IA013 – Tópico 9 – Parte 2
Computação Quântica

Carlos Renato Belo Azevedo
azevedo@dca.fee.unicamp.br
Laboratório de Bioinformática e Computação Bio-inspirada (LBiC)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
UNICAMP

Parte I

PARA QUE MECÂNICA QUÂNTICA?

Para que mecânica quântica?

- Segundo estimativas de 2001, 30% do PIB americano depende de invenções que só se tornaram possíveis graças à mecânica quântica.

Para que mecânica quântica?

- Vamos falar sobre moedas.

Para que mecânica quântica?

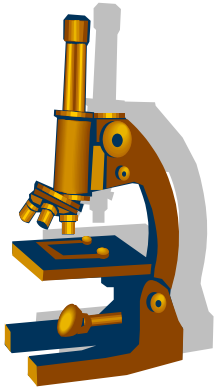
- Esse esquema funciona bem em grande escala.

Para que mecânica quântica?

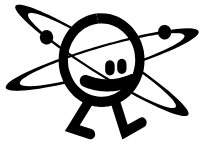
- E em escalas subatômicas?

Para que mecânica quântica?

- E em escalas subatômicas?



?



Para que mecânica quântica?

- E em escalas subatômicas?
  - Princípio da incerteza

Para que mecânica quântica?

- Para que possamos distinguir propriedades de objetos, precisamos exercer influência sobre os mesmos de forma a extrair informações relevantes.

Werner Karl **Heisenberg**

- 1925
  - Primeira versão matemática da MQ
  - Baseada em matrizes
- 1927
  - Princípio da incerteza de Heisenberg
- 1932
  - **Prêmio Nobel**

Princípio da Incerteza

- Não é possível conhecer ao mesmo tempo a localização exata e o momento linear exato de uma única partícula.
- O máximo que podemos pretender é prever a **probabilidade** de que um experimento produza este ou aquele resultado.

$$\Delta\chi\Delta\rho \geq \frac{\hbar}{2}$$

Princípio da Incerteza

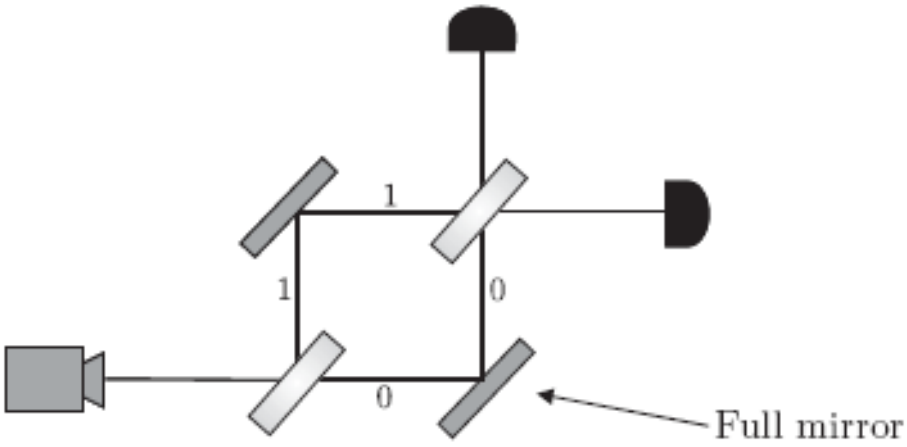
- Variáveis conjugadas
  - Uma é a transformada de Fourier da outra
    - Posição e momento linear;
    - Posição angular e momento angular;
    - Potencial elétrico e carga elétrica;
    - Potencial magnético e corrente elétrica;
    - Campo elétrico e polarização;
    - Potencial gravitacional e densidade de massa;
    - Energia e tempo.

Fenômenos Quânticos

- Superposição e Interferência
  - São as chaves para o **paralelismo quântico**
- O Interferômetro de Mach-Zehnder Quântico
  - Produz resultados contra-intuitivos;
  - Não pode ser descrito pela física clássica;
  - Possui uma explicação quântica “simples”.

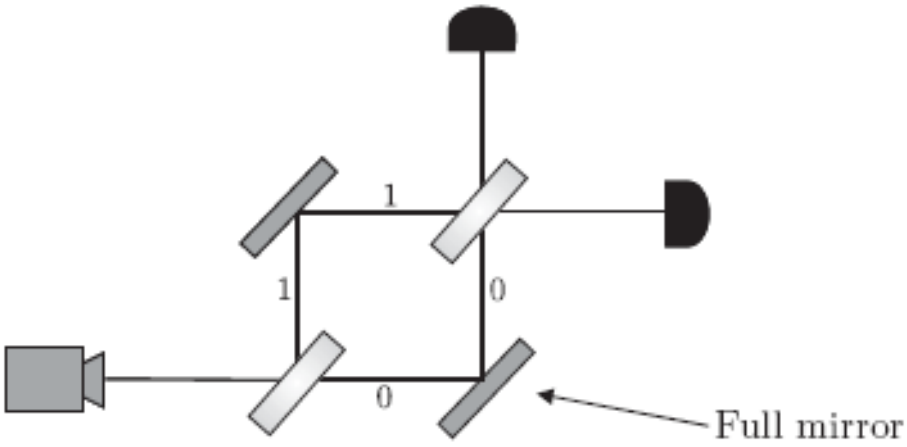
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Uma fonte de fótons;
  - Um par de espelhos semi-prateado (*beam splitter*);
  - Um par de espelhos (*full mirrors*)
  - Dois detectores de fótons;



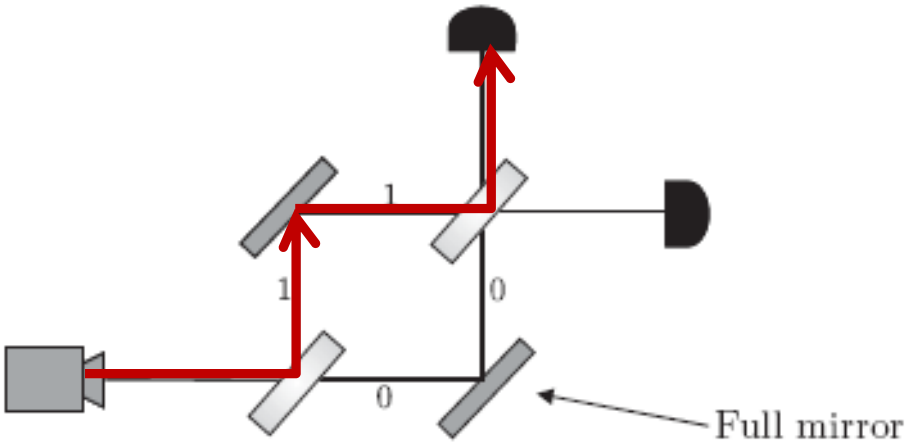
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - 50% dos fótons incidem no detector de cima;
    - 50 % dos fótons incidem no detector da direita.



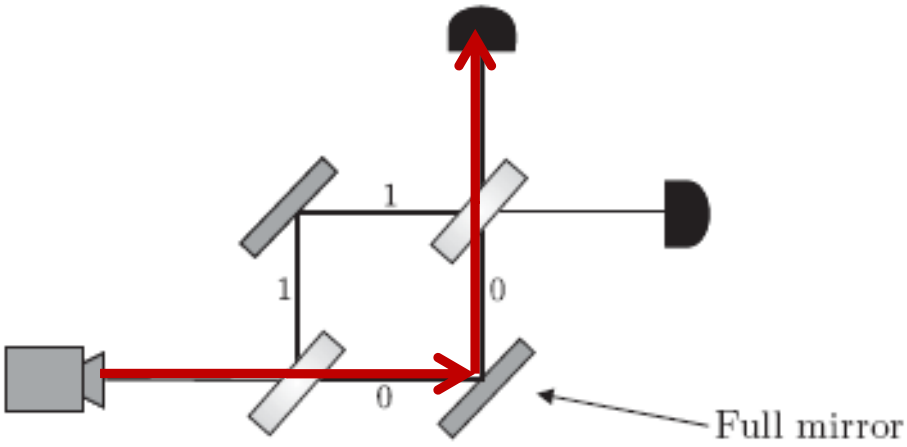
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector de cima) = ?
      - $P(R_1).P(R_2) = 0,25$



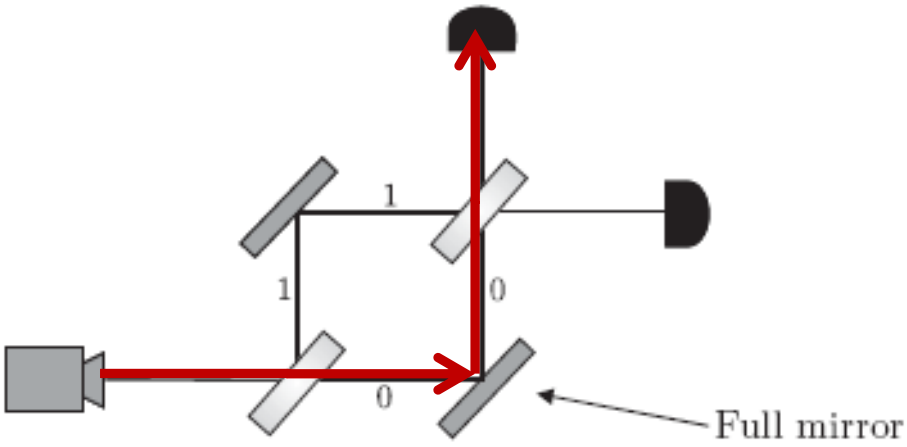
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector de cima) = ?
      - $0,25 + P(T_1).P(T_2)$



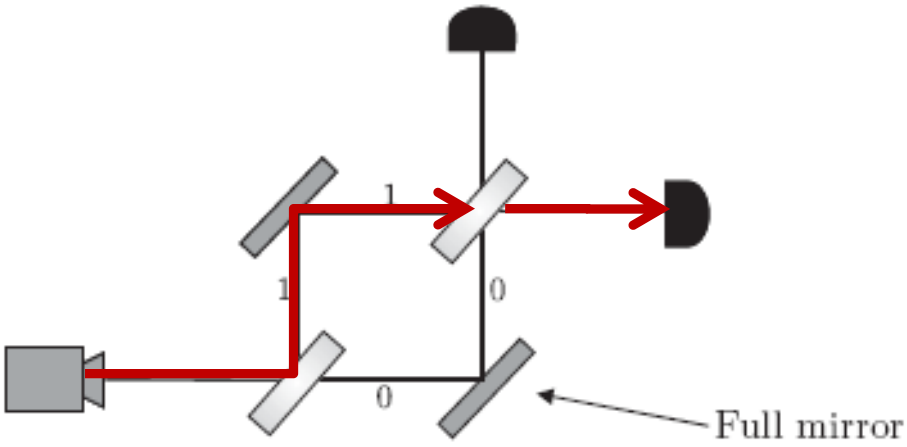
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector de cima) = 0,5
      - 0,25 + 0,25



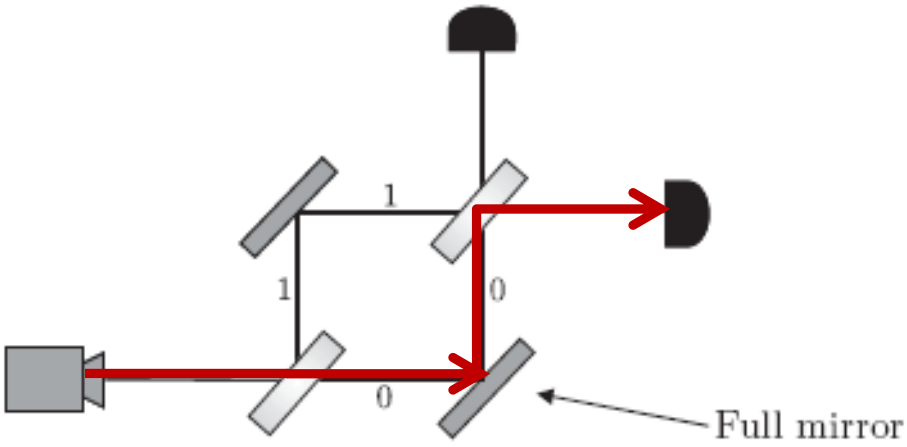
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector da direita) = ?
      - $P(R_1).P(T_2) = 0,25$



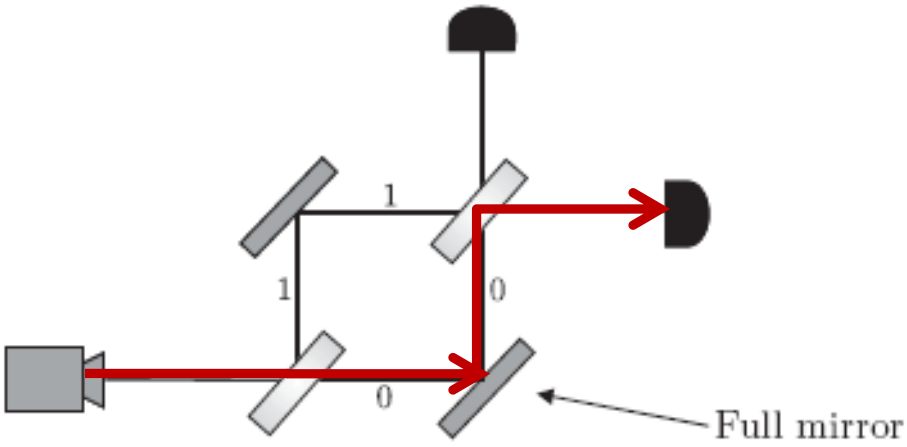
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector da direita) = ?
      - $0,25 + P(T_1).P(R_2)$



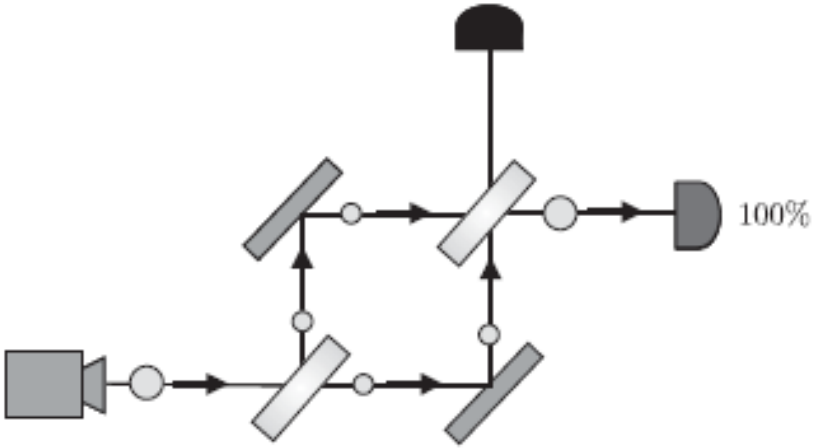
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Qual a predição da física clássica para esse sistema?
    - P(Fóton incidir no detector da direita) = 0,5
      - 0,25 + 0,25



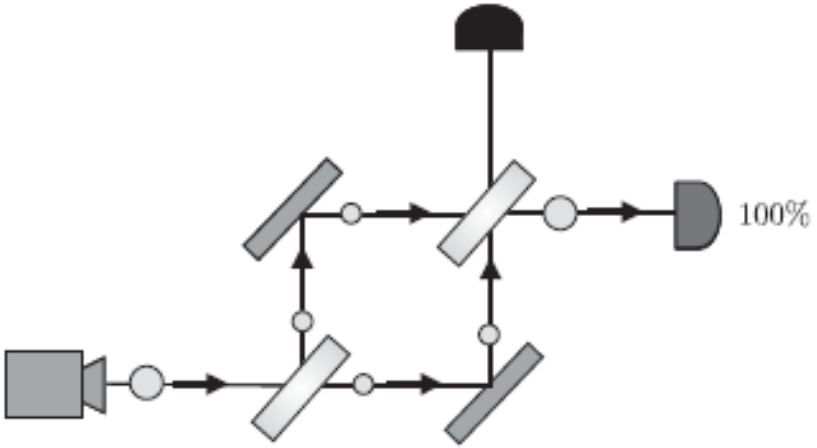
Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Tal predição não corresponde à realidade dos experimentos
    - 100% dos fótons são detectados à direita!
    - Os resultados não correspondem à intuição clássica!



Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - A física quântica modela o experimento com precisão
    - Os fenômenos responsáveis pelo estranho resultado:
      - **Superposição e Interferência**



Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Suponha que os segundo espelho semi-prateado seja retirado do sistema.
    - Então, de acordo com a física clássica, o fóton tomará um dos dois caminhos possíveis:

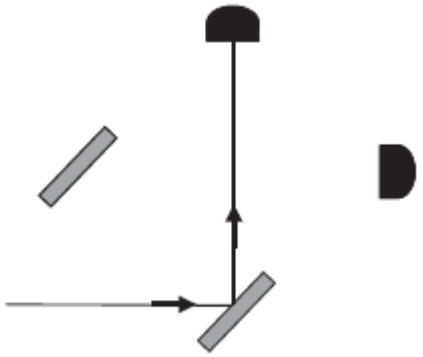


Fig. 1.11 The '0' path.

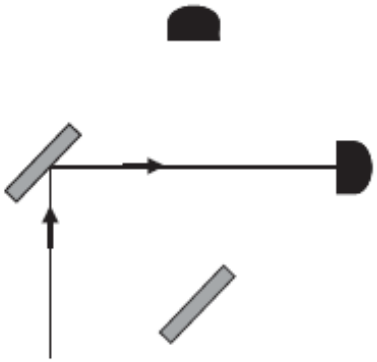


Fig. 1.12 The '1' path.

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Considere o estado de um fóton no caminho ‘0’ dado pelo vetor $\begin{pmatrix}1\\0\end{pmatrix}$ e, conversamente, $\begin{pmatrix}0\\1\end{pmatrix}$ o estado de um fóton no caminho ‘1’.

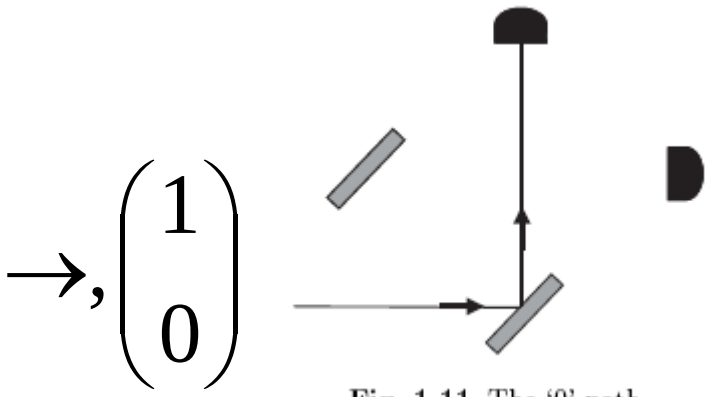


Fig. 1.11 The ‘0’ path.

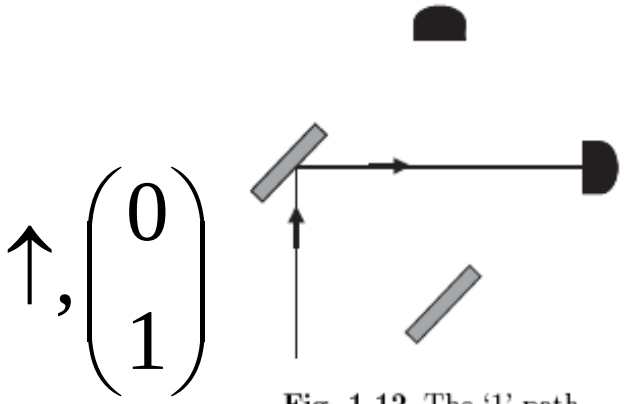


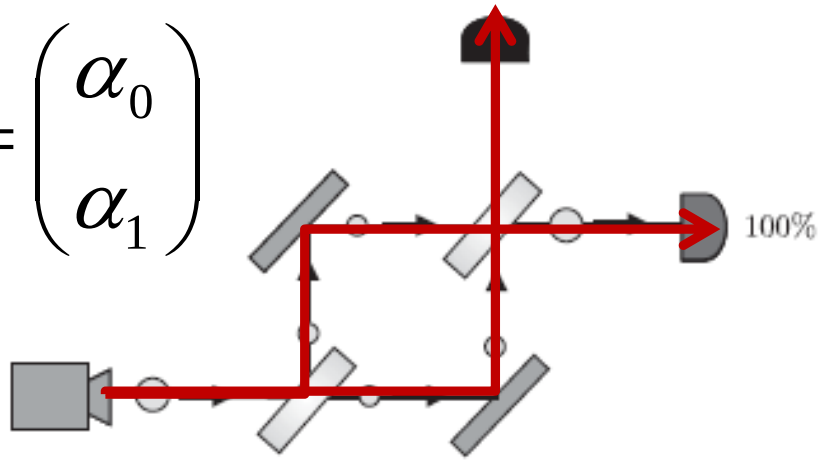
Fig. 1.12 The ‘1’ path.

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - A introdução do segundo espelho semi-prateado afeta o fóton de forma a criar uma **superposição** dos caminhos ‘0’ e ‘1’.

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

$$\rightarrow, \begin{pmatrix} 1 \\ 0 \end{pmatrix} e \uparrow, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - Superposição de estados base

$$\alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

$$P(\rightarrow) = |\alpha_0|^2 \qquad P(\uparrow) = |\alpha_1|^2$$

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - O seu vetor de estado é modificado pela ação da matriz

$$1/\sqrt{2}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - O fóton começa no estado $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
    - O novo estado será descrito como

$$1/\sqrt{2}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1/\sqrt{2}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$= 1/\sqrt{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + i/\sqrt{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - Se medido, as probabilidades de ser encontrado nos caminhos ‘0’ ou ‘1’ serão dadas de acordo com

$$P(\rightarrow) = \left| 1/\sqrt{2} \right|^2 = 1/2 \qquad P(\uparrow) = \left| i/\sqrt{2} \right|^2 = 1/2$$

$$1/\sqrt{2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + i/\sqrt{2} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - Se permitirmos que o fóton passe pelo segundo espelho semi-prateado, o seu estado será

$$\left(1/\sqrt{2} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \right) \left(1/\sqrt{2} \begin{pmatrix} 1 \\ i \end{pmatrix} \right) = \begin{pmatrix} 0 \\ i \end{pmatrix}$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - Se permitirmos que o fóton passe pelo segundo espelho semi-prateado, o seu estado será

$$\left(1/\sqrt{2}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}\right)\left(1/\sqrt{2}\begin{pmatrix}1\\ i\end{pmatrix}\right)=\begin{pmatrix}0\\ i\end{pmatrix}$$

$$\begin{pmatrix}0\\ i\end{pmatrix}=0\cdot\begin{pmatrix}1\\ 0\end{pmatrix}+i\cdot\begin{pmatrix}0\\ 1\end{pmatrix}$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - **Portanto, o resultado previsto pela MQ concorda com o resultado observado no experimento.**

$$\begin{pmatrix} 0 \\ i \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + i \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$P(\rightarrow) = \left|0\right|^2$$

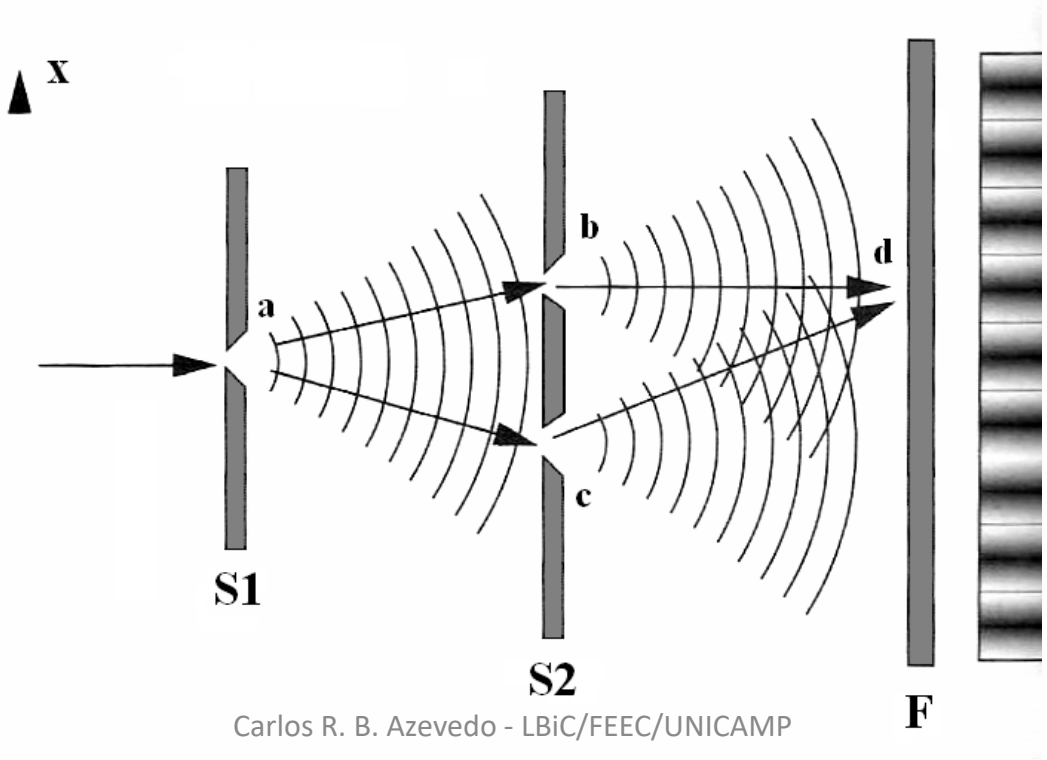
$$P(\uparrow) = \left|i\right|^2 = \left|i^2\right| = \left|-1\right| = 1$$

Fenômenos Quânticos

- O Interferômetro de Mach-Zehnder Quântico
  - De acordo com a MQ, o que acontece quando o fóton passa pelo primeiro espelho semi-prateado?
    - Na linguagem da MQ, o segundo espelho semi-prateado fez com que os dois caminhos em **superposição interferissem**, resultando no cancelamento do caminho ‘0’.

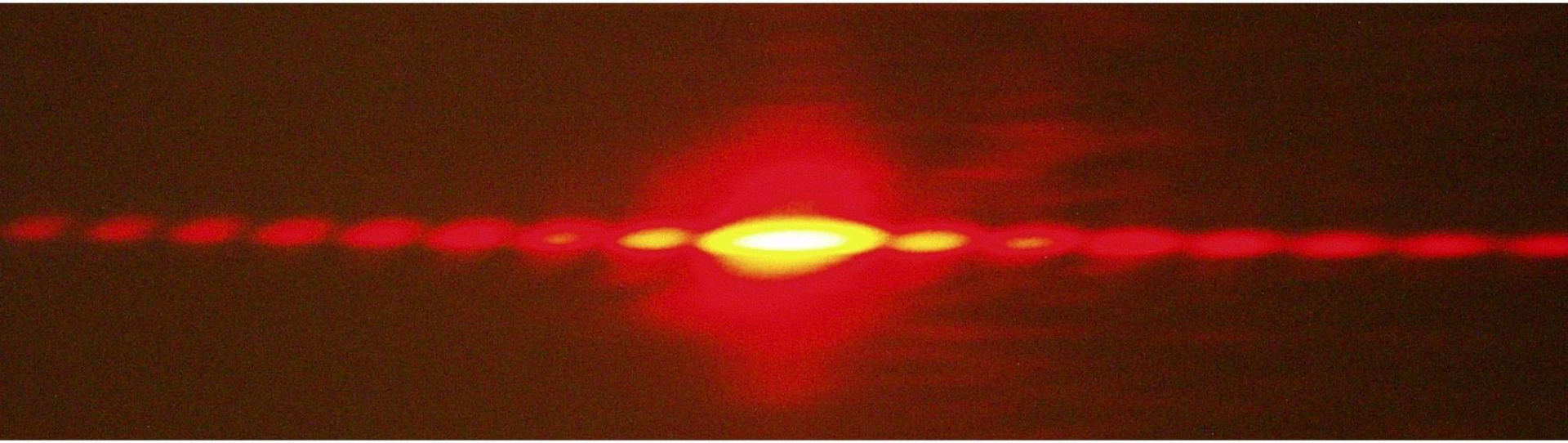
Fenômenos Quânticos

- Interferência clássica vs. quântica
  - O Experimento da Dupla Fenda



Fenômenos Quânticos

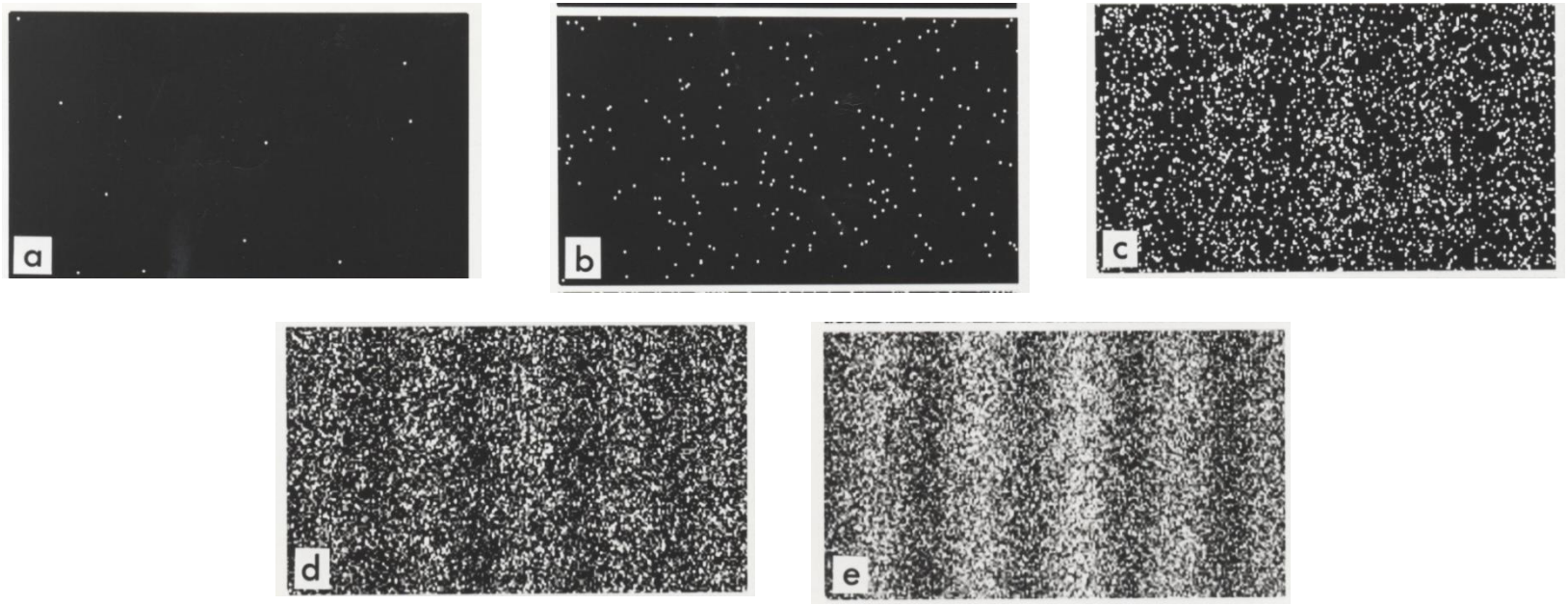
- Interferência clássica vs. quântica
  - O Experimento da Dupla Fenda
    - Interferência construtiva vs. Destrutiva



Pattern produced from a double slit.

Fenômenos Quânticos

- Interferência clássica vs. quântica
  - O Experimento da Dupla Fenda
    - **Versão quântica: o padrão de interferência permanece!**



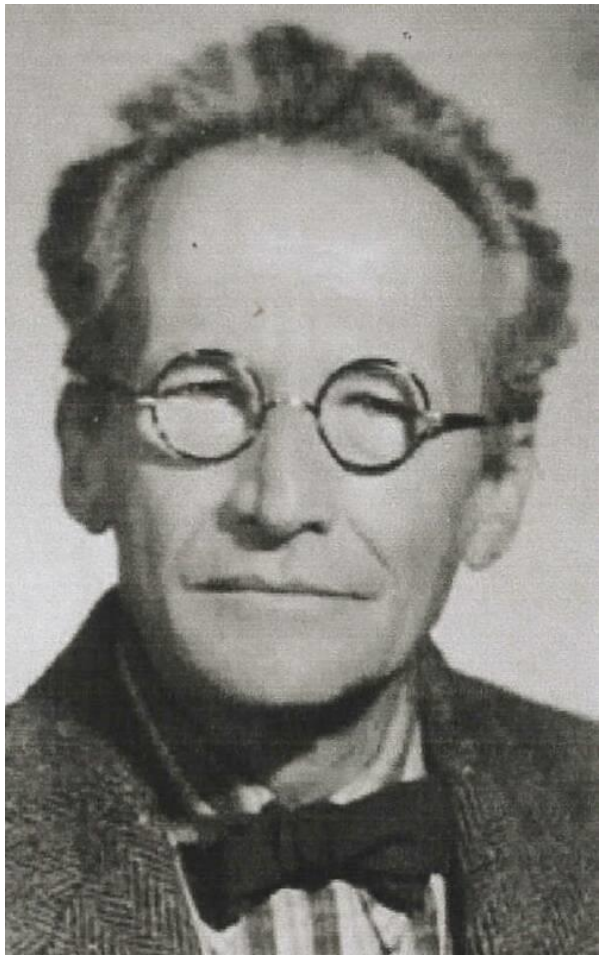
Fenômenos Quânticos

- Interferência clássica vs. quântica
  - O Experimento da Dupla Fenda
    - Na versão quântica, o que causa a interferência?
      - » Função de onda (probabilidade de encontrar o fóton em uma determinada posição após uma medição)

Louis-Victor-Pierre-Raymond **de Broglie**

- 1924
  - Dualidade partícula-onda da matéria
- 1929
  - **Prêmio Nobel de física**

Erwin Rudolf Josef Alexander **Schrödinger**



- 1926
  - Mecânica ondulatória
- 1933
  - **Prêmio Nobel de física**
- 1935
  - Artigo sobre o gato de Schrödinger

David Deutsch

- 1985
  - Concebeu a idéia de uma máquina de Turing quântica universal
  - Primeiro modelo formal
  - Linguagem de circuitos quânticos
- 1989
  - Primeiro algoritmo quântico

Perspectiva da Ciência da Computação

- David Deutsch, em 1985, se perguntou se as leis da física poderiam ser usadas para derivar uma versão ainda mais forte da tese de Church-Turing.
  - *Qualquer sistema **físico** finitamente realizável pode ser perfeitamente simulado por um dispositivo de computação universal.*
  - Seria então a máquina de Turing quântica proposta por Deutsch capaz de simular eficientemente qualquer processo físico?

Perspectiva da Ciência da Computação

- *"Em vez de procurar por hipóteses ad-hoc, Deutsch buscou nas teorias físicas fundamentos que pudessem conferir à tese de Church-Turing o status de tão sólida quanto as próprias teorias físicas. Em particular, David Deutsch tentou definir um aparato computacional que fosse capaz de simular eficientemente qualquer sistema físico arbitrário. Como as leis da física são, em última análise, quânticas, Deutsch foi naturalmente levado a considerar tais aparatos com base nos princípios da mecânica quântica. Esses aparatos, análogos das máquinas definidas por Turing 49 anos antes, levaram à concepção moderna de um computador quântico."* (NIELSEN; **CHUANG** p. 37, 2000)

Bits Quânticos

- Representação de um *quantum bit* (*qubit*)
  - Vetor unitário do Espaço de Hilbert 2-dimensional ($\mathcal{H}^2$):

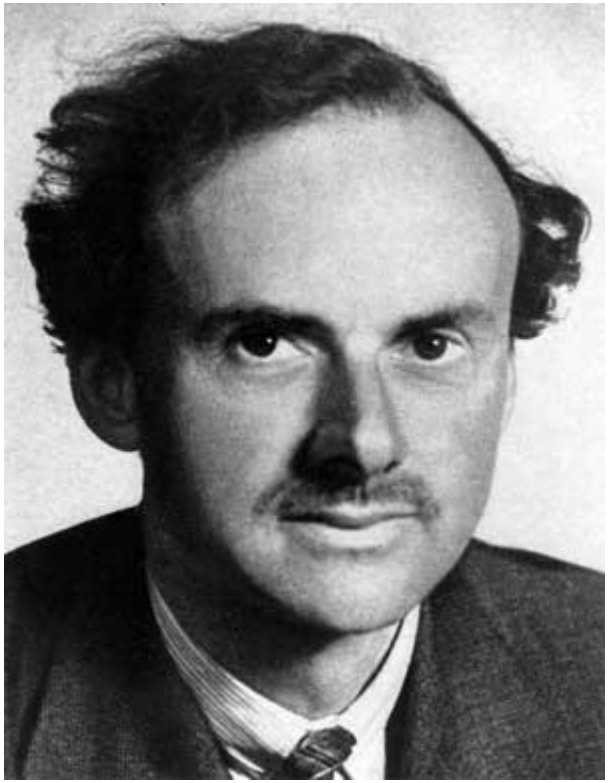
$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  - Os vetores |0> e |1> formam a base computacional;
  - α_0 e α_1 são as amplitudes da base.

Paul Adrien Maurice **Dirac**

- 1928
  - Equação que descreve o comportamento relativístico do elétron
  - Notação Bra-ket utilizada na computação quântica
- 1933
  - **Prêmio Nobel de física**



Bits Quânticos

- Representação de um *quantum bit* (*qubit*)
  - Vetor unitário do Espaço de Hilbert 2-dimensional ($\mathcal{H}^2$):

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

  - Os vetores |0> e |1> formam a base computacional;
  - α_0 e α_1 são as amplitudes complexas da base;
  - $|\psi\rangle$ é o vetor de estado do sistema de 1 *qubit*;
  - A soma do módulo ao quadrado das amplitudes é um.

Bits Quânticos

- Como representar matematicamente sistemas quânticos com vários qubits?
  - O espaço de estados de um sistema composto por dois *qubits* é dados pelo produto tensorial dos espaços de entrada $\mathcal{H}_1 \otimes \mathcal{H}_2$;
  - Se o primeiro sistema encontra-se no estado $|\psi_1\rangle$ e o segundo no estado $|\psi_2\rangle$, o estado do sistema composto será dado por $|\psi_1\rangle \otimes |\psi_2\rangle$.

Bits Quânticos

- Como representar matematicamente sistemas quânticos com vários qubits?

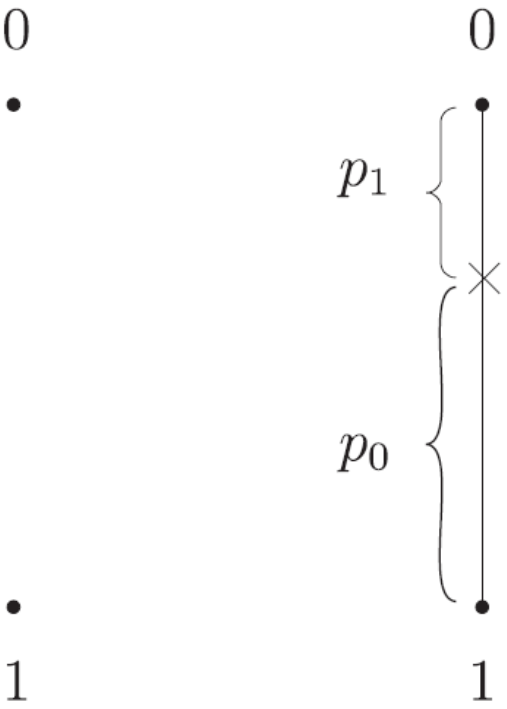
$$|\psi_1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$$

$$|\psi_1\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

$$|\psi_1\psi_2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

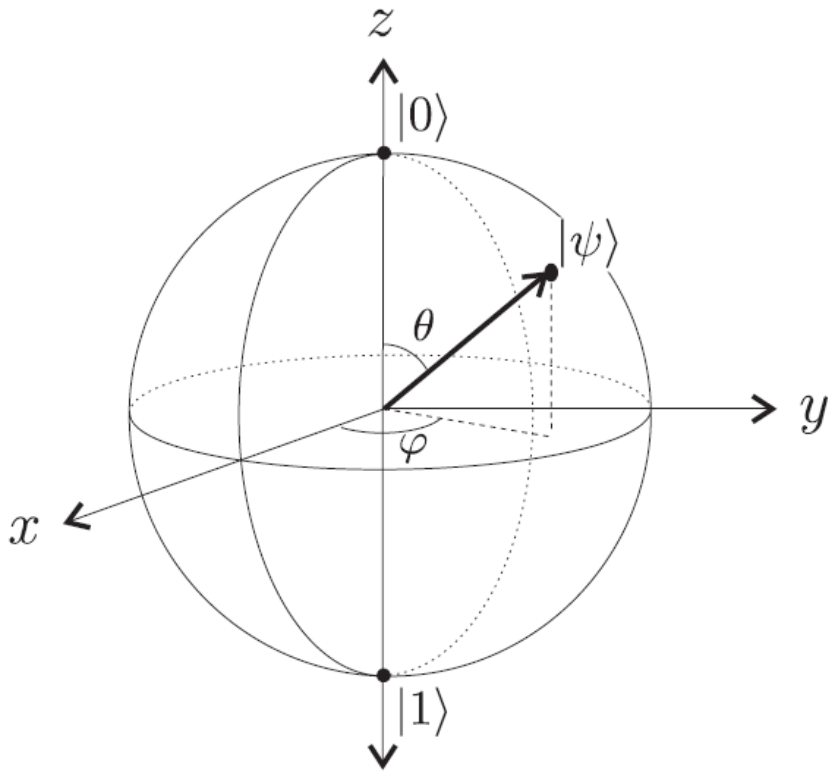
Portas Lógicas Quânticas

- Representação de 1 *qubit* na Esfera de Bloch



Bit clássico

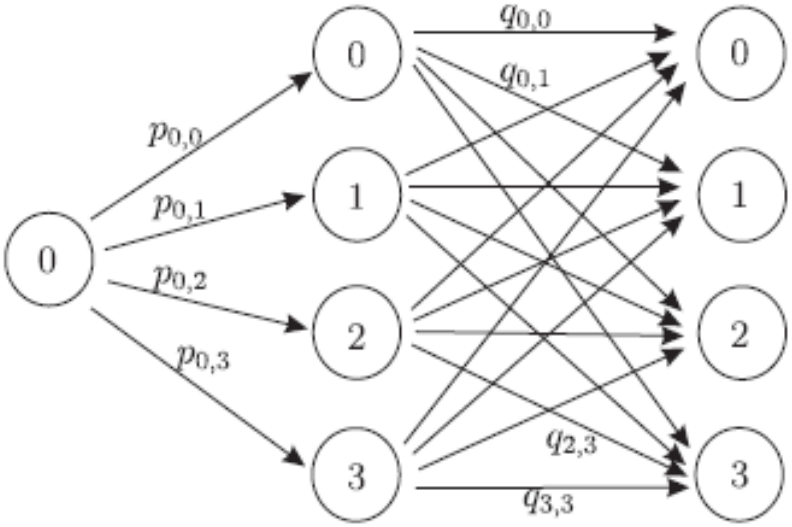
Bit probabilístico



Bit quântico

Estrutura de um Algoritmo Quântico

- Algoritmo probabilístico *vs.* quântico



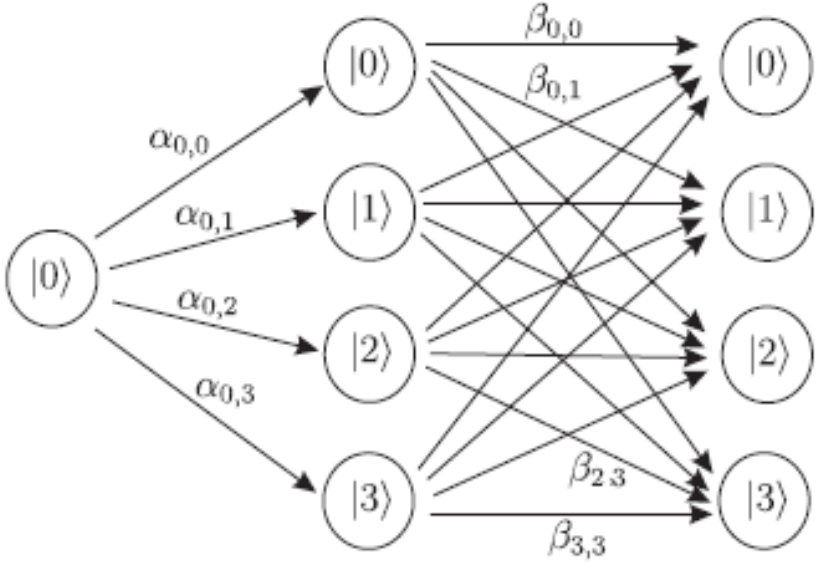
Na computação clássica, uma medida é realizada a cada transição de estado para que se possa calcular a distribuição de probabilidades da próxima transição.

Estrutura de um Algoritmo Quântico

- Algoritmo probabilístico *vs.* quântico

Na computação quântica, a medida é realizada apenas no final de todo o processo.

Portanto, a estrutura geral de um algoritmo quântico é:
-**Preparar a entrada em um estado clássico;**
- **Construir uma superposição dos estados clássicos;**
- **Aplicar as operações unitárias em seqüência;**
- **Medir o resultado.**



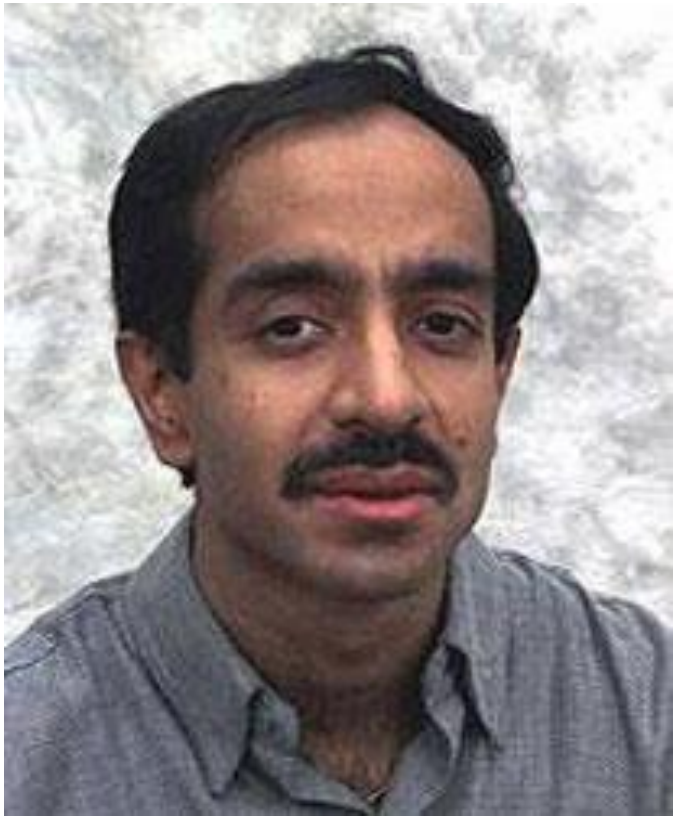
Parte III

APLICAÇÕES

Busca em Listas Desordenadas

- Definição do Problema
  - Suponha que você deseja descobrir o dono de um determinado número de telefone em sua agenda.
  - O único dado disponível é o número.
  - Os dados na agenda são ordenados por nome.
  - Se a ordem dos dados é completamente aleatória, o melhor algoritmo clássico é uma simples busca sequencial de complexidade $O(N)$.

Lov Grover



- 1996
  - Descobriu um algoritmo de pesquisa em bases de dados quânticas
  - Complexidade do algoritmo: $O(N^{1/2})$
  - Encontra o dado desejado com alta probabilidade

Busca em Listas Desordenadas

- O Algoritmo de Grover
  - Consiste de três passos:
    1. Preparar uma superposição de todas as entradas possíveis;
    2. Realizar *k* aplicações do operador de Grover;
    3. Medir o resultado.

Fatoração de Números Inteiros Grandes

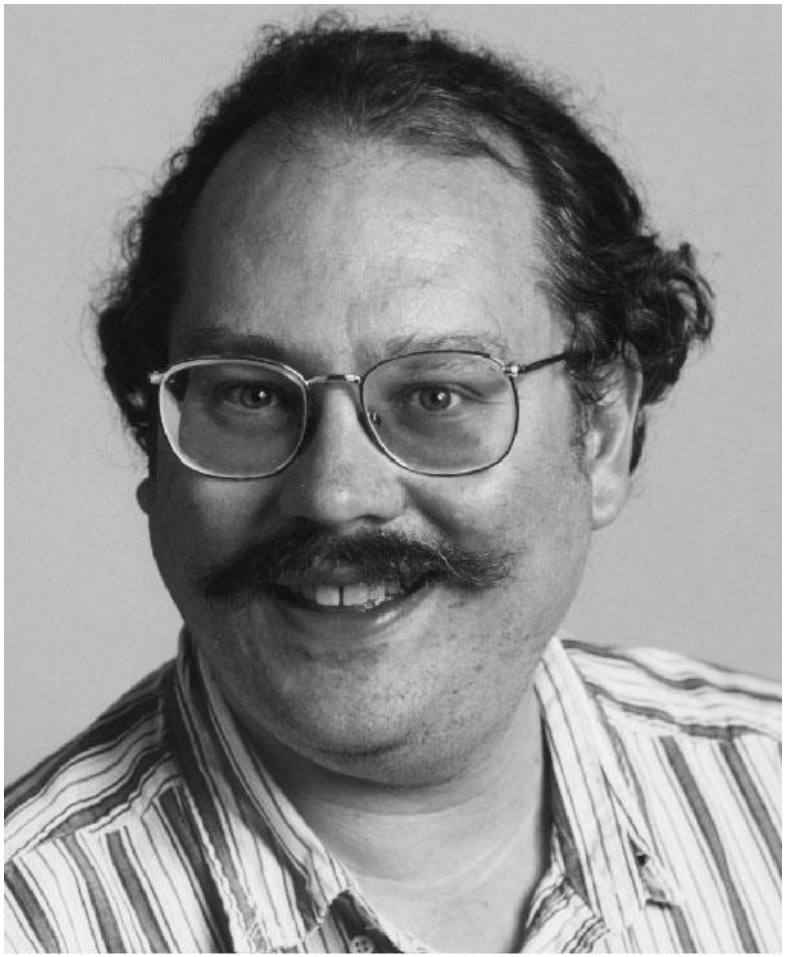
- Definição do Problema
  - Dado um número inteiro com *N* dígitos, encontrar os seus fatores primos.
    - (RSA200)=27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

Fatoração de Números Inteiros Grandes

- Definição do Problema
  - Encontrar os fatores primos de um inteiro
- Os fatores do RSA-200 possuem cerca de 100 dígitos.
  - Os fatores foram encontrados em 2005, consumindo cerca de 55 anos do processamento equivalente a um único núcleo em um intervalo aproximadamente um ano e meio, utilizando 80 processadores Opteron, 2.2 GHz.
    - *Fonte:* http://www.rsa.com/rsalabs/node.asp?id=2879

Peter Shor

- 1994
  - Descobriu um algoritmo quântico capaz de encontrar os fatores de um número primo em tempo polinomial



Fatoração
Clássica x Quântica

Quantidade de Bits	Algoritmo Clássico	Algoritmo de Shor
512	4 dias	**34 segundos**
1024	100 mil anos	**4.5 minutos**
2048	100 milhões de anos	**36 minutos**
4096	100 bilhões de anos	**4.8 horas**

Parte IV

IMPLICAÇÕES

Problemas NP-Completos

- Classe NP
  - Problemas cuja solução correta pode ser encontrada em tempo polinomial por uma máquina de Turing não-determinística.
- Um problema π é NP-completo se:
  - π pertence a classe de problemas NP;
  - A corretude de uma solução para π pode ser verificada em tempo polinomial;
  - Qualquer problema da classe NP pode ser reduzido a π;
  - Portanto, se existe um algoritmo determinístico capaz de resolver π em tempo polinomial, todos os demais problemas NP podem ser resolvidos eficientemente por tal algoritmo;
  - No entanto, acredita-se fortemente que tal algoritmo não exista.

Problemas NP-Completos

- O Problema de **U$ 1.000.000,00** (literalmente)

$$P \overset{?}{=} NP$$

  - Seria a tarefa de encontrar uma solução correta tão fácil quanto a de verificar a corretude de uma dada solução?
  - A Natureza é capaz de resolver problemas NP-completos?

D-Wave 2000Q

- Em 2017, a D-Wave Systems lançou comercialmente o 2000Q, um computador quântico de 2000 qubits a módicos US$ 15 milhões. O computador quântico anterior da companhia tinha 1.000 qubits. Os sistemas de 1.000 quibits da empresa canadense estão sendo testados pelo Google, NASA e pela Lockheed Martin.

D-Wave 2000Q

D-Wave
The Quantum Computing Company™

Bibliografia

- Rieffel e Polak: An introduction to quantum computing for non-physicists, *ACM Comput. Surv.*, Vol. 32, No. 3. (September 2000), pp. 300-335.
- Nielsen & Chuang: Quantum computation and quantum information, Cambridge Univ. Press, 2000.
- Kaye, Laflamme & Mosca: An introduction to quantum computing, Oxford University Press, 2007.
- Quantum Algorithm Zoo: http://math.nist.gov/quantum/zoo/
- Blog de Scott Aaronson: http://www.scottaaronson.com/blog/
- Artigo recente no The Guardian: http://www.guardian.co.uk/nanotechnology-world/the-future-of-computing-power-from-dna-hard-drives-to-quantum-chips