

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

- 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

Tópicos

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

Bits Quânticos

$\mathcal{H}_2 :=$ espaço de Hilbert de dimensão 2

Bits Quânticos

$\mathcal{H}_2 :=$ espaço de Hilbert de dimensão 2

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

Bits Quânticos

$\mathcal{H}_2 :=$ espaço de Hilbert de dimensão 2

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

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

Bits Quânticos

$\mathcal{H}_2 :=$ espaço de Hilbert 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

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

$$\alpha_0, \alpha_1 \in \mathbb{C} \text{ e } |\alpha_0|^2 + |\alpha_1|^2 = 1$$

Bits Quânticos

$\mathcal{H}_2 :=$ espaço de Hilbert 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

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

$$\alpha_0, \alpha_1 \in \mathbb{C} \text{ e } |\alpha_0|^2 + |\alpha_1|^2 = 1$$

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

Registradores Quânticos

\mathcal{H}_{2^n} := espaço de Hilbert de dimensão $2^n := \bigotimes_{i=1}^n \mathcal{H}_2$

Registradores Quânticos

\mathcal{H}_{2^n} := espaço de Hilbert de dimensão $2^n := \bigotimes_{i=1}^n \mathcal{H}_2$

$B_{2^n} := \{ |x\rangle : x \in \{0, 1\}^n \}$ base ortonormal de \mathcal{H}_{2^n}

Registradores Quânticos

\mathcal{H}_{2^n} := espaço de Hilbert de dimensão $2^n := \bigotimes_{i=1}^n \mathcal{H}_2$

$B_{2^n} := \{ |x\rangle : x \in \{0, 1\}^n \}$ base ortonormal de \mathcal{H}_{2^n}

$|x\rangle$ com $x \in \{0, 1\}^n$: **estados básicos**

Registradores Quânticos

\mathcal{H}_{2^n} := espaço de Hilbert de dimensão $2^n := \bigotimes_{i=1}^n \mathcal{H}_2$

$B_{2^n} := \{|x\rangle : x \in \{0, 1\}^n\}$ base ortonormal de \mathcal{H}_{2^n}

$|x\rangle$ com $x \in \{0, 1\}^n$: **estados básicos**

registrador quântico $|\psi\rangle$ é um vetor unitário em \mathcal{H}_{2^n}

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

$$\alpha_x \in \mathbb{C} \text{ e } \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Registradores Quânticos

\mathcal{H}_{2^n} := espaço de Hilbert de dimensão $2^n := \bigotimes_{i=1}^n \mathcal{H}_2$

$B_{2^n} := \{|x\rangle : x \in \{0, 1\}^n\}$ base ortonormal de \mathcal{H}_{2^n}

$|x\rangle$ com $x \in \{0, 1\}^n$: **estados básicos**

registrador quântico $|\psi\rangle$ é um vetor unitário em \mathcal{H}_{2^n}

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

$$\alpha_x \in \mathbb{C} \text{ e } \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

$|\psi\rangle$ é **superposição** de 2^n estados básicos

Exemplo

registrador $|\psi\rangle$ com 3 bits quânticos

$$|\psi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \frac{1}{\sqrt{8}}|010\rangle + \frac{1}{\sqrt{8}}|011\rangle + \frac{1}{\sqrt{8}}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|110\rangle + \frac{1}{\sqrt{8}}|111\rangle$$

Transformações

$U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$ transformação linear

U é **unitária** se $U^*U = UU^* = I$

Transformações

$U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$ transformação linear

U é **unitária** se $U^*U = UU^* = I$

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \xrightarrow{U} \sum_{x \in \{0,1\}^n} \alpha_x (U|x\rangle)$$

Transformações

$U : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n}$ transformação linear

U é **unitária** se $U^*U = UU^* = I$

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \xrightarrow{U} \sum_{x \in \{0,1\}^n} \alpha_x (U|x\rangle)$$

aplicação **simultânea** em 2^n estados básicos
(**paralelismo quântico**)

Medições

registrador $|\psi\rangle$ com n bits quânticos

$$|\psi\rangle := \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Medições

registrador $|\psi\rangle$ com n bits quânticos

$$|\psi\rangle := \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

obtemos um **único estado básico**:

dado um estado básico $|x\rangle$,

obtemos $|x\rangle$ com **probabilidade** $|\alpha_x|^2$

Medições

registrador $|\psi\rangle$ com n bits quânticos

$$|\psi\rangle := \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

obtemos um **único estado básico**:

dado um estado básico $|x\rangle$,

obtemos $|x\rangle$ com **probabilidade** $|\alpha_x|^2$

após medição, $|\psi\rangle = |x\rangle$,

onde $|x\rangle$ é o estado básico “sorteado” como acima.

Tópicos

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

Primalidade e Fatoração

Problema da **primalidade**:

Dado: um inteiro $n > 1$

Descobrir: se n é primo ou composto

Primalidade e Fatoração

Problema da **primalidade**:

Dado: um inteiro $n > 1$

Descobrir: se n é primo ou composto

Algoritmo: AKS (2002)

Primalidade e Fatoração

Problema da **primalidade**:

Dado: um inteiro $n > 1$

Descobrir: se n é primo ou composto

Algoritmo: AKS (2002)

Problema da **fatoração**:

Dado: um inteiro n composto

Descobrir: um fator de n

Primalidade e Fatoração

Problema da **primalidade**:

Dado: um inteiro $n > 1$

Descobrir: se n é primo ou composto

Algoritmo: AKS (2002)

Problema da **fatoração**:

Dado: um inteiro n composto

Descobrir: um fator de n

Algoritmo: Shor (1994)

Algoritmo de Shor: especificação

Recebe:

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

Algoritmo de Shor: especificação

Recebe:

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

Devolve:

um fator de n , com **probabilidade $\geq 1/2$** .

Algoritmo de Shor: características

Idéia:

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

Algoritmo de Shor: características

Idéia:

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

Consumo de tempo:

polinomial em $\log n$.

Algoritmo de Shor: características

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. $x \leftarrow \text{rand}\{2, \dots, n - 1\}$
2. $d \leftarrow \text{mdc}(x, n)$
3. se $d > 1$ ▷ único passo quântico
4. então devolva d
5. $r \leftarrow \text{ordem}(x, n)$ ▷ 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 $\text{mdc}(x^{r/2} - 1, n)$

Algoritmo de Shor: corretude

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 $\text{mdc}(x^{r/2} - 1, n)$ **é fator** de n

Algoritmo de Shor: corretude

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 $\text{mdc}(x^{r/2} - 1, n)$ **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: falha

Teorema:

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

Algoritmo de Shor: falha

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.

Álgebra

Álgebra (Teoria dos Grupos):

$r :=$ ordem de x , módulo n .

r é o período da seqüência

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

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**

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

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

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

Tópicos

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

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico		
modelo quântico		

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	
modelo quântico		

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	
modelo quântico	EQP	

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Espaço polinomial, modelo clássico: **PSPACE**

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Espaço polinomial, modelo clássico: **PSPACE**

Pode-se provar:

$$P \subseteq EQP$$

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Espaço polinomial, modelo clássico: **PSPACE**

Pode-se provar:

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

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Espaço polinomial, modelo clássico: **PSPACE**

Pode-se provar:

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

Classes de Complexidade

Tempo polinomial:

	resposta sempre certa	probabilidade de erro limitada
modelo clássico	P	BPP
modelo quântico	EQP	BQP

Espaço polinomial, modelo clássico: **PSPACE**

Pode-se provar:

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

Fim

Sítio: <http://www.ime.usp.br/~magal/quantum/>

Carlos: carlos.cardonha@gmail.com

Marcel: marcel.csilva@gmail.com

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