Introdução à Computação Quântica

Conrado Porto Lopes Gouvêa
RA 079724
Instituto de Computação - Universidade Estadual de Campinas
conradoplg@gmail.com

RESUMO
A computação quântica é uma área que tem o potencial de revolucionar o campo da computação. O nascimento da mecânica quântica no início do século XX teve profundas implicações em diversas áreas da ciência e influenciou a computação com a descoberta de que computadores baseados em fenômenos quânticos, ou computadores quânticos, eram capazes de realizar cálculos considerados intratáveis na computação clássica. Estre trabalho propõe fornecer uma introdução ao assunto, expondo os fundamentos da mecânica quântica relevantes, descrevendo como seria a arquitetura de um computador quântico e suas propriedades. Também descrevem-se algoritmo quânticos capazes de uma performance maior comparada a seus equivalentes clássicos.

Palavras-chave
Computação quântica, algoritmo quântico, arquitetura de computadores

1. INTRODUÇÃO
A teoria da mecânica quântica surgiu no século XX para explicar certos experimentos realizados que envolviam questões importantes da física - como, por exemplo, a aparente natureza dual da luz na forma de partícula e de onda. Apesar de sua complexidade (de fato, Richard Feynman escreveu: "Acredito que posso dizer com segurança que ninguém entende a física quântica" [7]), o campo continuou a crescer com o decorrer do século.

Paralelamente, Alan Turing concebeu o modelo matemático da máquina de Turing, que foi a base para a criação dos computadores. Baseados primeiramente em válvulas, evoluindo para transistores e circuitos integrados, os computadores aumentaram rapidamente de capacidade. Porém, sabia-se que tal crescimento um dia teria um fim, caso a mesma tecnologia fosse mantida. Nesse cenário, começou a se estudar se seria possível usar a mecânica quântica para conceber uma máquina computacionalmente mais poderosa que os computadores tradicionais - implementações da máquina de Turing, e que utilizam em sua maior parte apenas conceitos da física clássica.

Em 1984, David Deutsch publicou um artigo onde modelava uma máquina de Turing quântica. Ele mostrou que ela possuía propriedades que seriam incapazes de serem modeladas por uma máquina de Turing tradicional ao explorar o conceito chamado paralelismo quântico. De acordo com o autor, no futuro tal modelo poderia ser concretizado numa máquina real: o computador quântico [3].

Contudo, a incerteza do que um computador quântico realmente seria capaz fez com que o campo não se desenvolvesse rapidamente. Porém, em 1994, Peter Shor causou grande surpresa ao conceber um algoritmo quântico para fatorar números inteiros em tempo polinomial. Como a dificuldade do problema de fatoração (não se conhece nenhum algoritmo clássico polinomial para resolvê-lo [6]) serviu de base para muitos sistemas de criptografia assimétrica, a invenção de Shor teve um enorme impacto. Ela implicava que, quando fosse construído um computador quântico capaz de rodar o algoritmo, um grande número de sistemas criptográficos estariam quebrados (incluindo o RSA, utilizado largamente para comunicações seguras na internet).

O algoritmo de Shor foi a causa de uma grande corrida subseqüente para construir fisicamente o modelo criado por Deutsch. Já no fim dos anos 90 foram realizadas as primeiras computações quânticas, baseadas no armazenamento de informações no spin de átomos e sua manipulação através de ressonância magnética nuclear [2]. Outras arquiteturas também foram propostas e estão sendo estudadas.

2. FUNDAMENTOS
Para ilustrar alguns aspectos fundamentais da mecânica quântica, é possível realizar o seguinte experimento [12]. Os equipamentos necessários são uma fonte de luz e três filtros polaróides. Polaróides são capazes de filtrar luz não polarizada: como se sabe, a luz é composta de ondas, que possuem uma certa "direção" (polarização). Normalmente, a luz é não polarizada, o que significa dizer que emite ondas em direções aleatórias. Com o filtro polaróide, é possível obter luz polarizada numa única direção.

2.1 O Experimento
O experimento consiste, primeiramente, em observar o resultado de se colocar um filtro A (polarizado horizontalmente)

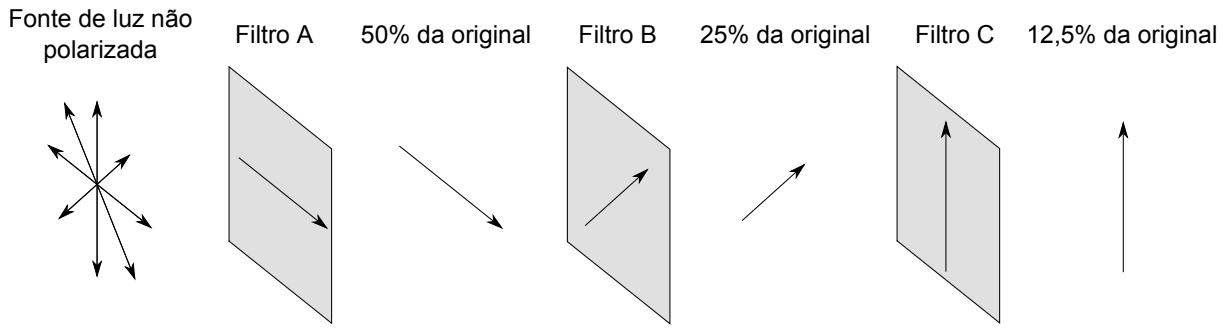

Figura 1: O resultado inesperado no experimento de três filtros

diante da fonte de luz. A saída obtida é luz polarizada horizontalmente. Aí já obtemos um resultado pouco intuitivo: espera-se que apenas uma pequena fração da luz original tenha a polarização "certa" para atravessar o filtro, mas o que se observa é que cerca de 50% da luz original atravessa o filtro.

Em seguida, coloca-se um filtro C polarizado verticalmente diante da saída do filtro A. Como a luz que ele recebe é polarizada horizontalmente, espera-se que nada consiga atravessá-lo. De fato, é o que acontece.

Porém, quando se coloca um filtro B polarizado em 45 graus entre A e C, obtém-se um resultado totalmente inesperado. Intuitivamente imagina-se que a adição de um novo filtro não irá alterar a saída do filtro C - que é de nenhuma luz. Mas o que acontece é a luz consegue atravessar C numa proporção de cerca de 12,5%. Este cenário é ilustrado na figura 1.

2.2 A Explicação

A polarização de um fóton pode ser representada por uma combinação linear de dois vetores base unitários: o primeiro representando a polarização horizontal e o outro a vertical (a base é arbitrária, qualquer dois vetores ortogonais unitários poderiam ser utilizados). Dessa forma, a polarização de um fóton pode ser dada por $|\psi\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ onde a e b são números complexos tal que $|a|^2 + |b|^2 = 1$. Diz-se que a polarização do fóton está em superposição dos dois estados: horizontal e vertical.

De acordo com os postulados da mecânica quântica, ao se realizar uma medição do estado do fóton, a superposição é destruída e ele passa a permanecer em um dos dois estados base. Quais são os estados base dependem do mecanismo utilizado na medição; no caso do filtro A, são os vetores horizontal e vertical. Considerando essas bases, a probabilidade de o estado $|\psi\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ ser medido como $|\uparrow\rangle$ é de $|a|^2$ e de ser medido como $|\rightarrow\rangle$ é de $|b|^2$. Adicionalmente, qualquer medição subseqüente utilizando a mesma base irá fornecer o mesmo resultado da primeira medição.

Agora pode-se explicar o que ocorreu no experimento. Um filtro polaróide é capaz de medir o estado quântico do fóton utilizando uma base que consiste na sua polarização e o vetor ortogonal a ela; além disso, ele somente deixa passar fótons cuja polarização medida seja igual à sua polarização. Portanto, o filtro A utiliza as bases $\{|\uparrow\rangle, |\rightarrow\rangle\}$ e deixa passar fótons medidos como estando no estado $|\rightarrow\rangle$. O filtro B utiliza as bases $\{|\nearrow\rangle, |\searrow\rangle\}$ e deixa passar fótons medidos como $|\nearrow\rangle$. Por fim, o filtro C utiliza as bases $\{|\uparrow\rangle, |\rightarrow\rangle\}$ e deixa passar fótons medidos como $|\uparrow\rangle$.

Portanto, como a luz original é polarizada aleatoriamente, metade dos fótons que atravessam A são medidos como horizontalmente polarizados, portanto ele conseguem atravessar o filtro. Caso passem então através do filtro C, como estão no estado $|\psi\rangle = 0\,|\uparrow\rangle + 1\,|\rightarrow\rangle$, serão medidos com 100% de probabilidade como sendo $|\rightarrow\rangle$ e serão totalmente bloqueados pelo filtro, que só deixa passar fótons medidos como $|\uparrow\rangle$. Contudo, caso o filtro B seja colocado entre os dois, ele medirá metade dos fótons no estado $|\rightarrow\rangle$ como estando em $|\nearrow\rangle$; deixando-os passar para o filtro C, que por sua vez medirá metade de tais fótons no estado $|\nearrow\rangle$ como estando em $|\uparrow\rangle$. Portanto, temos que 1/8 da luz original irá passar pela seqüência de filtros.

3. O QUBIT

Um bit quântico, ou qubit, é um vetor unitário num espaço vetorial complexo de duas dimensões com uma base particular fixa, denotada por $\{|0\rangle, |1\rangle\}$. No exemplo anterior, tal base pode corresponder à base $\{|\uparrow\rangle, |\rightarrow\rangle\}$ da polaridade de um fóton. Contudo, outros mecanismos podem ser usados, como o spin de um elétron ou de um núcleo.

Os estados $|0\rangle$ e $|1\rangle$ correspondem aos bits clássicos 0 e 1. Porém, ao contrário dos bits clássicos, um qubit pode estar numa superposição dos dois estados denotado por $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ como exposto anteriormente. Pode-se notar que um qubit pode estar em infinitos estados, variando-se os valores de a e b; porém só podemos obter um bit de informação dele - pois ao se realizar uma medição, o seu estado se colapsará em um dos estados $|0\rangle$ e $|1\rangle$.

A notação $|a_0 a_1 ... a_n\rangle$ vem da notação BraKet criada por Dirac que define uma entidade chamada Bra e outra Ket. Aqui só utilizaremos o Ket. Um Ket nada mais é que uma matriz de uma coluna (vetor) de números complexos cujo número de linhas é 2^n, com n sendo o número de bits no Ket, e cujos elementos são todos 0 com exceção do elemento da linha i onde i é o número em base binária dentro do Ket. Por exemplo, $|0\rangle$ é $(1,0)^T$; $|1\rangle$ é $(0,1)^T$; $|00\rangle$ é $(1,0,0,0)^T$; $|10\rangle$ é $(0,0,1,0)^T$; etc.

O poder dos computadores quânticos vêm do fenômeno chamado entrelaçamento que ocorre quando se opera com múltiplos qubits ao mesmo tempo. O espaço vetorial de dois

qubits, por exemplo, é composto pelo produto tensorial do espaço vetorial de cada qubit. Assim, o estado de dois qubits pode ser descrito através da combinação linear de quatro vetores base: $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$, com $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$, onde $|a|^2$ é a probabilidade do estado ser lido como $|00\rangle$, e assim sucessivamente. Generalizando, n qubits podem estar em superposição de 2^n estados base. Isso permite o computador quântico trabalhar em múltiplas computações simultaneamente, e com um fator exponencial. Deve-se lembrar, contudo, que só se consegue ler um desses valores: são fornecidos sempre n bits de informação. Tal fato parece inutilizar a capacidade do computador quântico; porém é possível utilizar alguma propriedade coletiva de todos os estados para se efetuar uma computação útil em tempo menor do que em um computador clássico.

Para se entender melhor o fenômeno do entrelaçamento, considere o estado $\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$. É impossível escrevê-lo em função somente de $|0\rangle$ e $|1\rangle$ [12]. Isso implica que eles estão relacionados de alguma forma. De fato, suponha que é feita uma leitura do primeiro qubit como sendo $|0\rangle$ (a probabilidade de isso acontecer é $\frac{1}{2}$). Se for feita uma leitura posterior do segundo qubit, será lido o estado $|0\rangle$ com 100% de probabilidade. Ou seja, uma leitura do primeiro qubit alterou o valor do segundo; pois antes da leitura do primeiro, tinha-se uma probabilidade de $\frac{1}{2}$ de se ler o estado $|1\rangle$ no segundo.

Esse fenômeno é a base do experimento EPR proposto por Einstein, Boris Podolsky e Nathan Rosen numa tentativa de mostrar que a mecânica quântica era inconsistente com a realidade [1]. Considere duas partículas entrelaçadas no estado $\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$ descrito acima. Suponha então que uma partícula é enviada para Alice, e outra partícula é enviada para Bob, e que os dois estão distantes arbitrariamente um do outro. Caso Alice leia a sua partícula e obtenha $|0\rangle$, uma leitura subseqüente feita por Bob em sua partícula resultará em $|0\rangle$. Mas se Alice ler $|1\rangle$, Bob lerá $|1\rangle$. Aparentemente, as duas partículas estão se comunicando instantaneamente, contrariando a teoria da relatividade que proíbe qualquer comunicação mais rápida que a velocidade da luz. Tal impasse foi resolvido por John Bell e Alain Aspect ao provarem que, apesar de tal fenômeno realmente ocorrer, é impossível usá-lo para se transportar informação [11].

4. PORTAS QUÂNTICAS

Com os qubits definidos, fica a questão: como realizar alguma computação sobre eles? A resposta está nas portas quânticas, análogas às portas lógicas clássicas. Um conjunto de qubits pode ser alterado de forma que pode ser representada por uma multiplicação por uma matriz unitária. Uma matriz unitária é qualquer matriz M tal que $MM^* = I$, onde M^* é a conjugada transposta de M e I a matriz identidade. Uma importante implicação desse fato é que toda computação quântica deve ser reversível [12].

Por exemplo, uma porta NOT é representada pela matriz

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Sua aplicação para o estado $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ consiste em

$$N(a\,|0\rangle + b\,|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = b\,|0\rangle + a\,|1\rangle$$

Outra porta importante é a porta controlled-not (CNOT) que opera em dois qubits, invertendo o segundo se o primeiro for 1. Para um estado simples como $|10\rangle$ é fácil ver sua operação:

$$CNOT\,|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

Para um estado entrelaçado, pode-se observar que a operação que o CNOT faz é trocar as probabilidades de ser ler o estado $|10\rangle$ com a de se ler o estado $|11\rangle$, desta forma:

$$\begin{aligned} CNOT(a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle) \\ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix} \\ = a\,|00\rangle + b\,|01\rangle + d\,|10\rangle + c\,|11\rangle \end{aligned}$$

Um computador clássico necessita de apenas um conjunto de portas para poder realizar uma computação. Tal conjunto é chamado universal; um exemplo são as portas AND e NOT, ou somente a porta NAND. O mesmo acontece com um computador quântico. Foi provado que é preciso de no máximo portas de dois qubits para se compor um conjunto de portas universais [4]. Um desses conjuntos consiste na porta CNOT e todas as portas que operam em um único bit. Tais portas quânticas podem ser implementadas, por exemplo, por operações de ressonância magnética em um par de elétrons ou de núcleos.

5. O COMPUTADOR QUÂNTICO

5.1 Requisitos

Para se construir um computador quântico, deve-se atender cinco requisitos [5]:

1. Um sistema físico escalável com qubits bem definidos
Deve existir uma entidade capacidade de representar o qubit, obedecendo aos critérios de comportamento quântico e de suportar dois estados tratados como 0 e 1. Deve-se conhecer o mecanismo para se manipular os qubits, assim como suas características internas. Vários métodos já foram propostos e alguns até demonstrados, como *ion-traps* (utilizando íons em uma campo eletromagnético) ou ressonância magnética nuclear com átomos.

2. Existência de um método para se inicializar os estados dos qubits
Tal requisito é lógico, ao se observar que para se realizar uma

computação deve-se conhecer o estado inicial do sistema. Ele também tem aplicações na correção de erro quântico descrita a seguir. É possível realizar a inicialização através de uma medição, que fará o sistema se colapsar em um determinado estado que, se não for o estado inicial desejado, pode ser convertido nele. A velocidade com que é possível inicializar um qubit é vital e pode limitar a velocidade de todo o sistema.

3. Tempos de decoerência longos, maiores que o tempo de operação das portas
Uma importante característica de um sistema quântico é que, com o tempo, ele interage com o ambiente e seu estado é alterado imprevisivelmente. Tal tempo é chamado tempo de decoerência, e é um dos problemas vitais da computação quântica. De fato, acreditava-se que a decoerência impedisse definitivamente a construção de computadores quânticos até que Peter Shor provou que era possível a realização da correção de erro quântica através de códigos de correção de erro.

4. Um conjunto universal de portas quânticas
Explicados na seção anterior. É importante notar que portas quânticas não podem ser implementadas perfeitamente; elas também podem causar erros. Contudo, tais erros podem ser contornados com o mesmo mecanismo de correção de erro usado para a decoerência.

5. Capacidade de ser medir qubits específicos
Outro requisito natural: evidentemente é necessário poder ler o resultado de uma computação de modo confiável. Este fator também é importante na correção de erro quântico.

5.2 Propriedades

Diferentes implementações de um computador quântico possuem diferentes propriedades. Para se poder realizar uma comparação dessas implementações é importante definir um conjunto representativo dessas propriedades; em [14] foi proposta uma taxonomia resumida a seguir.

1. Estacionário, voador ou móvel
Qubits podem ser representados por fenômenos estáticos (spins de núcleos e elétrons) e são ditos estacionários, ou então por fenômenos dinâmicos como fótons e são ditos voadores. Tecnologias estacionárias mas que permitem o movimento dos qubits físicos antes da aplicação de uma porta quântica são denominados móveis.

2. Sistema único ou composto
Um computador quântico pode ser composto na verdade de vários computadores idênticos que recebem os mesmos dados e realizam as mesmas operações; e são mais fáceis de se experimentar. Caso contrário, ele é denominado único.

3. Medição
A medição dos qubits pode possuir quatro características: ser paralelo ou serial no sentido de permitir ler vários qubits ou não ao mesmo tempo; necessitar ou não a interação com outro qubit para realizar a leitura; a velocidade de leitura; e a habilidade de ser poder efetuar a leitura em qualquer lugar ou de haver a necessidade de transportar os qubits para um lugar determinado. Essas propriedades possuem grande influência no desempenho de um sistema.

4. Método de correção de erro
A correção de erro quântica é dependente da arquitetura do sistema; e também pode ter um grande impacto na velocidade do sistema.

5. Desafios de fabricação
Certas arquiteturas propostas dependem de avanços tecnológicos difíceis de se obter; por esse motivo esta propriedade é vital na comparação dos sistemas.

6. Paralelismo de controle
Mesmo tendo as conhecidas vantagens sobre a computação clássica, a computação quântica pode ser bastante influenciada pelo paralelismo. Tal mecanismo dependerá de um controle paralelo que irá requerer circuitos clássicos de suporte.

7. Temperatura de operação
Muitas arquiteturas propostas requerem temperaturas baixas alcançadas somente com o uso de hélio líquido. Tal necessidade dificulta muito a sua possível construção em larga escala.

8. Equipamento de suporte
Certas arquiteturas dependem ainda de equipamento de suporte complexo, como microondas de alta freqüência; possivelmente em número proporcional ao número de qubits.

9. Total de qubits disponíveis
A principal propriedade do sistema; com impactos na sua velocidade, confiabilidade e escalabilidade. Qubits adicionais aos necessários para se realizar uma computação podem ser utilizados para paralelismo ou correção de erro adicional.

10. Endereçabilidade
Em alguns sistemas pode ser difícil endereçar um qubit específico; o que pode ter um grande impacto negativo.

11. Fiação
Em muitas arquiteturas propostas, somente qubits vizinhos podem ser operados por uma porta quântica. É necessário então um mecanismo para transportar fisica ou logicamente os qubits e deve-se definir a topologia usada no mecanismo (linha unidimensional, reticulado 2D, estrutura 3D).

12. Portas naturais
Além da universalidade, o conjunto de portas quânticas pode possuir três características: prover rotação arbitrária de qubits, operação comum que, se disponível, pode acelerar a performance dos algoritmos e que se indisponível deve ser simulada pelas portas básicas; complexidade da síntese de uma porta Toffoli, também muito utilizada em algoritmos quânticos; e se determinadas portas interferem em qubits que não sejam os operandos.

13. Coerência versus tempo de operação
Tecnologias baseadas em elétrons possuem um tempo de coerência menor por interagirem facilmente com o ambiente, por outro lado, tecnologias baseadas em efeitos nucleares são mais estáveis. Contudo, uma maior isolação do ambiente externo implica numa menor velocidade das portas quânticas.

14. Codificação lógica

Um qubit lógico pode ser representado em um sistema por mais de um elemento físico como íons e elétrons; o conjunto de elementos é denominado a codificação lógica do qubit.

15. Limites de escalabilidade
A escalabilidade de um sistema quântico depende de muitos dos fatores citados e é vital para a construção de um computador quântico real. Infelizmente, a maioria das arquiteturas já propostas não escala com sucesso.

16. I/O quântico
A possibilidade de se mover estados quânticos de uma máquina para outra permite várias aplicações. Essa comunicação pode ser realizada com um mecanismo chamado teletransporte quântico.

5.3 Tecnologia

Várias diferentes tecnologias já foram experimentadas para a implementação de um computador quântico [14]. A seguir discorre-se sobre suas características gerais.

1. NMR em solução
Nesta técnica, qubits são representados pelo spin de átomos de uma mólecula especialmente criada. Sob um campo magnético, é possível manipular esses qubits através de radiação microondas, endereçando cada átomo com freqüências diferentes. Várias cópias dessa mólecula ficam em uma solução, e cada uma representa um computador quântico (qualificando um sistema composto). Este método já foi utilizado para se fatorar o número 15 com o algoritmo de Shor, e já conseguiu alcançar 12 qubits. Infelizmente, não é considerado um método escalável porque o razão sinal/ruído cresce junto com o sistema.

2. Junção Josephson
São sistemas supercondutores, e possuem três tipos: os que representam qubits através de cargas, de fluxo ou de fase. Todos utilizam elétrons em pares denominados pares de Cooper. Possuem portas velozes e sua fabricação é relativamente simples, porém apresentam um tempo de coerência pequeno e são muito influenciados pelo ambiente.

3. NMR com silício
Neste sistema, qubits são representados pelo spin de átomos de ^{29}Si (isótopo 29 de silício) com spin 1/2 colocados em uma "ponte" micromecânica de ^{28}Si e ^{30}Si com spin 0, determinando efetivamente um sistema composto. São necessárias 10^5 cópias para se obter um sinal adequado. A leitura é feita com microscopia de força de ressonância magnética, e as operações através de radiação microondas. Apesar de possuir o maior tempo de decoerência conhecido, possui portas lentas e não permite I/O quântico.

4. Ion trap escalável
Este sistema é uma expansão de sistemas de *ion trap* que representam qubits nos níveis de energia de íons. Na versão escalável, os íons são movidos através de campos magnéticos para áreas onde são realizadas as operações utilizando pulsos de laser. Contudo, também apresenta portas lentas e limitações na operação e leituras concorrentes.

5. Totalmente óticos
Sistemas que utilizam fótons e que necessitam de fontes capazes de gerar um número preciso de fótons com um determinado intervalo de tempo. São fáceis de fabricar, porém suas portas têm uma qualidade baixa.

6. Pontos quânticos
Pontos quânticos são estruturas compostas por supercondutores que permitem posicionar elétrons em uma pequena área. Qubits podem ser definidos no número de elétrons no ponto ou no spin ou níveis de energia de elétrons individuais. Uma das desvantagens deste método é que cada qubit lógico precisa ser representado por múltiplos qubits físicos. Além disso, possui baixos tempos de coerência.

7. NMR em estado sólido de Kane
Sistema onde qubits são representados pelo spin de núcelos de átomos de fósforo em um substrato de silício. Possuem uma alta escalabilidade e bons tempos de decoerência, porém são complexos de se fabricar.

6. ALGORITMOS QUÂNTICOS

A grande motivação para a construção de computadores quânticos é a maior eficiência de algoritmos quânticos em relação a algoritmos clássicos. Os dois principais algoritmos desenvolvidos foram o de Shor e o de Grover.

6.1 Algoritmo de Shor

O problema da fatoração de números inteiros é muito utilizado na criptografia por acreditar-se que seja um problema difícil (exponencial). Contudo, Peter Shor causou surpresa ao descobrir um algoritmo que roda em tempo polinomial ($O(M^3)$, M o número de bits do produto) para realizar a fatoração de números inteiros. Isso significa que a construção de um computador quântico de tamanho suficiente irá tornar muitos algoritmos criptográficos, como o RSA, inseguros.

O algoritmo de Shor [13] se aproveita do fato que o problema da fatoração pode ser reduzido ao problema de encontrar o período de uma certa função. Para ilustrar, considere um número $N = p.q$ com p e q primos (pode-se generalizar para um número com qualquer quantidade de fatores). O problema de encontrar p e q dado N é equivalente ao de encontrar o período r da função $f(x) = a^x \mod N$ com a relativamente primo a N, pois pode-se mostrar que r dividirá $(q-1)(p-1)$.

O algoritmo consiste em criar uma superposição quântica sobre todos os números $a \mod N$, $a^2 \mod N$, $a^3 \mod N$, etc e achar o período dessa seqüência. Isso é realizado com a versão quântica da transformada discreta de Fourier. Com ela, obtém-se o período, e repetindo o processo com outros valores de a, consegue-se informação suficiente para se descobrir p e q.

6.2 Algoritmo de Grover

Um grande número de problemas podem ser classificados como buscas não estruturadas. O exemplo básico é a busca de um determinado elemento em uma lista não ordenada: não existe algoritmo mais eficiente do que simplesmente percorrer a lista buscando o elemento, tendo-se portanto um algoritmo de tempo $O(n)$ com n sendo o tamanho da lista. Vários outros problemas podem ser reduzidos a este, como a busca em banco de dados, coloração de grafos e ordenação [12].

Contudo, Lov Grover propôs um algoritmo quântico [9] capaz de realizar a busca não estruturada em tempo $O(\sqrt{n})$ (provado ser o menor tempo possível para algoritmo quânticos).

O algoritmo consiste, primeiramente, na inicialização de qubits de forma que se atinja uma superposição de estados, um para cada elemento da lista a ser procurada ($\frac{1}{\sqrt{n}}|00...1\rangle + \frac{1}{\sqrt{n}}|00...1\rangle + ... + \frac{1}{\sqrt{n}}|11...1\rangle$). Repete-se então uma seqüência de operações (por $\sqrt{n}$ iterações) de forma que cada iteração aumente a amplitude do estado desejado por $O(\frac{1}{\sqrt{n}})$. Após as interações, o estado desejado terá amplitude (e probabilidade) $O(1)$.

7. LINGUAGENS DE PROGRAMAÇÃO QUÂNTICAS

Embora a construção de computadores quânticos em larga escala ainda pareça distante, existe uma boa quantidade de pesquisa sendo feita com a suposição de que isso um dia será possível. Supondo-se que exista um computador quântico, levantam-se questões de como seria escrever um programa em um deles, das ferramentas utilizadas, e de como isso se compara com o que é feito com os computadores clássicos.

Como um computador quântico pode ser considerado um computador clássico com acesso a um "oráculo" quântico, é razoável considerar que muito da arquitetura atual dos computadores será preservada - caches, memórias, barramentos, etc. A grande diferença será realmente no núcleo quântico e também na forma com que os programas serão escritos.

As linguagens de programação quânticas [8] surgiram para cobrir este segundo ponto. Uma dessas linguagens é a QCL [10], baseada em C, que oferece sintaxe para se especificar registradores e operações quânticas. Até um interpretador está disponível [1], que atualmente simula os fenômenos quânticos classicamente (naturalmente, em tempo exponencial). Exemplos de códigos em QCL estão nos algoritmos 1 e 2.

Algoritmo 1 Operador da transformada discreta quântica de Fourier na linguagem QCL

```
operator dft(qureg q) {
  const n=#q;
  int i; int j;
  for i=1 to n {
    for j=1 to i-1 {
      V(pi/2^(i-j),q[n-i] & q[n-j]);
    }
    H(q[n-i]);
  }
  flip(q);
}
```

8. CONCLUSÃO

Os computadores quânticos apresentam uma enorme mudança na arquitetura de computadores. Ainda é desconhecida a plausabilidade da construção desses computadores em larga escala; talvez exista alguma barreira física que impeça isso de acontecer. Mas a sua existência permitira a realização de tarefas antes consideradas impossíveis e causaria uma grande revolução na computação. Por isso, o seu estudo é muito importante e servirá de base para o que, futuramente, poderá fazer parte do nosso cotidiano.

[1] `http://tph.tuwien.ac.at/~oemer/qcl.html`

Algoritmo 2 Procedimento em QCL que imprime um bit aleatório

```
procedure printrandom() {
  qureg q[1];
  int x;
  Mix(q);
  measure q, x;
  print x;
}
```

9. REFERÊNCIAS

[1] P. Amiri. Quantum computers. *Potentials, IEEE*, 21(5):6–9, 2002.

[2] D. Bacon and D. Leung. Toward a world with quantum computers. *Commun. ACM*, 50(9):55–59, 2007.

[3] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1934-1990)*, 400(1818):97–117, 1985.

[4] D. DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015–1022, 1995.

[5] D. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, 2000.

[6] A. Ekert and R. Jozsa. Quantum computation and shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733–753, 1996.

[7] R. Feynman. *The character of physical law.* MIT Press, 1967. ISBN: 0–262–56003–8.

[8] S. Gay. Quantum programming languages: survey and bibliography. *Mathematical Structures in Computer Science*, 16(04):581–600, 2006.

[9] L. K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, New York, NY, USA, 1996. ACM.

[10] B. Ömer. A procedural formalism for quantum computing. Master's thesis, Technical University of Vienna, 1998.

[11] J. Mullins. The topsy turvy world of quantum computing. *Spectrum, IEEE*, 38(2):42–49, 2001.

[12] E. Rieffel and W. Polak. An introduction to quantum computing for non-physicists. *ACM Comput. Surv.*, 32(3):300–335, 2000.

[13] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *IEEE Symposium on Foundations of Computer Science*, 0:124–134, 1994.

[14] R. Van Meter and M. Oskin. Architectural implications of quantum computing technologies. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 2(1):31–63, 2006.