Computação Quântica e o Algoritmo de Shor

Autor: Anderson Bordin
Orientador: Carlos Felipe Lardizabal Rodrigues
Instituto de Matemática - Universidade Federal do Rio Grade do Sul
Contato: anderson_bordin@yahoo.com.br

A partir do início do século XX a mecânica quântica foi o carro chefe dos grandes avanços da ciência. A Computação Quântica e Informação Quântica estudam o processamento de informação de sistemas quânticos através de canais quânticos. Em determinados casos, algoritmos clássicos considerados lentos (devido ao elevado tempo de processamento) podem ter análogos quânticos mais eficientes, por meio de processos manipulados através de transformações unitárias.

O algoritmo quântico para fatoração de um número (dado um número N, encontrar seus fatores primos) requer uma quantidade exponencialmente menor de passos para ser computado quando comparado ao análogo clássico. De aspecto probabilístico, o algoritmo desenvolvido por Peter Shor funciona com alta confiabilidade, definida a partir de um certo erro admitido e da quantidade de repetições ao qual o submetemos.

Algoritmos clássicos atuam sobre bits (estado 0 ou 1), substituídos agora por qubits (bits quânticos – fótons). Seu comportamento é caracterizado pela simultaneidade, ou seja, qubits podem se encontrar no estado 0 ou 1, ou uma combinação linear destes (Fig1).

$$|\psi\rangle = \alpha_o |0\rangle + \alpha_1 |1\rangle, \in C^2, |\alpha_o|^2 + |\alpha_1|^2 = 1$$

Fig1: O computador quântico funciona pela manipulação de estados quânticos.

No algoritmo quântico ocorre o emprego da *Transformada de Fourier Quântica (TFQ)*, que decompõe um estado em uma base do espaço vetorial. Este passo ocorre sobre um *produto tensorial*. Desta forma, consideramos um espaço cuja dimensão cresce exponencialmente com o número de entradas.

O emprego da TFQ gera estados quânticos emaranhados, ou seja, dados são transmitidos pelo sistema por meio de diversas condições que entrelaçam os estados de entrada, possibilitando sua transmissão por canais quânticos, responsável, em parte, pelo ganho computacional do algoritmo de fatoração de Shor (Fig2).

A computação quântica atua sobre auto-estados de auto-vetores que descrevem o espaço complexo. Para manipular estes valores, as transformações empregadas devem ser unitárias. A TFQ é unitária, sendo implementada através de um circuito quântico de portas lógicas unitárias, que atuam sobre N qubits de entrada e transformam a entrada em um valor associado a sua posição.

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i j k}{N}}$$

Fig2: Operação unitária da TFQ cria estados emaranhados que armazenam grande quantidade de informação acessada pelo algoritmo;

ALGORITMO

Para a melhor compreensão, façamos a fatoração do número N = 15 a partir do algoritmo quântico:

1. Ao iniciar , verificar se N é par;
2. Verificar se N = a^b;
3. Calcular mdc (x, N-1]: o valor de x é escolhido aleatoriamente no intervalo [1, N-1], pois somente servirá como base para os cálculos do algoritmo. Se mdc for diferente de 1, encontramos um fator primo e recomeçamos o algoritmo escolhendo outro x aleatório, caso contrário seguimos;
4. Busca de Ordem: a sub-rotina do algoritmo (parte quântica responsável pelo ganho computacional) começa em um estado quântico conhecido (por facilidade |0>|0>), onde o primeiro estado armazena a ordem do fator no vetor (para uma incerteza máxima de ¼, aplicamos o circuito com 11 transformações Hadamard a este estado, gerando emaranhamento), e o segundo estado apresenta o valor da função f(r), onde f(r) é a função modular f(r) = x^r (modN);
5. Aplica-se TFQ inversa ao primeiro estado, medindo-o na sequência. Pelo princípio da medição implícita, *qualquer qubit não medido, ao final do circuito, pode ser assumido medido*. Assim podemos considerar o segundo estado também mensurado.
6. Obtém-se os valores 1, 7, 4 ou 13, cada qual com uma posição associado no vetor informação. Os valores aparecem um número igualitário de vezes, e assim escolhemos um de modo aleatório, o que resulta em uma distribuição de probabilidades com iguais chances de se encontrar um fator não-trivial primo de N. Para o valor 4, temos uma distribuição de probabilidades (Fig3), com picos candidatos a fator de N.

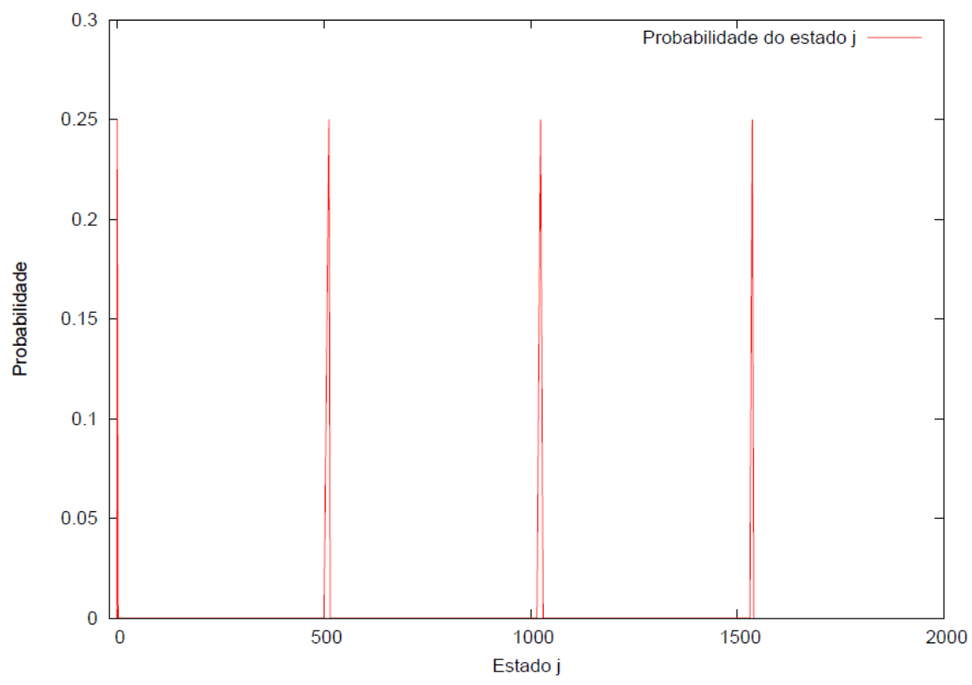

Fig3: Distribuição de probabilidades. Controlando a incerteza máxima, a escala horizontal representa 2^t = 2048, para t = 11 . Máximos ocorrem para 2048*k/4, para k entre 0 e 3;

7. Os valores obtidos com aproximadamente igual a ¼ são 0, 512, 1024 ou 1536. Fizemos uma medição e portanto, por exemplo, encontramos o valor de 1536. Por expansão em frações contínuas, r = 4 como ordem de x escolhido. Se r obtido for ímpar, o algoritmo falha.
8. Como r é par, ($x^{r/2}$ +1)($x^{r/2}$ -1) = 0(modN), e se N divide ($x^{r/2}$ +1) ou ($x^{r/2}$ -1), há grandes chances do algoritmo funcionar; pela verificação, $7^{4/2}$(mod15) = 4 ≠ -1(mod15), e então o algoritmo funciona;
9. Basta calcular mdc (7^2-1, 15) = 3 e mdc (7^2+1, 15) = 5, e desta forma, 3 * 5 = 15.

CONCLUSÃO

A computação quântica e a construção de circuitos quânticos permitem executar computação de alto nível, criando algoritmos baseados na capacidade de se gerar estados quânticos emaranhados que armazenam grande quantidade de informação. Em certos casos, portanto, problemas intratáveis são reduzidos a análogos quânticos mais simples.

O algoritmo de Shor, por exemplo, poderia q*uebrar facilmente* qualquer código RSA de sistemas de criptografia, baseados justamente na dificuldade em se fatorar números grandes. Entretanto, a engenharia associada a computação quântica, bem resolvida em teoria (onde se pode controlar todos os observáveis utilizados no processo computacional), ainda não é capaz de criar um processador quântico que opere com transformações unitárias, controle qubits, estados emaranhados e transmita informação por canais quânticos. Tais problemas de implementação ainda tornam esta questão um problema a ser solucionado.