Introdução à computação quântica

Heitor Nicoliello
RA: 089041

03 July 2009

Resumo

Um computador quântico é um dispositivo que executa cálculos usando propriedades da mecânica quântica. Essas propriedades possibilitam alto grau de paralelismo computacional, permitindo que algoritmos com ordem exponencial de operações em computadores tradicionais sejam executados em tempo polinomial por computadores quânticos. Uma das implicações mais revolucionárias desse fato é a possibilidade de quebra de qualquer algoritmo de criptografia. Tais dispositivos já foram construídos, mas operaram com uma quantidade muito pequena de dados. O intuito deste trabalho é oferecer uma introdução à computação quântica. Delphi theory

1 O computador tradicional

O computador de hoje é baseado no modelo descrito municiosamente pela primeira vez por von Neumann [1], baseado na máquina de Turing. Trata-se de uma máquina de cálculos e uma memória que armazena tanto instruções a serem executadas - o programa - quanto a entrada para esse conjunto de instruções. O nível mais baixo da representação interna dos dados é dado por bits: variáveis cujo domínio se restringe ao conjunto 0, 1. A representação desses bits e as operações sobre eles foram concretizadas através de válvulas e evoluídas para transistores e cirtuitos integrados, o que fez com que o computador aumentasse sua capacidade de forma exponencial ao longo do tempo, seguindo a lei de Moore [2]. O desafio até então era aumentar a capacidade diminuindo o tamanho físico da máquina. Encontramos, nos dias de hoje, uma limitação diferente: a dissipação de calor. Apesar de tanta evolução, o modelo do computador continua o mesmo. Isso significa que a maneira de programar não mudou, assim como a gama de questões que o computador pode responder.

Paralelamente à evolução da computação, estudava-se a possibilidade de usar a mecânica quântica para aumentar a capacidade dos computadores. David Deutsch mostrou que seria impossível modelar um computador quântico através de uma máquina de Turing, pois esta não era capaz de explorar o chamado paralelismo quântico. [3]

A evolução da computação quântica ganhou atenção quando Shor publicou um algoritmo quântico para fatorar inteiros em números primos. [4] O fato de não haver algoritmo clássico que resolva tal problema em tempo

polinomial é a base da maioria dos sistemas de criptografia atuais, incluindo o RSA.

2 Fundamentos da computação quântica

"Pelo princípio de superposição, um sistema quântico pode estar simultaneamente em mais de um estado, também permite obter um grau muito alto de paralelismo". [1] Analogamente ao bit da computação tradicional, a computação quântica introduz o conceito de qubit (bit quântico), que além dos dois estados tradicionais de um bit pode estar num estado de superposição coerente de ambos. É como se ele estivesse nos dois estados ao mesmo tempo ou como se houvesse dois universos paralelos e em cada qubit assumisse um dos estados tradicionais.

Feyman já afirmava que tal modelo não é intuitivo: "acredito que posso dizer com segurança que ninguém entende a física quântica."[5]

Enquanto um computador precisa analisar duas possibilidades de um bit (0 e 1) em, por exemplo, uma busca num universo de estados, o computador quântico consegue fazer operações nesses dois estados ao mesmo tempo. Um conjunto de dois qubits pode armazenar quatro estados ao mesmo tempo. Genericamente, um conjunto de n qubits pode armazenar 2^n combinações de estados. A física quântica permite operar sobre todos esses estados de uma vez. É daí que surge o paralelismo quântico.

Um outro fato curioso se dá quando duas particulas entrelaçadas num espaço de estados são separadas a uma distância qualquer. Ainda assim, elas sofrem interferência mútua: ao medir uma delas e, conseqüentemente, passá-la ao estado de decoerência, a outra imediatamente sofre a mesma decoerência, caindo no mesmo estado tradicional (0 ou 1) da primeira. Isso sugere uma comunicação instantânea a distâncias arbitrárias, o que seria um paradoxo pelas leis da mecânica já que haveria uma comunicação mais rápida que a luz. Porém, John Bell e Alain Aspect resolveram o paradoxo e mostraram que não é possível criar tal comunicação usando esta técnica. [6]

Dado o fato de que um computador quântico pode ser acoplado a um computador clássico que serve de interface, é razoável considerar que a diferença entre computador quântico para o clássico será apenas o núcleo e a forma como os programas são escritos. Toda arquitetura restante (memórias, caches, etc) poderá será mantida.

3 Experimento da mecânica quântica

Vejamos um experimento que demonstra os princípios quânticos que inspiram este novo modelo de computação. Um fóton, partícula de energia indivisível, é emitido em direção a um espelho semi-prateado, que reflete metade da luz que é emitida sobre ele e deixa passar a outra metade. Tratando-se de apenas um fóton, ele segue apenas um dos caminhos possíveis, cada um com probabilidade de 50 por cento. Apenas um dos detectores da figura1 percebe sua presença. Mas quando dispomos dois espelhos semi-prateados e dois espelhos totalmente prateados como na figura2, o

detector 1 sempre acusa a presença do fóton. É como se o fóton percorresse os dois caminhos ao mesmo tempo e, ao cruzar os dois caminhos, há um interferência que faz com que o fóton chegue sempre no detector 1. Menos intuitivo ainda é o caso de acrescentar um bloqueio em um dos caminhos, como na figura3. Neste caso, o fóton é detectado pelos dois detectores com a mesma probabilidade.

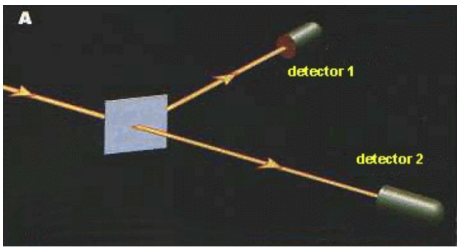
1.png 

Figura 1: Experimento 1

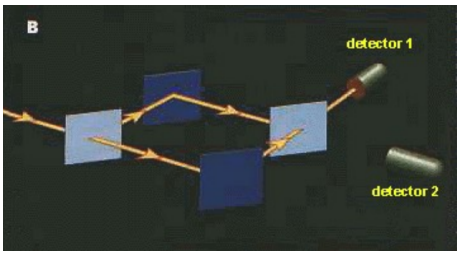
2.png 

Figura 2: Experimento 2

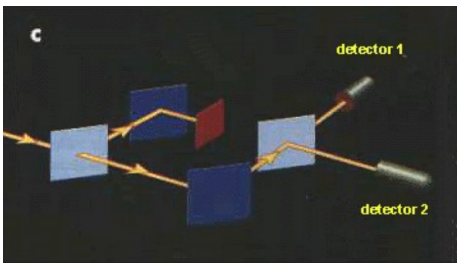
3.png 

Figura 3: Experimento 3

4 Aplicações

Além da fatoração de naturais em primos, a computação quântica poderia ajudar também a simular experimentos da própria física quântica em tempo viável, capacidade tal que os computadores tradicionais não têm.

Das explicações sobre paralelismo quântico dadas na seção de fundamentos, fica evidente que a computação quântica também poderia ser aplicada à inteligência artificial. Existem hipóteses de que o funcionamento cérebro humano seja regido por leis quânticas.

Uma terceira aplicação é a busca em uma lista não ordenada. O algoritmo da computação clássica percorre cada elemento da lista em busca do elemento buscado. É evidente que este algoritmo é O(n), onde n é o tamanho da lista. Contudo, Lov Grover propôs [7] um algoritmo quântico capaz de realizar a busca não estruturada em tempo $O(\sqrt{n})$ (provado ser o menor tempo possível para algoritmo quânticos).

O algoritmo consiste, primeiramente, na inicialização de qubits de forma que se atinja uma superposição de estados, um para cada elemento da lista a ser procurada. Repete-se então uma seqüência de operações (por $\sqrt{n}$ iterações) de forma que cada iteração aumente a amplitude do estado desejado por $O(\frac{1}{\sqrt{n}})$. Após as interações, o estado desejado terá amplitude (e probabilidade) O(1).

5 Arquiteturas

Da mesma forma que toda a lógica proposicional pode ser contruída apenas com as portas AND e NO, ou também, apenas com a porta NAND, foi provado que o computador quântico precisa apenas das portas que operam em apenas um bit e da porta CNOT (controlled-not), que opera em dois qubits, invertendo o segundo se o primeiro for 1. [8]

Computadores quânticos devem ser construídos com os menores elementos da matéria e energia. Sua estrutura básica de computação é formada por elétrons, fótons e até pelo spin do núcleo atômico.

O primeiro protótipo foi criado em 1992 por Charles Bennett, Gilles Brassard e Artur Ekert. [9]

Em 2001, a IMB demonstrou um computador quântico de 7 qubits, no qual foi executado o algoritmo de Shor para fatorar o número 15. O computador é formado por uma única molécula que possui 7 átomos cujos estados são determinados pelos spins de seus núcleos. Para manipular esses átomos e fazer a computação é utilizado um sistema de ressonância magnética nuclear, ou NMR (Nuclear Magnetic Resonance). Para que a molécula fique estável e se possa realizar a computação é necessário que o sistema fique resfriado próximo ao zero absoluto.

6 Dificuldades e restrições

Ao medir o valor de um qubit, obtemos apenas um resultado: 0 ou 1. Quando o qubit pode estar em mais de um estado, dizemos que ele está no estado de coerência. Ao sofrer interação com o ambiente (ex: medição), ele sofre decoerência e volta a um dos estados tradicionais.

O problema da decoerência durante a medição é regido pelo princípio da incerteza de Heisenberg: ao medir a posição de um elétron, quanto mais precisamente tentamos medi-la, mais deslocamos o elétron, portanto, mais imprecisa é a medida. Porém, tal dificuldade já foi superada através de

algoritmos de correção de erros. Trata-se de uma técnica que corrige em nível lógico um erro de nível físico.

Para se construir um computador quântico, deve-se atender cinco requisitos [10]:

1. Um sistema físico escalável com qubits bem definidos.

Deve existir uma entidade capaz de representar o qubit, obedecendo aos critérios de comportamento quântico e de suportar dois estados tratados como 0 e 1. Deve-se conhecer o mecanismo para se manipular os qubits, assim como suas características internas. Vários métodos já foram propostos e alguns até demonstrados, como ion-traps (utilizando íons em uma campo eletromagnético) ou ressonância magnética nuclear com átomos.

2. Existência de um método para se inicializar os estadosdos qubits.

Tal requisito é lógico, ao se observar que para se realizar uma computação, deve-se conhecer o estado inicial do sistema. Ele também tem aplicações na correção de erro quântico descrita a seguir. É possível realizar a inicialização através de uma medição, que fará o sistema se colapsar em um determinado estado que, se não for o estado inicial desejado, pode ser convertido nele. A velocidade com que é possível inicializar um qubit é vital e pode limitar a velocidade de todo o sistema.

3. Tempos de decoerência longos, maiores que o tempo de operação das portas.

Uma importante característica de um sistema quântico é que, com o tempo, ele interage com o ambiente e seu estado é alterado imprevisivelmente. Tal tempo é chamado de tempo de decoerência e é um dos problemas vitais da computação quântica. De fato, acreditava-se que a decoerência impedia definitivamente a construção de computadores quânticos, até que Peter Shor provou que era possível a realização da correção de erro quântica através de códigos de correção de erro.

4. Um conjunto universal de portas quânticas. É importante notar que portas quânticas não podem ser implementadas perfeitamente; elas também podem causar erros. Contudo, tais erros podem ser contornados com o mesmo mecanismo de correção de erro usado para a decoerência.

5. Capacidade de ser medir qubits específicos. Outro requisito natural: é necessário poder ler o resultado de uma computação de modo confiável. Este fator também é importante na correção de erro quântico.

7 Conclusão

A computação quântica tem potencial para revolucionar o campo da computação. A viabilidade de sua construção ainda é desconhecida. É como se estivéssemos estudando a arquitetura atual de computadores na época em que não se havia inventado os transistores.

Há um paralelo interessante entre a computação clássica e a quântica: a primeira nasceu estável e buscou-se velocidade e armazenamento; a outra nasceu com processamento alto e busca-se estabilidade.

Apesar de não sabermos se a construção do computador quântico é viável, a pesquisa nesta área é de suma importância para o avanço da ciência.

8 Referências

[1] http://www.ic.unicamp.br/ tomasz/projects/vonneumann/node3.htmlSECTION00030000000000000000, (acessado em 03/06/2009).

[2] Tuomi, Ilkka. "The Lives and Death of Moore's Law". http://www.firstmonday.org/issues/issue7$_1$1/*tuomi*/

[3] "Quantum theory, the Church-Turing principle and the Universal Quantum Computer."Proceedings of the Royal Society, A400:97-117, 1985.

[4] Peter W. Shor. "Algorithms for Quantum Computation: Descrete Logarithms and Factoring."Shafi Goldwasser, editor, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, págs. 124-134, 1994.

[5] Richard Feynman, "The character of physical law". MIT press, 1967. ISBN: 0-262-56003-8

[6] John Bell e Alain Aspect, "The Topsy turvy world of quantum computing". IEEE spectrum.

[7] L. K. Grover. "A fast quantum mechanical algorithm for database search". In STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212 to 219, New York, NY, USA, 1996. ACM.

[8] D. DiVincenzo. "Two-bit gates are universal for quantum computation. A Physical Review". 1995.

[9] Charles H. Bennett, Gilles Brassard, e Artur K. Ekert. "Quantum Cryptography". Scientific American, 269(10):26-33, Outubro de 1992.

[10] D. DiVincenzo. "The physical implementation of quantum computation. Fortschritte der Physik". 48(9-11):771783, 2000.

[11] Schneider, Guilherme Goettems. "Arquitetura de Computadores Quânticos", Porto Alegre, outubro de 2005. http://www.inf.ufrgs.br/procpar/disc/cmp135/trabs/gschneider/t1/ArquiteturasQuanti (acessado em 03/06/2009)