Computação Quântica

Rodrigo Minetto
Instituto de Computação
Universidade Estadual de Campinas
Campinas, São Paulo, Brasil
ra049243@ic.unicamp.br

RESUMO

Computadores tradicionais são acreditados serem máquinas de grande eficiência, pois as computações requeridas são realizadas em um tempo aceitável. Isto pode não ser verdade quando a computação quântica é levada em consideração.

O objetivo deste artigo é dar uma introdução à Computação Quântica. Alguns algoritmos ilustrarão o poder potencial da computação quântica. Por exemplo, para o problema de fatoração de números inteiros não há nenhum algoritmo clássico eficiente que o resolva, entretanto Peter Shor descobriu um eficiente algoritmo quântico polinômial para resolver o problema.

Outros aspectos básicos interessantes serão abordados, tais como mecânica quântica, bit quântico, portas lógicas quânticas e os potenciais ganhos de desempenho da computação quântica em relação a computação tradicional.

Palavras-Chave

Computação Quântica, Qubit, Algoritmo de Shor, Criptografia Quântica.

1. INTRODUÇÃO

Problemas de propagação de ondas em antenas de telefonia móvel, seqüenciamento genético, previsão de clima e renderização de filmes e imagens pertencem a diferentes áreas da ciência e têm em comum a complexidade de cálculos e necessidade de supercomputadores de grande capacidade de processamento para resolvê-los.

Computadores quânticos, dispositivos que usam as leis da mecânica quântica para processar informações, provocam na atualidade grande entusiasmo por suas potenciais capacidades de processamento, devido ao paralelismo quântico, matematicamente demonstradas, e porque foram experimentalmente testadas em laboratórios com diversos sistemas quânticos: fótons, spins nucleares, armadilha de íons, átomos em cavidade [6, 12], etc.

A grande esperança é que computadores quânticos, num estágio de desenvolvimento ainda longe do atual, possam resolver alguns problemas de grande complexidade computacional de uma maneira eficiente. A computação quântica se mostra bastante eficiente na resolução de alguns problemas antes tidos como intratáveis.

Este estudo tem por objetivo dar uma visão geral desse novo paradigma de computação: a computação quântica, [5, 11, 1].

O artigo é dividido como segue. Na seção 2 são apresentados os principais conceitos da computação quântica. A seção 3 discute as abordagens atuais para a construção de computadores quânticos. As idéias de dois importantes algoritmos quânticos são apresentadas na seção 4. As potenciais vantagens da computação quântica sobre a computação clássica são abordadas na seção 5. Finalmente, na seção 6 são apresentadas as conclusões deste artigo.

2. CONCEITOS

Nesta seção aborda-se os principais conceitos necessários aos estudos da computação quântica.

2.1 Mecânica Quântica

A *mecânica clássica* ou *mecânica newtoniana*, foi a primeira tentativa de descrever o comportamento mecânico dos objetos. Seu principal objetivo era estabelecer as regras da física para os objetos que realizam algum tipo de movimento e analisar as forças que atuam sobre estes.

No entanto, por meio de experimentos, cientistas observaram que as leis da mecânica clássica, não se aplicavam aos movimentos de objetos muito pequenos, nesta linha limite estão os objetos que são aproximadamente 100 vezes maiores que o átomo de hidrogênio. Surge então, a teoria da *mecânica quântica* que descreve o comportamento da matéria em seus componentes básicos tal como átomos, moléculas e núcleos, que por sua vez são compostos pelas partículas elementares.

Diferentemente do sistema clássico, onde os estados são caracterizados por valores bem definidos das grandezas físicas mensuráveis, tal como velocidade, posição e energia, determinar o estado de um sistema quântico corresponde a especificar probabilidades de encontrar determinados valores

para as grandezas físicas mensuráveis. Existe uma incerteza intrínsica (*incerteza de Heisenberg*) que descreve matematicamente o sistema como uma superposição coerente de estados distintos. A incerterza de Heisenberg diz que não se pode medir com segurança as propriedades básicas do comportamento subatômico. Deste modo, começa a se notar a impossibilidade de conhecer com infinita acuidade a posição e velocidade de uma partícula em um dado instante no tempo.

Usualmente, um sistema quântico é representado por um *espaço de Hilbert*, que denota um espaço vetorial complexo com produto escalar de dimensão talvez infinita.

2.2 Quantum Bit

A estrutura básica de informação na computação clássica é o bit, a estrutura análoga na computação quântica é o *quantum bit* ou *bit quântico*, também conhecido com *qubit*.

Um qubit é um estado quântico $|\psi\rangle$ da forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

onde α e $\beta \in \mathbb{C}$. Ou seja, o qubit $\psi\rangle$ pode colapsar na base $|0\rangle$ com probabilidade α^2, ou na base $|1\rangle$ com probabilidade β^2.

Um bit clássico é descrito de acordo com seu estado, 0 ou 1. Analogamente, um qubit é descrito de acordo com seu estado quântico. Dois estados quânticos possíveis para um qubit correspondem aos 0 e 1 de um bit clássico. Na mecânica quântica, no entanto, qualquer objeto que tenha dois estados diferentes, possui necessariamente diversos outros estados possíveis denominados sobreposições, dos quais resultam a existência de ambos os estados em graus variáveis.

Os estados dos qubits correspondem a pontos sobre a superfície de uma esfera, onde o 0 e 1 correspondem aos pólos sul e norte respectivamente. O contínuo de estados entre 0 e 1 dá origem a muitas das propriedades extraordinárias da informação quântica.

Pode-se codificar uma quantidade infinita de informações clássicas num único qubit, [8], mas não há como extrair essa informação. A mais simples tentativa de ler o estado do qubit, uma mensuração usual direta, resultará em 0 ou 1. Qualquer mensuração adotada apaga todas as informações contidas no qubit, à exceção do único bit que ela revela. Entretanto qualquer informação oculta que o qubit contenha é passível de manipulação, deste modo computações interessantes podem ser realizadas e a mensuração só ocorrerá quanto a computação estiver determinada.

A diferença entre as representações do bit clássico e o bit quântico pode ser visualizada na figura 1.

2.3 Portas Lógicas Quânticas

Qualquer ação computacional pode ser traduzida em termos de portas lógicas, fisicamente, um porta lógica consiste de alguns elementos de circuitos conectados entre si, onde o sinal observado na saída depende de uma determinada relação lógica entre os sinais da entrada.

Em um computador clássico, existem três portas lógicas elementares, NOT, AND e OR. Qualquer operação lógica pode ser construída a partir de combinações dessas portas. Uma porta lógica importante obtida através das elementares é a porta lógica XOR. A tabela 1 mostra o resultado dessas operações sobre os bits A e B.

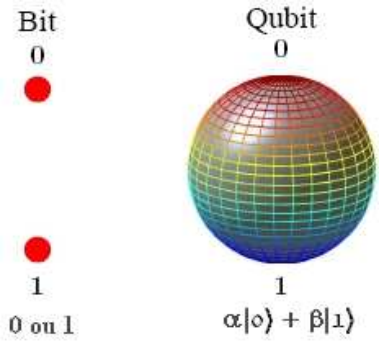

Figure 1: Estados do bit clássico e quântico.

Table 1: Tabela verdade para algumas operações lógicas.

A	B	A AND B	A OR B	NOT A	A XOR B
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	0	0

O princípio fundamental na mudança de estados em um sistema quântico são as transformações unitárias, que são transformações lineares inversíveis e cuja inversa é igual a sua conjugada transposta. Deste modo, vetores de estado são transformados por matrizes unitárias. Estas transformações são inerentes a qualquer sistema quântico dinâmico.

Em 1995, Barenco et al [3], mostraram que analogamente ao sistema clássico, é possível obter qualquer ação do computador quântico através de portas lógicas quânticas elementares. Estes também demonstraram que a porta XOR quântica, é a única porta de dois qubits necessária para se construir qualquer outra. As portas lógicas quânticas podem ser de um, dois ou n qubits.

A porta lógica quântica mais simples é a porta NOT. Esta porta lógica, denotada por Q-NOT, atua sobre um único qubit, e troca-o de estado

$$\text{Q-NOT}|0\rangle = |1\rangle \qquad \text{Q-NOT}|1\rangle = |0\rangle \tag{2}$$

A matriz de transformação para esta operação é dada por

$$\text{Q-NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3}$$

$$\text{Q-NOT}(|0\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle \tag{4}$$

onde $|0\rangle$ e $|1\rangle$ são definidos como os vetores $(1,0)^T$ e $(0,1)^T$ respectivamente. O conjunto $(|0\rangle, |1\rangle)$ forma uma base do

espaço de Hilbert associado com o qubit, que é chamada de base computacional.

A porta lógica quântica XOR atua diferente da sua respectiva porta lógica clássica. Esta porta modifica o estado de um dos qubits, chamado de qubit alvo, de forma condicionada ao estado do outro, chamado de qubit de controle. Se o estado do qubit de controle for zero o qubit alvo é mantido, caso contrário este é trocado. A aplicação da Q-XOR sobre os estados da base computacional produz

$$\text{Q-XOR}|00\rangle = |00\rangle \qquad \text{Q-XOR}|01\rangle = |01\rangle \tag{5}$$

$$\text{Q-XOR}|10\rangle = |11\rangle \qquad \text{Q-XOR}|11\rangle = |10\rangle \tag{6}$$

Uma consequência importante do fato das transformações quânticas serem unitárias é que elas são reversíveis, ou seja, podemos reverter a computação realizada. Computadores clássicos por outro lado, são expressos em passos que não são reversíveis. Por exemplo, não é possível recuperar a entrada depois de aplicar a porta AND clássica, caso esta não esteja armazenada em memória.

3. COMPUTADOR QUÂNTICO

Para se construir um hardware para um computador quântico, é necessário uma tecnologia que manipule os qubits. Deste modo, este hardware deve possuir os seguintes requisitos necessários

- armazenamento: os qubits precisam ser armazenados por períodos de tempo suficientes para completar as computações;
- isolamento: os qubits precisam estar isolados do ambiente para evitar erros por decoerência;
- leitura: é necessário que se possa realizar uma leitura de forma eficiente e confiável nos qubits;
- portas lógicas quânticas: é necessário a manipulação de qubits individuais e permitir a interação controlada entre eles;
- precisão: o hardware desenvolvido deve ser de alta precisão caso o dispositivo seja desenvolvido para cálculos confiáveis;
- inicialização: habilidade de preparar o sistema quântico a partir de um estado inicial, tal como o estado fundamental;
- controle: habilidade para submeter o sistema quântico a uma sequência controlável de transformações unitárias.

As três abordagens para a implementação de um computador quântico, que estão sendo investigadas, são descritas a seguir.

3.1 Armadilha de Íons

Nesta abordagem cada qubit é representado por um íon aprisionado em uma armadilha linear. O estado quântico vibracional de cada íon é uma combinação linear do estado fundamental $|0\rangle$ e um estado excitado metaestável de longa duração interpretado como $|1\rangle$.

Nesta abordagem os íons podem ser muito bem isolados e a leitura destes pode ser realizada através de um laser. Quando o laser ilumina os íons, cada qubit no estado $|0\rangle$ absorve e reemite a luz do laser e assim fluoresce. Por outro lado, os qubits no estado $|1\rangle$ permanecem escuros.

Devido a um fenômeno fisíco denominado repulsão mútua de Coulomb os íons são suficientementes separados de modo que eles podem ser individualmente endereçados por pulsos de laser. Através da determinaçao correta do tempo de duração do pulso do laser e pela escolha da fase apropriada para este, os pulsos de laser podem preparar qualquer combinação linear de $|0\rangle$ e $|1\rangle$.

No entanto a parte mais complicada no desenvolvimento e construção do hardware é realizar a interação dos qubits para a construção de portas lógicas.

3.2 Eletrodinâmica Quântica de Cavidade

A idéia desta abordagem é aprisionar vários átomos nêutros dentro de uma cavidade ótica de altíssima qualidade. A informação quântica pode, então, ser armazenada dentro dos estados internos dos átomos.

Os átomos interagem indiretamente através do seu acoplamento com o modo normal do campo eletromagnético na cavidade, ou, pode-se também, armazenar um qubit na polarização de um fotón, tal como é realizado pelo laser na figura 2.

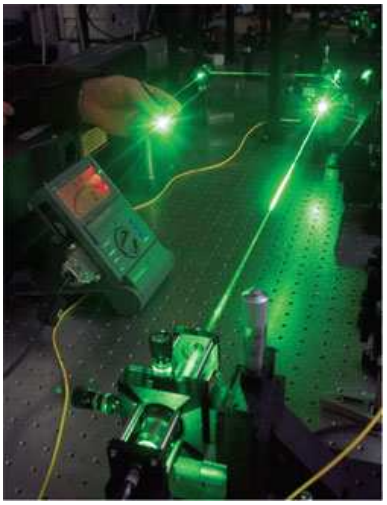

Figure 2: Tecnologias que envolvem estados quânticos, para a construção de um futuro computador quântico comercial. Canhão de laser para polarização de fótons.

Através da sintonização de transições com pulsos a laser, pode-se induzir a transição em um átomo que está condicionado ao estado interno de outro átomo.

3.3 Ressonância Magnética Nuclear

A ressonância magnética nuclear é atualmente a abordagem mais promissora, nesta abordagem os qubits são spins nucleares em moléculas particulares. Cada spin pode estar alinhado ou anti-alinhado caso um campo magnético seja aplicado constantemente. Deste modo, os spins demoram um longo período até se tornarem incoerentes. Assim é possível, que os qubits sejam armazenados por um período de tempo considerável.

Através de um campo magnético oscilatório podem ser realizadas transformações unitárias sobre os spins. As leituras podem ser feitas através da medição do sinal de voltagem induzido pelo momento magnético precedente.

Atualmente já se consegue desenvolver dispositivos de 3-qubits com esta tecnologia.

4. ALGORITMOS QUÂNTICOS

Nesta seção são apresentados dois algoritmos quânticos. Existem vários, os mais importantes são mostrados na figura 3. Esta figura também mostra como os cientistas estão mapeando a vasta topografia da computação quântica. Alguns processos mais simples, como o de teleportação e criptografia quântica são bem compreendidos. Em constraste, fenômenos complexos como o da correção de erros quânticos, algoritmo de Shor, algoritmo de Groove e a transformada quântica de Fourier continuam cercadas de grandes áreas ainda não compreendidas.

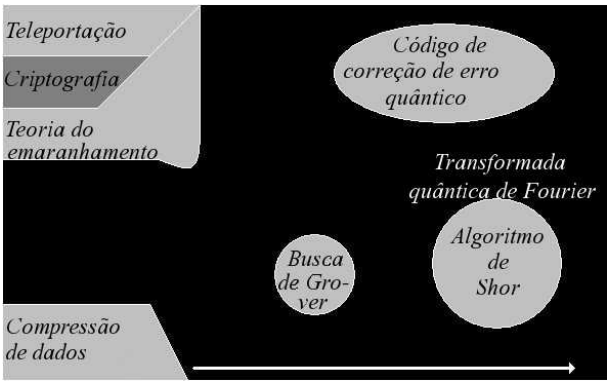

Figure 3: Topografia da computação quântica. Alguns processos mais simples, como o de teleportação e criptografia quântica são bem compreendidos. Em constraste, fenômenos complexos como os algoritmos de Shor e Groove continuam cercados por grandes áreas ainda não compreendidas. Figura adaptada de [8].

Os algoritmos quânticos possuem propriedades importantes que os respectivos algoritmos clássicos não possuem. Por exemplo, o algoritmo para o envio de uma chave criptográfica pode detectar se algum intruso, interceptou a transmissão, [10]. Já outros dois algoritmos são melhores levando em consideração o tempo em que podem resolver certos problemas. Na computação, as duas principais classes de algoritmos são: a classe polinomial e a exponencial. Um algoritmo é dito polinomial quando o número de operações elementares que ele emprega é limitado superiormente por αn^{λ}, e exponencial quando limitado superiormente por $\alpha\lambda^{n}$, onde n é o tamanho da entrada, e α e λ são constantes positivas quaisquer.

O algoritmo de Shor resolve o problema da fatoração de números primos em tempo polinomial onde a melhor versão clássica leva tempo exponencial. Já o algoritmo de Lov Groover [7], realiza uma pesquisa em uma lista não estruturada de n-itens com tempo $O(\sqrt{n})$ passos em um computador quântico. No caso clássico, a mesma pesquisa é realizada em $O(n)$ passos. Contudo a técnica de Groover fornece um aumento de velocidade polinomial mas não exponencial como no caso de Shor. Ainda assim é um grande avanço, que indica uma vantagem dos computadores quânticos sobre os clássicos.

4.1 Fatoração de Números Primos

Em 1994, Peter Shor obteve resultados inéditos em algoritmos quânticos, mostrando que problemas de fatoração de números inteiros compostos podem ser resolvidos em tempo polinomial em um computador quântico [9], a intratabilidade computacional desses problemas para os computadores clássicos é o padrão computacional assumido pela criptografia moderna para garantir a segurança de sistemas criptográficos. O resultado de Shor foi o principal motivo que alavancou o interesse pela computação quântica no mundo.

Para ilustrar o caráter exponencial da fatoração de números primos podemos considerar o seguinte caso: Seja um número composto n. Um método para determinar dois fatores primos de n consiste em aplicar o seguinte algoritmo clássico: dividir n por cada um dos termos de 1 a $\sqrt{n}$. Este procedimento precisa de $\sqrt{n}$ operações, mas como o número n pode possuir log$n$ dígitos têm-se que este processo precisa $2^{(\log n)/2}$ passos. Pode-se dizer que este processo é exponencial no número de dígitos de n.

Os algoritmos clássicos mais eficientes que resolvem o problema da fatoração utilizam o fato que este problema pode ser reduzido a encontrar o período de uma função. O algoritmo de Shor também utiliza essa redução.

O algoritmo de Shor é executado em $O(\log n)$ passos em um computador clássico e $O((\log n)^2 \log\log n)$ passos em um computador quântico. O algoritmo é definido da seguinte forma

```
Algoritmo SHOR (n)
1 escolha um inteiro 1 < x < n aleatoriamente
2 se mdc (x, n) > 1
3    então devolva mdc (x, n)
4 seja r o período da função f(a) = x^a mod n
5 se r for ímpar ou x^r/2 = -1 (mod n)
6    então o procedimento falhou
7 devolva mdc(x^r/2 + 1, n)
```

onde n é o número a ser fatorado.

Os passos de 1 a 3 procuram achar um co-primo ao número n. Pois se o mdc(x, n) for maior que 1 e x é menor que n logo o resultado do mdc é um dos fatores primos que compõe n. Estes passos podem ser executados em um computador clássico.

O passo quântico necessário ao algoritmo está em calcular o período da função presente na linha 4 do algoritmo. Para isto é necessário criar um registrador quântico com duas partes $|\psi\rangle = |0\rangle|0\rangle$, na primeira parte do registrador, o algoritmo coloca uma sobreposição de inteiros os quais são os a's da função f(a), serão escolhidos os a's para serem inteiros de 0 até $q-1$, onde q é uma potência de dois, tal que $n^2 < q < 2n^2$, o q deve escolhido neste intervalo para que a aproximação na *transformada quântica de fourier* seja suficientemente boa. Então o algoritmo calcula $x^a \mathrm{mod} n$ para cada número armazenado na primeira parte do registrador quântico e armazena o resultado na segunda parte do registrador. Devido ao paralelismo quântico, esta etapa é feita em apenas um passo, pois o computador quântico calcula $x^{|a\rangle} \mathrm{mod} n$. Com mais alguns passos, inclusive executando a transformada quântica de fourier é possível determinar os fatores primos que constituem um dado n em tempo polinomial.

Caso o passo 5 seja verdadeiro, ou seja, r é ímpar, implica que não é possível decompor f(a) assim é necessário retornar ao passo 1 e escolher um x diferente do que havia sido escolhido.

A tabela 2 contém estimativas do tempo de fatoração de vários tamanhos de números usando o algoritmo clássico e o de Shor, onde ambos os algoritmos estão sendo processados a uma velocidade de 100MHz.

Table 2: Tempo de fatoração para diversos tamanhos de números utilizando o algoritmo de Shor e o clássico.

N. de bits do inteiro n	Algoritmo de Shor	Algoritmo Clássico
512	3.4 seg	10^4 anos
1024	4.5 seg	10^{10} anos
2048	36 min	10^{19} anos
4096	4.8 horas	10^{31} anos

4.2 Criptografia Quântica

Ao contrário da criptografia atual, a criptografia quântica deve continuar segura quando os computadores quânticos se expadirem.

Um modo de enviar uma chave quanticamente criptografada entre emissor e receptor requer que um laser transmita fótons isolados que podem ser polarizados de dois modos. No primeiro, os fótons são posicionados verticalmente ou horizontalmente (modo retilíneo). No segundo, são orientados 45 graus à esquerda ou à direita da vertical (modo diagonal). Em ambos os modos, as posições opostas dos fótons representam os bits 0 e 1, tal como pode ser visualizado na figura 4.

O emissor, que os criptográfos por convenção chamam de Alice, envia um sequência de bits, optando aleatoriamente por enviar os fótons no modo retilíneo ou diagonal. O receptor, chamado de Bob, toma uma decisão igualmente aleatória do modo como medirá os bits que chegam. O princípio da incerteza de Heisenberg impõe que ele só pode medir os bits em um dos modos, e não em ambos. Somente os bits que Bob mediu da mesma maneira como foram enviados por Alice estarão com certeza na direção correta, preservando assim o valor apropriado.

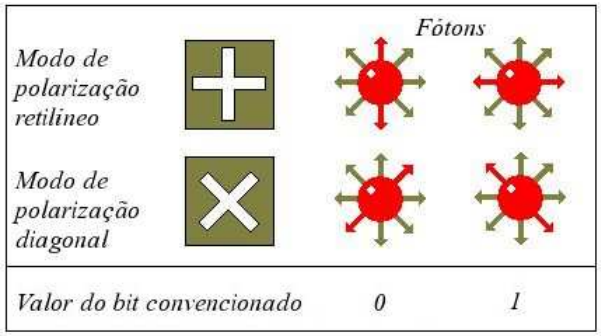

Figure 4: Filtros de detecção para a recepção de fotóns.

Se algum espião tentar interceptar esse fluxo de fotóns e realizar a medição no modo errado, mesmo que o espião reenvie os bits a Bob exatamente como os viu, este introduzirá erros no sistema. Alice e Bob podem detectar a presença de espiões comparando bits selecionados para ver se contêm erros, a ilustração do esquema pode ser visualizada na figura 5.

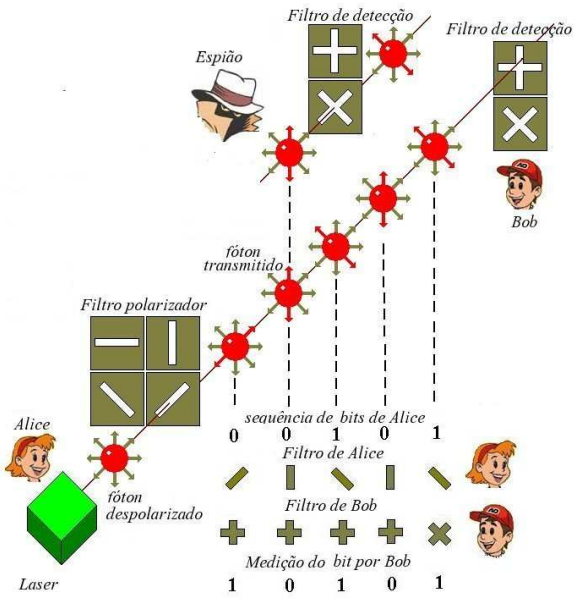

Figure 5: Para evitar que espiões, obtenham uma chave criptográfica, Alice e Bob a enviam através de fótons emitidos por um laser e polarizados com um filtro. Qualquer interceptação do sistema pode ocasionar erros no sistema. Figura adaptada de [10].

Finalmente após a transmissão, Bob se comunica com Alice, figura 6, diálogo que não precisa ser secreto, para informar qual dos dois modos usou para receber cada fóton. Mas ele não revela o valor 0 ou 1 representado por cada fóton. Alice então informa a Bob quais modos foram medidos corretamente. Ambos ignoram os fótons que não foram observados do modo correto. Os modos medidos corretamente constituem a chave criptográfica que serve como entrada de dados

para um algoritmo usado para criptografar e decifrar a mensagem.

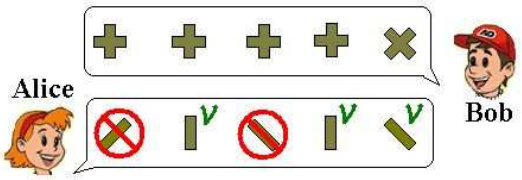

Figure 6: Diálogo entre Alice e Bob, não necessariamente secreto, para definir a chave criptográfica.

5. COMPUTADORES CLÁSSICOS X COMPUTADORES QUÂNTICOS

Um computador clássico com três bits de memória pode apenas armazenar três caracteres (uns ou zeros). Um computador quântico pode armazenar 16 valores analógicos em pares para formar 8 números complexos. Em um dado instante, ele poderia conter os valores listados na tabela 3.

A primeira coluna mostra todos os estados possíveis para os três bits. Um computador clássico apenas suporta um destes padrões de cada vez. Um computador quântico pode colocar-se na sobreposição de assumir os 8 estados ao mesmo tempo. A segunda coluna mostra a "amplitude" para cada um dos 8 estados. Estes 8 números complexos são uma imagem dos conteúdos de um computador quântico num determinado momento. Durante a computação, estes 8 números irão modificar e interagir uns com os outros, a interação entre dois ou mais sistema quânticos, aqui representados por bits, é conhecida na física como *emaranhamento* e dita que o estado final de um sistema pode depender do estado final de outro. Neste sentido, um computador quântico de 3-qubits tem muito mais memória do que um computador clássico de 3-bits.

No entanto, não existe nenhuma forma de ver diretamente estes 8 números. Quando o algoritmo é terminado, é feita uma medição. A medida fornece uma simples linha de 3-bits, e elimina todos os 8 números complexos. A linha fornecida é gerada aleatoriamente. A terceira coluna da tabela calcula a probabilidade de cada linha. Neste exemplo, há uma probabilidade de 14% de que a linha fornecida seja "000" , de 4% de que seja "001" , e assim sucessivamente. Cada probabilidade é encontrada com a execução da raiz quadrada do número complexo.

Um algoritmo num computador quântico irá dar início a todos os números complexos de modo a se equivalerem a valores, por isso todos os estados terão probabilidades equivalentes. A lista de números complexos pode ser vista como um vetor de 8 elementos. Em cada passo do algoritmo, esse vetor é modificado ao multiplicá-lo por uma matriz que advém da própria máquina, matriz esta que implementa as portas lógicas quânticas.

Esta operação pode ser realizada disparando um curto pulso de radiação em um recipiente de moléculas. Diferentes tipos de pulsos resultam em diferentes matrizes. O algoritmo para o computador quântico consiste em que pulsos usar e em que ordem. A sequência é usualmente escolhida de modo que todas as probabilidades tendam a zero exceto uma. Essa probabilidade não nula corresponde à linha que contém a resposta correta. Para um dado algoritmo, as operações serão sempre feitas na mesma ordem. Não existe regras "if then" para variar a ordem, já que não há maneira de ler a memória antes da medição final.

Table 3: Probabilidade de retorno de uma sequência de 3-bits caso seja efetuada uma medição.

Estado	Amplitude	Probabilidade
*	$a + ib$	$(a^2 + b^2)$
000	$0.37 + i0.04$	0.14
001	$0.11 + i0.18$	0.04
010	$0.09 + i0.31$	0.10
011	$0.30 + i0.30$	0.18
100	$0.35 + i0.43$	0.31
101	$0.40 + i0.01$	0.16
110	$0.09 + i0.12$	0.02
111	$0.15 + i0.16$	0.05

Do ponto de vista do aumento exponencial de velocidade oferecido por computadores quânticos para certos problemas computacionais, é natural perguntar se computadores quânticos podem resolver problemas NP-completo (subconjunto dos "mais difíceis" problemas não-determinísticos polinomiais) em tempo polinomial. Um resposta afirmativa teria grande consequência, uma vez que vários importantes problemas computacionais se incluem nesta categoria. Entretanto, pesquisas mostraram [4, 2], que uma máquina de turing quântica (uma máquina de turing é um modelo abstrato de um computador, que se restringe apenas aos aspectos lógicos do seu funcionamento) deve levar tempo exponencial para resolver problemas NP-completo. O que aparenta excluir a possibilidade de descobrir um algoritmo quântico eficiente para esta classe de problemas.

6. CONCLUSÃO

Ainda não está claro para a tecnologia presente se será possível suportar um computador quântico no futuro. Entretanto a tentativa de construção deste será de suma importância tanto para áreas teóricas como para as áreas experimentais.

Mas embora os computadores quânticos possam ser ordens de grandeza mais rápidos que os computadores clássicos, estes ainda, não podem solucionar problemas que os computadores clássicos não conseguem resolver tendo memória e processamento suficientes, pois uma máquina de turing pode simular um computador quântico. Deste modo, a existência de computadores quânticos não pode refutar a tese de Church-Turing, que enuncia que qualquer função que seria naturalmente considerada computável pode ser computada por uma máquina de Turing.

E finalmente, é importante conhecer os limites de nossas abilidades experimentais em controlar a natureza no nível quântico, e as investigações nesta área fundamental justificam todos os esforços na direção da computação quântica.

A história da tecnologia da computação tem envolvido uma

sequência de mudanças, de um tipo de realização física para outro, de válvulas até transitores até circuitos integrados e assim por diante. O passo para a estrutura molecular - nível quântico - está sendo o próximo.

7. REFERÊNCIAS

[1] F. L. Alves. Computação Quântica - Fundamentos Físicos e Perspectivas. Mografia de Graduação - Universidade Federal de Lavras.

[2] A. Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 636–643, 2000.

[3] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

[4] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *IEEE Symposium on Foundations of Computer Science*, pages 352–361, 1998.

[5] J. J. D. Bulnes. Emaranhamento e Separabilidade de Estados em Computação Quântica por Ressonância Magnética Nuclear. Tese de Doutorado - Centro Brasileiro de Pesquisas Físicas.

[6] J. I. Cirac, L. M. Duan, and P. Zoller. Quantum optical implementation of quantum information processing. *Proceedings of the International School of Physics Enrico Fermi*, page 263, 2002.

[7] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219, Maio 1996.

[8] M. A. Nielsen. Regras para um mundo quântico complexo. In *Scientific American Brasil*, volume 7, pages 80–89, Dezembro 2002.

[9] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.SCI.STATIST.COMPUT.*, 26:1484, 1997.

[10] G. Stix. Os segredos mais bem guardados - Criptografia Quântica. In *Scientific American Brasil*, volume 33, pages 38–45, Fevereiro 2005.

[11] A. L. Vignatti, F. S. Netto, and L. F. Bittencourt. Uma Introdução a Computação Quântica. Mografia de Graduação - Universidade Federal do Paraná.

[12] P. Zoller, J. I. Cirac, L. Duan, and J. J. Garcia-Ripoll. Implementing quantum information processing with atoms, ions and photons. *Lecture notes from Les Houches Summer School*, pages 0–14, 2003.