Computação Quântica: Estado da Arte

Bruno Leonardo Martins de Melo, Túlio Vinícius Duarte Christofoletti

Bacharelado em Ciências da Computação, 6ª fase, 2003
INE - Departamento de Informática e Estatística
Universidade Federal de Santa Catarina (UFSC), Brasil, 88040-900
brunomm@inf.ufsc.br, tulio@inf.ufsc.br

Resumo

Este artigo apresenta o estado da arte da Computação Quântica, consistindo em uma breve introdução, o que é, sua história e origem, quem são os principais pesquisadores no âmbito mundial, as dificuldades no uso deste tipo de tecnologia e suas principais aplicações.
Palavras-chave: Computação Quântica, qubit, spin

Abstract

This article presents the state of the art of the Quantum Computation, consisting of one brief introduction, what it is, its history and origin, who are the main researchers in the world-wide scope, the difficulties in the use of this type of technology and its main applications.
Key-words: Quantun Computation, qubit, spin

Introdução

O presente artigo tem por objetivo despertar o interesse dos alunos sobre a Computação Quântica.

A nossa proposta é dar uma visão geral e bastante ampla desta área de estudo tão nova da computação. Foge do nosso escopo a abordagem de conceitos profundos da mecânica quântica nos quais se baseia a computação quântica. Uma vez que este artigo vai ser divulgado no âmbito acadêmico, tais conceitos serão abstraídos. Tomaremos por base os mais recentes estudos sobre o tema reconhecidos internacionalmente.

O que é Computação Quântica

A computação quântica é uma proposta para realizar o processo da computação usando álgebra quântica. A mecânica quântica — a teoria que governa os fenômenos físicos no mundo microscópico, onde átomos e moléculas simples existem numa escala de ângstrons (0,1 trilionésimo de metro) — é fundamental nesse processo.

O computador clássico opera com uma seqüência de zeros e uns, de modo que qualquer ação computacional pode ser traduzida em última instância por uma seqüência desses algarismos. E esses zeros e uns, são na verdade estados lógicos

Um computador quântico opera basicamente baseado nas regras de incerteza do quantum. Sempre que se chega ao nível das partículas individuais, nada é absoluto (um elétron pode girar de uma maneira ou de outra, mas pode também existir como uma mistura de spins). Num certo sentido o elétron seria indeciso, com isso cada bit de informação quântica poderia ser incerto. Em vez de *um-ou-outro*, como na lógica digital, um qubit quântico poderia ser *ambos-e*, ou seja, representar 0 e 1 ao mesmo tempo. Esses qubits poderiam existir simultaneamente como uma combinação de todos os números de dois bits possíveis quando se têm dois qubits. Adicionando um terceiro qubit, pode-se ter a combinação de todos os números de três bits possíveis. Esse sistema cresce exponencialmente.

Com isso, uma coleção de qubits poderia representar uma fileira de números ao mesmo tempo, e um computador quântico poderia processar toda uma entrada de dados simultaneamente.

História

Em 1959 o cientista norte americano Richard Feynman propõe a nanotecnologia. Em 1981, começa a propagar a idéia da computação

matemática. Feyman ganhou o prêmio Nobel de física em 1995.

O interesse pela computação quântica teve início quando Feynman concluiu, em 1982, que os sistemas clássicos não seriam capazes de modelar eficientemente os sistemas mecânicos quânticos e que estes só poderiam ser modelados utilizando outro sistema quântico. Feynman sugeriu que computadores baseados nas leis da mecânica quântica ao invés das leis da física clássica poderiam ser usados para modelar sistemas mecânicos quânticos.

Deutsch foi o primeiro a levantar o questionamento de uma real maior capacidade de processamento dos computadores quânticos em relação aos clássicos em 1985. Com esta questão, ele estendeu a teoria da computação e ainda mais com o desenvolvimento do computador quântico universal e a máquina quântica de Turing (Deutsch, 1985). Foi ele também o primeiro a publicar um algoritmo quântico, o Problema de Dois Bits de Deutsch em 1989 (Deutsch 1989). Este algoritmo poderia responder se uma função é balanceada ou constante.

Até 1990, computação quântica era apenas uma curiosidade. Isto só mudou quando, em 1994, Shor publicou o seu algoritmo para computadores quânticos que resolve o problema de fatoração de números grandes (Shor, 1994). Com este algoritmo, um número seria fatorado muito mais rapidamente do que com máquinas clássicas e por isso ficou conhecido como "killer application".

A fatoração de números grandes é a base de alguns sistemas de criptografia como RSA (em homenagem a Ronald Rivest, Adi Shamir e Leonard Adelman, os primeiros a propor o método em 1978). Deste modo, o algoritmo de Shor passou a despertar interesse em vários setores da comunidade científica. A partir desse interesse, surgiram outros algoritmos quânticos, tais como o algoritmo para logaritmos discretos de Shor, outro de fatoração de Jozsa (Jozsa, 1997) , entre outros.

Enquanto o número de algoritmos quânticos crescia, os esforços no sentido de produzir um hardware quântico também aumentavam. Técnicas como ressonância nuclear magnética (NMR) e armadilha de íons são usadas com sucesso no desenvolvimento de sistemas com 3 e 5 qubits.

Atualmente, a maioria das pesquisas envolvidas em computação quântica concentra-se no desenvolvimento do hardware. Nesta área, os pesquisadores estão principalmente focados em ressonância magnética.

Centros de Pesquisa

-IBM's Almaden Research Center: Em agosto de 2000, o físico Isaac Chuang e sua equipe do Centro de Pesquisa de Almaden da IBM anunciaram para o mundo o desenvolvimento do BigBlue. Trata-se de computador quântico de 5 qubits baseados na técnica de rotação do núcleo do átomo (spin up = 1 e spin down = 0) e medição através de ressonância magnética nucléica usada normalmente em hospitais e em laboratórios de química.

São cinco átomos de Fluoreno dentro de uma molécula especialmente projetada de forma que os spins do núcleo do fluoreno possam funcionar como qubits programados por radiofrequência.

Com esta molécula, a equipe de Chuang resolveu em um único passo um problema matemático para o qual computadores convencionais requereriam repetidos ciclos de execução. O problema, chamado "order-finding" consiste em achar o período de uma determinada função. Ë um problema matemático típico no qual se baseiam aplicações importantes como a criptografia.

Chuang diz que as primeiras aplicações da computação quântica seriam como co-processadores para funções específicas, tais como busca em uma base de dados e para a solução de difíceis problemas matemáticos.

-Open Qubit - Quantum Computing: Este projeto é desenvolvido por pessoas de todas as partes do mundo. Aqui é feito o compartilhamento de idéias e código sobre a Computação Quântica. O objetivo principal era de escrever um simulador de um computador quântico para demonstrar o algoritmo de fatoração de Shor e sua eficiência na Computação Quântica. Posteriormente, estender este código para uma API mais genérica que permitiria a implementação de qualquer outro algoritmo quântico.

-National Institute of Standards Technology: Em 1996, seus pesquisadores provaram que pode-se estar ao mesmo tempo em dois lugares separados do espaço (um estado físico da mecânica quântica, denominado superposição).

O experimento publicado no ano de 2000 melhora o trabalho realizado em 1996, no qual os pesquisadores isolaram um íon de Berilium (um átomo sem um de seus elétrons da camada mais externa) em uma armadilha eletromagnética e o

confinou o íon a uma pequena região do espaço menor que um milionésimo de centímetro, o que ocasiona a sua quase imobilidade.

O que a equipe do NIST fez, diferentemente do ano de 1996 foi separar os dois estados a uma distância de quase 10 átomos. Embora, pareça extremamente pequena para a nossa percepção esta distância é enorme quando tratamos de elétrons. Na verdade o que aconteceu foi que os pesquisadores do NIST cruzaram uma ponte entre a mecânica quântica e o mundo real - o que vemos em nossa vida cotidiana.

Dificuldades

Um dos grandes problemas para a construção de um computador quântico é conseguir um isolamento perfeito, pois qualquer alteração de campo magnético, choque de moléculas de ar, um fóton aleatório pode transformar os qubits de *ambos-e* para *um-ou-outro*.

Aplicações

O físico do MIT, Seth Lloyd, estava fatorando o algoritmo descoberto por Peter Shor do Laboratório de Pesquisa da AT&T – uma descoberta que foi direto ao coração da moderna criptografia. Na maioria dos esquemas atuais de criptografia, incluindo esquemas utilizados para enviar números de cartão de crédito e outras informações sensíveis pela Internet, um bisbilhoteiro pode decifrar o código de uma determinada mensagem simplesmente fatorando um número muito grande. Agora, a fatoração de números pequenos é trivial – crianças de escola primária aprendem que 12 = 2 x 2 x 3. Mas fatorar números grandes é um dos problemas mais difíceis na ciência da computação. Não importa quão inteligente seja o algoritmo, na realidade o tempo exigido para fatorar números cada vez maiores cresce exponencialmente. Vá além de algumas centenas de dígitos e mesmo a capacidade das máquinas mais modernas no mundo será superada. O tempo de fatoração excederá o tempo de existência do universo.

Ou melhor, isso aconteceria com um computador convencional. Shor provou que um computador quântico poderia fatorar números grandes num prazo que aumenta somente algumas potências do tamanho do número – crescimento rápido, certamente, mas nem remotamente tão verdade, um computador convencional precisaria rodar por bilhões de anos para fatorar um número de 400 dígitos. Uma máquina quântica poderia fazer o serviço em cerca de um ano. A implicação era que códigos "indecifráveis" poderiam ser agora decifrados. e com este anúncio a Agência de Segurança Nacional, o Pentágono, a comunidade de criptografia e toda a comunidade de computação acordaram para o fato de que a computação quântica não era mais um domínio exclusivo dos teóricos. Peter Shor estava mostrando a possibilidade de uma aplicação real e importante.

Além disso, o giro nuclear dentro de uma determinada molécula tende a interagir muito bem. Se tomarmos como exemplo o clorofórmio, uma molécula consistente de um átomo de carbono ligado a três átomos de cloro e um átomo de hidrogênio. Quando o núcleo de hidrogênio e o núcleo do carbono estão girando da mesma forma, seus níveis de energia serão diferentes de quando eles estão girando em direções opostas.

A tecnologia para manipular estes giros nucleares já está muito madura. Ela é chamada de ressonância magnética nuclear, ou RMN, e é rotineiramente utilizada em análise química e aparelhos de imagem de ressonância magnética hospitalar. É uma simples questão de adaptar espectrômetros RMN comerciais para executar a computação quântica.

Nada disso significa que estaremos trocando nosso micro por laptops quânticos em pouco tempo. a computação quântica está quase no estágio de prova do princípio, com um longo caminho até que seja desenvolvido mesmo o equivalente qubit de máquinas a válvulas da época da II Guerra Mundial como o Eniac. Muito mais provável é que acessórios quânticos a máquinas convencionais – "co-processadores" – realizarão tarefas específicas, da mesma forma que uma placa gráfica realiza as tarefas mais difíceis.

O que exatamente serão estas tarefas, entretanto, é uma questão ainda não-resolvida. O físico do MIT Edward Farhi salienta que o estudo de algoritmos quânticos ainda está em sua infância. Os dois melhores descobertos até agora – o de Shor e o de Grover – serão sem dúvida seguidos por muitos mais, abrindo aplicativos que vão muito além de fatoração e busca. No entanto, diz Farhi, "um computador quântico não é necessariamente rápido, é um dispositivo que ataca problemas de uma maneira diferente. ainda estamos tentando entender o que torna um problema passível daquele tipo de abordagem. Você tem de escolher seu problema com cuidado para aproveitar a mágica

Na prática, acrescenta Farhi, a maneira como co-processadores quânticos serão usados dependerá muito de seu custo. e esta é uma questão complicada. No laboratório Almaden da IBM, por exemplo, o núcleo do computador quântico de Chuang é pequeno e barato: moléculas contendo qubits dissolvidas em algumas gotas de solvente incolor dentro de um tubo de vidro menor que seu dedo mínimo. Mas o espectrômetro MNR que faz funcionar o computador é um cilindro prateado de 30 metros de altura rodeado por grandes maços de fios e canos – a maior parte dos quais necessários para atender ao hélio líquido que resfria os magnetos supercondutores do espectrômetro. Se futuros co-processadores quânticos seguirem esse padrão, eles serão enormes monstros multimilionários que encherão salas inteiras, e que somente poderão ser comprados por governos. Neste caso, os computadores quânticos podem ser restritos a tarefas de segurança como criptografia e coleta de dados de inteligência.

Mas um dispositivo monstruoso como este pode não se inevitável. O grupo de Gershenfeld no Laboratório de Mídia do MIT está trabalhando num computador NMR compacto que funciona em temperatura ambiente. Eles esperam que esse dispositivo seja um protótipo de co-processador quântico que fornecerá energia a pequenos aparelhos baratos – periféricos instalados sobre a mesa como uma impressora ou scanner atual. Se isso provar ser o padrão, então poderemos ver uma nova geração de hackers quânticos trabalhando quase da mesma maneira como faziam seus antecessores no início da revolução do computador pessoal, criando uma profusão de software quântico inovador.

Conclusão

A cada dia surgem várias novidades na área da informática. Algumas perduram e são adotadas como padrão, outras desaparecem em função de vários fatores como não ser muito aceita no mercado ou não ser adequada para resolver os novos desafios que surgem.A computação quântica não é uma idéia tão recente no campo da física, e talvez não tenha muito futuro na área da informática. Mas só o tempo e o futuro podem nos dar alguma certeza, de qualquer forma a possibilidade de um processamento paralelo eficiente.

Agradecimentos

Agradecemos ao professor Jorge Muniz Barreto por nos dar mais esta oportunidade de ampliar nossos horizontes numa área até agora pouco abordada pelo nosso curso.

Referências

[1] A. S. Garcia, "Queremos Saber – Física - UFSC", *www.fisica.ufc.br*, questão. 93

[2] Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer, Proceedings of the Royal Society of London, 1985, A 400, pp97-117

[3] Shor, Peter W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings, 35th Annual Symposium on Foundations of Computer Science (IEEE Press, November 1994)

[4] Jozsa, Richard. Quantum Algorithms and the Fourier Transform, Submitted to Proc. Roy. Soc. Lond. A for the Proceedings of the Santa Barbara Conference on Quantum Coherence and Decoherence

[5] The Stanford-Berkeley-MIT-IBM NMR Quantum Computation Project, in http://squint.stanford.edu/

[6] Open Qubit | Quantum Computing, in http://www.openqubit.org/

[7] Centre for Quantum Computation, in http://www.qubit.org/

[8] Quantum Information and Computation - Caltech-MIT-USC, in http://www.theory.caltech.edu/~quic/

[9] Quantum Information at Los Alamos National Laboratory,in http://p23.lanl.gov/Quantum/quantum.html

[10] Quantum Information at IBM Almaden, in http://www.almaden.ibm.com/st/projects/quantum/intro/