Computação Quântica: Complexidade e Algoritmos

Carlos H. Cardonha, Marcel K. de Carli Silva e Cristina G. Fernandes (orientadora)

Instituto de Matemática e Estatística – Universidade de São Paulo

O que é um computador quântico?

Um computador quântico explora os efeitos da mecânica quântica para acelerar seus cálculos, diferente dos computadores atuais, cujo funcionamento é totalmente governado pelas leis da física clássica.

O modelo quântico de computação foi inicialmente idealizado por Feynman para simular eficientemente sistemas quânticos de partículas, nos anos 80. Mas foi apenas em 1994, quando Shor descobriu um algoritmo quântico eficiente para fatoração de inteiros, que a teoria da computação quântica recebeu um forte impulso e uma enorme divulgação.

Acredita-se que não existe um algoritmo eficiente para fatorar inteiros no modelo clássico de computação. O sistema de criptografia de chave pública mais utilizado atualmente, o RSA, baseia-se justamente na dificuldade de se fatorar inteiros grandes. Assim, o algoritmo quântico de fatoração combina tanto relevância teórica quanto prática. Além disso, fornece evidências de que o modelo quântico de computação pode ser mais poderoso que o modelo clássico.

Naturalmente, o poder computacional do modelo quântico é objeto de estudo da teoria da complexidade computacional. Apesar da suposta superioridade deste modelo, há evidências de que computadores quânticos não podem resolver eficientemente problemas **NP**-completos. A busca continua, porém, por algoritmos quânticos eficientes para outros problemas difíceis.

A grande dificuldade atualmente é, entretanto, tecnológica: não se sabe se é viável a construção de um computador quântico capaz de lidar com números suficientemente grandes. Já se tem notícia de computadores construídos segundo o modelo quântico, mas todos de pequeno porte. Em 2001, por exemplo, foi construído um computador quântico com 7 *qubits* (o correspondente aos bits dos computadores tradicionais). O algoritmo de fatoração de Shor foi executado neste computador para fatorar o número 15.

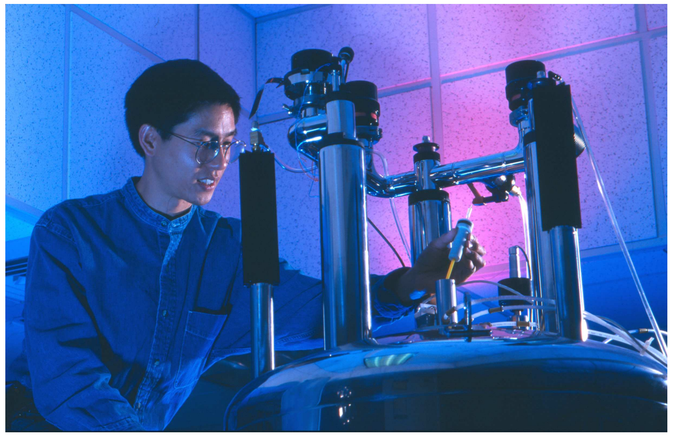

Figura 1: Dr. Isaac Chuang, da IBM, e um computador quântico com 7 qubits, construído com a tecnologia NMR (Nuclear Magnetic Resonance), que fatorou o número 15 utilizando o algoritmo de Shor.

O modelo quântico de computação

- Um bit armazena um valor bem definido: ou 0 ou 1. Já um qubit (bit quântico) armazena uma superposição de 0 e 1. Um qubit é escrito como $\alpha_0|0\rangle + \alpha_1|1\rangle$, onde $\alpha_0, \alpha_1 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 = 1$.
- Um registrador com n bits armazena um valor bem definido entre 0 e $2^n - 1$. Já um registrador com n qubits armazena uma superposição de todos os valores entre 0 e $2^n - 1$.
- Uma porta lógica sobre um registrador com n bits é uma função sobre o conjunto $\{0, \ldots, 2^n - 1\}$. Já uma porta quântica sobre um registrador com n qubits é uma função bijetora sobre o conjunto de superposições de valores entre 0 e $2^n - 1$.
- Ler o valor armazenado num registrador (digamos, durante a depuração de um programa) em nada altera este valor. Já a leitura de um registrador quântico que esteja numa superposição tem, como resultado probabilístico, um único valor contido na superposição; imediatamente, a superposição que existia antes é irreversivelmente alterada (e perdida). Em resumo, apesar de existir uma superposição, não se consegue enxergá-la, e o valor que conseguimos ler é sorteado.
- A aplicação de uma porta quântica a um registrador de n qubits age simultaneamente sobre todos os valores da superposição em que se encontra o registrador. Esse fenômeno é o paralelismo quântico.
- Com o paralelismo quântico, podemos obter o valor de uma função para 2^n elementos de seu domínio através de uma única aplicação de uma porta quântica que a calcule. Utilizando uma manipulação inteligente das superposições, podemos extrair propriedades globais de tal função com mais facilidade que no modelo clássico. Por exemplo, é mais fácil encontrar o período de uma função no modelo quântico.

O algoritmo de fatoração de Shor

- recebe como entrada um inteiro n composto, ímpar, e que não seja potência de um primo. Isso não é problema, pois existe um algoritmo eficiente que decide se um inteiro é potência de outro.
- devolve um fator de n com alta probabilidade (limitada inferiormente por uma constante).
- consome tempo polinomial em $\lg n$.
- o algoritmo tem um único passo quântico.
- reduz o problema de encontrar um fator de n para o de encontrar o período de uma função:

Algoritmo Shor (n)
1 escolha um inteiro $1 < x < n$ aleatoriamente
2 se $\text{mdc}(x, n) > 1$
3 então devolva $\text{mdc}(x, n)$
4 seja r o período da função $f(a) = x^a \bmod n$ ▷ passo quântico
5 se r for ímpar ou $x^{r/2} \equiv -1 \pmod{n}$
6 então o procedimento falhou
7 devolva $\text{mdc}(x^{r/2} + 1, n)$

- É fácil provar que, se o algoritmo devolve um valor, este é um fator de n.
- Não é tão fácil provar que a probabilidade de falha é $\leq 1/2$: precisa-se fazer um uso não ingênuo do Teorema Chinês do Resto e do Teorema dos Grupos Cíclicos, resultados poderosos da Álgebra.
- Também é fácil provar que r é o menor inteiro positivo tal que $x^r \equiv 1 \pmod{n}$.
- O passo quântico, de busca do período, utiliza uma "versão quântica" da transformada discreta de Fourier, que trabalha com superposições. A transformada discreta de Fourier é a função $F : \mathbb{C}^n \to \mathbb{C}^n$, com $F : (a_0, \ldots, a_{n-1}) \mapsto (b_0, \ldots, b_{n-1})$, onde $b_k := \sum_{j=0}^{n-1} a_j \omega_n^{jk}$ e $\omega_n := \exp\{2\pi i/n\}$ é a n-ésima raiz complexa da unidade.

Complexidade Computacional no modelo quântico

- Assim como no modelo clássico, é preciso formalizar algoritmos como máquinas de Turing para avaliar o consumo de recursos valiosos, como tempo e espaço.
- É muito mais difícil a formalização de uma máquina de Turing quântica, devido aos cuidados com a superposição.
- Como as portas quânticas são funções bijetoras, todas as computações devem ser reversíveis, isto é, deve ser possível partir de uma resposta e chegar a uma entrada. Isso dificulta até mesmo a codificação de construções primitivas básicas, como condicionais e laços.
- Existe uma máquina de Turing quântica universal, que recebe como entrada a descrição de outra máquina de Turing quântica e uma entrada, e simula a execução desta máquina para esta entrada, com um atraso polinomial.
- A construção desta máquina universal, novamente, é consideravelmente mais difícil que no modelo clássico, pois envolve superposição de estados e decomposição eficiente de matrizes unitárias arbitrárias em matrizes unitárias simples, de suporte pequeno, denominadas matrizes quase-triviais.
- Existe uma série de resultados relacionando classes de complexidade quânticas e clássicas. Considere as seguintes classes de complexidade clássicas, cujos problemas são de decisão: **P** é a classe dos problemas resolvidos deterministicamente em tempo polinomial, **BPP** a dos problemas resolvidos por um algoritmo probabilístico com probabilidade de erro limitada por uma constante, **PSPACE** a dos problemas resolvidos deterministicamente em espaço polinomial. Agora considere as seguintes classes quânticas: **EQP** dos problemas resolvidos com resposta exata no modelo quântico e em tempo polinomial, e **BQP** dos problemas resolvidos no modelo quântico em tempo polinomial e com probabilidade de erro limitada por uma constante. Então é possível provar que $\mathbf{P} \subseteq \mathbf{EQP} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$.

Para saber mais

Preparamos um texto completo, com todo o conteúdo estudado. Ele pode ser encontrado no site

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

Os autores podem ser contactados através dos seguintes endereços de e-mail:

`cardonha@ime.usp.br`,
`magal@ime.usp.br`,
`cris@ime.usp.br`.

Este trabalho foi parcialmente financiado pela FAPESP, processos número 03/13236-0 e 03/13237-7.