Algoritmo de Shor para fatoração de inteiros

Eliseu Venites Filho[1], Sandra Denise Prado[2]

1 Autor, Engenharia Física, UFRGS – eliseuv@live.com
2 Orientadora, IF UFRGS

Por quê computação quântica?

Computação pode ser vista como processamento de informações, ou seja evolução física da informação, que por sua vez é sempre representada por graus de liberdade de um sistema físico. Um computador é um dispositivo físico, então eficiência, limitações de armazenamento e processamento são dependentes de leis físicas.

Atualmente, o modelo teórico de computação é a máquina de Turing, que captura todo o poder computacional da física clássica, mas como disse Feynman, a natureza não é clássica, então para melhor aproveitarmos o poder computacional de sistemas físicos, devemos trabalhar com uma diferente representação da realidade: a mecânica quântica. A mecânica quântica difere muito da mecânica clássica em processos que são permitidos por leis físicas, o que nos permite aproveitar de modos de computação inéditos. A computação quântica estuda e explora os efeitos quânticos para solucionar problemas de complexidade computacional, comunicação e criptografia.

Outro ponto é que a lei de Moore que tem funcionado bem desde 1965 prevê que os componentes vão atingir escala subatômica em 2015, nesse ponto a mecânica clássica falha completamente.

Fatoração de inteiros

Trataremos de um problema muito antigo e que tem maravilhado matemáticos de todas as épocas, a fatoração de números inteiros em primos, problema para o qual não se conhece nenhum algoritmo clássico eficiente.

Felizmente, em 1994, Peter Shor, trabalhando na Bell Labs, formulou um algoritmo que resolve o problema em tempo polinomial no número de digitos do número.

Além da importância intrínseca ao problema da fatoração, podemos ressaltar que o algoritmo de Shor representa um verdadeiro desafio a Tese forte de Church-Turing, pois é a primeira evidência de que computadores quânticos são inerentemente mais poderosos.

Também, algoritmos eficientes para fatoração podem ser utilizados para quebrar chaves do sistema RSA de criptografia.

Introdução aos qubits

Em computação quântica trabalhamos com o objeto matemático que chamamos de *qubit* (*quantum bit* em analogia ao bit clássico). Assim como sua versão clássica, o qubit pode assumir os valores $|0\rangle$ ou $|1\rangle$, mas além disso, também é possível uma combinação linear desses valores:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Nós podemos examinar o qubit para ver se ele está no estado $|0\rangle$ ou $|1\rangle$, mas não podemos determinar seu estado (valores de α e β). Para descobrir o valor do qubit fazemos medições, que retornam $|0\rangle$ com probabilidade $|\alpha|^2$ e $|1\rangle$ com probabilidade $|\beta|^2$. Como probabilidades sempre somam 1, o estado $|\psi\rangle$ é sempre normalizado.

Depois da medição, o qubit é dito colapsar para o estado medido, ou seja, todas as observações posteriores vão retornar o mesmo valor e ele pode ser tratado como um bit clássico.

Ideia do algoritmo

O algoritmo de Shor se baseia na ideia de reduzir o problema de fatoração ao problema de encontrar a ordem de um inteiro em relação a outro. A ordem de um inteiro x < N em relação a N é o menor inteiro r, tal que

$$x^r = 1 (mod N)$$

Esse problema também não pode ser resolvido eficientemente por um computador clássico, mas é o período da função

$$f(k) = x^k (mod N)$$

então utilizando a sub-rotina do cálculo quântico de período, podemos solucioná-lo.

Referências

NIELSEN, M. A.; CHUANG, I. L. *Quantum computation and quantum information.* Cambridge University Press

SHOR, P. W.; *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20--22, 1994