Computação Quântica: Complexidade e Algoritmos

Carlos H. Cardonha

Marcel K. de Carli Silva

Cristina G. Fernandes (orientadora)

Departamento de Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

Apoio financeiro FAPESP (03/13236-0 e 03/13237-7)

Tópicos

▷ Breve histórico e descrição do trabalho

- O modelo quântico de computação
- O algoritmo de fatoração de Shor
- Relações entre classes de complexidade

Breve Histórico

- Feynman (82): explorar efeitos quânticos
- Deutsch (85, 89): formalização do modelo
- Shor (94): fatoração eficiente de inteiros
- Grover (96): busca em tempo proporcional a $\sqrt{n}$
- Bernstein e Vazirani (97): complexidade computacional

Descrição do Trabalho

Estudo básico do modelo quântico de computação.

Parte do Marcel: Aspectos Algorítmicos. Algoritmos de

- Deutsch, Deutsch-Jozsa e Simon
- Shor
- Grover

Descrição do Trabalho

Estudo básico do modelo quântico de computação.

Parte do Marcel: Aspectos Algorítmicos. Algoritmos de

- Deutsch, Deutsch-Jozsa e Simon
- Shor
- Grover

Parte do Carlos: Resultados de Complexidade.

- Máquinas de Turing quânticas
- Máquina de Turing quântica universal
- Classes quânticas de complexidade e relação com clássicas

Tópicos

- Breve histórico e descrição do trabalho

▷ O modelo quântico de computação

- O algoritmo de fatoração de Shor

- Relações entre classes de complexidade

Bits Quânticos

$\mathcal{H}_2 := \mathbb{C} \times \mathbb{C}$ espaço vetorial de dimensão 2

Bits Quânticos

$\mathcal{H}_2 := \mathbb{C} \times \mathbb{C}$ espaço vetorial de dimensão 2

$B_2 := \{|0\rangle, |1\rangle\}$ base ortonormal de $\mathcal{H}_2$

Bits Quânticos

$\mathcal{H}_2 := \mathbb{C} \times \mathbb{C}$ espaço vetorial de dimensão 2

$B_2 := \{|0\rangle, |1\rangle\}$ base ortonormal de $\mathcal{H}_2$

$|0\rangle$ e $|1\rangle$: estados básicos

Bits Quânticos

$\mathcal{H}_2 := \mathbb{C} \times \mathbb{C}$ espaço vetorial de dimensão 2

$B_2 := \{|0\rangle, |1\rangle\}$ base ortonormal de $\mathcal{H}_2$

$|0\rangle$ e $|1\rangle$: estados básicos

bit quântico $|\phi\rangle$ é um vetor unitário em $\mathcal{H}_2$

$$|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$\alpha_0, \alpha_1 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 = 1$, pois $|\phi\rangle$ tem norma 1

Bits Quânticos

$\mathcal{H}_2 := \mathbb{C} \times \mathbb{C}$ espaço vetorial de dimensão 2

$B_2 := \{|0\rangle, |1\rangle\}$ base ortonormal de $\mathcal{H}_2$

$|0\rangle$ e $|1\rangle$: estados básicos

bit quântico $|\phi\rangle$ é um vetor unitário em $\mathcal{H}_2$

$$|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$\alpha_0, \alpha_1 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 = 1$, pois $|\phi\rangle$ tem norma 1

$|\phi\rangle$ é superposição de estados básicos

Principais Características: Superposição

Um bit quântico armazena uma superposição de 0 e 1

Principais Características: Superposição

Um bit quântico armazena uma superposição de 0 e 1

Exemplo:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Principais Características: Superposição

Um bit quântico armazena uma superposição de 0 e 1

Exemplo:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Um registrador com n bits quânticos armazena uma superposição de 2^n estados básicos

Principais Características: Superposição

Um bit quântico armazena uma superposição de 0 e 1

Exemplo:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Um registrador com n bits quânticos armazena uma superposição de 2^n estados básicos

Exemplo: $n = 2$

$$\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle$$

Principais Características

Ao tentarmos “enxergar” uma superposição, modificamos (perdemos) esta irreversivelmente
(Princípio da Incerteza)

Principais Características

Ao tentarmos “enxergar” uma superposição, modificamos (perdemos) esta irreversivelmente
(Princício da Incerteza)

No modelo clássico, portas lógicas são funções de bits em bits.
No modelo quântico, as equivalentes “portas lógicas” são funções bijetoras de bits quânticos em bits quânticos.

Exemplo: função de negação — $f(0) = 1$ e $f(1) = 0$

Principais Características

Facilidade de extração de propriedades globais de uma função. Exemplo: período.

Principais Características

Facilidade de extração de propriedades globais de uma função. Exemplo: período.

Exemplo:
função $f(a) := 2^a \bmod 5$
$\langle f(0), f(1), f(2), \ldots \rangle = \langle 1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, \ldots \rangle$
período 4

Tópicos

- Breve histórico e descrição do trabalho
- O modelo quântico de computação

▷ O algoritmo de fatoração de Shor

- Relações entre classes de complexidade

Algoritmo de Shor

Recebe:

um inteiro n composto, ímpar,
que não uma potência de primo
(n tem pelo menos 2 divisores primos).

Algoritmo de Shor

Recebe:

um inteiro n composto, ímpar,
que não uma potência de primo
(n tem pelo menos 2 divisores primos).

Devolve:

um fator de n, com alta probabilidade.

Algoritmo de Shor

Idéia:

transforma problema da fatoração em busca do período de uma função.

Algoritmo de Shor

Idéia:

transforma problema da fatoração em busca do período de uma função.

Consumo de tempo:

polinomial em $\log n$.

Algoritmo de Shor

Idéia:

transforma problema da fatoração em busca do período de uma função.

Consumo de tempo:

polinomial em $\log n$.

Observação:

um único passo quântico!

Algoritmo de Shor

Shor (n)

1. $x \leftarrow$ rand$\{2, \cdots, n-1\}$
2. $d \leftarrow$ mdc(x, n)
3. se $d > 1$ $\quad\triangleright$ único passo quântico
4. então devolva d
5. $r \leftarrow$ ordem(x, n) $\quad\triangleright$ menor $a > 0$ tal que $x^a \equiv 1 \pmod{n}$
6. se r é ímpar ou $x^{r/2} \equiv -1 \pmod{n}$
7. então FALHOU!
8. senão devolva mdc$(x^{r/2} - 1, n)$

Algoritmo de Shor

Teorema:

$r :=$ menor $a > 0$ com $x^a \equiv 1 \pmod{n}$
se r par e $x^{r/2} \not\equiv -1 \pmod{n}$
então mdc$(x^{r/2} - 1, n)$ é fator de n

Algoritmo de Shor

Teorema:

$r :=$ menor $a > 0$ com $x^a \equiv 1 \pmod n$
se r par e $x^{r/2} \not\equiv -1 \pmod n$
então mdc$(x^{r/2} - 1, n)$ é fator de n

Prova:

$(x^{r/2} + 1)(x^{r/2} - 1) = x^r - 1$ é múltiplo de n

$x^{r/2} + 1$ não é múltiplo de n

$x^{r/2} - 1$ não é múltiplo de n

Fatores de n separados entre $x^{r/2} + 1$ e $x^{r/2} - 1$.

Algoritmo de Shor

Teorema:

Se n tem m divisores primos,
então probabilidade de falha $\leq 1/2^{m-1}$

Algoritmo de Shor

Teorema:

Se n tem m divisores primos,
então probabilidade de falha $\leq 1/2^{m-1}$

Prova:

Teorema Chinês do Resto e
Fato: $\mathbb{Z}_{p^k}$ é cíclico se p primo ímpar.

Algoritmo de Shor

Álgebra (Teoria dos Grupos):

$r :=$ ordem de x, módulo n.

r é o período da seqüência

$$\langle x^0 \bmod n, x^1 \bmod n, x^2 \bmod n, x^3 \bmod n, \ldots \rangle.$$

r é o período da função $f(a) := x^a \bmod n$.

Busca do Período

Algoritmo quântico

encontra o período da função $f(a) := x^a \bmod n$ em tempo polinomial em $\log n$ e com alta probabilidade.

Busca do Período

Algoritmo quântico

encontra o período da função $f(a) := x^a \bmod n$ em tempo polinomial em $\log n$ e com alta probabilidade.

Utiliza "versão" quântica (trabalhando com superposições) da Transformada Discreta de Fourier

$$\mathbb{C}^n \ni (a_0, \ldots, a_{n-1}) \mapsto (b_0, \ldots, b_{n-1}) \in \mathbb{C}^n$$

$$\text{onde } b_k := \sum_{j=0}^{n-1} a_j \omega_n^{jk}$$

$\omega_n := \exp\{2\pi i/n\}$ é n-ésima raiz complexa da unidade.

Tópicos

- Breve histórico e descrição do trabalho
- O modelo quântico de computação
- O algoritmo de fatoração de Shor

▷ Relações entre classes de complexidade

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico
- $\mathbf{BPP}$: tempo polinomial no modelo clássico e probabilidade de falha limitada por constante

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico
- $\mathbf{BPP}$: tempo polinomial no modelo clássico
  e probabilidade de falha limitada por constante
- $\mathbf{PSPACE}$: espaço polinomial no modelo clássico

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico
- $\mathbf{BPP}$: tempo polinomial no modelo clássico
  e probabilidade de falha limitada por constante
- $\mathbf{PSPACE}$: espaço polinomial no modelo clássico
- $\mathbf{EQP}$: tempo polinomial no modelo quântico

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico
- $\mathbf{BPP}$: tempo polinomial no modelo clássico e probabilidade de falha limitada por constante
- $\mathbf{PSPACE}$: espaço polinomial no modelo clássico
- $\mathbf{EQP}$: tempo polinomial no modelo quântico
- $\mathbf{BQP}$: tempo polinomial no modelo quântico e probabilidade de falha limitada por constante

Classes de Complexidade

Classe dos problemas resolvidos em

- $\mathbf{P}$: tempo polinomial no modelo clássico
- $\mathbf{BPP}$: tempo polinomial no modelo clássico e probabilidade de falha limitada por constante
- $\mathbf{PSPACE}$: espaço polinomial no modelo clássico
- $\mathbf{EQP}$: tempo polinomial no modelo quântico
- $\mathbf{BQP}$: tempo polinomial no modelo quântico e probabilidade de falha limitada por constante

Pode-se provar:

$$\mathbf{P} \subseteq \mathbf{EQP} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$$

Direções futuras

- Estudo de mais algoritmos quânticos
- Generalização dos algoritmos exponencialmente mais rápidos (Hidden Subgroup Problem)
- Uso de idéias quânticas no modelo clássico
- Códigos resistentes a falha
- Mais resultados de complexidade

Fim

Sítio:
`http://www.linux.ime.usp.br/~magal/quantum/`

Carlos: `cardonha@ime.usp.br`

Marcel: `magal@ime.usp.br`

Cristina (orientadora): `cris@ime.usp.br`