Breve Introdução à Computação Quântica

Felipe Portavales Goldstein
Instituto de Computação
Avenida Albert Einstein, 1251
Campinas, Brasil
felipe.goldstein@ic.unicamp.br

Gustavo Lima Chaves
Instituto de Computação
Avenida Albert Einstein, 1251
Campinas, Brasil
gustavo.chaves@ic.unicamp.br

Peterson Katagiri Zilli
Instituto de Computação
Avenida Albert Einstein, 1251
Campinas, Brasil
peterson.zilli@ic.unicamp.br

RESUMO

A computação quântica surgiu no início da década de 80 em resposta às previsões de esgotamento da atual tecnologia da computação até 2020, segundo às leis de Moore. Ela traz consigo idéias da teoria clássica da informação, da ciência da computação e da física quântica, e tem atraído pesquisadores por causa da sua potencialidade no uso do paralelismo quântico como ferramenta para resolver problemas matemáticos mais eficientemente.

O objetivo deste trabalho é proporcionar uma breve introdução à computação quântica, e relacioná-la com tópicos das demais ciências. Ao longo do texto, idéias básicas sobre informação quântica, como *qubits* e portas quânticas, são delineadas. O computador universal quântico é então descrito de acordo com o modelo de Church-Turing. Algoritmos para tal computador são discutidos, em especial o algoritmo de fatoração de Shor.

Apesar de todo o avanço da pesquisa nessa área, construir um computador quântico universal parece estar muito além das capacidades da tecnologia atual. Entretanto, alguns princípios físicos da informação quântica já estão sendo testados em dispositivos de laboratório, em pequena escala. A situação experimental dessa ciência é brevemente analisada, e são citados idéais básicas para realização de maquinas quânticas, baseadas nos princípios de armadilha de átomos, de cavidades ópticas e dos métodos de ressonância magnética nuclear (NMR).

Palavras-Chave

Computação Quântica, Algoritmos Quânticos, Teoria da Informação Quântica, Criptografia Quântica, Hardware para Computação Quântica

1. INTRODUÇÃO

A história da tecnologia de fabricação de computadores tem envolvido uma seqüência de mudanças bastante atraentes, de um tipo de realização física para outro (de engrenagens para relés, de válvulas para transistores, para circuítos integrados, e outros). Seguindo esses passos nota-se a trajetória da miniaturização dos componentes lógicos, até o ponto em que milhões de transistores são colocados em um *chip* de silício do tabanho de uma moeda. Dessa forma, a construção está se aproximando do ponto em que uma porta lógica será fisicamente construída a partir de alguns poucos átomos. Nessa escala, as interferências geradas dentro do próprio processador, causadas por fenômenos quânticos, se tornam muito relevantes. Além disso, a corrida pelo aumento na velocidade do *clock* dos microprocessadores têm levado a uma situação em que o calor gerado pelo consumo de energia é tão grande que se torna inviável a utilização desses mecanismos.

Neste contexto, muitos podem imaginar que a computação quântica chega como uma solução para se diminuir o tamanho das portas lógicas e/ou possibilitar o aumento da velocidade do *clock* de um possível processador quântico similar a um processador clássico. O que acontece, contudo, é que a tecnologia e o modelo computacional quântico vão além disso. Oferecendo mais do que a compressão de bits e bits em um chip de silício, ou que a multiplicação da velocidade do *clock* do processador. "Este novo modelo é capaz de suportar um tipo de computação inteiramente novo com algoritmos qualitativamente novos baseado em princípios quânticos" [2].

É como se fosse dado ao teórico da computação o poder de projetar seu algoritmo da forma que um físico quântico o pensaria. Isso porque, fundamentalmente, qualquer computador é uma máquina física, e qualquer computação que venha a executar é apenas um experimento de física. A física quântica provê propriedades únicas que nunca foram usadas com propósito de computação, como o possível uso de efeitos essencialmente quânticos para a resolução eficiente de problemas matemáticos.

O restante desse texto está organizado como segue: na seção 2 fala-se sobre teoria de coputação e modelos computacionais; discorre-se sobre a informação clássica e quântica na seção 3; na seção ...

2. TEORIA DA COMPUTAÇÃO

A encarnação moderna da ciência da computação[1] foi prenuciada pelo grande matemático Alan Turing. Ele desenvolveu em detalhes uma noção abstrata do que se poderia agora chamar de computador programável, um modelo de computação conhecido como *Máquina de Turing*. Esse cientista demostrou a existência da *Máquina de Turing Universal* que pode ser usada para simular qualquer outra máquina de Turing. Ademais, ele afirmou que a Máquina de Turing Universal *captura completamente* o significado de se realizar uma tarefa por meios algoritmicos. Isto é, se um algoritmo pode ser realizado em *qualquer* peça de *hardware*, então existe um algoritmo equivalente para uma Máquina de Turing Universal que realiza exatamente a mesma tarefa que o algoritmo original. Esta declaração, conhecida como a *tese de Church-Turing*, asserta a equivalência entre o conceito físico de que classes de algoritmos podem ser executados em *algum dispositivo físico* com o rigor matemático de uma Máquina de

[1]As origens da ciência da computação são perdidas na história. Por exemplo, tabelas cuneiformes indicam que ao tempo de Hamurabi (cerca de 1750 A.C.) os babilônios tinham desenvolvido algumas idéias algoritmicas bem sofisticadas.

Turing Universal. A larga aceitação desta tese levou ao desenvolvimento de uma rica teoria de ciência da computação.

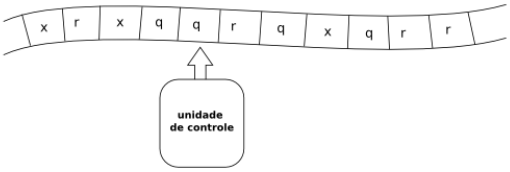

Figura 1: Ilustração da Máquina de Turing.

O que foi observado em meados de 1970 é que parecia que o modelo de computação da Máquina de Turing (fig 1) era ao menos tão poderoso quanto qualquer outro modelo de computação, no sentido de que um problema que podia ser resolvido eficientemente em algum modelo de computação também poderia ser resolvido eficientemente no modelo da Máquina de Turing. Esta observação foi codificada em uma versão fortalecida da tese de Church-Turing:

Qualquer processo algoritmico pode ser simulado eficientemente usando-se a máquina de Turing.

O primeiro grande desafio à tese forte de Church-Turing surgiu também em meados de 1970, quando Robert Solovay e Volker Strassen mostraram que é possível testar se um inteiro é primo ou composto usando-se um *algoritmo randômico*. Isto é, o teste de Solovay-Strassen para primalidade usava aleatoriedade como parte *essencial* do algoritmo. O algoritmo não determinava se um dado inteiro era primo ou composto com certeza. Ao invés disso, o algoritmo podia derterminar que um número era *provavelmente* primo (ou, do contrário, composto). Repetindo o teste de Solovay-Strassen algumas vezes é possível determinar com aproximada certeza se um número é primo ou composto. Na época que o teste foi proposto não havia nenhum teste determinístico para primalidade conhecido. Assim, parecia que computadores com acesso um gerador aleatório de números seria capaz de eficientemente realizar tarefas computacionais sem soluções eficientes em uma máquina de Turing determinística convencional. Este desafio parece ser facilmente resolvido por uma simples modificação na tese forte de Church-Turing:

Qualquer processo algoritmico pode ser simulado eficientemente usando-se uma máquina de Turing probabilística.

Esta modificação *ad hoc* da tese forte de Church-Turing leva a um sentimento delicado. Não seria o caso de que algum dia ainda outro modelo de computação permitiria resolver eficientemente problemas que não são eficientemente solucionáveis com o modelo de computação de Turing?

Motivado por esta questão, em 1985 David Deutsch questionou se as leis da física poderiam ser usadas para *derivar* uma versão ainda mais forte da tese de Church-Turing. Ele esforçou-se em definir um dispositivo computacional que seria capaz de eficientemente simular um sistema físico *arbitrário*. Uma vez que as leis da física são quânticas, ele foi naturalmente levado a considerar dispositivos computadores baseados nos princípios da mecânica quântica.

O que modelo de computador quântico de Deutsch desencadeou (ver apêndice A) foi um desafio à forma forte da tese de Church-Turing. Deutsch questionou se é possível que um computador quântico eficientemente resolva problemas que não têm solução eficiente em um computador clássico, mesmo em uma máquina de Turing probabilística. Este memorável primeiro passo foi aprimorado na década subsequente por muitas pessoas, e tem-se hoje uma vasta e bela teoria, já subdividida em vários ramos [11].

3. INFORMAÇÃO QUÂNTICA

"Qualquer processamento de informação é sempre realizado de formas físicas" – recentemente, esse enunciado aparentemente inocente com implicações nada triviais levou uma explosão teórica e experimental de inovações, cujos pesquisadores afirmam estarem criando uma nova disciplina fundamental: a teoria quântica da informação.[3]

O estudo de questões relativas a informação, na sua forma clássica, também é recente. Na mesma época em que a ciência da computação "explodia" nos anos 1940, outra revolução tomava lugar na nossa compreensão de *comunicação*. Em 1948, Claude Shannon publicou o que seria as fundações da teoria moderna da informação e comunicação.

Shannon desenvolveu, na teoria clássica da informação, dois teoremas básicos. O primeiro quantifica os recursos físicos necessários para se transmitir ou armazenar uma certa quantidade de informação num canal livre de ruídos. O segundo quantifica a quantidade de informação útil que pode ser transmitida através de um canal com ruídos. Para "proteger" a informação a ser transmitida num canal com ruído, códigos corretores de erro foram desenvolvidos [11].

Basicamente, o que Shannon fez foi *definir matematicamente o conceito de informação*. Na teoria quântica da informação faz-se o mesmo. Assim como o *bit* é o conceito fundamental da computação clássica e da informação clássica, a computação quântica e a informação quântica são construídos sobre um conceito análogo, o *bit quântico*, que a seguir será definido. É importante ressaltar que toda a modelagem matemática do conceito do bit quântico independe de sua implementação, o que fornece grande praticidade à teoria quântica em geral.

Como trata-se de um modelo muito diferente do que se está acostumado (na computação clássica), será apresentada uma pequena motivação, antes do conceito de bit quântico, que delineia as propriedades quânticas e contra-intuitivas da matéria física (que são a base do poder computacional que se esta a expor).

3.1 Interferência: o Experimento de Duas Fendas

Considere o aparato físico mostrado na figura 2. Elétrons emitidos do canhão à esquerda passam através da parede com duas fendas e colidem com a parede (fig. 2 (a)), onde suas quantidades são contadas como função da posição x por um detector móvel. Quando a fenda 2 é coberta (fig. 2 (b)), a distribuição de probabilidades para a posição do elétron é dada por $P_1(x)$, que é máxima exatamente onde a trajetória balística faria colidir mais elétrons, como esperado. Quando a outra fenda é fechada (fig. 2 (c)), a distribuição é $P_2(x)$, que é similar. Agora, para particulas normais, quando ambas as fendas estão abertas, esperaria-se obter a distribuição $P_{12}(x) = P_1(x) + P_2(x)$, a soma das distribuições anteriores (fig. 2 (d)). Entretanto, não é este o caso: estes elétrons produzem um padrão de *interferência*, que oscila entre zero e a soma de distribuições esperada (fig. 2 (e)). Este comportamento é análogo ao que se esperaria para ondas, ao invés de partículas, e é uma propriedade importante de sistemas quânticos.

O experimento nos mostra que probabilidades são insuficientes – probabilidades são números positivos e não podem se cancelar quando somadas. Se houvessem probabilidades *negativas* isto funcionaria. Acontece que em mecânica quântica o que se tem são *amplitudes de probabilidade* ϕ_i, que são números complexos cujas normas fornecem probabilidades $P_i = |\phi_i|^2$. Para o experimento de fendas duplas, a distribuição de saída é $P_{12}(x) = |\phi_1(x) + \phi_2(x)|^2 = P_1(x) + P_2(x) + 2\Re e(\phi_1(x)\phi_2(x))$. As oscilações vêm do terceiro termo, de interferência [15].

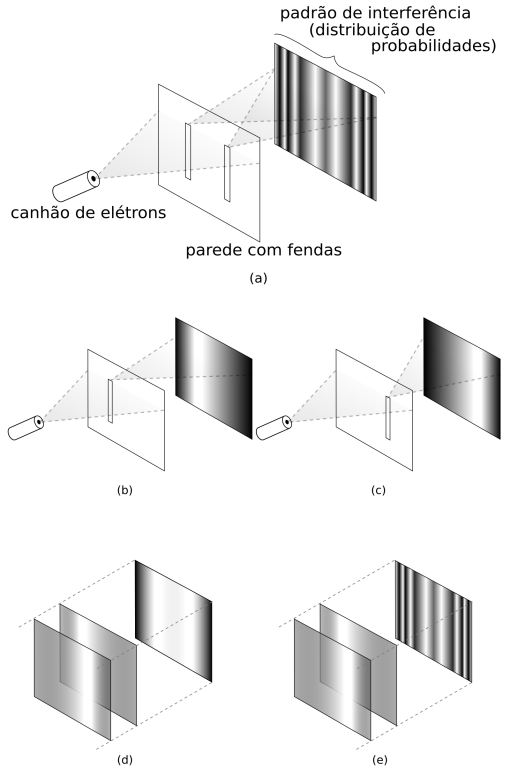

Figura 2: (a) Para as duas fendas abertas, a distribuição de probabilidades segue o padrão de interferência; (b) Com a fenda da esquerda aberta, a distribuição de probabilidades é máxima exatamente onde a trajetória balística faz colidir mais elétrons; (c) Com a fenda da direita aberta; (d) Com ambas as fendas abertas, esperaria-se obter a distribuição como sendo a soma das distribuições anteriores; (e) Com ambas as fendas abertas, o que ocorre é o padrão de interferência que oscila entre zero e a soma de distribuições esperada.

O interesse está em como informação pode ser representada por um estado quântico. Para fazê-lo, será apresentado um sistema físico muito simples.

3.2 Bits Quânticos

Um bit quântico (*"qubit"*) é um sistema de dois estados, como o elétron nos dois níveis mais baixos de energia de um átomo de Hidrogênio (fig 3). O elétron tem amplitudes de probabilidade α e β de de estar ou no estado base ($n = 0$) ou no estado excitado ($n = 1$), respectivamente. Poderia-se dizer que o elétron não decidiu onde ele deveria estar, e então existe parcialmente em ambos os estados de energia.

Uma vez que o elétron definitivamente existe, a probabilidade total deve ser um, o que significa que $|\alpha|^2 + |\beta|^2 = 1$. Pode-se, dessa forma, representar o estado quântico de um qubit como um vetor unitário $(\alpha\ \beta)^T$. Mas uma notação mais conveniente, que será adotada dos físicos[2], é denotar o estado do qubit como $|\psi\rangle$ (um $|\cdot\rangle$ é chamado "ket", que nada mais é que uma notação para estados quânticos em mecânica quântica), que é, para nosso átomo de Hidrogênio, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. [5, 4]

O paradoxo do qubit é que ele parece conter uma quantidade infinita de informação, uma vez que seu estado é representado por dois graus *contínuos* de liberdade. Entretanto, esta conclusão é infundada, devido a uma propriedade adicional e extremamente importante de sistemas quânticos.

Quando um qubit é medido, apenas um de dois resultados são obtidos: ou zero ou um. Uma medição de $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ resultará em 0 com probabilidade $|\alpha|^2$, levando ao estado $|\psi'\rangle = |0\rangle$, ou em 1 com probabilidade $|\beta|^2$, levando ao estado $|\psi'\rangle = |1\rangle$. Nota-se que o estado pós-medição do sistema é um novo estado, que é consistente com o resultado da medição.

[2]Esta notação é chamada notação de Dirac, após o famoso físico Paul Dirac, que a inventou.

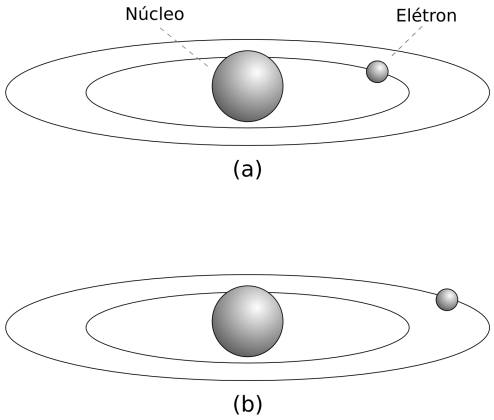

Figura 3: (a) O elétron no estado base ($n = 0$); (b) O elétron no estado excitado ($n = 1$).

Assim, de uma única medição, obtém-se apenas um único bit de informação sobre α e β – e o paradoxo está resolvido. Apenas se infinitamente muitos qubits preparados identicamente fossem medidos seria possível obter α e β completamente. Então, em certo sentido, um qubit contém grande quantidade de "informação escondida" – enquanto ele não é medido (ele se encontra em estado de sobreposição das bases).

Esta é uma parte importante do que será explorado na computação quântica, como será visto adiante, considerando as propriedades de múltiplos qubits [15].

Apesar da estranheza, qubits são decididamente reais, sua existência e comportamento foram extensivamente validados por experimentos, e muitos sistemas físicos podem ser usados para se concretizar qubits. É possivel realizar qubits através de duas diferentes polarizações de um fóton; do alinhamento de spin nuclear num campo magnético uniforme; ou até de dois estados de um elétron orbitando um átomo, como no nosso exemplo.

3.3 Múltiplos Qubits

Um sitema quântico composto por vários qubits também é chamado de *registrador quântico*. Suponha agora um registrador de dois qubits. Se eles fossem representados por átomos de hidrogênio, por exemplo, então classicamente haveria quatro estados possíveis, 00, 01, 10 e 11, para os dois elétrons. Matematicamente falando, o sistema de dois qubits tem *quatro estados da base computacional* denotados por $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Como um par de qubits também pode existir em superposições destes estados, então obtêm-se coeficientes complexos associados a cada um dos estados – associa-se uma amplitude de probabilidade. Dessa forma pode-se representar o vetor de estado descrevendo os dois átomos como

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,, \qquad (1)$$

onde $\sum_{x=\{0,1\}^2} |\alpha_x|^2 = 1$ (condição de normalização). Similarmente ao caso para um qubit só, o resultado da medição de x ocorre com probabilidade $|\alpha_x|^2$, resultando no estado $|x\rangle$. Pode-se, também, medir apenas um subconjunto dos bits; o resultado é similar: medir o primeiro bit resultaria em 0 com probabilidade $|\alpha_{00}|^2 + |\alpha_{01}|^2$, resultando no estado

de pós-medição

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \quad (2)$$

Note como $|\psi'\rangle$ é re-normalizado para ter comprimento unitário. [11, 15].

Um importante estado de um registrador de dois qubits é o estado de *Bell* ou estado de *par EPR*,

$$\frac{|00\rangle + |01\rangle}{\sqrt{2}}. \quad (3)$$

Esse estado aparentemente inócuo é responsável por muitas surpresas na computação e na informação quântica. Ele é o ingrediente chave no teleporte quântico e na codificação superdensa (que permite o envio de dois bits de informação clássica, enviando um único qubit), e é o protótipo para muitos outros estados quânticos interesantes. O estado de Bell tem a propriedade de que, depois de medir o primeiro qubit, obtêm-se dois resultados possíveis: 0 com probabilidade 1/2, deixando o estado pós-medição como $\varphi'|00\rangle$. e 1 com probabilidade 1/2, deixando o estado pós-medição como $\varphi'|11\rangle$. A medida do segundo quibit sempre reptorna o mesmo resultado da medida do primeiro qubit, ou seja, os resultados de medidas estão correlatos. [14, 7]

Estas correlações têm sido assunto de intenso interesse e desde um famoso paper de Einstein, Podolsky e Rosen, no qual eles foram os primeiros a apontar propriedades estranhas como o estado de Bell. As idéias deles foram tomadas e grandemente trabalhadas por John Bell, quem provou um resultado surpreendente: "as correlações de medida no estado de Bell são mais fortes do que poderia existir entre sistemas clássicos".

Generalizando ainda mais, pode-se considerar um sistema de n qubits. Os estados computacionais básicos desse registrador estão na forma $|x_1x_2...x_n\rangle$, e então um estado quântico de tal sistema é especificado por 2^n amplitudes. Para $n = 500$ este número é maior que o número estimado de átomos no Universo! A tentativa de armazenar todos esses números complexos não seria possível em qualquer computador clássico concebível. Em princípio, porém, a natureza manipula tal enorme quantidade de dados, até mesmo para sistemas contendo apenas poucas centenas de átomos. É como se a natureza estivesse mantento 2^{500} pedaços de papel de rascunho escondidos por perto, nos quais ela executa seus cálculos enquanto o sistema evolui. Esse enorme potencial computacional é alguma coisa que se muito tentará tomar como vantagem nos próximos anos. Mas como se pode pensar da mecânica quântica como computação?

3.4 Circuitos Quânticos

A computação quântica, assim como a clássica, manipula sua informação através de portas lógicas. Algumas diferenças existem, no modelo quântico (e são elas que dão maior poder computacional para os algoritmos quânticos). A representação gráfica de circuitos clássicos é, de certa forma, próxima da realidade física do circuito implementado. Por exemplo, linhas correspondem a fios e bifurcações significam que a corrente elétrica passa por ambos os fios. Nos circuitos quânticos, os fenômenos ocorrem de outra forma, como será visto.

3.4.1 Notação e Convenções

Para apresentar as convenções usadas em circuitos quânticos, será utilizado um circuito (porta U-controlada) em que a entrada e a saída são um estado de 2 qubits (figura 4).

Aqui é apresentada, baseados na figura, as convenções em circuitos quânticos:

- **Entrada:** considera-se conjuntamente os qubits de entrada, matematicamente o que é chamado de seu produto tensorial (os qubits não devem ser considerados individualmente).

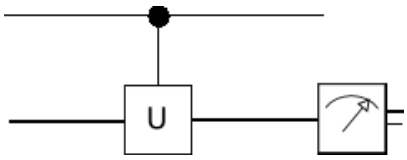

Figura 4: Porta quântica U-controlada.

- **Linhas horizontais:** as linhas que aparecem não são necessariamente fios. Elas representam a evolução de um qubit, podendo ser apenas a passagem do tempo ou, por exemplo, o deslocamento de um fóton.
- **Sentido:** o circuito descreve a evolução do sistema quântico no tempo, da esquerda para a direita. Com isso, não há sentido em aparecer retroalimentação, que pode ocorrer em um circuito clássico.
- **Linhas verticais:** o segmento vertical que aparece unindo os símbolos • e o U dentro de uma caixa informa que o circuito atua simultaneamente nos dois qubits. A linha vertical representa o sincronismo, e não o envio de informação. Portanto, não são permitidas nem junções, nem bifurcações de qubits.
- **Controle:** o símbolo • indica que o qubit representado nessa linha é um qubit de controle, ou seja, caso esteja no estado $|1\rangle$, a porta U realiza a operação; caso esteja no estado $|0\rangle$, a porta U não realiza operação alguma. Caso o qubit de controle seja um estado superposto ou os 2 qubits estejam emaranhados, não é possível compreender o comportamento individual do qubit de controle e do qubit alvo. Deve-se considerar a ação do operador unitário, que representa todo o circuito, atuando simultaneamente nos 2 qubits.
- **Saída:** os qubits que compõem a saída do circuito podem ou não ser medidos. Como o qubit inferior está sendo medido (o símbolo de medida está indicado na figura 4), o resultado será 0 ou 1.

Vistas as principais convenções, será apresentada algumas portas quânticas. Primeiramente, portas de 1 qubit. No caso clássico, há apenas uma possibilidade: a porta NOT. O mesmo não ocorre nos circuitos quânticos, como será visto.

Antes de prosseguir, deve ser feita uma observação. A importância do estudo de portas lógicas em computação quântica baseia-se no fato de que toda matriz unitária 2×2 pode ser representada por um circuito quântico de 1 qubit e vice-versa. Sendo assim, a evolução no tempo de um sistema quântico isolado, dado por um qubit, pode ser representada tanto matematicamente (por uma transformação unitária) quanto logicamente (por um circuito quântico) [12].

3.4.2 Porta NOT Quântica

No caso clássico, a porta NOT troca o 1 por 0 e vice-versa. A generalização para o caso quântico é dada por um operador X que satisfaz

$$X|0\rangle = |1\rangle \;\; e \;\; X|1\rangle = |0\rangle. \quad (4)$$

Com isso, verifica-se facilmente que a representação matricial do operador X é dada por

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (5)$$

Com a porta NOT quântica, existem situações sem contrapartida no caso clássico, pois, se a entrada $|\varphi\rangle$ for uma superposição dos estados $|0\rangle$ e $|1\rangle$,

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

a saída será

$$X|\varphi\rangle = \beta|0\rangle + \alpha|1\rangle$$

A porta X é apenas uma das portas de 1 qubit, já que há infinitas matrizes unitárias 2×2.

3.4.3 Porta CNOT Quântica

Outra porta, essa atuando em estados de 2 qubits, é a contrapartida quântica do circuito clássico da porta XOR. Ela tem 2 qubits de entrada, o de controle e o alvo (figura 5). Uma porta controlada, como já foi visto (figura 4), age dependendo do valor do qubit de controle. Ela é "ativada" se o qubit de controle estiver no estado $|1\rangle$, e nada faz, se ele estiver no estado $|0\rangle$. Essa descrição é adequada apenas quando o qubit de controle está nos estados $|0\rangle$ ou $|1\rangle$. Entretanto, o que distingue a porta CNOT quântica da clássica é que, na porta CNOT quântica, os qubits alvo e de controle podem ser estados superpostos.

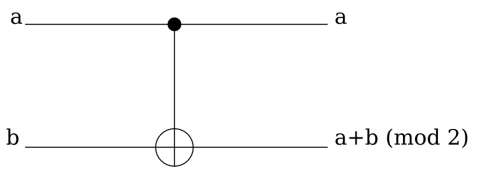

Figura 5: Porta quântica CNOT.

A ação da porta CNOT pode ser caracterizada pelas transformações operadas nos elementos da base computacional associada, ou seja,

$$|00\rangle \rightarrow |00\rangle\,,$$
$$|01\rangle \rightarrow |01\rangle\,,$$
$$|10\rangle \rightarrow |11\rangle\,,$$
$$|11\rangle \rightarrow |10\rangle\,.$$

Note que é possível representar essa ação na base computacional de forma mais esquemática por

$$|i,j\rangle \rightarrow |i, i \oplus j\rangle\,,$$

onde $i, j \in 0, 1$ e $\oplus$ é a adição módulo 2.[1, 6]

4. ALGORITMOS QUÂNTICOS

Pode-se encontrar uma tarefa que um computador quântico realizará melhor do que um computador clássico? A resposta para esta questão é, como nos mostram os estudiosos de computação quântica, sim. É apresentada, a seguir, uma idéia geral de um dos algoritmos quânticos mais importantes, o algoritmo de Shor.

4.1 Fatorando em Computadores Quânticos: o algoritmo de Shor

Em 1994, Peter Shor descreveu um algoritmo quântico que resolve o problema da fatoração em primos em tempo polinomial. Esse algorimo foi batizado como "Algoritmo de Shor" e é o mais importante resultado obtido até agora na computação quântica. O resultado de Shor foi o principal motivo que alavancou o interesse do estudo da computação quântica ao redor do mundo. A seguir será dada uma breve noção do que vem a ser o algoritmo.

Uma forma ingênua de fatorar um número inteiro n é baseada em checar o resto da divisão de n por algum número p menor que a raiz quadrada de n. Se o resto é 0, concluí-se que p é um fator. Este método é de fato muito ineficiente: com um computador que fazer testes para 10^{10} $p's$ por segundo (isto é mais rápido que qualquer computador já construído), o tempo médio para encontrar o fator de um número de 60 dígitos (decimais) excederia a idade do universo.

Ao invés deste método de divisão ingênuo, computadores quânticos contam com uma técnica levemente diferente para realizar fatorização eficiente. Realmente, é possivel mostrar que fatorar um número pode ser relacionado ao problema de avaliar o período de uma função. Para explicar como este método funciona, toma-se um exemplo simples: imagine que se quer encontrar os fatores primos de $n = 15$. Para fazê-lo, toma-se um número aleatório a menor que n, por exemplo $a = 7$, e define-se a função $f(x) = 7^x \bmod 15$. A matemática nos diz que $f(x)$ é periódica e que seu período r pode ser relacionado com os fatores de 15. Em nosso exemplo, pode-se checar que o período é $r = 4$ ($f(x)$ é avaliada em 1, 7, 4, 13, 1, 7, 4... para os valores de $x = 0, 1, 2, 3, 4, 5, 6...$). Com essa informação, computar os fatores de n apenas requer que seja avaliado o máximo divisor comum de n e $a^{\frac{r}{2}} \pm 1$. Em nosso exemplo, o cálculo de do máximo divisor entre 15 e $50 = 7^{\frac{4}{2}} + 1$ ou $(48 = 7^{\frac{4}{2}} - 1)$ retorna, de fato, os valores 5 (ou 3), os fatores primos de 15.

Obviamente, computadores clássicos não podem realizar este método: encontrar o período de $f(x)$ requer que avalie-se esta função muitas vezes. De fato, os matemáticos nos dizem que o número médio de avaliações requeridas para se achar o período é da mesma ordem do número de divisões necessárias com o método ingênuo que foi descrito primeiramente. Com um computador quântico, a situação é completamente diferente: colocando um registrador quântico em uma superposição de estados representando 0, 1, 2, 3, 4... é possível computar em um único passo os valores de $f(0)$, $f(1)$, $f(2)$... . Estes valores são codificados em estados superpostos de um registrador quântico, e encontrar o período a partir deles requer outro passo (conhecido como *transformada de fourier quântica*[3]), que pode também ser executado muito eficientemente em um computador quântico [2], e então, encontra-se os fatores do número original. O que põe em risco os sistemas de criptografia atuais, baseados em chaves.

4.2 Criptografia Quântica

O propósito da criptografia é transmitir informação de tal forma que o acesso a ela seja restrito inteiramente a um destinatário específico. Atualmente, os métodos de criptografia mais utilizados são baseados em chaves de bits suficientemente longas, e a cifragem/decifragem do texto só pode ser feita de posse dessa chave. Uma vez que a chave esteja definida, a comunicação subsequente envolve o envio de criptogramas sobre um canal público o qual é vulnerável a todos os observadores. Entretanto, existe o problema de que, mesmo mantendo a mensagem criptografada, deve-se mandar a chave através de meios convencionais, também. Logo, nenhum sistema clássico de criptografia baseado em chaves é 100% seguro, pois a chave poderia ser descoberta, e fatorada.

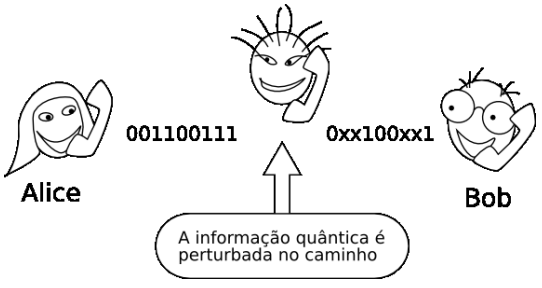

Figura 6: Criptografia quântica e o espião.

Contudo, se, por um lado, a computação quântica parece estar querendo colaborar com espiões e terroristas, por outro lado também, é possível utilizá-la para tornar invioláveis as mensagens trocadas entre computadores. De fato, ao interceptar uma mensagem clássica, um espião precisa descobrir quais são os bits que estão sendo transmitidos de um computador a outro. Descobrir o valor dos bits significa

[3]Não será dado detalhes desta operação. Para saber mais, consulte [11].

medi-los de algum modo. Na computação quântica, entretanto, o que se troca são q-bits, e a medição do estado de um q-bit acarreta uma perturbação grande demais para permanecer oculta. Ou seja, o processo de espionagem leva à descoerência (figura 6), o que pode ser quantificado de modo preciso. Alguém até poderia espionar, mas não passaria desapercebido. Estas idéias podem ser levadas a cabo com todo detalhe, de modo a produzir um esquema de transmissão segura de informação quântica. Inclusive, já existem experiências reais onde se troca, com absoluta segurança, informação quântica. Do exposto se conclui que a criptografia quântica é uma área florescente.

Um aspecto interessante da troca segura de informação quântica se refere à impossibilidade genérica de se copiar qubits com absoluta fidelidade. Isto se expressa matematicamente pelo teorema da não clonagem. No caso clássico, é fácil clonar informação, como no caso das máquinas de xerox ou copiadoras de CDs. No caso quântico, entretanto, o teorema da não clonagem impede a cópia de qubits. Caso contrário, seria possível elaborar um número suficientemente grande de cópias de um dado qubit, usando isto para descobrir seu estado sem nenhuma perturbação. Ou seja, se poderia medir o estado do qubit efetuando medidas de suas cópias e não dele próprio, evitando a descoerência. Na analogia do jogo de cara ou coroa, se repetiria o jogo copiando o estado da moeda em pleno vôo e avaliando o resultado. Caso fosse encontrado o valor "cara" em 40% das vezes e o valor "coroa" em 60%, a conclusão seria que a moeda original estaria descrita pelo qubit composto por 40% de cara e 60% de coroa. Esta conclusão não implicaria em nenhuma perturbação do estado da moeda, já que foram as suas cópias que foram medidas! Entretanto, o teorema da não clonagem descarta esta experiência: não é possível copiar informação quântica com absoluta fidelidade, e sem perturbar o estado original.[8, 9]

Para se ter uma idéia do quanto a área da criptografia quântica está evoluindo, a empresa *NEC* em 2004 conseguiu realizar com sucesso um experimento no qual a geração contínua de uma chave criptografica quântica permitiu o envio de informações num canal de dados completamente seguro. A geração de chaves foi feita utilizando uma rede optica como as que existem atualmente (cabos de fibra óptica), à velocidade de 13 Kbps por uma distância de 16 Km. Ao que tudo indica a *NEC* pretende lançar em pouco tempo, um produto comercial que utiliza esta técnica.

4.3 O Algoritmo de Grover

Além da criptografia quântica, existem aplicações da computação quântica ao problema da busca em bancos de dados. Um exemplo a este respeito é fornecido pelos programas de busca na Internet. O algoritmo de Grover nos proporciona um método quântico de acelerar o processo de procura em bancos de dados. No caso do algoritmo de Grover, o ganho não é tão espetacular quanto no caso do algoritmo de Shor. A título de comparação, se o número de etapas envolvidas no algoritmo clássico de busca for 1000, então esta mesma busca poderá ser efetuada com o algoritmo de Grover com um número aproximado de 32 etapas. Mesmo assim, trata-se de um avanço respeitável, levando em conta os terabits em bancos de dados da Internet.

5. IMPLEMENTAÇÃO DE COMPUTADORES QUÂNTICOS

Dados os caminhos para potenciais aplicações para processamento de informações quânticas, como é possível executá-las em sistemas físicos reais? Na pequena escala de poucos qubits já existem inúmeras propostas de trabalho para dispositivos de processamento de informações quânticas.

Talvez a forma mais fácil de as concretizar seja baseada em técnicas *ópticas*, isto é, de radiação eletromagnética. Dispositivos simples como espelhos e *beamsplitters* podem ser usados para realizar manipulações elementares em fótons. Interessantemente, uma dificuldade maior tem sido produzir fótons separados sucessivamente; experimentalistas têm, ao invés disto, optado por usar esquemas que produzem fótons únicos "de vez em quando", randomicamente, e esperar até que tal evento ocorra. Criptografia quântica, codificação superdensa e teletransporte quântico foram todos realizados usando-se tais técnicas ópticas (ver [11]). Uma vantagem destas técnicas é que fótons tendem a ser portadores altamente estáveis de informação quântica mecânica. Uma desvantagem é que fótons não interagem diretamente uns com os outros. Em ves disto, a interação tem que ser mediada por outra coisa, como um átomo, o que introduz ruído adicional e complicações no experimento. Uma interação *efetiva* entre dois fótons é preparada, que essencialmente funciona em dois passos: o fóton número um interage com o átomo, que por sua vez interage com o segundo fóton, causando uma interação completa entre os dois fótons.

Um esquema alternativo é baseado em métodos que aprisionam diferentes tipos de átomos: existe a *armadilha de íons* (ion trap), em que um pequeno número de átomos carregados são aprisionados em um espaço confinado; e *armadilhas de átomos neutros* (neutral ion traps), para aprisionar átomos desprovidos de carga em um espaço confinado. Esquemas de processamento de informação quântica baseados em armadilhas de átomos usam os átomos para armazenar qubits. Radiação eletromagnética também aparece nestes esquemas (mas de uma forma diferente da qual foi referida na abordagem "óptica" do processamento de informação quântica). Nestes esquemas, fótons são usados para manipular a informação armazenada nos átomos, ao invés de um lugar para armazenar informação. Portas quânticas de um único qubit podem ser executadas aplicando-se pulsos apropriados de radiação eletromagnética a átomos individuais. Átomos vizinhos podem interagir um com o outro via (por exemplo) forças de dipolo que permitem portas quânticas serem efetuadas. Ademais, a natureza exata da interação entre átomos vizinhos pode ser modificada aplicando-se pulsos apropriados de radiação eletromagnética sobre os átomos, dando ao experimentalista controle sobre quais portas são executadas no sistema. Finalmente, medição quântica pode ser efetuada nestes sistemas usando-se a técnica (a muito tempo estabelecida) de *saltos quânticos* (quantum jumps), que implementa com excelente acurácia as medições na base computacional utilizada na computação quântica.

Outra classe de esquemas de processamento de informação quântica é baseado na *Ressonância Magnética Nuclear* (Nuclear Magnetic Ressonance), muitas vezes conhecida pelas suas inicias, NMR. Estes esquemas armazenam informação quântica nos *spins nucleares* de átomos em moléculas, e manipulam esta informação usando radiação eletromagnética. Tais esquemas trazem dificuldades especiais, porque na NMR não é possível acessar diretamente núcleos individuais. Ao invés disto, um número enorme (em torno de 10^5) de moléculas essencialmente idênticas são armazenadas em solução. Pulsos eletromagnéticos são aplicados na amostra, levando cada molécula a responder aproximadamente da mesma forma. Deve-se pensar em cada molécula como sendo um computador independente, e na amostra como contendo um número enorme de computadores trabalhando em paralelo (classicamente). O processamento de informação quântica por NMR enfrenta três dificuldades especiais que a torna diferente de outros esquemas de processamento de informação quântica. Primeiramente, as moléculas são preparadas deixando-as em equilíbrio em temperatura ambiente, que é tão maior que energias de giro de spin que os spins se tornam quase completamente orientados randomicamente. Este fato torna o estado inicial particularmente mais "ruidoso" que o desejável

para processamento de informação quântica[4]. Um segundo problema é que a classe de medições que podem ser usadas em NMR não abrange todas as medições mais gerais de que se gostaria de realizar em processamento de informação quântica. Todavia, para muitas instâncias de processamento de informação quântica a classe de medições permitida na NMR é suficiente. Em terceiro, pelo fato de moléculas não poderem ser individualmente enderessadas na NMR, é natural perguntar-se como qubits individuais podem ser manipulados de maneira apropriada. Felizmente, diferentes núcleos na molécula podem ter propriedades diferentes que os permitem ser individualmente endereçados – ou pelo menos ser endereçados em uma escala suficientemente granular para permitir as operações essenciais da computação quântica [11]. Resultados muito prósperos já foram alcançados pelo IBM Almaden Research Center [10], onde uma máquina quântica de sete átomos e NRM, foi construído com sucesso e executou corretamente o algoritmo de Shor, fatorando o número 15. Esse computador utilizou cinco átomos de flúor e dois de carbono.

6. CONCLUSÕES

O campo de computação quântica está crescendo rapidamente, uma vez que várias universidades e companhias de computação estão pesquisando este assunto. Espera-se que este ritmo cresça com o fato de que mais pesquisa tem sido feita em aplicações práticas. Apesar de máquinas práticas estarem anos a frente da nossa atual tecnologia, esta idéia antes apenas imaginária e longínqua tem se tornado cada vez mais tangível. Resultados boms já têm sido obtidos, como a construção de uma máquina quântica funcional através da NMR, pela IBM, ou pelos experimentos em pequena escala envolvendo implementações baseadas em fótons.

Talvez o mais importante desafio a partir de agora é construir um registrador quântico suficientemente grande com qubits individualmente endereçáveis. O que poderá ser visto em um futuro próximo será computações quânticas feitas em registradores quânticos incrementalmente maiores. Métodos como NMR parecem muito adequadas a tais realizações no atual estágio.

Outro desafio seria a concepção de novos algoritmos quânticos. Trata-se de uma tarefa árdua, pois deve-se pensar nas propridades quânticas da matéria para criar os algoritmos. Ademais, os problemas a serem enfrentados devem ser tais que não exista solução correspondente no modelo de computação clássico que seja eficiente, pois seria de certa forma inútil o esforço empregado em se achar um algoritmo quântico.

Enfim, há muito o que ser descoberto na área, que é indubitavelmente promissora, tanto na área de arquitetura de computadores, quanto na teoria de computação. As próximas décadas nos mostrarão os rumos que esta teoria tomará.

7. REFERÊNCIAS

[1] P. H. Artur Ekert and H. Inamori. Basic concepts in quantum computation. *Centre for Quantum Computation - University of Oxford*, Janeiro 2000.

[2] A. Barenco, A. Ekert, A. Sanpera, and C. Machiavello. A short introduction to quantum computation. *La Recherche*, Novembro 1996.

[3] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Royal Society of London*, 1985.

[4] D. Deutsch. It from qubit. *Centre for Quantum Computation, Clarendon Laboratory - University of Oxford*, Setembro 2002.

[5] D. Deutsch. Qubit field theory. *Centre for Quantum Computation, Clarendon Laboratory - University of Oxford*, Janeiro 2004.

[6] D. Deutsch and A. Ekert. Machines, logic and quantum physics. *Centre for Quantum Computation, Clarendon Laboratory - University of Oxford*, Novembro 1999.

[7] D. Deutsch and P. Hayden. Information flow in entangled quantum systems. *Centre for Quantum Computation, Clarendon Laboratory, University of Oxford*, Junho 1999.

[8] A. Ekert. Quantum cryptoanalysis - introduction. Março 1995.

[9] A. Ekert. What is quantum cryptography. Março 1995.

[10] N. Gershenfeld and I. L. Chuang. Quantum computing with molecules. *IBM Almaden Research Center*.

[11] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[12] R. Portugal, C. C. Lavor, L. M. Carvalho, and N. Maculan. Uma introdução à computação quântica. 2004.

[13] A. Steane. Quantum computing. Julho 1997.

[14] A. M. Steane. A quantum computer only needs one universe. *Centre for Quantum Computation, Department of Atomic and Laser Physics, University of Oxford*, Outubro 2002.

[15] U. Vazirani. Quantum physics & church-turing. *Notas de aula de Computação Quântica*, 1997.

[4]Este ruído pode ser superado pelo que se conhece por *correção de erros quântica*.

APÊNDICE

A. O COMPUTADOR UNIVERSAL QUÂNTICO

O computador quântico é primeiramente uma máquina que é uma construção teórica, cujo propósito é permitir o processamento de informação quântica ser analisado formalmente. Em particular, ele estabelece o Princípio de Church-Turing introduzido na seção 2. Eis uma "receita" para um computador quântico, baseada naquela de Deutsch:

Um computador quântico é um conjunto de n qubits sobre os quais as seguintes operações são experimentalmente possíveis:

1. Cada qubit pode ser preparado em algum estado $|0\rangle$.
2. Cada qubit pode ser medido na base $\{|0\rangle, |1\rangle\}$.
3. Uma porta quântica universal (ou conjunto de portas) pode ser aplicada para qualquer subconjunto de tamanho fixo dos qubits.
4. Os qubits não evoluem a não ser via as tranformações supracitadas.

Esta "receita" circunda as idéias principais. O modelo físico de computação para se projetar tal computador é o modelo em malha (*network model*), em que portas lógicas quânticas (ver seção 3.4) são aplicadas seqüencialmente em um conjunto de qubits. Em um computador clássico eletrônico, portas lógicas estão espalhadas espacialmente em uma placa de circuitos, mas no computador quântico, tipicamente imagina-se as portas lógicas como interações ligadas e desligadas no *tempo* (como já foi explicado), com os qubits em posições fixas [13].