Introdução à Computação Quântica

Tony Minoru Tamura Lopes - ra017502

Instituto de Computação
Universidade Estadual de Campinas

MO401 - Julho de 2006

Sumário

1. Introdução à Computação Quântica
   - Motivação
   - Fenômenos Quânticos
   - Qubits
   - Modelo de Computador
   - Criptografia
   - Estado Atual e Conclusões

Motivação

Necessidade de processadores mais rápidos

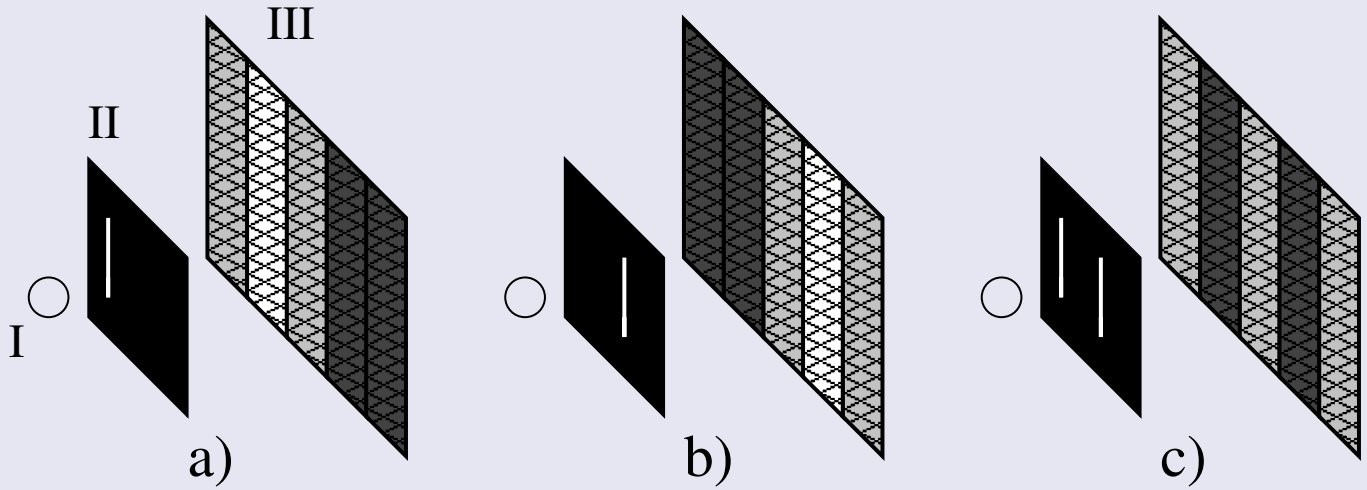
- Miniaturização dos chips
- Limite teórico em 2020
- Poucos átomos para representar um bit
- Necessidade da Quântica

Revolução nas Bases da Computação

- Nova forma de básica de informação
- Novos limitantes inferiores
- Novo paradigma de Computação

Fenômenos Quânticos

Experimento das Duas Fendas



- **Interferência**
- Incerteza de Heisenberg
- Probabilidades

Fenômenos Quânticos

Estado Quântico

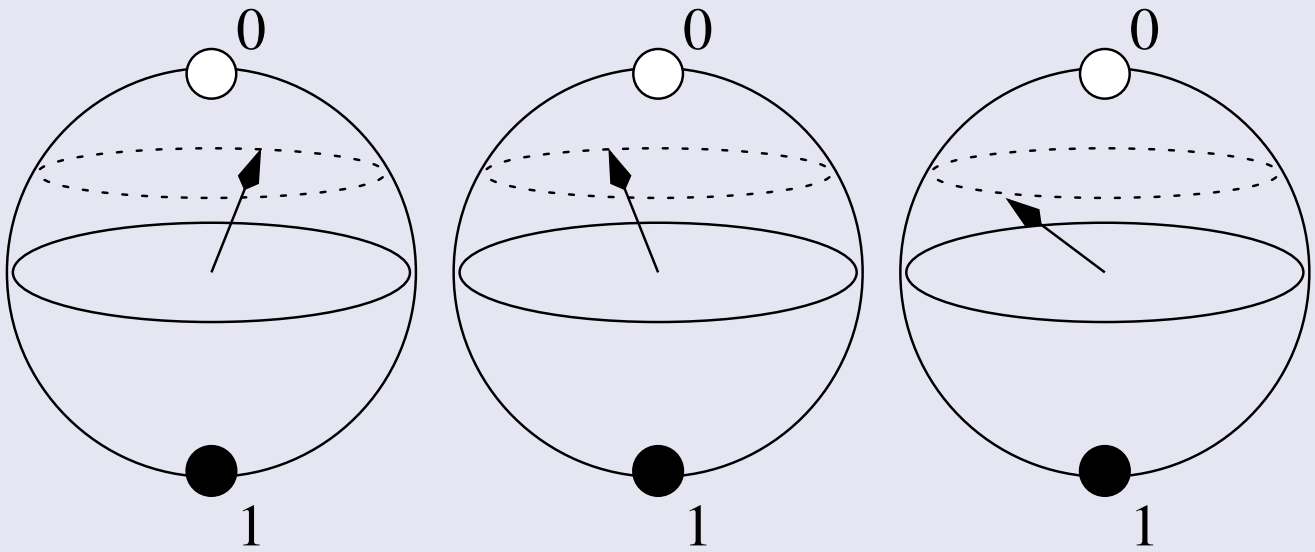
Passagem pela fenda é um estado quântico $|\psi\rangle$!

$$|\psi\rangle = c_0|\text{passa pela fenda } 1\rangle + c_1|\text{passa pela fenda } 2\rangle$$

- *Espaço vetorial complexo de dimensão finita* (Hilbert)
- $c_0 = c_1 = \frac{1}{\sqrt{2}}$
- $|c_0|^2 + |c_1|^2 = 1$
- **Superposição**

Qubit

Qubit



- Qualquer sistema quântico com dois estados

Qubit

Representação do Qubit

- $|Q\rangle = \alpha|0\rangle + \beta|1\rangle$
- $\alpha, \beta \in \mathbb{C}$
- $|\alpha|^2 + |\beta|^2 = 1$
- Fases diferentes, mesma probabilidade.

Transformação do Qubit

- Funcionamento básico
- $In = (\alpha\ \beta)^T$
- $Out = XIn = (\alpha'\ \beta')^T$
- Transformação X é unitária

Múltiplos Qubits

Registrador Quântico

- $|\psi\rangle = c_0 |0\rangle|0\rangle|0\rangle + c_1 |0\rangle|0\rangle|1\rangle + c_2 |0\rangle|1\rangle|0\rangle + \cdots + c_7 |1\rangle|1\rangle|1\rangle$
- 2^n valores ao mesmo tempo!
- 2^n operações!
- **Paralelismo Quântico**

Estados Emaranhados

- $|Q\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)$
- **Não-Localidade**

Necessidades

Necessidades

- Reversibilidade
- Portas lógicas universais

Portas Quânticas

Rotação de 1-Qubit

$$U_{\sqrt{\text{NOT}}}|0\rangle = \left(\frac{1}{2} + \frac{i}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{i}{2}\right)|1\rangle$$
$$U_{\sqrt{\text{NOT}}}|1\rangle = \left(\frac{1}{2} - \frac{i}{2}\right)|0\rangle + \left(\frac{1}{2} + \frac{i}{2}\right)|1\rangle$$

E para a operação NOT:

$$\text{NOT}|0\rangle = U_{\sqrt{\text{NOT}}}U_{\sqrt{\text{NOT}}}|0\rangle = |1\rangle$$
$$\text{NOT}|1\rangle = U_{\sqrt{\text{NOT}}}U_{\sqrt{\text{NOT}}}|1\rangle = |0\rangle$$

Portas Quânticas

NOT-Controlado

$$U_{\mathrm{CN}}|00\rangle = |00\rangle$$
$$U_{\mathrm{CN}}|01\rangle = |01\rangle$$
$$U_{\mathrm{CN}}|10\rangle = |11\rangle$$
$$U_{\mathrm{CN}}|11\rangle = |10\rangle$$

- Lógica condicional
- Produz estados *emaranhados*

Fatoração de Inteiros

- Segurança em Comunicações
- Intratabilidade é conjectura
- Melhor algoritmo clássico: 193 dígitos
- 2000 dígitos?

Algoritmo de Shor

Período de Função

- $f_n(a) = x^a \bmod n$, $mdc(x, n) = 1$
- $f_n(x + r) = f(x)$ e r é o período da função
- $\mathrm{mdc}(x^{r/2} - 1, n)$ quase sempre um fator não-trivial

Exemplo

- $n = 15$ e $x = 8$
- $f_{15}(a) = 8^a \ mod\ 15$ para $a = \{0, 1, 2 \dots\}$
- $\{1, 8, 4, 2, 1, 8, 4, 2, 1, \dots\}$
- $f_{15}(a + 4) = f(a)$, portanto, $r = 4$
- $\mathrm{mdc}(8^{4/2} - 1, 15) = \mathrm{mdc}(63, 15) = 3$
- 5 e 3 são os fatores.

Algoritmo de Shor

Obtendo r

- Obter r é $O(2^L)$ classicamente

$$|f_n\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} |x\rangle |f_n(x)\rangle$$

- $|x\rangle$ emaranhado a $|f_n(x)\rangle$
- Ao medir $|f_n(x)\rangle$ temos y_0
- $|x\rangle$ se torna superposição de x tais que $f_n(x) = y_0$

Algoritmo de Shor

Obtendo r

$$|\psi\rangle = \frac{1}{\sqrt{k}} \sum_{p=0}^{k-1} |x_0 + p.r\rangle$$

$$\mathcal{F}|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{x_0 j}{r}} |j\frac{n}{r}\rangle$$

- FFT é polinomial em Quântica
- Extrai-se r após no máximo $O(L)$ medições de $c = j\frac{n}{r}$

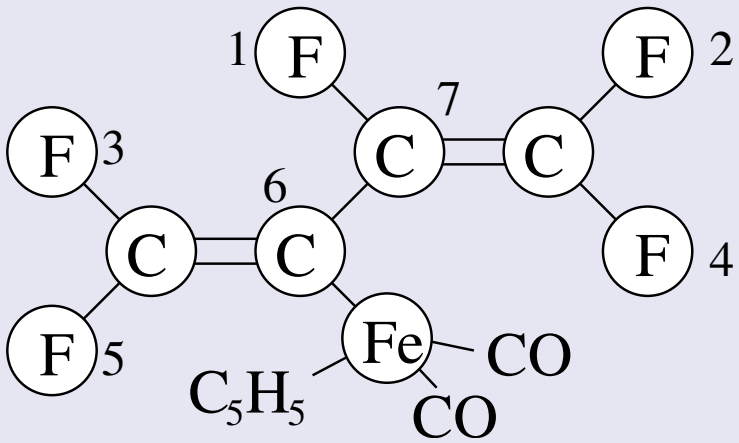
Estado Atual

Criptografia Quântica

- Canal seguro de comunicação é viável, **Não-Clonabilidade**

Computação Quântica

- Implementações de Algoritmos
- Ressonância Magnética de Núcleo



Conclusões

Conclusões

- Área ampla
- Muitos fenômenos "bizarros"
- Necessidade de Estabilidade
- Computação Quântica ainda distante