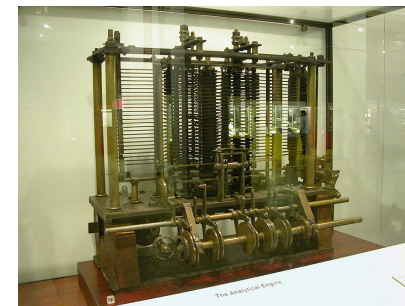


Tear de Jacquard (1801)

Charles Babbage: primeiro projeto
de computador programável – Engenho
Analítico

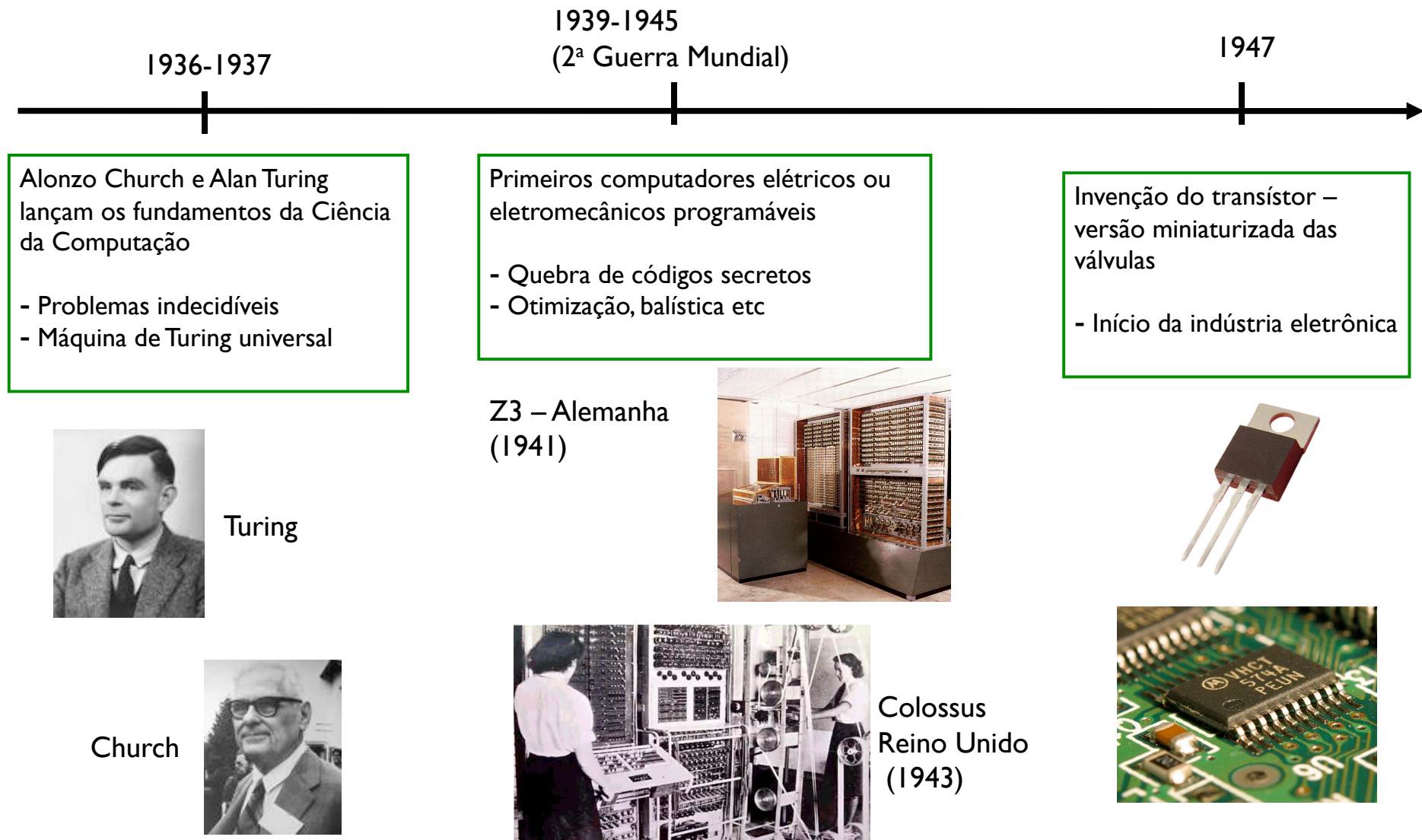


Engenho
Diferencial
(1822/1991)



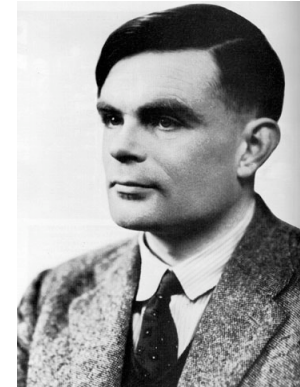
Engenho Analítico
(parte)(1837-1991)
- 10m x 30m,
movido a vapor!

Linha do tempo – computação



Ciência da Computação

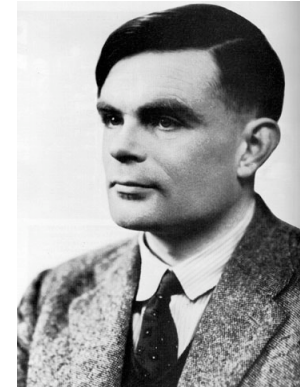
- **Alan Turing** (1935) - Formalização matemática dos conceitos de:
 - procedimento preciso para calcular algo - *algoritmo*
 - um tipo simples de computador



Ciência da Computação

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

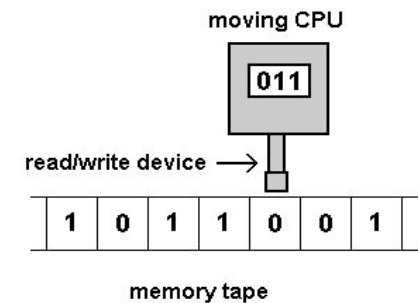
- procedimento preciso para calcular algo - *algoritmo*
- um tipo simples de computador



- **Máquina de Turing**

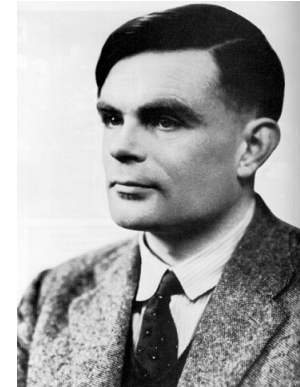
- CPU se movimenta de acordo com programa, lendo e apagando dados
- simples, mas capaz de *qualquer* computação:

- ➡ **Tese de Church-Turing**



Ciência da Computação

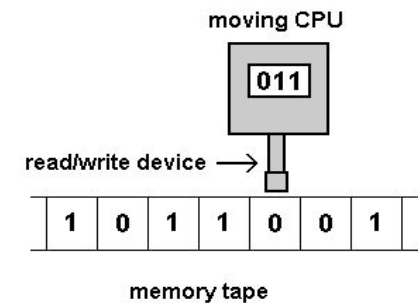
- **Alan Turing** (1935) - Formalização matemática dos conceitos de:
 - procedimento preciso para calcular algo - *algoritmo*
 - um tipo simples de computador



- **Máquina de Turing**

- CPU se movimenta de acordo com programa, lendo e apagando dados
- simples, mas capaz de *qualquer* computação:

- ➔ **Tese de Church-Turing**



- Resultados:

- existem problemas **incomputáveis**
- (ex: decidir se um dado programa vai ou não entrar em 'loop' sem fim.
- problemas computacionais podem ser divididos, grosso modo, entre *tratáveis* e *intratáveis*.

Intratabilidade computacional

- Considere
 - Problema computacional com entrada de d dígitos;
 - Algoritmo que usa N portas lógicas/passos computacionais.

Problema tratável: N é proporcional a polinômio de d .

- Ex.: multiplicação de dois números de d dígitos.

$$N \sim d^2$$

Intratabilidade computacional

- Considere
 - Problema computacional com entrada de d dígitos;
 - Algoritmo que usa N portas lógicas/passos computacionais.

Problema tratável: N é proporcional a polinômio de d .

- Ex.: multiplicação de dois números de d dígitos.
 $N \sim d^2$

Problema intratável: N cresce mais rápido do que qualquer polinômio.

- Ex.: fatoração de inteiro de d dígitos.
- Melhor algoritmo conhecido: $N \sim 2^d$
- ➡ resultado: fatorar um número de 400 dígitos levaria **bilhões de anos** neste computador!!

Intratabilidade computacional

- Considere
 - Problema computacional com entrada de d dígitos;
 - Algoritmo que usa N portas lógicas/passos computacionais.

Problema tratável: N é proporcional a polinômio de d .

- Ex.: multiplicação de dois números de d dígitos.
 $N \sim d^2$

Problema intratável: N cresce mais rápido do que qualquer polinômio.

- Ex.: fatoração de inteiro de d dígitos.
- Melhor algoritmo conhecido: $N \sim 2^d$
- ➡ resultado: fatorar um número de 400 dígitos levaria **bilhões de anos** neste computador!!

• Problemas **intratáveis** são importantes:

- **Fatoração**: chave para quebrar códigos criptográficos (RSA)
- **Otimização**: aumento de rendimento na indústria
- **Problemas científicos** em geral

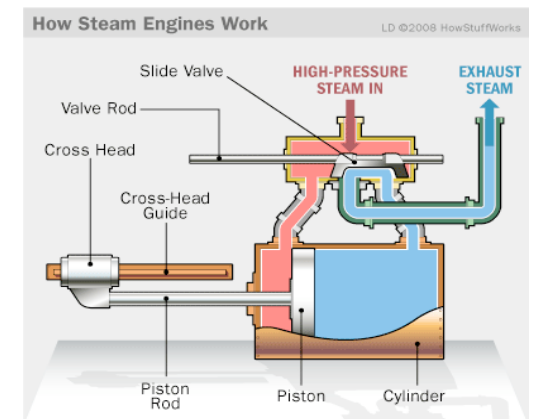
Mas... e a Física?

- A ciência da computação não levava em conta que a **computação é um processo físico**.
- **Leis físicas** determinam os limites dos computadores:

Mas... e a Física?

- A ciência da computação não levava em conta que a **computação é um processo físico**.
- **Leis físicas** determinam os limites dos computadores:

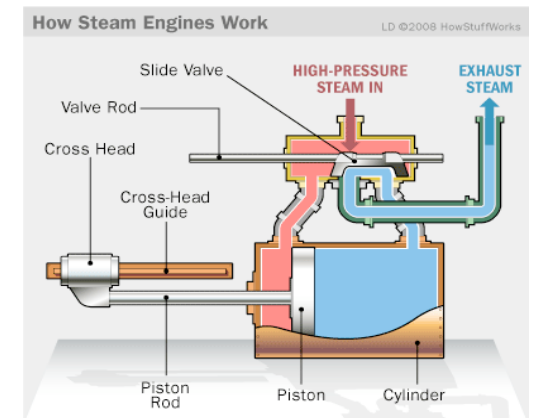
Ex: a Termodinâmica indica que computadores poderiam em princípio processar informação *sem gastar energia* (portanto sem 'esquentar'), porém sempre precisarão da energia mínima $kT \cdot \ln 2$ ($\sim 3 \times 10^{-21} \text{ J}$) para *apagar cada bit de memória* ao iniciar uma nova computação. (Os computadores atuais gastam bem mais, por ineficiências práticas).



Mas... e a Física?

- A ciência da computação não levava em conta que a **computação é um processo físico**.
- **Leis físicas** determinam os limites dos computadores:

Ex: a Termodinâmica indica que computadores poderiam em princípio processar informação *sem gastar energia* (portanto sem ‘esquentar’), porém sempre precisarão da energia mínima $kT \ln 2$ ($\sim 3 \times 10^{-21} \text{ J}$) para *apagar cada bit de memória* ao iniciar uma nova computação. (Os computadores atuais gastam bem mais, por ineficiências práticas).



qual a teoria mais abrangente que descreve a dinâmica de máquinas que computam?

Física Quântica

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**

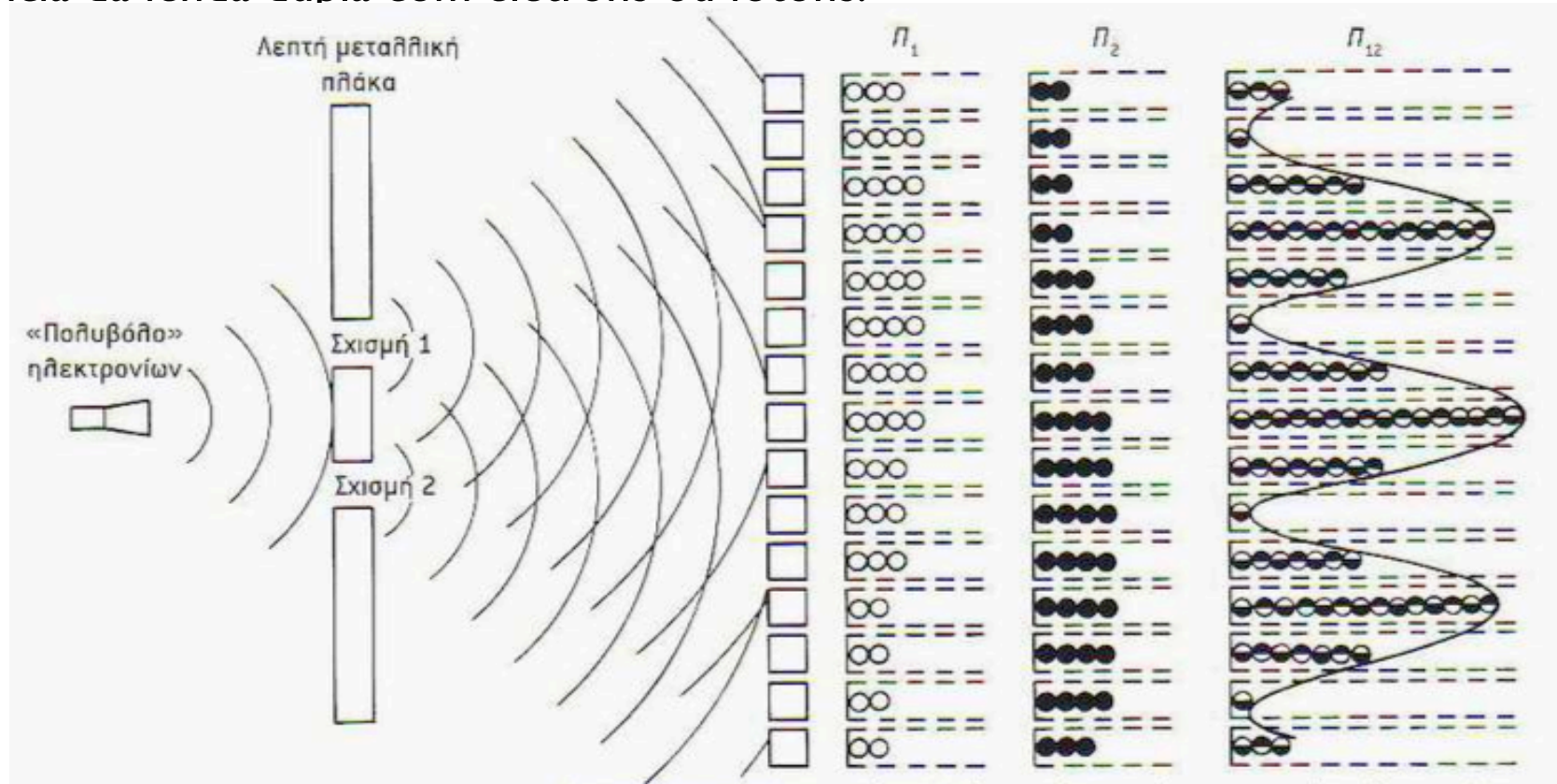
Física quântica

- Desenvolvida na década de 1920 para descrever sistemas microscópicos: fótons (luz), elétrons, átomos, etc.
- Muito diferente das teorias físicas anteriores (“clássicas”):
 - Descrição **probabilística**
 - Possibilidade de “**superposição**” - combinação simultânea de propriedades classicamente contraditórias, como por exemplo ‘estar em dois lugares ao mesmo tempo’



Relembrando: Fenda dupla

Experiência da fenda dupla com elétrons ou fótons:



Tela

P_1

P_2

P_{12} = detecções com
as duas fendas abertas.

Para explicar o padrão, as partículas precisam ter passado por ambas as fendas -> “superposição” de duas posições!

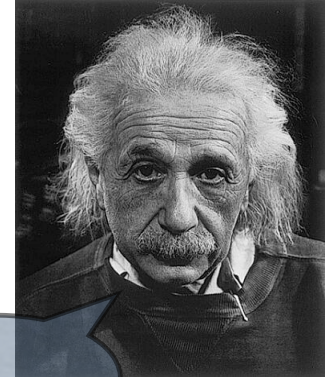
Física quântica

- Desenvolvida na década de 1920 para descrever sistemas microscópicos: fótons (luz), elétrons, átomos, etc.
- Muito diferente das teorias físicas anteriores (“clássicas”):
 - Descrição **probabilística**
 - Possibilidade de “**superposição**” - combinação simultânea de propriedades classicamente contraditórias, como por exemplo ‘estar em dois lugares ao mesmo tempo’
 - **Emaranhamento quântico** - correlações fortes entre propriedades de partículas separadas

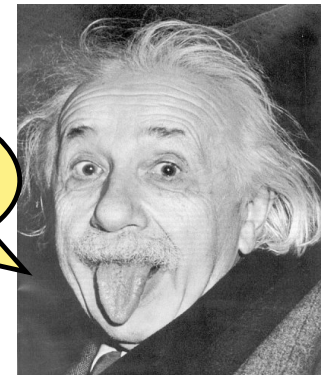


Física quântica

- Desenvolvida na década de 1920 para descrever sistemas microscópicos: fótons (luz), elétrons, átomos, etc.
- Muito diferente das teorias físicas anteriores (“clássicas”):
 - Descrição **probabilística**
 - Possibilidade de “**superposição**” - combinação simultânea de propriedades classicamente contraditórias, como por exemplo ‘estar em dois lugares ao mesmo tempo’
 - **Emaranhamento quântico** - correlações fortes entre partículas de partículas separadas



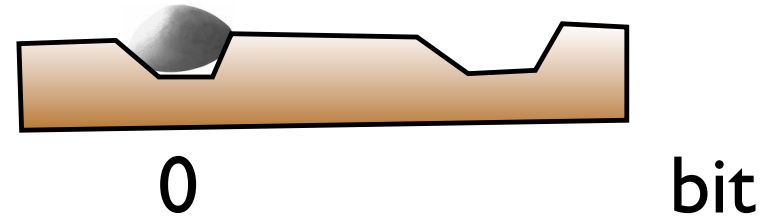
Deus não joga dados!



Fantasmagórica ação a distância!

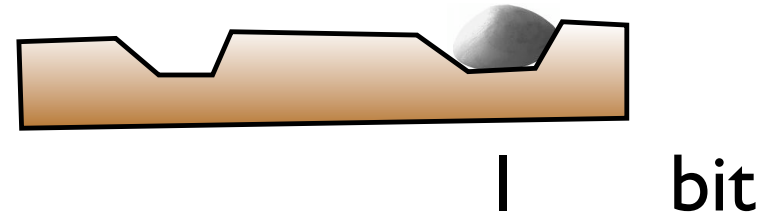
Superposições e informação

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



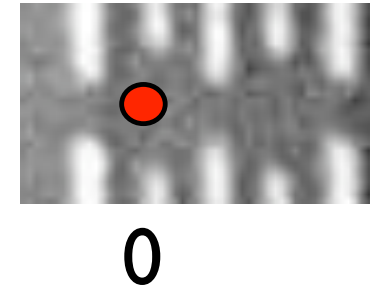
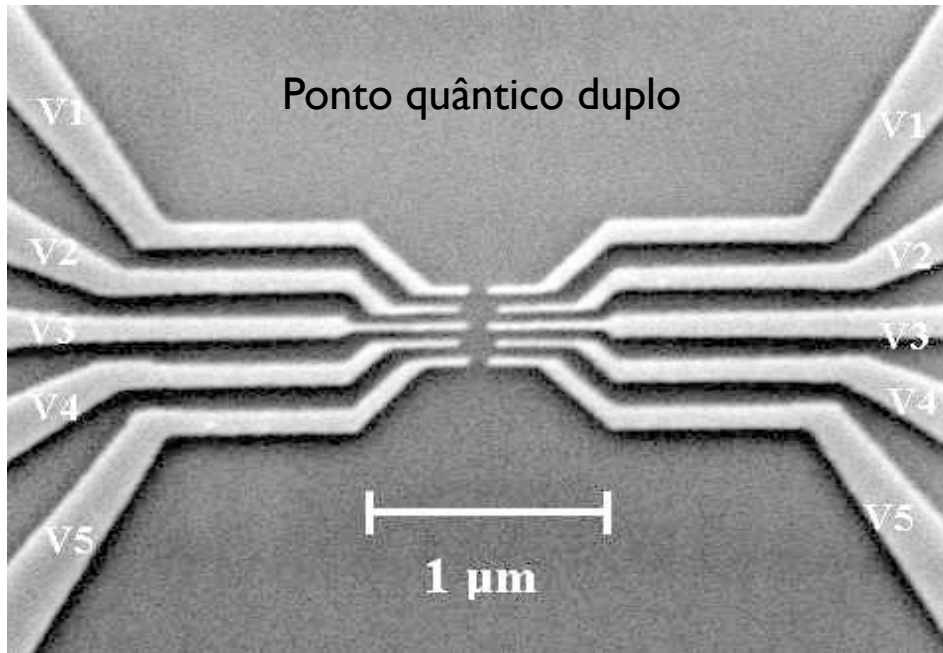
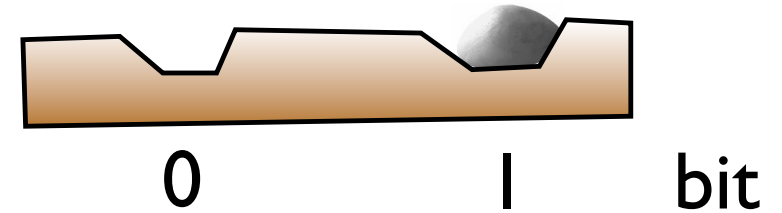
Superposições e informação

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



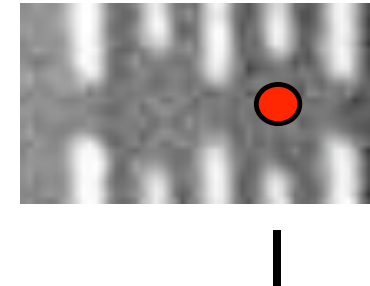
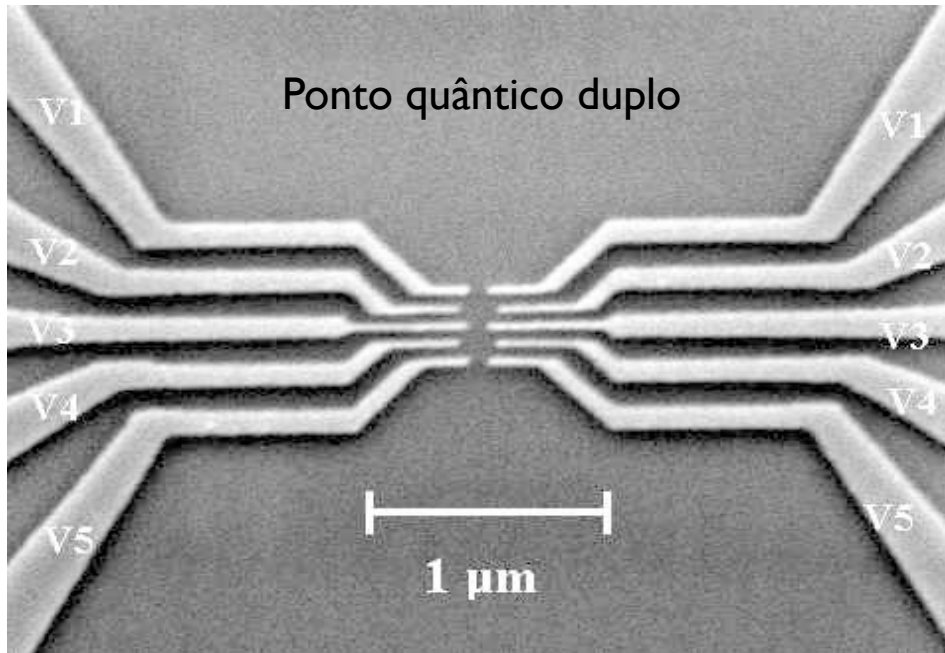
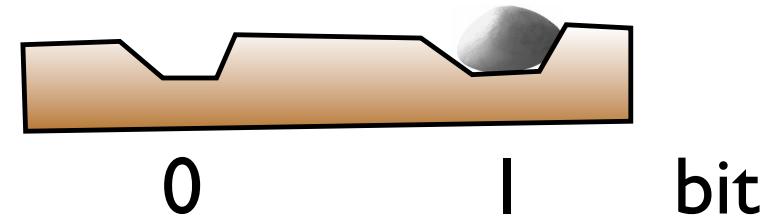
Superposições e informação

- Física clássica: objeto tem posição bem-definida
- (2 posições codificam 1 bit)
- Física quântica: elétron pode estar numa situação de superposição de 2 posições



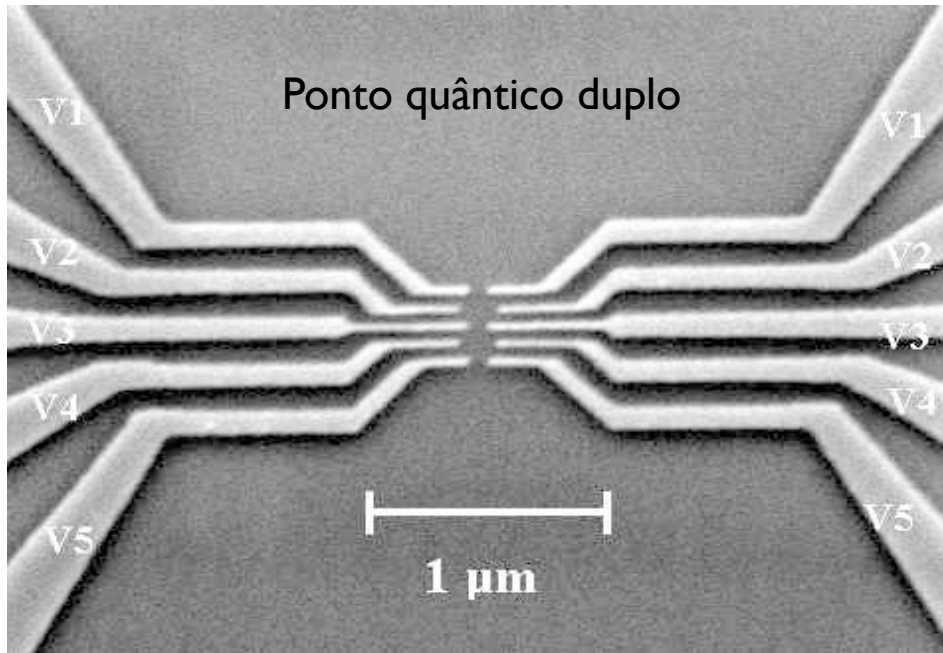
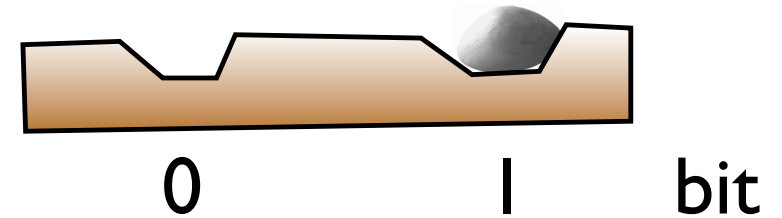
Superposições e informação

- Física clássica: objeto tem posição bem-definida
- (2 posições codificam 1 bit)
- Física quântica: elétron pode estar numa situação de superposição de 2 posições



Superposições e informação

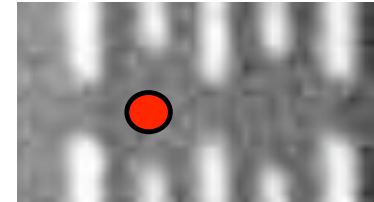
- Física clássica: objeto tem posição bem-definida
- (2 posições codificam 1 bit)
- Física quântica: elétron pode estar numa situação de superposição de 2 posições



Superposição
de 0 e 1 !

Superposições e informação

- A física quântica permite novas operações computacionais
- estado inicial: 0



0

Superposições

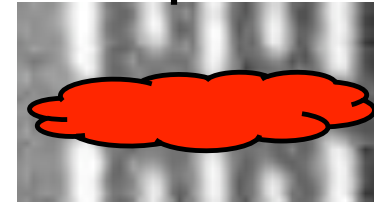
- A física quântica permite novas operações computacionais:
 - estado inicial: 0
 - Operação especial com eletrodos cria superposição



Superposições

- A física quântica permite novas operações computacionais:
 - estado inicial: 0
 - Operação especial com eletrodos cria superposição

qbit



Superposições

- A física quântica permite novas operações computacionais:
 - 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

Superposições

- A física quântica permite novas operações computacionais:
 - estado inicial: 0
 - Operação especial com eletrodos cria superposição

Medida da posição revela

- 50% das vezes em 0
- 50% das vezes em 1

• P: qual a diferença para uma situação em que o elétron está, de fato, em uma das posições, apenas não sabemos qual?

• R: A superposição é sensível ao que fizermos nas duas posições!

qbit



$p=1/2$ 0

$p=1/2$ 1



Superposições

- A física quântica permite novas operações computacionais:
 - estado inicial: 0
 - Operação especial com eletrodos cria superposição

Medida da posição revela

- 50% das vezes em 0
- 50% das vezes em 1

• P: qual a diferença para uma situação em que o elétron está, de fato, em uma das posições, apenas não sabemos qual?

• R: A superposição é sensível ao que fizermos nas duas posições!

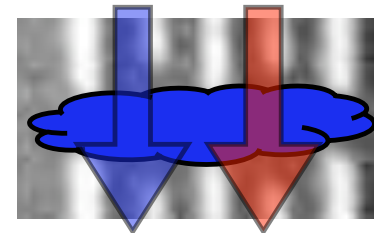
Aplicamos pulsos lasers **nas duas posições**

qbit



$p=1/2$ 0

$p=1/2$ 1



Superposições

- A física quântica permite novas operações computacionais:

- estado inicial: 0
- Operação especial com eletrodos cria superposição

Medida da posição revela

- 50% das vezes em 0
- 50% das vezes em 1

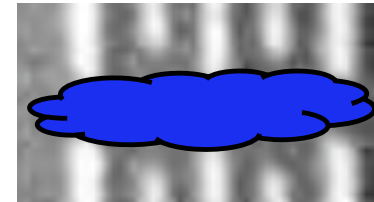
qbit



$p=1/2$ 0

$p=1/2$ 1

- P: qual a diferença para uma situação em que o elétron está, de fato, em uma das posições, apenas não sabemos qual?



- R: A superposição é sensível ao que fizermos nas duas posições!

Aplicamos pulsos lasers **nas duas posições**

$P=3/4$ 0

$p=1/4$ 1

Em seguida, medida da posição revela mudanças nas probabilidades de encontrar o elétron em cada ponto.

Superposições

- A física quântica permite novas operações computacionais:

- estado inicial: 0
- Operação especial com eletrodos cria superposição

Medida da posição revela

- 50% das vezes em 0
- 50% das vezes em 1

- P: qual a diferença para uma situação em que o elétron está, de fato, em uma das posições, apenas não sabemos qual?

- R: A superposição é sensível ao que fizermos nas duas posições!

Aplicamos pulsos lasers **nas duas posições**

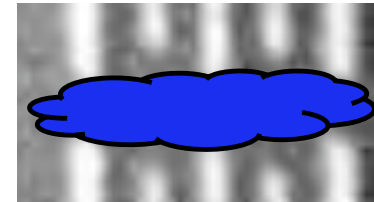
Em seguida, medida da posição revela mudanças nas probabilidades de encontrar o elétron em cada ponto.

qbit



$p=1/2$ 0

$p=1/2$ 1



$P=3/4$ 0

$p=1/4$ 1

Não-localidade quântica

Linha do tempo – computação e Física

1961

Formulação do **Princípio de Landauer**:

-Mínimo de energia dissipada por operação lógica irreversível



1973

Charles Bennett

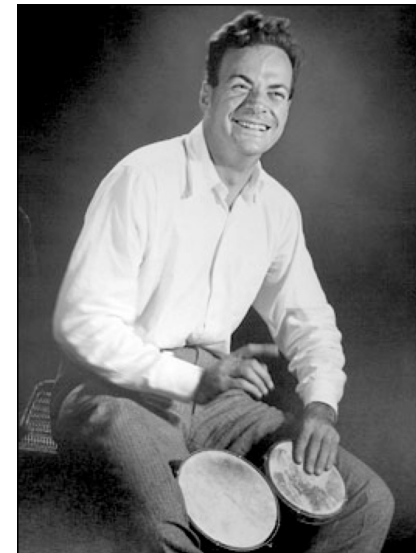
- Como fazer computação reversível, em princípio sem gasto de energia



1982

Richard Feynman

-Sistema quântico bem controlado para simular outros sist. quânticos

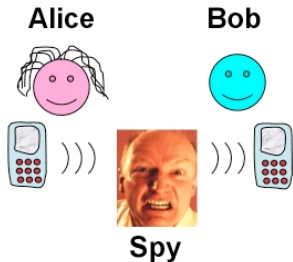


Linha do tempo – computação e Física

1984

Bennett/Brassard

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



1985

David Deutsch

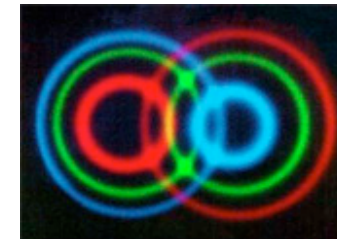
- Descreveu **uma máquina de Turing quântica**, e mostrou que ela poderia resolver alguns problemas mais rapidamente que um computador clássico



1991

Artur Ekert

- Criptografia quântica baseada em emaranhamento – E91



Pioneiros da computação quântica

- **Richard Feynman** (1982)

- cálculo de propriedades de sistemas quânticos parece ser um problema intratável
 - sistema quântico muito bem controlado poderia servir para calcular essas propriedades de maneira eficiente
- computador quântico



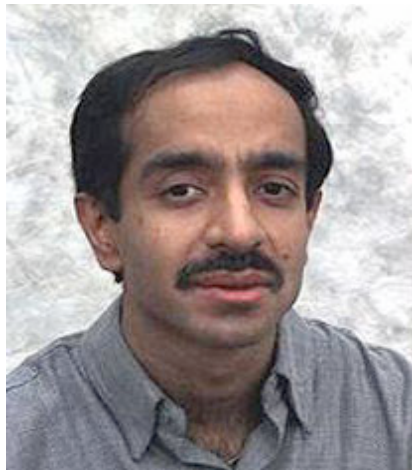
- **David Deutsch** (1985)

- estudou as propriedades de uma máquina de Turing quântica
- mostrou que ela poderia resolver um problema em menos passos que um computador clássico

Pioneiros da computação quântica

- **Peter Shor** (1994)

- computadores quânticos podem **encontrar os fatores primos de números inteiros** em tempo polinomial - *exponencialmente* mais rápido que os computadores usuais!
- Isso é extremamente importante, pois a (suposta) dificuldade deste problema está na base dos principais códigos usados para a segurança de comunicações, por exemplo na internet (protocolo RSA)



- **Lov Grover** (1996)

- algoritmo de busca em base de dados
- desempenho (número necessário de consultas à base de dados)

$$N \rightarrow \sqrt{N}$$

- útil para acelerar solução de problemas intratáveis

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 ($15 = 3 \times 5$)
 - criação de superposições e controle de poucos qbits em diversos sistemas
- Ainda à procura de um sistema que possibilite um computador quântico útil...

Computando com qbits

- Escolhemos sistema quântico para codificar zeros e uns.
Ex: níveis de energia eletrônicos de íons presos em armadilha

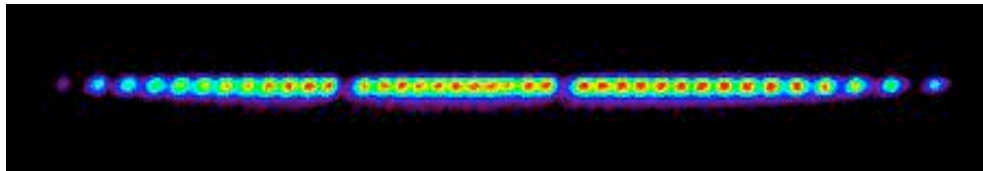
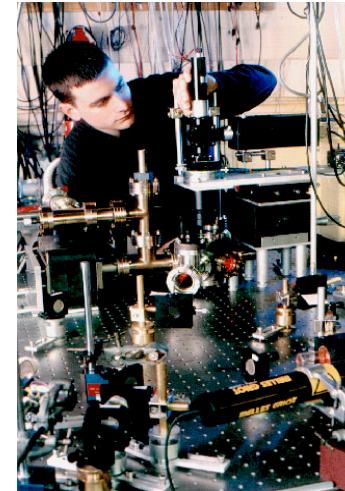
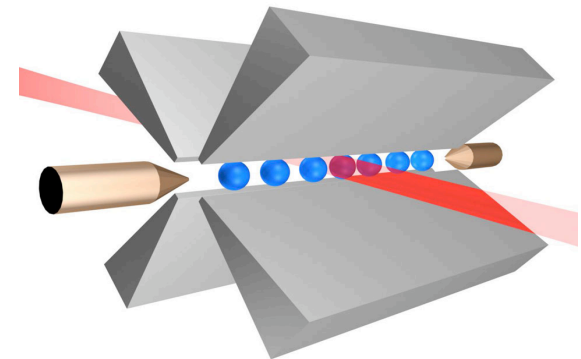


Foto de íons armadilhados



Ion trap
Steane group
(Oxford)



Computando com qbits

- Escolhemos sistema quântico para codificar zeros e uns.
Ex: níveis de energia eletrônicos de íons presos em armadilha

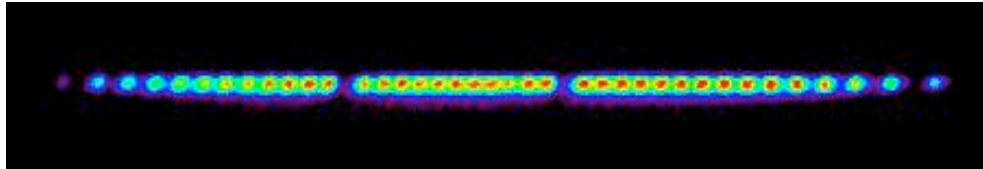
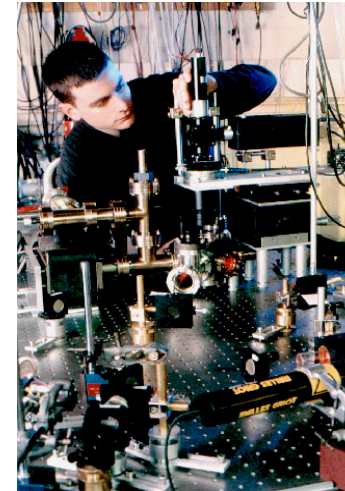
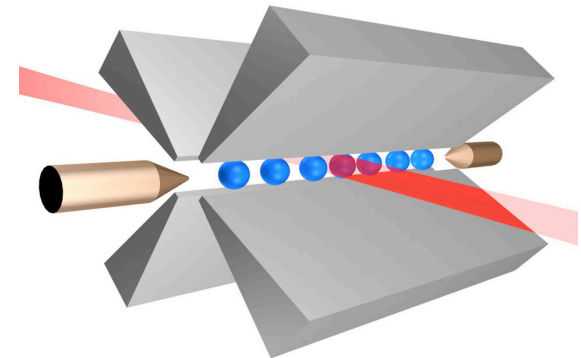


Foto de íons armadilhados



Ion trap
Steane group
(Oxford)

- Modificamos as superposições quânticas de maneira controlada.
Ex: pulsos laser em conjuntos de íons



Computando com qbits

- Escolhemos sistema quântico para codificar zeros e uns.
Ex: níveis de energia eletrônicos de íons presos em armadilha

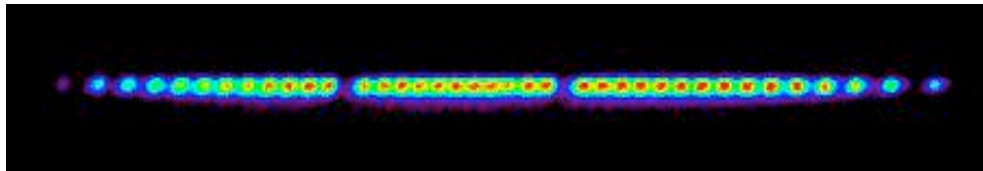
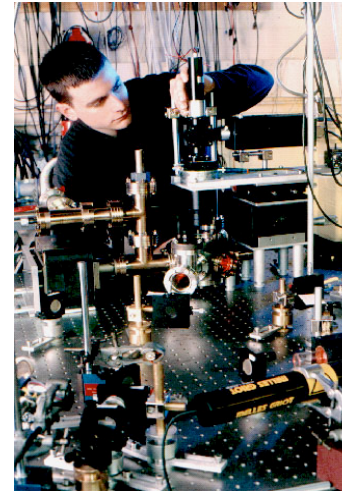
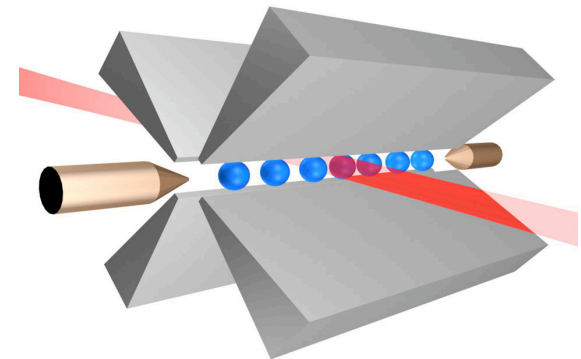


Foto de íons armadilhados



Ion trap
Steane group
(Oxford)

- 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...

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

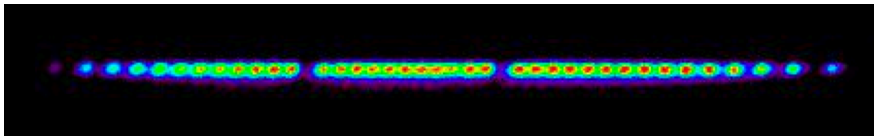
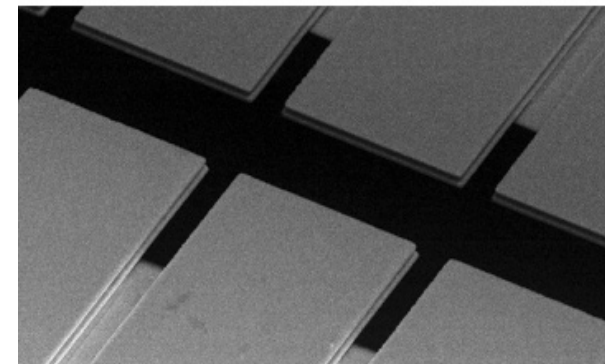
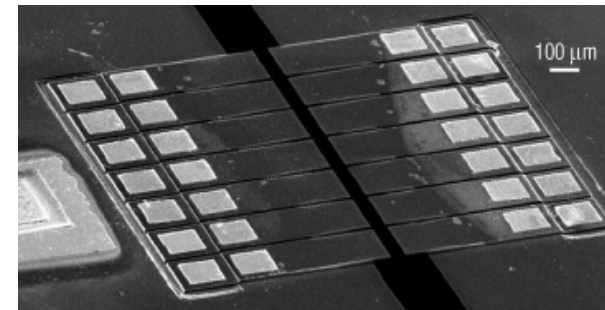
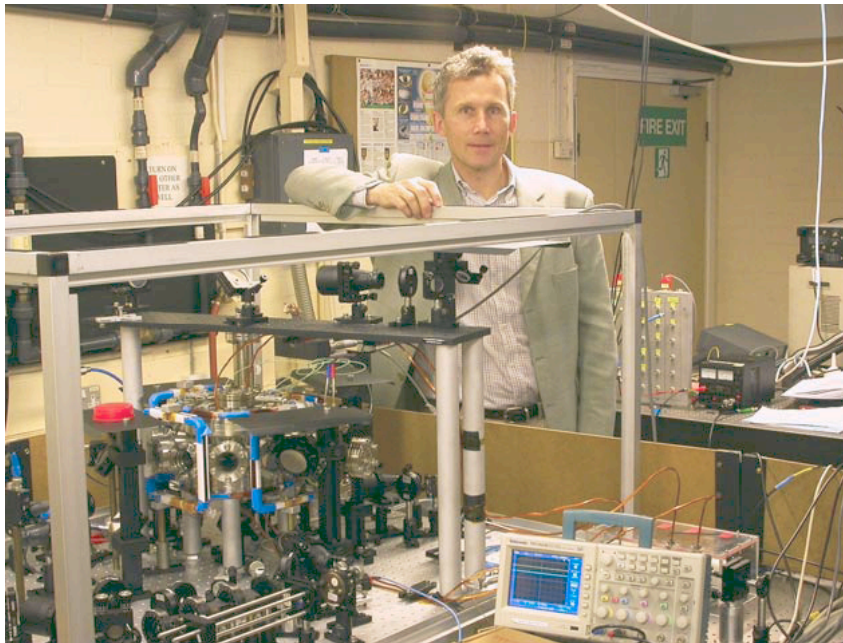


Foto de íons armadilhados



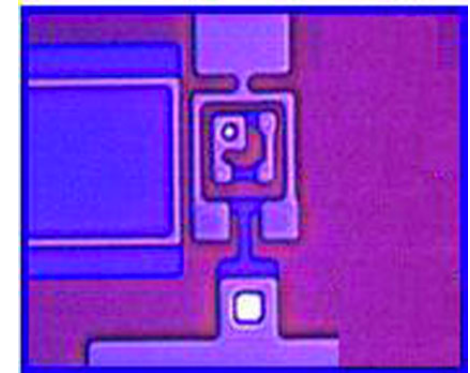
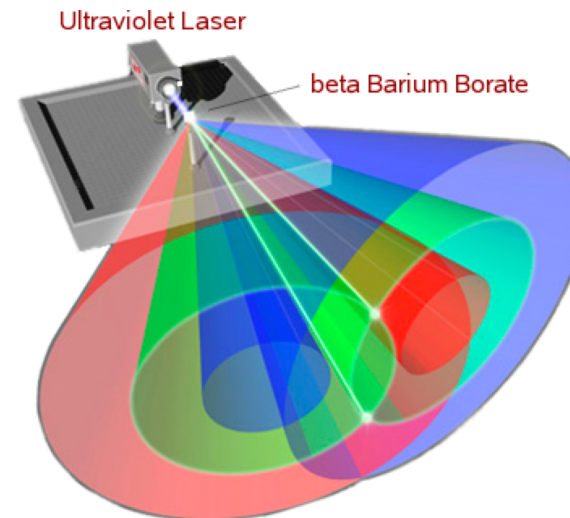
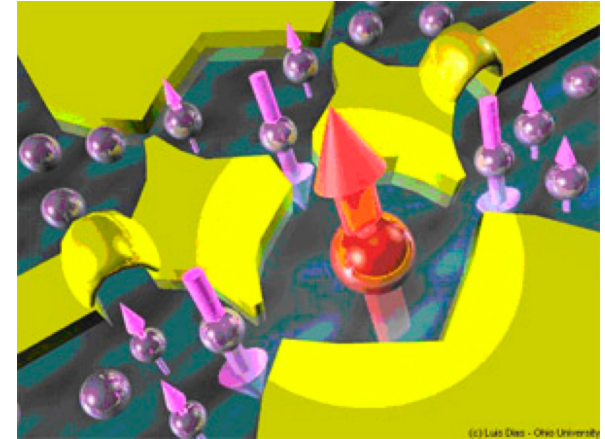
micro-armadilha de íons

Laboratório (Chris Foot - Oxford)

Construindo um computador quântico: possibilidades

•Outras alternativas:

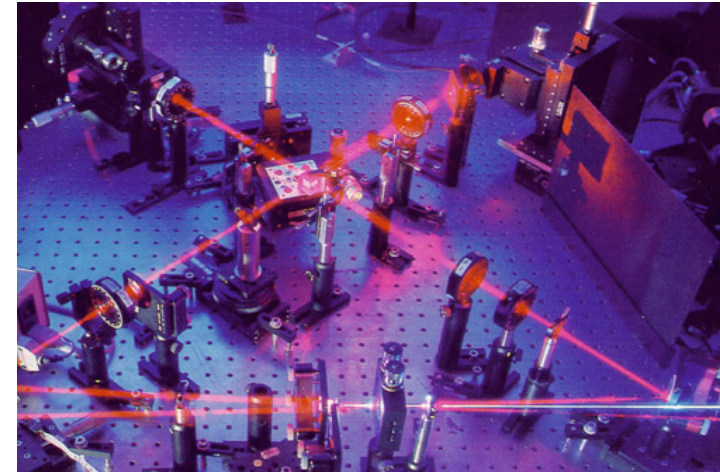
- elétrons presos em pontos quânticos
- ressonância nuclear em líquidos
- luz laser (ótica quântica)
- circuitos supercondutores
- [??????]



??????????

Computando com qbits

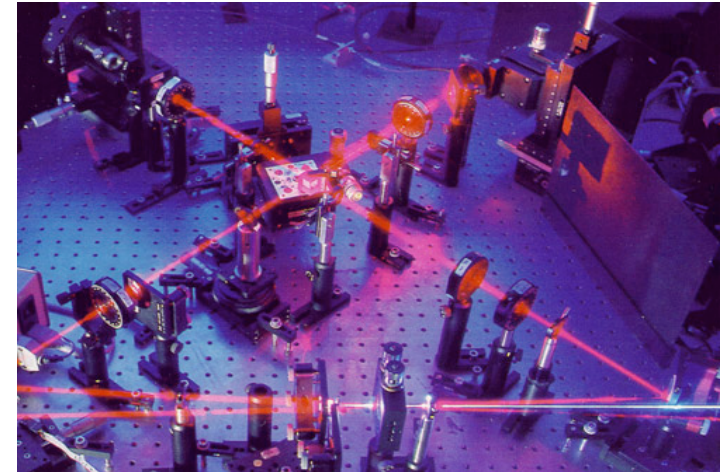
- Dificuldades:
 - acesso experimental x isolamento
 - fragilidade das superposições (*descoerência*)
 - controle preciso dos sistemas usados



Computando com qbits

- Dificuldades:

- acesso experimental x isolamento
- fragilidade das superposições (*descoerência*)
- controle preciso dos sistemas usados



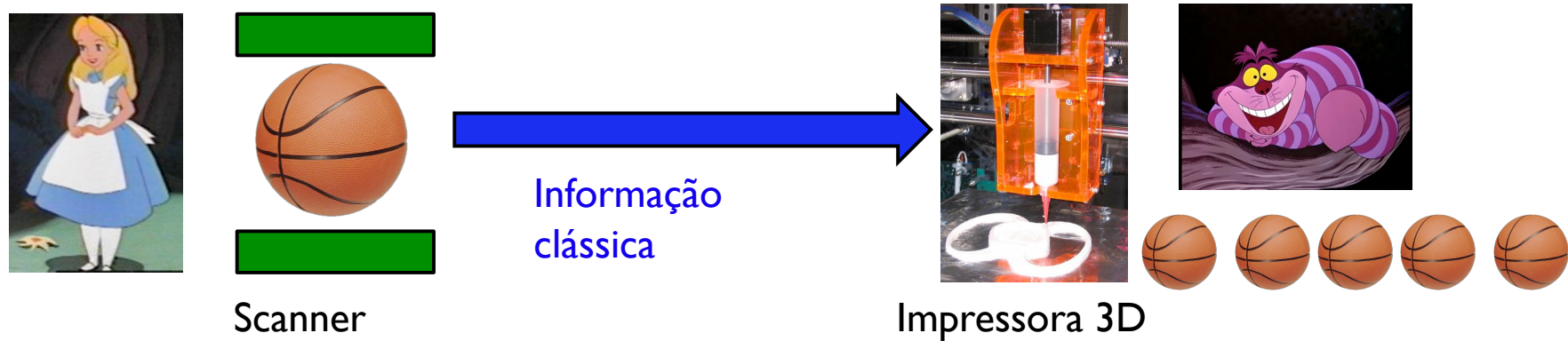
- Situação experimental atual:

- criptografia quântica comercial
- demonstração de alguns algoritmos em versão 'brinquedo', como o algoritmo de fatoração ($15 = 3 \times 5!$)
- criação de superposições e controle com até ~ 10 qbits em diversos sistemas
- Ainda não se sabe como construir um computador quântico realmente útil

- Mas ... Há outras aplicações interessantes além da computação...

Teletransporte

Teletransporte: equivale a conjunto perfeito de scanner/impressora.

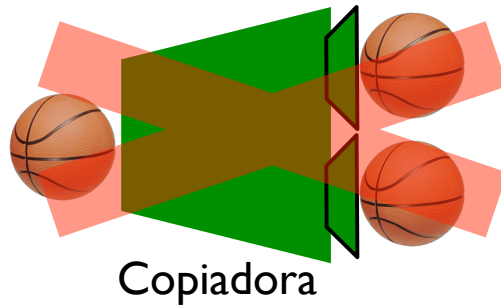


Problema: não dá para obter toda a informação de uma única cópia de sistema quântico –
(Princípio da Incerteza de Heisenberg)

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.

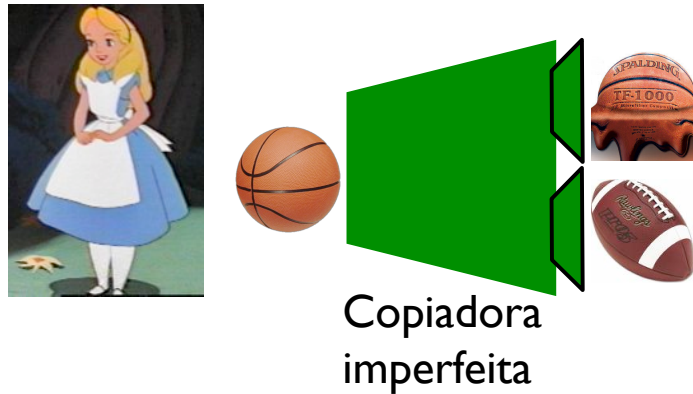


Problema: não dá!

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

Copiadoras quânticas

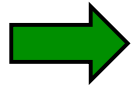
Copiadora quântica (*quantum cloning machine*): usa evolução quântica para criar **cópias imperfeitas** de um sistema quântico.



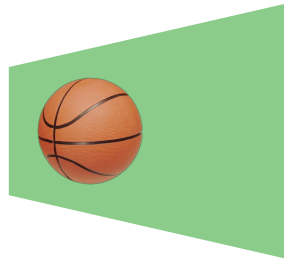
Copiadoras imperfeitas são possíveis – os limites são impostos pela MQ

Teletransporte quântico

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

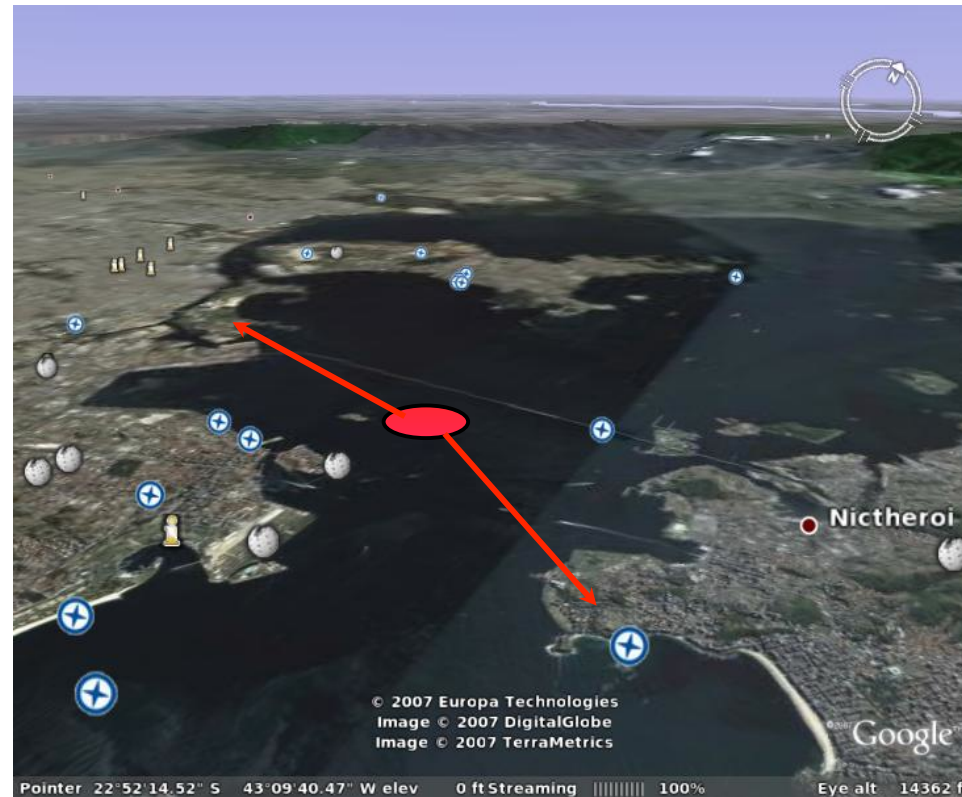


Impossível classicamente, mas possível se usarmos efeitos quânticos.



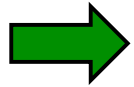
Emaranhamento

- 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

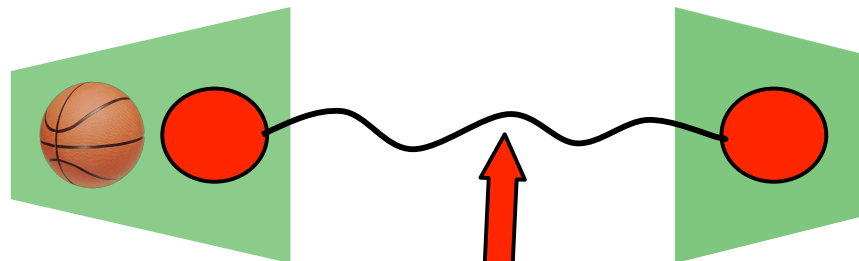


Teletransporte quântico

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



Impossível classicamente, mas possível se usarmos efeitos quânticos.



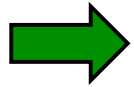
Par de sistemas emaranhados

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

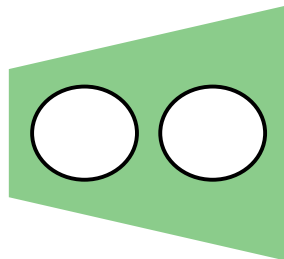
1 - A e B dispõem de par de partículas emaranhadas.

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.

Outras aplicações de informação quântica

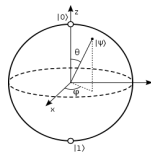
Criptografia quântica



A



Fótons individuais

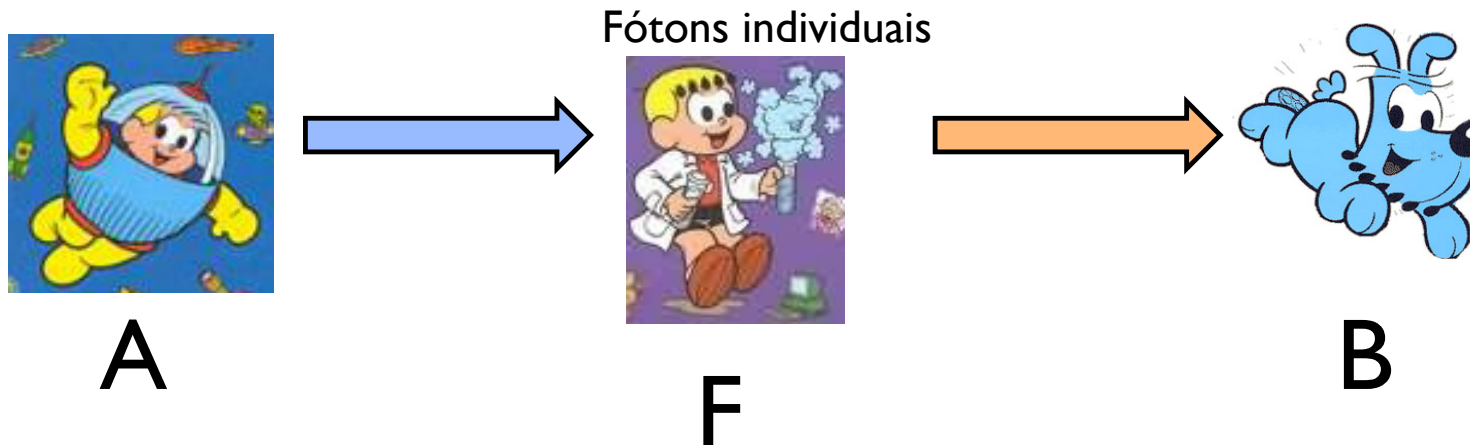


B

- A se comunica com B através de canal quântico (ex: polarização de fótons)

Outras aplicações de informação quântica

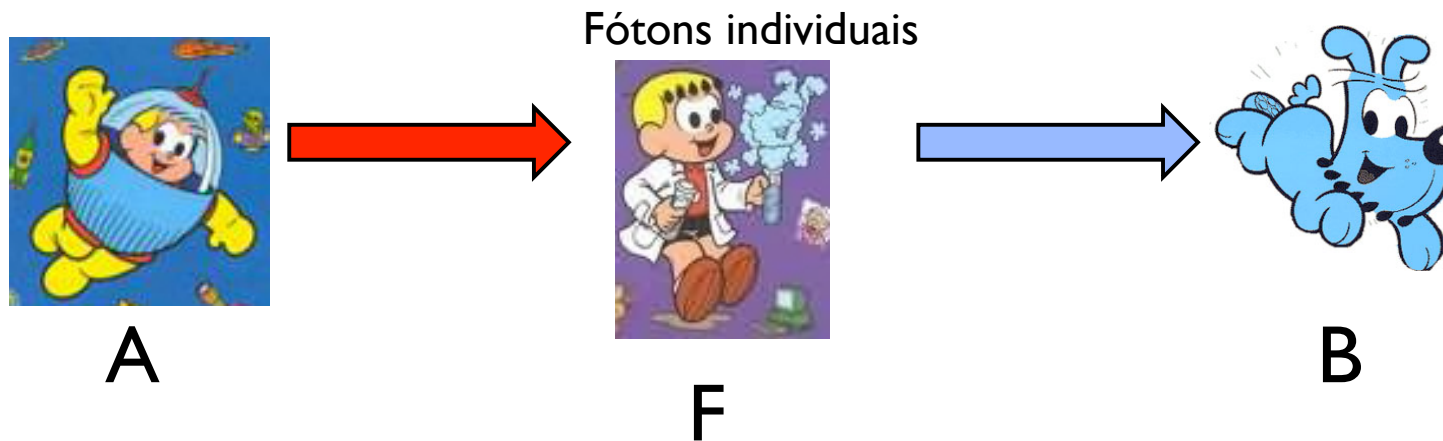
Criptografia quântica



- 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

Criptografia quântica

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)



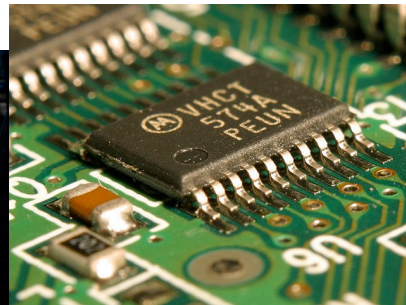
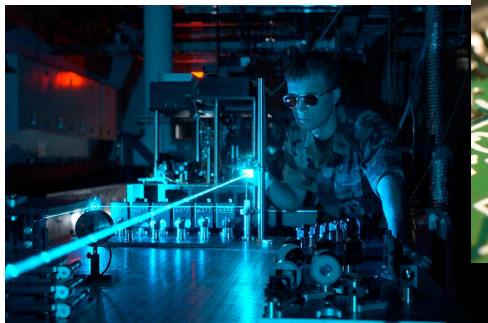
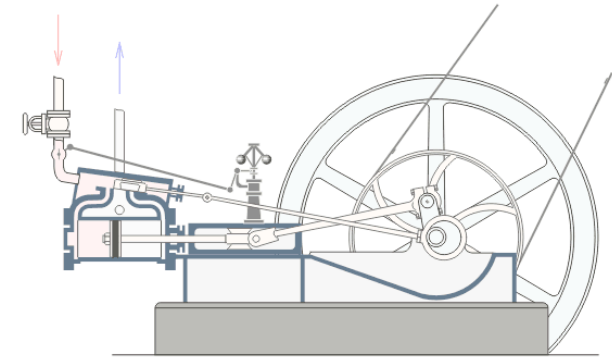
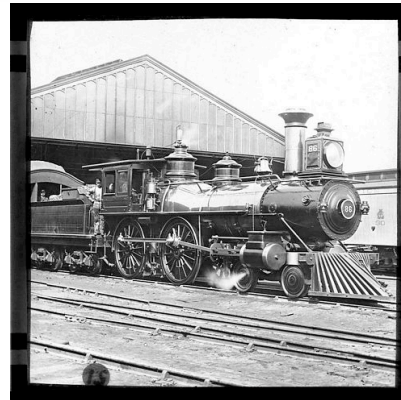
- MagiQ Technologies (EUA)



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

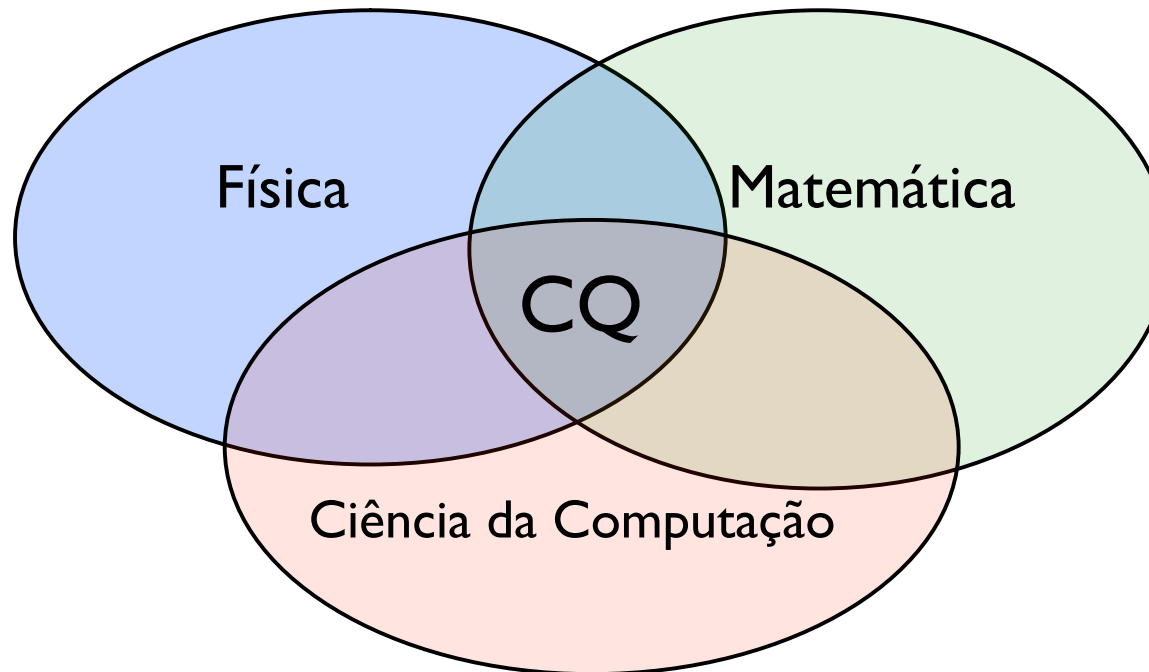
Metrologia

- 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:

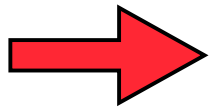
Instituto Nacional de Ciência e Tecnologia (INCT) de Informação Quântica - CNPq
- 20 grupos de pesquisa em 7 estados, predominância de físicos

Fora:

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

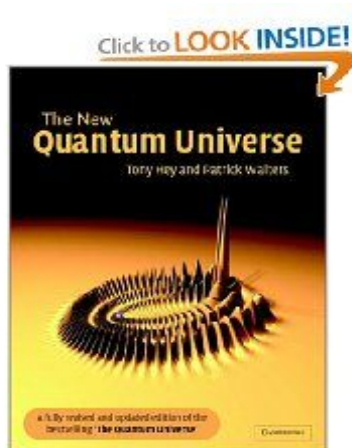
Perspectivas – Computação Quântica

- 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



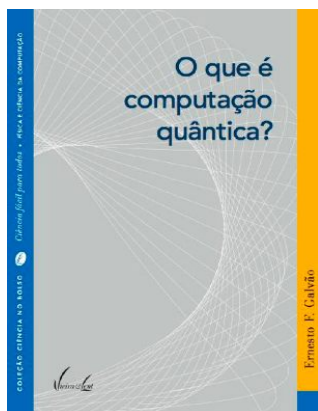
“The new quantum universe”, Tony Hey and Patrick Walters (Cambridge University Press, 2003)

• “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 grupo de Óptica e Informação Quântica da UFF para mais informações e dicas de leitura na web:



<http://infoptics.if.uff.br/>