Introdução à Computação Quântica

Ian Liu Rodrigues
Kaio Karam Galvão

MO401 - Arquitetura de Computadores I
27 de junho de 2011

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

Introdução

Motivação

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Advento do transistor: rápida evolução do hardware

Motivação

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Advento do transistor: rápida evolução do hardware
- Miniaturização

Motivação

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Advento do transistor: rápida evolução do hardware
- Miniaturização
- Lei de Moore

Motivação

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Advento do transistor: rápida evolução do hardware
- Miniaturização
- Lei de Moore
- Tamanho dos componentes: efeitos quânticos
  - Impossível operar segundo os princípios da física clássica
  - Limitador no aumento do poder de computação

Motivação

Introdução
Motivação
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Advento do transistor: rápida evolução do hardware
- Miniaturização
- Lei de Moore
- Tamanho dos componentes: efeitos quânticos
  - Impossível operar segundo os princípios da física clássica
  - Limitador no aumento do poder de computação
- Mudança de paradigma na construção de computadores: Computação Quântica

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

O Bit Quântico

Qubit

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema quântico: espaço vetorial complexo (espaço de estados)

Qubit

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema quântico: espaço vetorial complexo (espaço de estados)
- Qubit: sistema quântico com base ortonormal de estados $\{|0\rangle, |1\rangle\}$

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema quântico: espaço vetorial complexo (espaço de estados)
- Qubit: sistema quântico com base ortonormal de estados $\{|0\rangle, |1\rangle\}$
- Estado de um qubit: $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ (superposição de estados) α e β: amplitudes

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema quântico: espaço vetorial complexo (espaço de estados)
- Qubit: sistema quântico com base ortonormal de estados $\{|0\rangle, |1\rangle\}$
- Estado de um qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (superposição de estados) α e β: amplitudes
- Medição: apenas os estados $|0\rangle$ e $|1\rangle$ são observados
  - $|\alpha|^2$ = probabilidade de se observar o estado $|0\rangle$
  - $|\beta|^2$ = probabilidade de se observar o estado $|1\rangle$
  - $|\alpha|^2 + |\beta|^2 = 1 \rightarrow$ vetor unitário

Múltiplos qubits

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema com **dois** qubits:
  base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

Múltiplos qubits

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema com **dois** qubits:
  base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- Estado do sistema:
  $|\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |01\rangle + \alpha_3 |10\rangle + \alpha_4 |11\rangle$
  4 amplitudes

Múltiplos qubits

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema com **dois** qubits:
  base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- Estado do sistema:
  $|\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |01\rangle + \alpha_3 |10\rangle + \alpha_4 |11\rangle$
  4 amplitudes
- Sistema com n qubits:
  2^n estados base $\rightarrow$ 2^n amplitudes

Múltiplos qubits

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Sistema com **dois** qubits:
  base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- Estado do sistema:
  $|\psi\rangle = \alpha_1 |00\rangle + \alpha_2 |01\rangle + \alpha_3 |10\rangle + \alpha_4 |11\rangle$
  4 amplitudes
- Sistema com n qubits:
  2^n estados base $\rightarrow$ 2^n amplitudes
- Condição de normalização:
  $\sum_{i=1}^{2^n} |\alpha_i|^2 = 1$

Transformações

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Vetor de estado de um qubit: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

Transformações

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Vetor de estado de um qubit: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Matriz de tranformação: $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$

Transformações

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Vetor de estado de um qubit: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Matriz de tranformação: $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$
- Exemplo: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$

  Inversão das amplitudes

Transformações

Introdução
O Bit Quântico
Qubit
Múltiplos qubits
Transformações
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- Vetor de estado de um qubit: $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Matriz de tranformação: $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$
- Exemplo: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$
  Inversão das amplitudes
- Matriz unitária: não altera a magnitude do vetor

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

Portas e Circuitos Quânticos

Portas de 1 qubit

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- NOT: inverte amplitudes de um qubit
  $|0\rangle \rightarrow |1\rangle$ e $|1\rangle \rightarrow |0\rangle$

Portas de 1 qubit

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

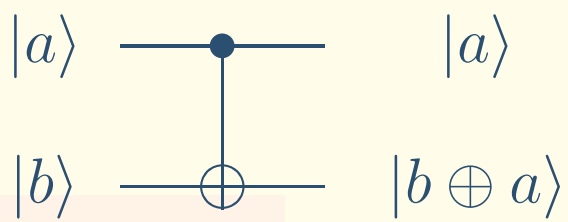
- NOT: inverte amplitudes de um qubit
  $|0\rangle \rightarrow |1\rangle$ e $|1\rangle \rightarrow |0\rangle$
- Porta Z $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow -|1\rangle$
  $$\begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- NOT: inverte amplitudes de um qubit
  $|0\rangle \rightarrow |1\rangle$ e $|1\rangle \rightarrow |0\rangle$
- Porta Z $|0\rangle \rightarrow |0\rangle$ e $|1\rangle \rightarrow -|1\rangle$
  $$\begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$
- Porta de Hadamard
  $$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$$

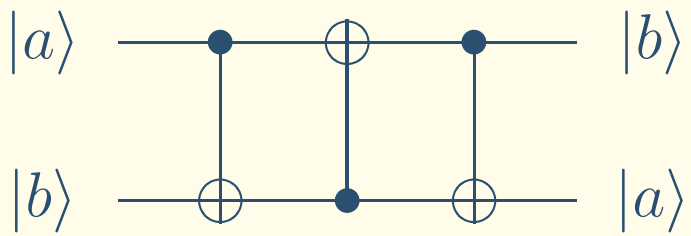
Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- NOT-controlado (CNOT)
  entradas: qubit controle, qubit alvo
  saídas: qubit controle, qubit alvo alterado
  $|00\rangle \rightarrow |00\rangle$
  $|01\rangle \rightarrow |01\rangle$
  $|10\rangle \rightarrow |11\rangle$
  $|11\rangle \rightarrow |10\rangle$
- Opera como um XOR
- Diagrama de circuito:



Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Portas de 1 qubit
Portas de 2 qubits
Circuito
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões

- SWAP: permuta os estados de dois qubits
  $|a, b\rangle \rightarrow |b, a\rangle$
- Composto de 3 portas CNOT
- Diagrama:



Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Definição
Exemplo
Exemplo (cont)
Emaranhamento
Algoritmos Quânticos
Conclusões

Produto Tensorial

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Definição
Exemplo
Exemplo (cont)
Emaranhamento
Algoritmos Quânticos
Conclusões

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$
- Então $C = A \otimes B$ vale

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

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$
- Então $C = A \otimes B$ vale

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

- Propriedades

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$
- Então $C = A \otimes B$ vale

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

- Propriedades
  - Associativa

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$
- Então $C = A \otimes B$ vale

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

- Propriedades
  - Associativa
  - Distributiva com a soma

Definição

- A, B matrizes de tamanho $m \times n$ e $r \times s$
- Então $C = A \otimes B$ vale

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

- Propriedades
  - Associativa
  - Distributiva com a soma
  - Outras propriedades

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$
$$(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B).$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Definição
Exemplo
Exemplo (cont)
Emaranhamento
Algoritmos Quânticos
Conclusões

- Aplicar Hadamard no primeiro qubit de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Exemplo

- Aplicar Hadamard no primeiro qubit de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Multiplicar o 1º qubit por H e o segundo por I

Exemplo

- Aplicar Hadamard no primeiro qubit de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Multiplicar o 1º qubit por H e o segundo por I
- Observe que

$$\begin{aligned} |\psi'\rangle &= H \otimes I \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ &= \frac{1}{\sqrt{2}} H|0\rangle\, I|0\rangle + \frac{1}{\sqrt{2}} H|1\rangle\, I|1\rangle \end{aligned}$$

Exemplo (continuação)

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Definição
Exemplo
Exemplo (cont)
Emaranhamento
Algoritmos Quânticos
Conclusões

- Então o estado transformado fica

$$|\psi\rangle = \frac{|00\rangle + |10\rangle + |01\rangle - |11\rangle}{2}$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Definição
Algoritmos Quânticos
Conclusões

Emaranhamento

Definição

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Definição
Algoritmos Quânticos
Conclusões

- Forte relação entre dois ou mais qubits

Definição

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Definição
Algoritmos Quânticos
Conclusões

- Forte relação entre dois ou mais qubits
- Não pode ser decomposto como um produto tensorial

Definição

- Forte relação entre dois ou mais qubits
- Não pode ser decomposto como um produto tensorial
- Exemplo de estado emaranhado:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Definição
Algoritmos Quânticos
Conclusões

- Forte relação entre dois ou mais qubits
- Não pode ser decomposto como um produto tensorial
- Exemplo de estado emaranhado:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Exemplo de estado não emaranhado:

$$\begin{aligned} |\psi'\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes \frac{1}{2}(|0\rangle + |1\rangle) \end{aligned}$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmos Quânticos

Codificação Super Densa

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- n-qubits quânticos contém a mesma quantidade de informação que n-bits convencionais!

Codificação Super Densa

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- n-qubits quânticos contém a mesma quantidade de informação que n-bits convencionais!
- A não ser que Alice e Bob compartilhem qubits emaranhados

Codificação Super Densa

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- n-qubits quânticos contém a mesma quantidade de informação que n-bits convencionais!
- A não ser que Alice e Bob compartilhem qubits emaranhados
- Neste caso 1-qubit pode conter a informação de 2-bits

Codificação Super Densa

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- n-qubits quânticos contém a mesma quantidade de informação que n-bits convencionais!
- A não ser que Alice e Bob compartilhem qubits emaranhados
- Neste caso 1-qubit pode conter a informação de 2-bits
- Isto é chamado de codificação super densa

Exemplo de protocolo

- Alice tem o 1º qubit e Bob tem o 2º de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Exemplo de protocolo

- Alice tem o 1º qubit e Bob tem o 2º de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Alice quer enviar os bits $a = 0$ e $b = 1$ para Bob

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Exemplo de protocolo

- Alice tem o 1º qubit e Bob tem o 2º de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Alice quer enviar os bits $a = 0$ e $b = 1$ para Bob
- Então ela aplica σ_x no seu qubit e envia para Bob

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

Exemplo de protocolo

- Alice tem o 1º qubit e Bob tem o 2º de

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Alice quer enviar os bits $a = 0$ e $b = 1$ para Bob
- Então ela aplica σ_x no seu qubit e envia para Bob

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

- Bob aplica U_{CN} em $|\psi'\rangle$

$$|\psi''\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

e depois Hadamard, obtendo $|01\rangle$

Algoritmo de Deutsch

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- Problema: A função $f : \{0, 1\} \to \{0, 1\}$ é constante?

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmo de Deutsch

- Problema: A função $f : \{0, 1\} \to \{0, 1\}$ é constante?
- Método clássico: avalie $f(0)$ e $f(1)$ e veja se $f(0) = f(1)$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmo de Deutsch

- Problema: A função $f : \{0, 1\} \to \{0, 1\}$ é constante?
- Método clássico: avalie $f(0)$ e $f(1)$ e veja se $f(0) = f(1)$
- O método clássico avalia duas vezes

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

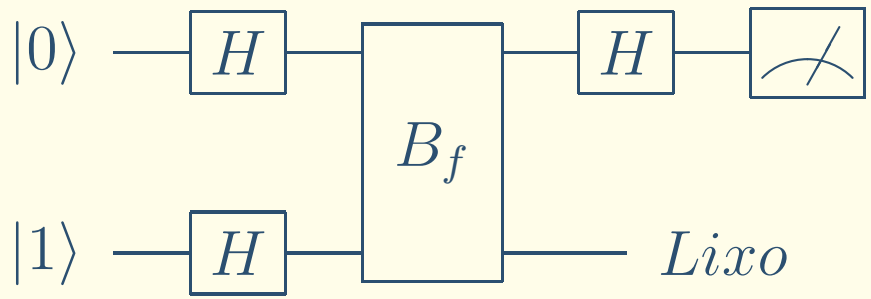
Algoritmo de Deutsch

- Problema: A função $f : \{0,1\} \to \{0,1\}$ é constante?
- Método clássico: avalie $f(0)$ e $f(1)$ e veja se $f(0) = f(1)$
- O método clássico avalia duas vezes
- No computador quântico define-se $B_f \left|a\right\rangle \left|b\right\rangle = \left|a\right\rangle \left|b \oplus f(a)\right\rangle$

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmo de Deutsch

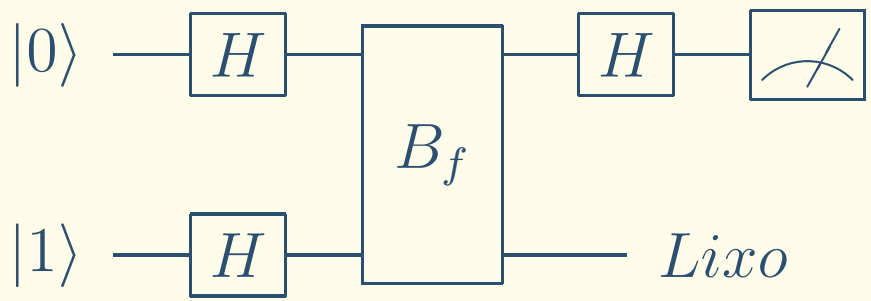
- Problema: A função $f : \{0,1\} \to \{0,1\}$ é constante?
- Método clássico: avalie $f(0)$ e $f(1)$ e veja se $f(0) = f(1)$
- O método clássico avalia duas vezes
- No computador quântico define-se $B_f \left|a\right\rangle \left|b\right\rangle = \left|a\right\rangle \left|b \oplus f(a)\right\rangle$
- Aplica o circuito



Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmo de Deutsch

- Problema: A função $f : \{0,1\} \to \{0,1\}$ é constante?
- Método clássico: avalie $f(0)$ e $f(1)$ e veja se $f(0) = f(1)$
- O método clássico avalia duas vezes
- No computador quântico define-se $B_f \left|a\right\rangle \left|b\right\rangle = \left|a\right\rangle \left|b \oplus f(a)\right\rangle$
- Aplica o circuito



- O 1º qubit vale $f(0) \oplus f(1)$

Algoritmo de Simons I

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- Seja $f : \{0,1\}^n \to \{0,1\}^n$ função

Algoritmo de Simons I

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- Seja $f : \{0,1\}^n \to \{0,1\}^n$ função
- Existe s tal que $f(x) = f(y)$ se e só se $x \oplus y = s$

Algoritmo de Simons I

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- Seja $f : \{0,1\}^n \to \{0,1\}^n$ função
- Existe s tal que $f(x) = f(y)$ se e só se $x \oplus y = s$
- Quem é s?

Algoritmo de Simons I

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- Seja $f : \{0,1\}^n \to \{0,1\}^n$ função
- Existe s tal que $f(x) = f(y)$ se e só se $x \oplus y = s$
- Quem é s?
- No modelo clássico, o melhor algoritmo leva $O(2^{\frac{n}{2}})$

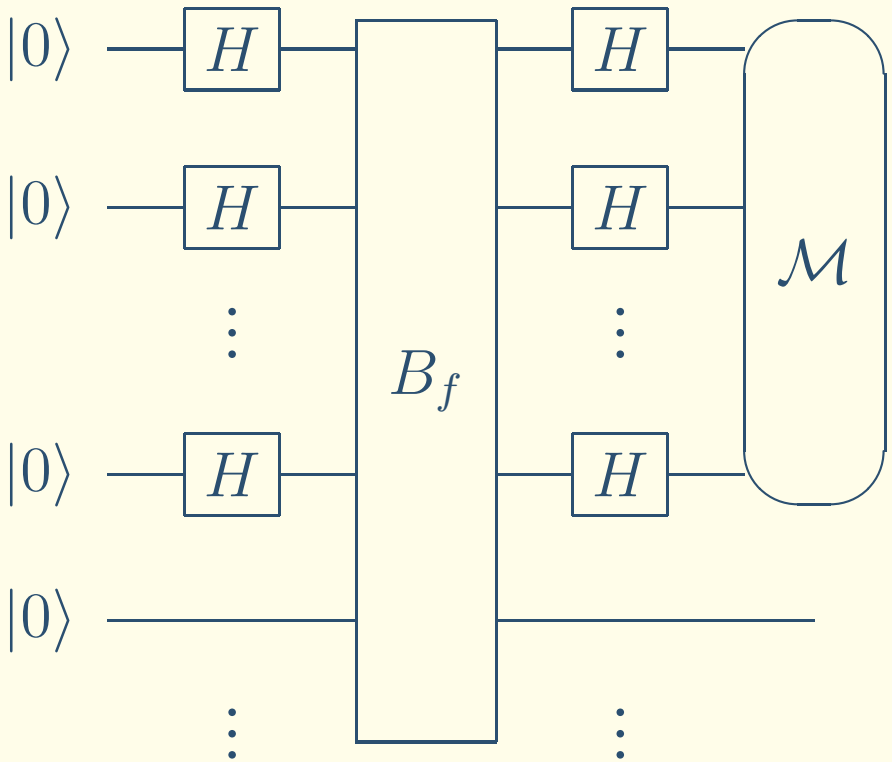
Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

Algoritmo de Simons I

- Seja $f : \{0,1\}^n \to \{0,1\}^n$ função
- Existe s tal que $f(x) = f(y)$ se e só se $x \oplus y = s$
- Quem é s?
- No modelo clássico, o melhor algoritmo leva $O(2^{\frac{n}{2}})$
- No computador quântico leva $O(n)$ operações

Algoritmo de Simons II

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões



Algoritmo de Simons III

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- A leitura dos n primeiros qubits nos dá um vetor y tal que $y \cdot s = 0$

Algoritmo de Simons III

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- A leitura dos n primeiros qubits nos dá um vetor y tal que $y \cdot s = 0$
- Fazemos $n - 1$ leituras, obtendo um sistema linear

$$\begin{aligned} y_1 \quad &\cdot \quad s_1 = 0 \\ &\vdots \\ y_{n-1} \quad &\cdot \quad s_{n-1} = 0 \end{aligned}$$

Algoritmo de Simons III

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- A leitura dos n primeiros qubits nos dá um vetor y tal que $y \cdot s = 0$
- Fazemos $n - 1$ leituras, obtendo um sistema linear

$$\begin{aligned} y_1 \quad &\cdot \quad s_1 = 0 \\ &\vdots \\ y_{n-1} \quad &\cdot \quad s_{n-1} = 0 \end{aligned}$$

- Resolvemos para s e obtemos um resultado

Algoritmo de Simons III

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Codificação Super Densa
Exemplo de protocolo
Algoritmo de Deutsch
Algoritmo de Simons I
Algoritmo de Simons II
Algoritmo de Simons III
Conclusões

- A leitura dos n primeiros qubits nos dá um vetor y tal que $y \cdot s = 0$
- Fazemos $n-1$ leituras, obtendo um sistema linear

$$\begin{aligned} y_1 \quad &\cdot \quad s_1 = 0 \\ &\vdots \\ y_{n-1} \quad &\cdot \quad s_{n-1} = 0 \end{aligned}$$

- Resolvemos para s e obtemos um resultado
- Probabilidade de se obter um sistema linear após $4m$ medidas

$$\left(1 - \frac{1}{4}\right)^{4m} < e^{-m}.$$

Conclusões

Introdução
O Bit Quântico
Portas e Circuitos Quânticos
Produto Tensorial
Emaranhamento
Algoritmos Quânticos
Conclusões
Conclusões

- Quebra no paradigma de arquitetura de computadores
- Novas complexidades para problemas conhecidos
- Algoritmos eficientes para problemas tradicionalmente difíceis