UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA

PPGC – PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

CMP 135
Arquiteturas Especiais de Computadores
Prof. Philipe Navaux

Computação Quântica

Francisco José Prates Alegretti

MC083/2004

Computação Quântica

Francisco José Prates Alegretti

1. INTRODUÇÃO

Este texto contém reflexões sobre Computação Clássica e Computação Quântica. É feita uma análise sobre os computadores que possuímos atualmente, as suas limitações e as possibilidades para o futuro. São apresentados alguns conceitos básicos sobre a Arquitetura de Von Neumann e a Computação Quântica. O enfoque do texto é sobre a significância desses conceitos e as conseqüências que eles implicam na Ciência da Computação.

2. COMPUTAÇÃO CLÁSSICA

O computador tal qual o conhecemos atualmente é baseado na arquitetura de *Von Neumann*. Um computador de Von Neumann faz uma distinção clara entre elementos de processamento e armazenamento de informações, isto é, possui processador e memória separados por um barramento de comunicação. Mais especificamente, destaca-se duas características em particular sobre um computador de Von Neumann: a organização da memória e o método de processamento. As palavras de memória podem conter tanto instruções como dados. O processamento, por sua vez, é seqüencial, podendo conter desvios condicionais ou incondicionais. O reflexo dessas características nos computadores que temos na prática é a existência do *program counter* (que é incrementado a cada instrução) e da memória principal (que contém os programas executáveis e seus arquivos de dados). Essas são as duas características mais importantes da arquitetura de Von Neumann; elas definem não apenas o computador em si, mas tudo o que está associado com ele, ou seja, desde os algoritmos que são elaborados até a eficiência com que conseguimos resolver determinados problemas.

Para ilustrar melhor a importância dessas características da arquitetura de Von Neumann, considere o exemplo a seguir. Quando um programador implementa um *software*, computacionalmente, ele está escrevendo um algoritmo para solucionar determinado problema. A forma como a maioria dos programadores pensa e imagina essa solução é de forma seqüencial, não apenas porque pensamos de forma seqüencial, mas porque os computadores que construímos e utilizamos há cinqüenta anos também trabalham de forma seqüencial. A programação (estruturada, lógica ou funcional) e o processamento seqüencial são conseqüências diretas da arquitetura de Von Neumann. Mesmo novos paradigmas de programação, como a Orientação a Objetos, ainda estão restritos a Von Neumann.

Essa forma de organizar o computador, apesar de impor algumas restrições, é extremamente eficiente para a maioria das aplicações de um computador moderno. Provavelmente não existe forma melhor de realizar cálculos matemáticos, editar textos, armazenar bancos de dados ou acessar a Internet; um computador de Von Neumann é a melhor máquina para executar essas tarefas. Entretanto, para algumas áreas específicas, como a Inteligência Artificial por exemplo, talvez seja necessário um novo instrumento

computacional. De fato, os programas de Inteligência Artificial mais avançados do mundo estão muito longe de alcançar algo semelhante à inteligência humana.

Entretanto, a culpa por não se conseguir uma inteligência artificial de alto nível não pode ser atribuída somente ao hardware. O problema da IA pode ser tanto de software como de hardware. Não se pode afirmar que não existem programas ou máquinas inteligentes porque os computadores atuais não têm potência ou velocidade de processamento suficientes para suportar uma IA avançada. O problema pode ser a nossa falta de conhecimento (ou criatividade) para elaborar os algoritmos necessários. Assim, os processadores atuais podem ser até mais que suficientes para executar uma inteligência artificial ao nível da inteligência humana; nós é que não sabemos ainda como implementar os algoritmos. Por outro lado, a ausência desses algoritmos pode ser uma conseqüência da falta de computadores suficientemente poderosos. O fato é que não sabemos onde está o problema: no hardware, no software ou em ambos.

2.1. A Lei de Moore

Uma das características mais famosas da informática é a chamada Lei de Moore. Essa lei afirma que a velocidade do computador é dobrada a cada 18 meses. Isso quer dizer que os computadores ficam duas vezes mais rápidos a cada 1,5 ano. Essa lei é mantida desde o surgimento do primeiro PC[1], em 1981.

O primeiro microprocessador da Intel foi o 4004, lançado em 1971. Era um processador de 4 bits, com "apenas" 2300 transistores. Sua velocidade de operação era de 400 KHz (kilohertz, não megahertz). A tecnologia de fabricação atingia uma densidade de 10 mícron. Atualmente, o processador mais avançado da Intel é o Pentium 4 de 3.6 GHz. Esse processador possui 42 milhões de transistores; o chip é fabricado com tecnologia CMOS (*Complementary Metal Oxide Silicon*) a uma escalada de 0,09 mícron.

Assim como toda a tecnologia, a CMOS possui um limite; especula-se que o limite da CMOS seja de 0,05 mícron (NIEMEIER 2001). Apesar de estarmos próximos de atingir esse limite, eventualmente, outra tecnologia sucederá a CMOS. A candidata mais provável é a SiGe (Silício Germânio). Projeções calculam que em 2012 um microprocessador possuirá aproximadamente 10^{10} transistores e atingirá velocidades da ordem de 10 a 15 GHz. Mesmo que essa nova tecnologia, por sua vez, também chegue ao seu limite e outra a suceda, eventualmente, chegar-se-á ao limite atômico. Nesse nível não será mais fisicamente possível fabricar nada menor.

Este é um ponto que vale a pena salientar, pois ele nos leva a uma das mais importantes conclusões sobre a Computação Digital. Desde o surgimento do primeiro computador digital, até os dias de hoje, nunca houve uma *revolução* significativa na computação. O que aconteceu nos últimos 50 anos foi, na verdade, a simples evolução da *tecnologia*. Surgiram computadores menores e mais rápidos. A tecnologia evoluiu das válvulas, para os transistores e, finalmente, para os microchips. De fato, foi uma evolução

[1] PC é o nome do computador pessoal da IBM, do qual surgiram vários clones e, também, do qual a maioria dos computadores de hoje em dia evoluíram (ou seja, um Pentium consegue executar um programa escrito para o PC original). O primeiro clone do IBM PC foi feito pela Compaq. Entretanto, já existam outros microcomputadores antes do PC. O mais famoso é o Apple II, lançado em 1978. Atualmente, a Apple fabrica os computadores Macintosh. O primeiro microcomputador do mundo foi o Altair 8800, da empresa MITS, lançado em 1975. Esse computador utilizava o processador 8080 da Intel, de 8 bits.

impressionante e a uma velocidade surpreendente. Entretanto, *nunca* surgiu um computador mais poderoso. Computacionalmente, tudo o que um Pentium faz, um XT já fazia (XT era o nome de um dos primeiros computadores pessoais da IBM, equipado com o chip 8086; o IBM PC original vinha com o 8088, uma versão mais barata do 8086). A informática evoluiu em termos de velocidade, mas não em termos de poder computacional. Em outras palavras, um Pentium faz cálculos mais rápidos, mas não faz nenhum cálculo que um 8086 não faça.

Mais cedo ou mais tarde, a tecnologia digital atingirá seu limite. Chegar-se-á ao ponto em que não será possível aumentar a velocidade dos processadores. Será necessária uma alteração no computador em si, ou a descoberta de uma tecnologia totalmente nova. Para modificar o computador deve-se, no mínimo, mudar a Arquitetura de Von Neumann. Uma mudança de arquitetura implica na reorganização dos elementos de um computador de tal forma a melhorar a funcionalidade do computador; em outras palavras, removendo certas restrições que são implicitamente impostas pela arquitetura de Von Neumann.

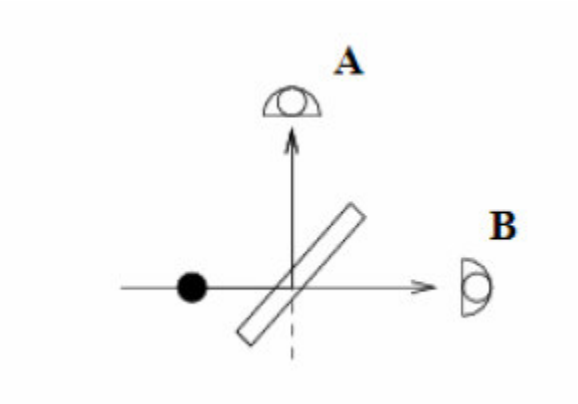
Existem várias propostas não convencionais de computação sendo pesquisadas atualmente. Algumas envolvem até a utilização de moléculas de DNA (ácido desoxirribonucléico). Entre as diversas alternativas ao computador digital, uma das mais interessantes e promissoras é o computador quântico. A próxima seção deste texto explica conceitos básicos sobre a computação quântica, descrevendo os mais importantes marcos dessa área do conhecimento.

3. COMPUTAÇÃO QUÂNTICA

Em um computador quântico a unidade básica de informação é o *qubit* (*quantum bit*). Um *qubit* pode assumir os valores de 0 ou 1, assim como um bit (*binary digit*) convencional. A diferença é que o *qubit* pode assumir ambos os valores de 0 ou 1 *ao mesmo tempo*! É nessa propriedade particular que está todo o poder computacional de um computador quântico. Apesar de ser pouco intuitivo (especialmente em uma cultura digital, onde tudo é exatamente 0 ou 1) e até mesmo contraditório com a física clássica, esse fenômeno quântico pode ser observado em laboratório, através de uma experiência conhecida como "divisão de raio".

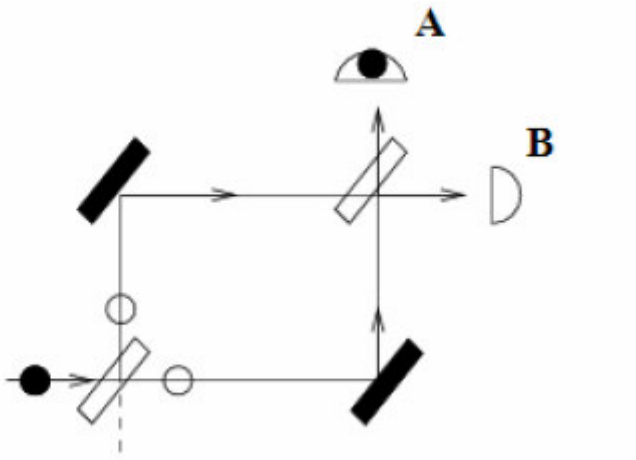
3.1. Dividindo o Fóton

Nessa experiência, uma fonte de luz é colocada em direção a uma lente. Adicionalmente, dois sensores óticos (A e B) são posicionados de tal forma de detectem as duas possíveis trajetórias do raio emitido pela fonte, conforme a figura abaixo. A fonte de luz emite um único fóton por vez, várias vezes. Sabe-se que um fóton é indivisível, ou seja, ele não pode ser particionado em duas unidades menores. Finalmente, a lente utilizada no experimento é tal que pode direcionar o fóton verticalmente, em direção ao sensor A, ou horizontalmente, em direção ao sensor B.



Dada a configuração do experimento, intuitivamente, espera-se que o fóton de luz emitido pela fonte seja refletido randomicamente pela lente e atinja um dos sensores óticos com a mesma probabilidade. De fato, esta experiência constata que o fóton é detectado em cada um dos sensores com a mesma probabilidade. Ou seja, em metade dos casos atinge o sensor A e, na outra metade, o sensor B. Até agora, a física clássica concorda com a física quântica.

Entretanto, a física quântica afirma que o fóton passa por ambas as trajetórias *simultaneamente*, todas as vezes! É aqui que a física quântica começa a diferenciar-se da física clássica e os conceitos ficam cada vez menos intuitivos. Para verificar essa afirmação é realizada uma nova experiência, onde dois espelhos e mais uma lente são acrescentados, conforme ilustrado na figura a seguir. A segunda lente utilizada é idêntica à primeira e os espelhos sempre refletem a luz na mesma direção.

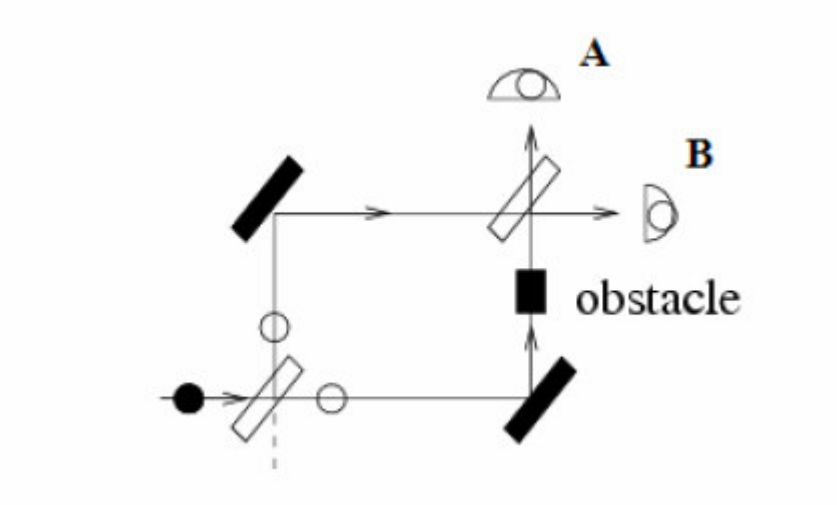


Nesta experiência, como na anterior, emite-se apenas 1 único fóton por vez, várias vezes. Entretanto, desta vez, verifica-se que apenas um dos sensores registra o fóton, *todas* as vezes. Ou seja, a probabilidade de que o fóton atinja um dos sensores (A ou B) é de 100% enquanto a do outro é nula. A explicação para esse fenômeno é que o fóton passa pelos dois caminhos possíveis simultaneamente, criando uma interferência no ponto de

intersecção (a segunda lente), anulando a probabilidade do fóton alcançar o outro sensor. Esse efeito é chamado de *single-particle interference*.

Em outras palavras, isso quer dizer que tudo o que pode acontecer, de fato, acontece. Mas como isso pode acontecer se na primeira experiência o fóton era detectado em ambos os sensores com a mesma probabilidade? Eles não deveriam atingir os dois sensores em todos os casos? A resposta da física quântica é que quando observamos o sistema todas as possibilidades colapsam em uma única ocorrência em particular, que é a realidade tal qual a conhecemos (talvez seja dessa parte da física quântica que autores de ficção científica inspirem-se e imaginem universos paralelos!). Isso quer dizer que o simples ato de observar o sistema pode influenciá-lo, alterando o seu desfecho. Conforme será explanado adiante, essa é uma das principais dificuldades em construir um computador quântico.

A única forma de observar que o fóton percorre as duas trajetórias ao mesmo tempo é através da interferência causada pela intersecção dos dois estados possíveis do sistema. Se for colocado um obstáculo sobre uma das trajetórias, conforme ilustrado pela figura a seguir, os sensores passam a registrar fótons como na primeira experiência, ou seja, com probabilidade de 0,5.



Essa experiência demonstra o princípio básico da computação quântica e o enorme potencial para processamento paralelo de um computador quântico. Os exemplos apresentados a seguir quantificam melhor esse potencial.

3.2. O Algoritmo de Shor

Desde a proposição da computação quântica por Richard Feymann não houveram muitos avanços significativos na área até 1994. Nesse ano, o pesquisador Peter Shor, dos laboratórios da AT&T Bell escreveu um algoritmo que utiliza propriedades do computador quântico para realizar a fatoração de números inteiros grandes (na ordem de 10^{200} dígitos) em tempo polinomial. Esse algoritmo quântico, que ficou conhecido como algoritmo de Shor, foi publicado no artigo "*Algorithms for Quantum Computation: Discrete Logarithms*

Factoring". O algoritmo utiliza justamente a propriedade da superposição quântica para conseguir reduzir, através de funções quânticas específicas, a complexidade do tempo de solução do problema de fatoração de exponencial para polinomial. O entendimento das funções quânticas que são utilizadas no algoritmo de Shor requer uma explicação matemática bastante extensa, que fogem do escopo desde texto. A aplicação imediata do algoritmo de Shor é na área de criptografia. A segurança dos sistemas de criptografia de chave pública baseia-se justamente na dificuldade de fatoração de números muito grandes; com a implementação prática de um computador que consiga realizar esses cálculos de forma rápida a segurança desses sistemas de criptografia estará comprometida. No entanto, conforme explicado a seguir, a tecnologia atual consegue construir computadores quânticos de apenas 7 qubits.

3.3. O Computador Quântico da IBM

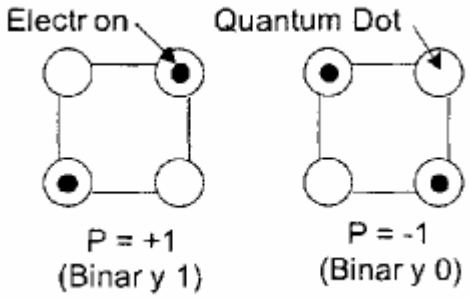
O algoritmo de Shor é um marco da computação quântica porque ele foi o primeiro algoritmo a utilizar as funcionalidades particulares de um computador quântico para otimizar a solução de um problema. A publicação do algoritmo de Shor desencadeou uma avalanche de novas pesquisas e experiências na computação quântica. Em dezembro de 2001, cientistas do Centro de Pesquisas da IBM em Almaden conseguiram construir um computador quântico de 7 qubits. Nesse computador foi implementado o algoritmo Shor, que conseguiu realizar corretamente a fatoração do número 15. Obviamente, esse computador não consegue quebrar nenhum sistema de criptografia. A importância desse experimento é que ele comprova a viabilidade da computação quântica. As principais dificuldades enfrentadas nesse primeiro momento são mais tecnológicas do que teóricas, como a alta incidência de erros nos computadores quânticos construídos até agora.

O computador quântico da IBM foi implementado através de uma molécula com 7 spins: o núcleo da molécula era constituído por 5 átomos de fluorina e 2 átomos de carbono. A programação do computador é feita através de pulsos de rádio-freqüência. A leitura dos resultados é feita por ressonância magnética nuclear (RMN), a mesma tecnologia dos aparelhos de tomografia computadorizada de hospitais. A operação do computador exige temperaturas baixas, a fim de reduzir a incidência de erros.

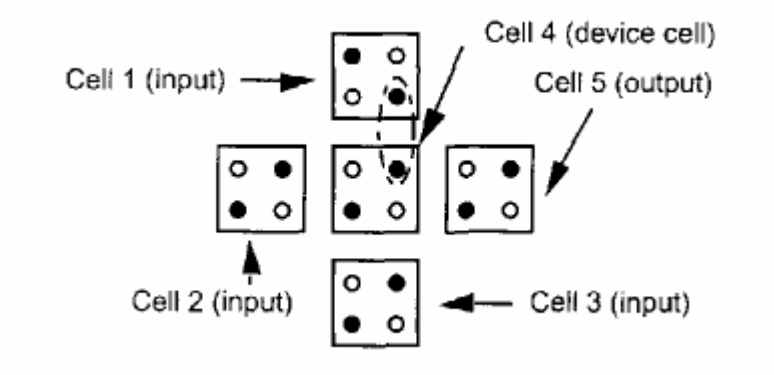
3.4. Tecnologias

Além da tecnologia de *Quantum Spins*, também existem propostas de um Autômato Celular Quântico. A unidade básica desse tipo de computador é a célula quântica. Cada célula quântica é constituída por 4 pontos quânticos (*quantum dots*), conforme ilustrado pela figura a seguir. Uma célula quântica possui dois elétrons. Através da *Repulsão de Coulumb*, os elétrons procuram manter-se em um estado de repouso, ou seja, naquele estado em que gastem menos energia. A fórmula de *Coulumb* afirma que a força de repulsão é inversamente proporcional à distância dos corpos; assim, quanto menor a distância entre os elétrons, maior será a força de repulsão entre eles. Por isso, os elétrons em uma célula quântica tendem sempre a ocupar os pontos quânticos de extremos opostos da célula. O *tunelamento* de elétrons torna possível a sua locomoção de um ponto quântico para outro. Em termos de computação, a disposição dos elétrons dentro da célula quântica é

equivalente ao *spin* dos elétrons no computador com quantum spins. São utilizadas chapas de capacitância para erguer barreiras de potencial para a construção das células quânticas. Entretanto, essa tecnologia requer a utilização de temperaturas baixíssimas: 70 milikelvins.



A partir das células quânticas é construída uma estrutura chamada de *three-input gate* (vide figura a seguir). Essa estrutura é formada por 5 células quânticas: 3 células de entrada, 1 célula de "processamento" e 1 célula de saída. Basicamente, o funcionamento dessa estrutura é da seguinte forma: a repulsão de elétrons mantém a polarização no mínimo; assim, a célula de processamento é induzida a assumir o estado da maioria das demais células de entrada. Finalmente, a célula de saída copia o resultado, de tal forma que a polarização dessa célula não influencie a computação da célula de processamento. Com as *three-input gate* é possível construir estruturas de alto nível, como portas lógicas, por exemplo (o detalhamento do funcionamento dessas estruturas é bastante complexo e extenso, e foge do escopo deste trabalho).



3.5. Problemas

A principal dificuldade enfrentada na construção de um computador quântico é a alta incidência de erros. Entre as causas dos erros está o próprio ambiente: a influência do meio sobre o computador quântico pode causar a alteração de qubits. Esses erros podem causar incoerência no sistema, invalidando toda a computação.

Uma dificuldade adicional é, ironicamente, a implicação de um dos princípios da Mecânica Quântica que tornam a Computação Quântica interessante em primeiro lugar. A Física Quântica afirma que o ato de medir ou observar um sistema quântico destrói a

superposição de estados. Isso quer dizer que, se for feita uma leitura dos dados durante a execução de programa em um computador quântico, todo o processamento será perdido. Assim, a maior dificuldade é conseguir corrigir um erro sem de fato medir o sistema. Isso é conseguido através da *coerência de fase*. Essa técnica permite a correção de erros sem comprometer o sistema. Para tanto, é utilizada a ressonância magnética nuclear para copiar um único bit de informação quântica de três spins nucleares de moléculas de tricloroetileno. Basicamente, a técnica utiliza a observação indireta para efetuar a correção de erros e manter a coerência do sistema.

Tendo em vista todas essas dificuldades é que fica evidente a importância da experiência realizada pela IBM: os cientistas conseguir superar todos esses contratempos e implementar, na prática, o algoritmo de Shor em um computador quântico.

4. CONCLUSÃO

Para realizar a maioria dos cálculos matemáticos, editar textos ou navegar na Internet, os computadores atuais (baseados na arquitetura de Von Neumann) são a melhor solução. De fatos, os processadores atuais são extremamente eficientes para realizar essas tarefas. Entretanto, em áreas como a Inteligência Artificial, torna-se interessante a utilização de outros tipos de computadores e arquiteturas. Em algoritmos de reconhecimento de imagens ou processamento da fala, por exemplo, a execução seqüencial e o armazenamento de dados da arquitetura de Von Neumann (que são tão eficientes para outras aplicações) tornam-se uma restrição que acaba limitando o desempenho desses sistemas. Para esse tipo de aplicação, torna-se mais interessante um tipo de computador que possua bastante poder de processamento paralelo para facilitar o reconhecimento de padrões (o princípio comum de solução desses problemas). Entre as diversas propostas alternativas, o computador quântico apresenta-se como a opção mais promissora, justamente porque a computação quântica é a que mais se diferencia da arquitetura de Von Neumann, com um poder de processamento paralelo maciço.

Portanto, o computador quântico não será utilizado para resolver os problemas que um computador clássico já resolve eficientemente. A computação quântica será aplicada em problemas que ainda não possuem solução eficiente, como a Inteligência Artificial e a Criptografia.

5. BIBLIOGRAFIA

Becket, P., Jenning, A. **Towards Nanocomputer Architecture.** 7th Asia Pacific Computer Systems Architecture Conference, Melbourne, Australia – 2002. Conferences in Research and Practice in Information Technology, Vol. 6.

Freivalds, R. **How to Simulate a Free Will in a Computational Device?** AMC, 1999.

Gershenfeld, N., West, J. **The Quantum Computer.** Scientific America, 2000.

Knill, E. **Quantum Randomness and Nondeterminism.** Los Alamos National Laboratory, 1996.

Niemier, M. T., Kogge, P. M. **Exploring and Exploiting Wire-Level Pipelining in Emerging Technologies.** IEEE, 2001.

Rieffel, E., Wolfgang, P. **An Introduction to Quantum Computing for Non-Physicists.** ACM Computing Surveys, Vol. 32, No. 3, September 2000, pp. 300-335.

Sarkar, P. **A Brief History of Cellular Automata.** ACM Computing Surveys, Vol. 32, No. 1, March 2000.

Skadron, K. **The Role of Processor Architecture in Computer Science.** Fundamentals of Computer Science Committee, National Academy of Science, 2001.

Wikipedia Encyclopedia. **Quantum Computer.** http://en.wikipedia.org/

Wikipedia Encyclopedia. **Shor's Algorithm.** http://en.wikipedia.org/