Disciplina: Arquitetura de Computadores

Professor: Humberto Antônio Ribas Moraes

Atividade 3: Computador Quântico.

Computador Quântico

Um Computador Quântico é uma máquina que executa seu processamento baseado nas propriedades quânticas da matéria, criando um novo e revolucionário modo de armazenar e tratar dados.

Algumas destas propriedades são tão fantásticas que só existem a nível microscópico, não é possível descrevê-las com exemplos práticos do mundo.

Localizar todos os fatores primos de um número grande pode ser uma tarefa muito difícil. Um computador quântico poderia resolver este problema muito rapidamente. Se um número tiver *n* bits (ou seja, se tiver o comprimento de *n* dígitos quando escrito em binário), então um computador quântico com um pouco mais de 2*n* qubits poderá encontrar os seus fatores. Também poderá solucionar um problema relacionado, chamado problema do *logaritmo discreto*. Esta capacidade poderia permitir a um computador quântico quebrar qualquer dos sistemas criptográficos atualmente em uso. A maior parte das cifras de chave pública mais populares poderiam ser quebradas com rapidez, incluindo formas da cifras RSA, ElGammal e Diffie-Helman. Estas cifras são utilizadas para proteger páginas web seguras, email encriptado e muitos outros tipos de dados. A quebra destes códigos poderia ter um impacto significativo. A única forma de tornar seguro um algoritmo com o RSA seria tornar o tamanho da chave maior do que o maior computador quântico que pudesse ser construído. Parece provável que possa sempre ser possível construir computadores clássicos com mais bits que o número de qubits no maior computador quântico, e se verificar que isto é verdade, então algoritmos como o RSA poderão permanecer seguros.

Se um computador quântico fosse baseado nos prótons e nêutrons de uma molécula, seria talvez demasiado pequeno para ser visível, mas poderia factorizar números inteiros com milhares de bits. Um computador clássico a correr algoritmos conhecidos também poderia factorizar estes números, mas para o conseguir fazer antes que o sol desaparecesse, teria de ser maior que universo conhecido. Seria algo inconveniente construí-lo.

A teoria do Computador Quântico dentro da ciência da computação existia desde a época de Albert Einstein (anos 50), mas somente nos anos 80 foram feitas as primeiras tentativas de se construir algo semelhante ao magnífico computador quântico.

É possível destacar que a ciência da computação já saiu da era Eletrônica e deu os primeiros passos na era Quântica, pois atualmente já existem alguns protótipos construídos de computadores com tais propriedades.

Alguns destes protótipos já estão em funcionamento dentro de centros de pesquisa em Universidades, mas nenhum deles provou ainda ser muito prático, pois necessitam de muita energia ou mesmo de refrigeração extrema (algo em torno de 200 graus celsius abaixo de zero.

O Uso das Propriedades Quânticas pela Ciência da Computação

O mundo quântico é um mundo estranho para os leigos, porém o mesmo já vem sendo explorado com êxito pela ciência da computação.

A principal propriedade quântica que está sendo estudada, sendo esta a base do computador quântico, é a chamada Propriedade da Sobreposição.

Esta propriedade não existe no mundo macroscópico (mundo visível a olho nu pelos humanos). Tal propriedade define que um elétron pode girar para a esquerda, girar para a direita ou então girar para os dois lados simultaneamente, gerando 3 estados possíveis e diferentes.

Uma analogia ao mundo real seria: é como se um copo de água tivesse a possibilidade de estar cheio, vazio ou então cheio e vazio ao mesmo tempo!

Dentro do escopo da ciência da computação, este fato define que através das propriedades dos elétrons, podemos criar um bit de 3 estados, ao invés do bit tradicional que tem 2 estados (0 ou 1).

Este bit mais poderoso, foi denominado pelos especialistas em ciência da computação como Bit Quântico (qubit).

Comparação Entre Bit e Qubit na Ciência da Computação

Confira abaixo uma pequena comparação entre as tecnologias dos computadores eletrônicos (atuais) e os computadores quânticos (do futuro).

Capacidade de Processamento

Levando em conta o processamento dentro da ciência da computação, o computador quântico é mais eficiente pois trabalha com uma quantidade mais densa de informações ao mesmo tempo.

Alguns problemas que um computador eletrônico levaria milhares de anos para resolver, um computador quântico seria capaz de resolver em alguns minutos.

O bit quântico é mais denso, pois ao contrário do bit eletrônico tradicional que armazena 2 tipos diferentes de estados, o bit quântico é capaz de armazenar 3 tipos:

Capacidade de Memória

Levando em conta a capacidade de armazenamento de dados na ciência da computação, um qubit pode armazenar muito mais dados em muito menos espaço.

Veja como apenas alguns qubits armazenam a mesma quantidade de informações que alguns bilhões de bits:

Tabela de Equivalência entre Qubits e Bits	
Qubits (Tecnologia Quântica)	**Bits (Tecnologia Eletrônica)**
1 qubit	2 bits
2 qubits	4 bits
3 qubits	8 bits
5 qubits	32 bits
10 qubits	1.024 bits = 1 Kilo Bit
20 qubts	1.048.576 bits = 1 Giga bit
30 qubits	1.073.741.824 bits = 1 Tera bit

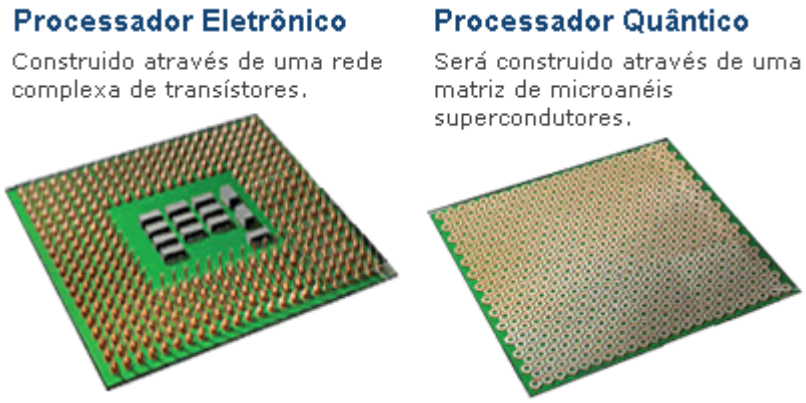
Tecnologia de Construção dos Processadores

O processador, de um modo resumido, é o núcleo do computador, sendo o componente que realiza todos os cálculos principais e operações da máquina.

Confira abaixo as tecnologias básicas para se construir um processador eletrônico e um processador quântico:

Processador Eletrônico: É o processador presente no computador pessoal, segue os conceitos da ciência da computação tradicional, trabalhando basicamente com sinais eletrônicos. É composto por 10 a 100 milhões de pequenos transistores, estes transistores são organizados de modo a formar estruturas complexas de processamento. Cada transistor é capaz de trabalhar com 1 bit por vez.

Processador Quântico: É o processador que será usado nos computadores quânticos, não segue os conceitos clássicos da ciência da computação, trabalhando de um modo totalmente inédito. É composto por alguns milhares de microanéis supercondutores. Cada anel funciona de modo independente um do outro, sendo capaz de processar vários qubits ao mesmo tempo.



Tudo indica que os computadores quânticos um dia irão substituir os computadores atuais. Outro fato em questão será que o primeiro computador quântico comercial tem a tendência de superar o computador eletrônico mais avançado em apenas 1 geração. Há relatos porém, que atualmente a tecnologia necessária para produzir um computador quântico eficiente ainda está além do alcance humano.

O melhor computador quântico que foi construído até hoje, custou uma fortuna, só funcionou por alguns segundos (demonstração) e trabalhou com apenas 16 qubits.

História do Desenvolvimento dos Computadores Quânticos na Ciência da Computação

Década de 50 – Primeiras teorias e especulações sobre a aplicação das leis da física quântica na construção de computadores.

1981 – O físico Richard Feyman, Nobel de Física de 1965, enquanto estava estudando física quântica, criou a primeira proposta para o uso das propriedades quânticas para processar programas de computador, criando a primeira idéia sobre um computador quântico. Suas idéias revolucionárias foram apresentadas em uma conferência de física no MIT, foi o início da aplicação das leis quânticas na ciência da computação.

1985 – O físico Israelense David Deustch, da Universidade Oxford, descreveu matematicamente o primeiro computador quântico universal (máquina de Turing Quântica). A ciência da computação tradicional é baseada na teoria da Máquina de Turing, que é o computador eletrônico universal, a computação quântica também poderia ter uma engenharia semelhante.

1994 – O professor de matemática aplicada Peter Shor, enquanto estava trabalhando na AT&T, criou o primeiro programa puramente quântico (não poderia ser rodado em computadores comuns, somente em quânticos). Esse programa, o Algoritmo de Shor, permitiria a um computador quântico fatorar grandes números em segundos. Para fazer estes mesmo cálculos, um computador eletrônico levaria meses!

1996 – O matemático Lov Grover, da Bell Labs, também desenvolve o seu programa quântico. Batizado de Speedup, este programa foi o primeiro algoritmo para pesquisa de bases de dados armazenadas em bits quânticos (qubits).

1999 – São desenvolvidos no **MIT** os primeiros protótipos de um computador quântico real.

2007 – A empresa Canadense **D-Wave** afirmou ter construído o primeiro processador quântico da história da humanidade, batizado de Orion. O Orion é um processador híbrido de 16 qubits que também poderia processar bits tradicionais. Embora tenha feito algumas demonstrações, a comunidade científica recebeu a notícia com muita desconfiança, pois a D-Wave nunca publicou em nenhuma revista ou jornal maiores detalhes sobre esta CPU. Os especialistas em física e ciência da computação afirmam, categoricamente, que só seria possível construir uma máquina assim no ano de 2030.

É interessante que as alunos que possuam interesse em Ciência da Computação tenham oportunidade de cursar uma universidade que garanta o aprimoramento de estudos, com palestras e seminários focados na área. Os livros auxiliam muito nos estudos, mas nada justifica a vivência na prática.

http://www.guiadacarreira.com.br/artigos/ciencia/computador-quantico-ciencia-computacao/

http://pt.wikipedia.org/wiki/Computador_qu%C3%A2ntico