Computação Quântica: Modelo e Algoritmos

Marco Aurélio Stefanes

DCT/UFMS

Histórico da Computação Quântica

- 82 Fleynman - computador que explore efeitos quânticos
- 85-97 Teoria da Computação Quântica
- 94 - Algoritmo de Shor para fatoração de inteiros
- 2001 - Computador Quântico de 7 bits (IBM)
- 2006 - Computador Quântico de 12 bits (Waterloo)

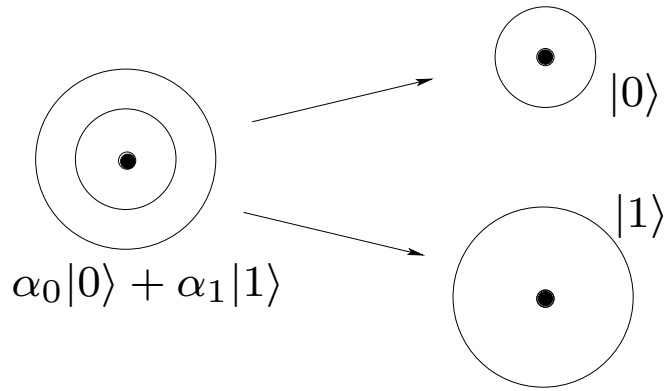
Introdução

- Q-bits - estados quânticos do elétron
  - Estático $|0\rangle$
  - Excitado $|1\rangle$
- Princípio da superposição
  Estado do eletrón - combinação da forma:
  $\alpha_0|0\rangle + \alpha_1|1\rangle$ onde
  $\alpha_0, \alpha_1 \in \mathbf{C}$
  $\alpha_0^2 + \alpha_1^2 = 1$
  α é a amplitude — Probabilidade (negativa!)

Unidade do Computador Quântico: Q-bit

Introdução

- Ao medir o estado $\alpha_0|0\rangle + \alpha_1|1\rangle$ teremos $|0\rangle$ com prob $|\alpha_0|^2$ **ou** $|1\rangle$ com prob $|\alpha_1|^2$



- Registrador quântico
  $|\phi\rangle = \sum_{x\in\{0,1\}^k} \alpha_k|x\rangle$ onde: $\sum_{x\in\{0,1\}^k} \alpha_k = 1$
- Ex. $k = 2$
  $|\phi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$

Produto Tensorial

Estado quântico de n q-bits
$|\phi\rangle = |\phi_0\rangle, |\phi_1\rangle, \cdots, |\phi_{n-1}\rangle$
é
$|\phi\rangle = |\phi_{n-1}\rangle \otimes |\phi_{n-2}\rangle \otimes \cdots \otimes |\phi_0\rangle$ onde,

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

Ex. com $|\phi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ e $|\phi_0\rangle = \beta_0|0\rangle + \beta_1|1\rangle$
temos o **entrelaçamento**
$|\phi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$

Medição parcial de *n* q-bits

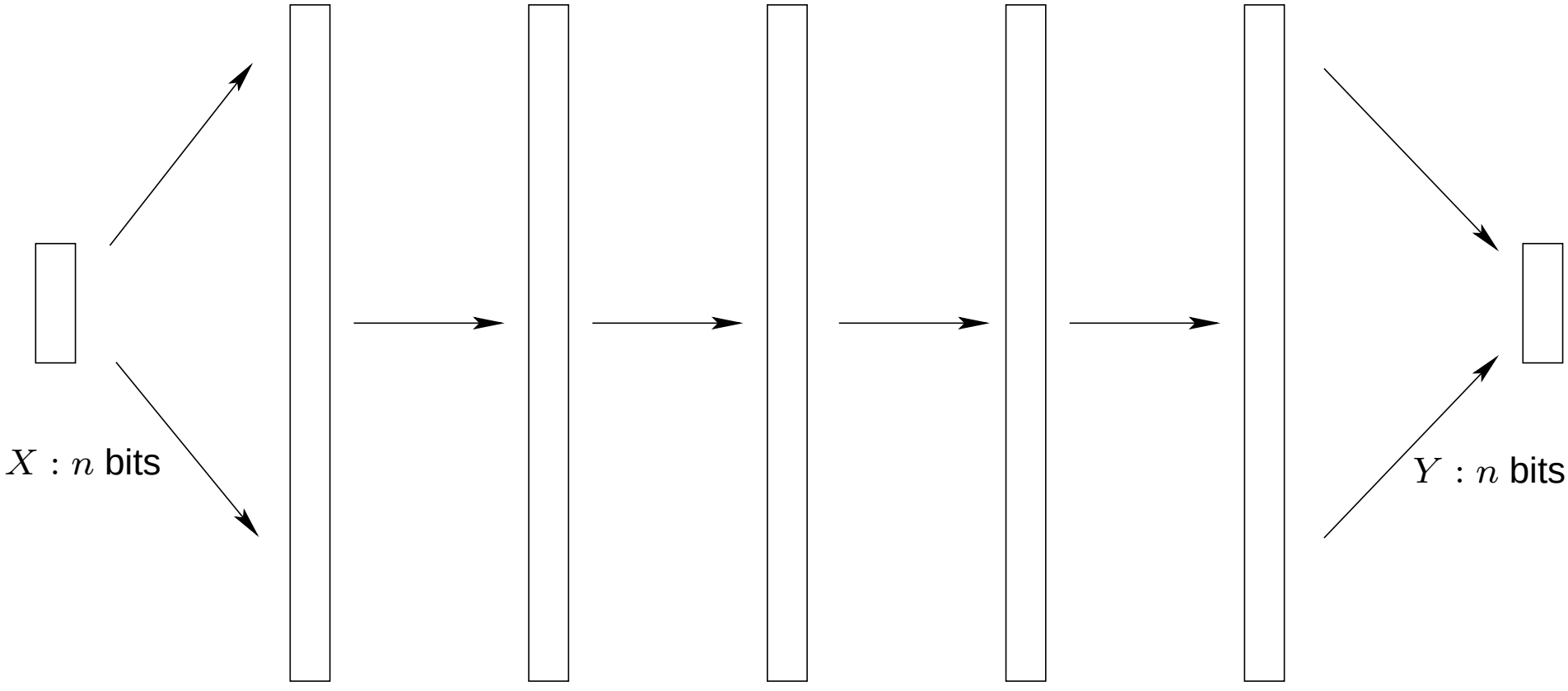
Seja $|\phi\rangle = \sum_{x \in \{0,1\}^k} \alpha_k |x\rangle$ um registrador

Medição de $|\phi_j\rangle$

- valor observado é $|0\rangle$ com
  $p_0 = \sum\{|\alpha_x|^2 : x \in \{0,1\}^n \text{ e } x_j = 0\}$ e
  $|\phi'\rangle = \frac{\sum\{\alpha_x|x\rangle : x \in \{0,1\}^n \text{ e } x_j = 0\}}{p_0}$
- valor observado é $|1\rangle$ com
  $p_1 = \sum\{|\alpha_x|^2 : x \in \{0,1\}^n \text{ e } x_j = 1\}$ e
  $|\phi'\rangle = \frac{\sum\{\alpha_x|x\rangle : x \in \{0,1\}^n \text{ e } x_j = 1\}}{P_1}$

Este é o paralelismo quântico

Algoritmos Quânticos



Superposição exponencial

Transformada de Hadamard

Porta Quântica: Transformação reversível

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

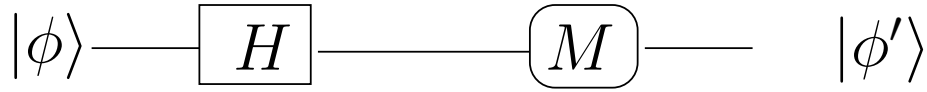
Sendo

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

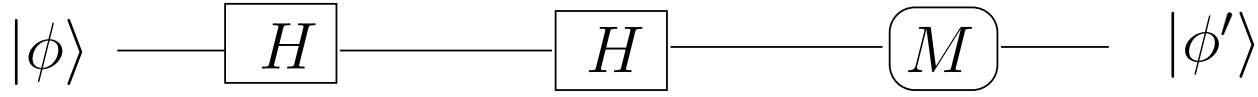
Transforma $|\phi\rangle = |0\rangle$ em

$$H|\phi\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\alpha_0|0\rangle + \alpha_1|1\rangle)$$

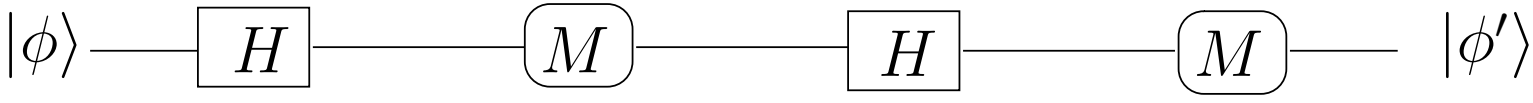
Circuitos Hamadard



(1) Circuito de Hamadard com medição



(2) Dupla porta de Hamadard

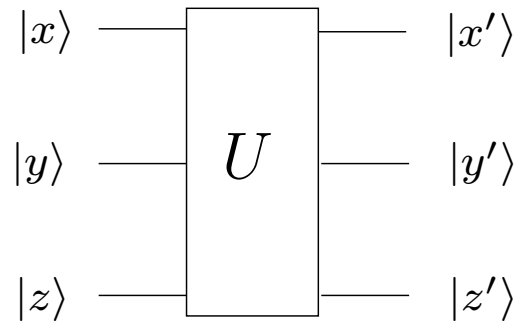


(3) Hamadard dupla com medição intercalada

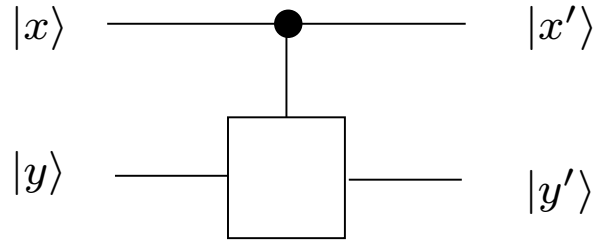
Circuitos Quânticos

Circuitos Reversíveis

- **OU**: $|\phi\rangle = |x\rangle \otimes |y\rangle \otimes |z\rangle$ gera
  $|\phi'\rangle = |x\rangle \otimes |y\rangle \otimes |z \oplus (x \vee y)\rangle$

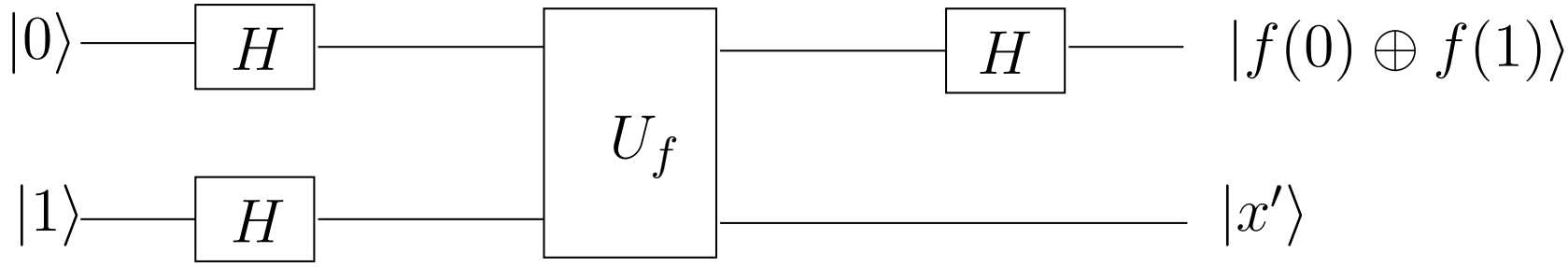


- Porta V controlada por x



Problema de Deutsch

Dada uma caixa preta lógica U_f, determine se $f(0) = f(1)$ ou se $f(0) \neq f(1)$



No modelo clássicos são necessárias duas aplicações de U_f e no modelo quântico apenas uma para determinar se U_f é balaceada ou não.

Conclusão

- Computadores Quânticos são viáveis
  - Resolvem vários problemas
  - Teoria difícil
- Ganhos de tempos exponeciais
  - Transformada de Fourier Quântica
  - Fatoração de Inteiros
  - Busca em Base de Dados