Monografia: Computação Quântica

Caio Teixeira da Quinta (5889856), Naiane Ayone Yanachi (9345189) e Renan Cerqueira Afonso Alves (5894150)

MAC 5742-0219 Introdução à Programação Concorrente, Paralela e Distribuída

1. Introdução

Esse documento tem como objetivo apresentar os conceitos principais envolvendo Computação Quântica. A primeira parte destina-se a apresentar o Contexto Histórico em que surgiram as primeiras ideias sobre o tema (Seção 2). A seção seguinte explica alguns conceitos básicos, como o que são os qubits, emaranhamento e superposição. Na sequência, na Seção 4, alguns exemplos algoritmos quânticos são apresentados. Formas de comunicação quântica são discutidas na Seção 5. a Seção 6 contém perspectivas para o futuro da área e as considerações finais são apresentadas na Seção 7.

2. Contexto Histórico

A primeira menção sobre a possibilidade de um computador quântico foi feita em uma conferência realizada em 1981 no MIT na qual físico Richard Feynman defendia ser possível tirar vantagens da mecânica quântica para construir uma máquina capaz de efetuar simulações físicas que não seriam possíveis em um computador convencional. Um ano depois Feynman publicaria um resumo de sua apresentação no artigo *Simulating Physics with Computers*.

Em 1984 o também físico David Deutsch publicou o artigo *Quantum theory, the Church-Turing principle and the universal quantum computer* no qual provava que todas a capacidades computacionais de qualquer máquina finita obedecendo as leis da computação quântica estão contidas em uma única máquina e apresentou um modelo completo e geral para a computação quântica.

Entretanto foi somente em 1994 que houve novos avanços na área quando o professor de matemática aplicada Peter Shor desenvolveu o Algoritmo de Shor, capaz de fatorar grandes números numa velocidade muito superior à dos computadores convencionais. O algoritmo de Shor será explicado em um seção à parte nesse documento.

3. Princípios de Computação Quântica

3.1. O que são Qubits?

Os qubits (pronuncia-se "quil-bits") são a unidade básica da computação quântica, definidos em analogia aos bits da computação clássica.

O qubit é uma abstração de propriedades quânticas observadas na matéria, de forma que a teoria da computação quântica busca abstrair especificidades dos cálculos físicos subjacentes [11].

Assim, os qubits são definidos sobre um espaço vetorial bidimensional com coordenadas complexas, ou seja, um qubit é um vetor definido sobre $\mathbb{C}^2$ (também chamado de espaço de Hilbert). Em particular, os valores $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ e $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ são usados como base do espaço vetorial, de forma que um qubit qualquer pode ser descrito como $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, sendo que $\alpha, \beta \in \mathbb{C}$, com a condição de contorno $\alpha^2 + \beta^2 = 1$ [16].

O símbolo $|\rangle$ é chamado *ket*, e faz parte da notação *bra-ket* de Dirac, comumente utilizada em mecânica quântica. Um $\langle|$ (*bra*) representa um vetor linha enquanto que um $|\rangle$ (*ket*) representa um vetor coluna.

Uma forma alternativa de se representar um qubit é através da esfera de Bloch. A princípio poderia se pensar que não é possível representar um qubit em $\mathbb{R}^3$, já que possui quatro graus de liberdade (i.e duas coordenadas complexas). Porém a condição de contorno $\alpha^2 + \beta^2 = 1$ remove um grau de liberdade, permitindo mapear um qubit em uma esfera de $\mathbb{R}^3$ de raio unitário. Esta representação será útil para prover alguma intuição no significado das portas lógicas descritas na Seção 3.2.

Superposição e emaranhamento são duas propriedades fundamentais do mundo quântico que podem ser utilizadas para fins de computação. Uma superposição é o nome que se dá a uma combinação linear dos elementos da base. Ao realizar uma medição dos elementos da base $|0\rangle$ ou $|1\rangle$, obtém-se o equivalente a um bit clássico 0 ou 1. Porém, ao medir um qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ em estado de superposição, a medição irá resultar em um bit clássico 0 com probabilidade de α^2 ou em um bit clássico 0 /caioAcho que aqui é 1 não? com probabilidade de β^2. Qubits que provém 50% de obter 0 ou 1 são particularmente interessante, como o qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Emaranhamento é uma propriedade não possui um análogo no mundo clássico, observável em sistemas com múltiplos qubits. Um conjunto de qubits está em um estado de emaranhamento se, apesar do resultado da medição de cada qubit não ser determinístico por estar em superposição, é possível prever o valor da medição de um outro qubit com base no resultado da primeira

medição. Um exemplo de estado emaranhado é $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, observe que não é possível determinar o estado de cada qubit de forma independente.

3.2. Portas lógicas Quânticas

Assim como um computador convencional, uma ação em uma máquina quântica também pode ser executada a partir de portas elementares.

Isto é possível devido ao fato de existir uma interação controlada entre um qubit "alvo" e o exterior. Assim, existem portas de 1 qubit, de 2 qubits e, em geral, de N qubits.

Por outro lado, existem diferenças entre as portas clássicas e quânticas, sendo a principal delas o fato de que certas operações clássicas, como por exemplo a AND ou a OR, são irreversíveis, ao passo que as operações quânticas são sempre reversíveis, pois estão associadas a transformações unitárias [13].

Conforme dito na Seção 3.1, a esfera de Bloch é útil para visualizar algumas transformações das portas lógicas quânticas elementares. A Figura 1 exibe um exemplo de esfera de Bloch. Um qubit $|\psi\rangle$ é um ponto da esfera unitária, descrito pelos ângulos θ e ϕ. Nesta representação, o qubit $|0\rangle$ é equivalente a um vetor na direção $\hat{\mathbf{z}}$, enquanto que o qubit $|1\rangle$ é equivalente a um vetor na direção $-\hat{\mathbf{z}}$.

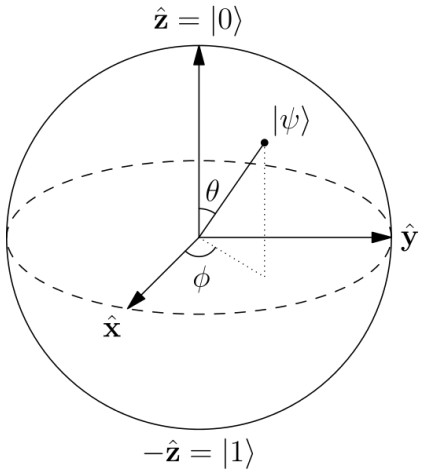

Figura 1: Esfera de Bloch

As portas de Pauli são as portas lógicas quânticas mais básicas, chamadas de X, Y e Z por representarem uma rotação de π radianos em torno dos eixos $\hat{\mathbf{x}}$, $\hat{\mathbf{y}}$ e $\hat{\mathbf{z}}$, respectivamente. A porta X também é chamada de NOT, pois é capaz de alterar o estado de $|0\rangle$ para $|1\rangle$ e vice-versa.

A porta de Hadamard (H) é importante pois é capaz de colocar os qubits $|0\rangle$ ou $|1\rangle$ em superposição. Matematicamente, utilizar esta porta é equivalente a uma rotação em torno do eixo $\hat{\mathbf{x}} + \hat{\mathbf{z}}$.

Há outras portas lógicas que atuam em um único qubit, por exemplo, rotações de $\frac{\pi}{2}$ e $\frac{\pi}{4}$ em torno do eixo z (portas S e T).

A porta lógica CNOT atua em dois qubits e seu comportamento é semelhante a um ou-exclusivo clássico. O CNOT pode ser utilizado para criar emaranhamento entre dois qubits. Existem muitas outras portar lógicas quânticas, por exemplo a porta de Toffoli (semelhante à operação lógica "e"), porém as descritas acima são as mais elementares.

Adicionalmente, é interessante ressaltar que as portas lógicas podem ser representadas como matrizes, provendo assim uma ferramenta algébrica para a verificação de encadeamento de operações.

3.3. Uma possível implementação - Computing Liquids

Dentre as possíveis implementações de um computador quântico um das que obteve maior sucesso em minimizar o tempo de *decoherence* de modo a executar um maior número de operações utilizando-se dos qubits é a técnica de utilizar moléculas de um líquido como representação de *bits* quânticos.

Em seu artigo *Quantum Computing with Molecules*[15] Neil Gershenfeld e Isaac L. Chuang descrevem uma técnica baseada no uso de Ressonância Magnética Nuclear (*Nuclear Magnetic Ressonance*) que produz fortes campos eletromagnéticos nos núcleos das moléculas presentes em um líquido fazendo com que o alinhamento das mesmas seja modificado segundo a direção do campo, alterando seu *spin*.

Dois desses alinhamentos (paralelos ou anti-paralelos) correspondem a dois estados quânticos com energias diferentes,o que constitui um qubit.

Um átomo com *spin* paralelo ao campo gerado pode ser interpretado como 1 enquanto o *spin* anti-paralelo seria o 0 de forma que, dependendo da duração do pulso aplicado, existe a possibilidade dos *spins* estarem tanto paralelos como anti-paralelos o que significaria em mecânica quântica a um estado 0 ou 1 simultaneamente.

No experimento apresentado no artigo foi utilizado um líquido composto de moléculas de clorofórmio (CHCl3) de modo a simular uma porta lógica XOR. Supondo que os hidrogênios sempre estejam alinhados para cima ou para baixo, paralelos ou não com o campo magnético aplicado verticalmente, e os átomos de carbonos estejam sempre rotacionados em 90^{o} de modo que a velocidade do *spin*, rápida ou devagar, irá representar um estado diferente (Figura 2).

O maior tempo encontrado para os experimentos com fluídos sugerem que é possível realizar cerca de 1000 operações preservando o estado de *coherence*.

4. Algoritmos

As propriedades de superposição e emaranhamento são pouco intuitivas e pode ser difícil pensar em algoritmos quânticos mais eficientes que os clássicos, fazendo uso destas propriedades em conjunto com as portas lógicas básicas. Esta seção descreve alguns algoritmos quânticos consagrados e a comparação da complexidade computacional em relação ao melhor algoritmo clássico conhecido.

4.1. Deutsch e Deutsch–Jozsa

Este algoritmo será explicado com mais detalhes por ser o mais fácil de compreender, ao mesmo tempo que é possível observar o potencial da computação quântica. As informações desta seção foram compiladas a partir de algumas referências [16, 14, 3].

O problema de Deutsch consiste em verificar, dado um oráculo que implementa uma função $f : \{0, 1\} \rightarrow 0, 1$, se a função é constante ou balanceada. Um oráculo pode ser definido como uma caixa preta que produz resultados, porém sem que se saiba seu funcionamento interno (ou seja, a função f não é conhecida a priori). Uma função balanceada é aquela que metade de suas saídas é 0 e a outra metade é 1, independente da ordem.

A Tabela 1 contém todas as possibilidades de função f. Utilizando computação clássica, é necessário verificar o resultado de f para as duas entradas possíveis para saber com certeza se f é constante ou balanceada, portando o oráculo é consultado duas vezes. Com o algoritmo de Deutsch, é possível obter a resposta do problema com apenas uma consulta ao oráculo.

Tabela 1: Possibilidades de funções para o problema de Deutsch

x	$f'(x)$	$f''(x)$	$f'''(x)$	$f''''(x)$
0	0	0	1	1
1	0	1	0	1

A Figura 3 exibe o circuito quântico do algoritmo. O qubit de cima é inicializado com $|0\rangle$ e o de baixo com $|1\rangle$. O operador U_f mapeia a entrada $|x\rangle\,|y\rangle$ para $|x\rangle\,|y \oplus f(x)\rangle$. Antes de ser fornecida ao operador U_f, da entrada sofre a transformada de Hadamard. Para obter o resultado do algoritmo, basta aplicar novamente a transformada de Hadamard no qubit de cima e medir o seu valor, se for 0 a função é constante, senão a função é balanceada. É possível demonstrar algebricamente a corretude do algoritmo, porém não vamos reproduzir a prova por brevidade.

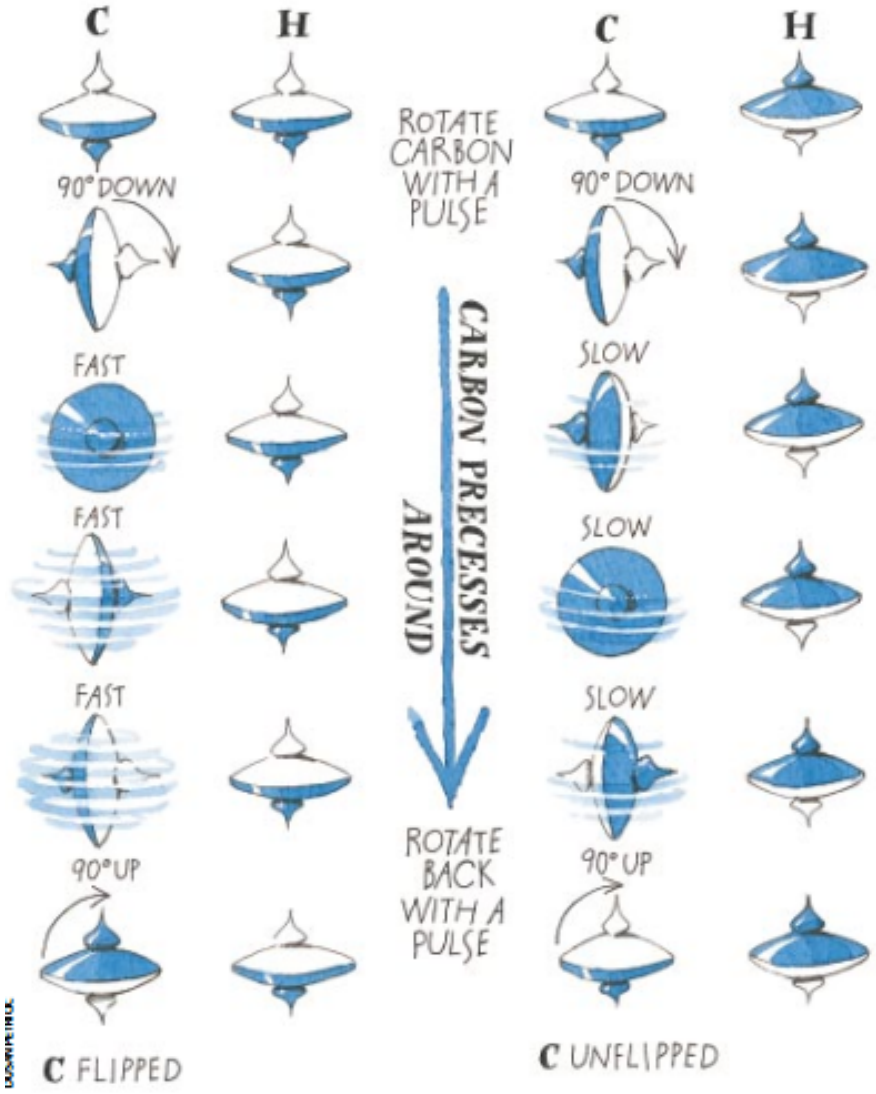

Figura 2: Porta Lógica XOR implementada em uma molécula de Clorofórmio (CHCl3)

Fonte: Quantum Computing with Molecules [15]

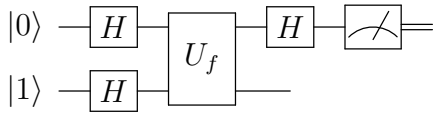

Figura 3: Circuito quântico do algoritmo de Deutsch

Observe o exemplo da Figura 4, que mostra o circuito para a função $f(x) = x$ (note que a porta lógica cnot é utilizada, que representa a operação $\oplus$). Ao executar este circuito em um simulador de circuitos quânticos é obtido o valor 1 com 100% de probabilidade, indicando uma função balanceada.

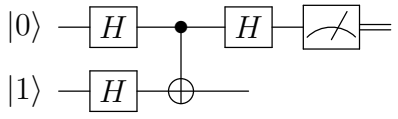

Figura 4: Circuito quântico do algoritmo de Deutsch para função $f(x) = x$

O algoritmo de Deutsch-Jozsa é uma generalização do problema de Deutsch, pois a função f é definida sobre um tamanho de entrada arbitrário, ou seja $f : \{0,1\}^n \rightarrow 0,1$ e é prometido que f é constante ou balanceada (por exemplo, não seria permitida uma função como a tabela verdade de AND). O circuito quântico é semelhante ao da Figura 3, bastando aumentar a quantidade de qubits inicializados em 0 para n. Para resolver este problema, um algoritmo clássico necessitaria de $2^{n-1}+1$ consultas ao oráculo no pior caso, enquanto que o algoritmo de Deutsch-Jozsa necessita de apenas 1 independentemente do valor de n.

4.2. Busca de Grover

A busca de Grover é uma boa introdução para algoritmos quânticos por demonstrar como as qualidades de um sistema quântico podem ser usadas para melhorar os limites inferiores de algoritmos clássicos fazendo uso da superposição de estados.

Enquanto em computadores clássicos uma busca em um conjunto não pode ser realizada com complexidade menor que O(n) a Busca de Grover é um algoritmo para computadores quânticos capaz de, com alta probabilidade, realizar uma busca em $O(\sqrt{n})$.

O algoritmo de Grover faz parte de uma classe de algoritmos que utiliza o que é chamado de amplificação de amplitude. A chave desses algoritmos é o

deslocamento de fase de um estado dentro do sistema quântico, que satisfaça alguma condição específica, em cada iteração.

Uma síntese de como o algoritmo funciona foi descrita no documento *Introduction to Quantum Algorithms* [5] no qual é explicado que a amplificação de amplitude no algoritmo é feita por uma série de execuções da Iteração de Grover (Figura 5), um processo que consiste em duas partes (*quantum oracle* e *diffusion transform*) no qual são realizadas sucessivas iterações que modificam as probabilidades associadas a cada entrada e verificam se a busca foi finalizada.

As Iterações são feitas sem que o algoritmo perca as propriedades de sobreposição de estados, não reduzindo-o a um estado binário.

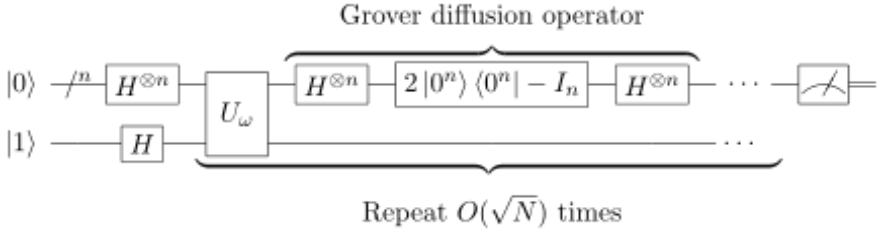

Figura 5: Diagrama para o Algoritmo de Grover

O algoritmo pode oferecer um *speedup* quadrático em relação a outros algoritmos implementados em um computador convencional. É possível, por força bruta, quebrar uma chave criptográfica simétrica de 128-bits em cerca de $2^{64} = 1.84467441 \cdot 10^{19}$ iterações [4].

4.3. Algoritmo de Shor

O algoritmo de Shor foi publicado originalmente me 1994 por Peter Shor e tem como objetivo resolver o problema da fatoração de grandes inteiros em tempo polinominal o que tornaria possível quebrar chaves RSA por exemplo.

A solução proposta parte do princípio de que existe apenas uma única fatoração possível para então reduzir o problema da fatoração em outro, encontrar o período em uma sequência de números [10]. Por exemplo, dada sequência das potências de 2:

$$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, \ldots$$

Agora observe a sequência de 2 mod 15.

$$2, 4, 8, 1, 2, 4, 8, 1, 2, 4, \ldots$$

É possível observar que a sequência começa a repetir-se, no caso o perído de repetição é 4, ou seja, a cada 4 números ela recomeça.

Segundo a fórmula de Euler dado um x não divisível por dois primos p e q a sequência abaixo irá repetir-se para algum período que divide igualmente (p-1)(q-1):

$$x \text{ mod N}, x^2 \text{ mod N}, x^3 \text{ mod N}, x^4 \text{ mod N}, \ldots$$

O problema é que o número de repetições pode tornar-se tão grande quanto o próprio N o que torna qualquer algoritmo clássico incapaz de resolver o problema, contudo o algoritmo de Shor propõe o uso de uma superposição quântica de 1 a N para encontrar a solução.

O algoritmo de Shor pode ser dividido em 5 passos, sendo que o segundo passo consiste em encontrar os períodos das sequências através de transformações de Fourier e é o responsável pelo *speedup* quântico do algoritmo, em resumo: [12]

Para fatorar um um inteiro n grande (assumindo n ímpar sem perda de generalidade):

1. Escolha um inteiro positivo aleatório e calcule seu máximo divisor comum.
2. Use um computador quântico para determinar o período P da sequência: x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...
3. Se P é um inteiro ímpar, retorne para o passo 1. A probabilidade de que P seja ímpar é$(\frac{1}{2})^k$, onde k é o número de fatores primos distintos de n. Se P é par, proceda para o próximo passo.
4. Como P é par: $(m^{P/2} - 1)(m^{P/2} - 1) = m^p - 1 = 0$ mod n. Se $m^{P/2} + 1 = 0$ mod n, então volte para o passo 1. Se $m^{P/2} + 1 \neq 0$ mod n, então vá para o passo 5. É possível mostrar que a probabilidade de $m^{P/2} + 1 = 0$ mod n é menor que$(\frac{1}{2})^{k-1}$, onde k denota o número de números primos distintos de n.
5. Calcule o $d = mdc(m^{P/2} - 1, n)$ usando o algoritmo de Euclides. Como $m^{P/2} + 1 \neq 0$ mod n, então é possível mostrar que d é um fator não trivial de n. Termine com a resposta d.

Resta então o problema de encontrar o período P da sequência. O algoritmo de Shor utiliza-se da sobreposição de estados quânticos de forma que, definida uma função f para o período, ele irá avaliar a função simultaneamente em todos os pontos.

Infelizmente a mecânica quântica não permite acessar essa informação diretamente, ao invés disso uma medição precisará ser realizada na qual apenas um dos possíveis valores irá restar ao final. Por conta disso, a sobreposição será sempre modificada para outro estado que irá retornar o período correto com maior probabilidade através de uma transformação de Fourier. Os passos para encontrar o período são (Figura 6):

1. Crie uma sobreposição de estados, isso pode ser feito aplicando portas de Hadamard para todos os qubits no registrador de entrada.
2. Implemente uma função f como uma transformação quântica. Shor usou repetidas "Exponenciações pelo Quadrado"(*Exponentiation by squaring*), um método para computação rápida de grandes potências inteiras positivas de um número, para implementar sua transformação.
3. Realize uma transformação de Fourier quântica.

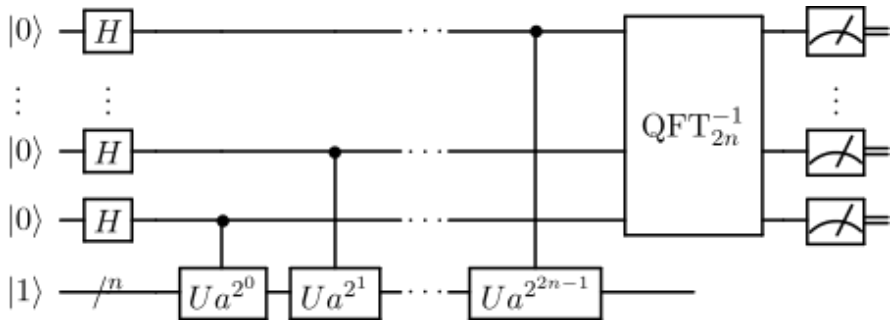

Figura 6: Sub rotina Quântica no Algoritmo de Shor

Apesar de ter sido proposto há mais de 20 anos o maior número fatorado utilizando esse algoritmo foi 21 em 2012 devido às limitações tecnológicas atuais.

O algoritmo tem tempo $\mathrm{O}(\log N^3)$ e necessita da ordem de $3 \log N$ qubits para ser executado [19].

5. Comunicação

Dentre as aplicações que a computação quântica pode proporcionar, existe uma grande expectativa com relação à criptografia e segurança de dados. Isso é explicado devido às características que só a computação quântica abrange.

5.1. No-Cloning Theorem

Existe um teorema que é capaz de provar que, se o estado quântico de um qubit é desconhecido, não é possível obter uma exata cópia dele. A prova a seguir é uma simplificação da prova real do Teorema da Não-Clonagem.

Suponha que temos um operado U que copia um estado quântico Ψ em outra partícula, conforme indicado pela Equação 1.

$$U\left|\Psi\right\rangle\left|0\right\rangle = \left|\Psi\right\rangle\left|\Psi\right\rangle \tag{1}$$

Usando a notação de Dirac, que todo estado quântico é uma superposição, reescrevemos a pergunta da seguinte forma, qual o valor de $U(a\left|0\right\rangle + b\left|1\right\rangle)\left|0\right\rangle$?

Sabendo que o produto tensor distribui sobre a superposição. Temos então duas possíveis derivações da expressão acima. A primeira é distribuir o produto tensor antes de distribuir o operador U.

$$\begin{aligned} U(a\,|0\rangle + b\,|1\rangle)\,|0\rangle &= U(a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|0\rangle) \\ &= Ua\,|0\rangle\,|0\rangle + Ub\,|1\rangle\,|0\rangle \\ &= Ua\,|0\rangle\,a\,|0\rangle + Ub\,|1\rangle\,b\,|1\rangle \\ &= Ua^2\,|00\rangle + Ub^2\,|11\rangle \end{aligned}$$

Mas, se efetuarmos a clonagem e depois distribuirmos, iremos obter:

$$\begin{aligned} U(a\,|0\rangle + b\,|1\rangle)\,|0\rangle &= (a\,|0\rangle + b\,|1\rangle)(a\,|0\rangle + b\,|1\rangle) \\ &= a\,|0\rangle\,a\,|0\rangle + a\,|0\rangle\,b\,|1\rangle + b\,|1\rangle\,a\,|0\rangle + b\,|1\rangle\,b\,|1\rangle \\ &= a^2\,|00\rangle + ab\,|01\rangle + ab\,|10\rangle + b^2\,|11\rangle \end{aligned}$$

Vejamos que as derivações são diferentes para as duas expansões. Já que o único passo duvidoso que se tomou foi supor que tal operador U existe, temos que tal operador não pode existir.

Note que, se a ou b forem zero, obtêm-se o mesmo resultado das duas derivações. Porém, se esse for o caso, não há sobreposição dado que a e b são amplitudes de estados em superposição. Nesses casos de estado $|0\rangle$ ou $|1\rangle$, pode-se simplesmente medir o estado da partícula e então realizarmos a cópia. Porém, ao medir estamos implicando que o qubit está em um desses dois estados e portanto, sabemos algo sobre ele, o que não invalida o teorema.

5.2. Criptografia Quântica

Caso os computadores quânticos fossem viáveis hoje em dia, muitos métodos de encriptação se tornariam obsoletos. Isso porque algoritmos quânticos já foram desenvolvidos e são bem mais eficientes que os clássicos. Tais algoritmos conseguiriam desencriptar mensagens por força bruta em tempo significantemente menor. Novos modelos quânticos foram criados para acompanhar a crescente tecnologia.

5.3. Quantum Key Distribution (QKD)

O *QKD* (distribuição de chaves quânticas) resolveria o problema de comunicar uma chave criptograda compartilhada entre duas partes comunicantes de forma segura. O *QKD* pode, em teoria, impedir que alguém intercepte a chave sem revelar sua presença. Sua segurança conta com o efeito que ocorre quando fótons são medidos.

Idealmente, os dados quânticos seriam transmitidos por fótons, devido a sua alta velocidade e baixa interação com o ambiente. Mas para isso necessitaríamos de uma capacidade de mover essa informação quântica de fótons para qubits e vice-versa. Diferentes implementações de qubits provavelmente necessitarão de diferentes soluções para mover emaranhamentos e superposições entre partículas e fótons.

Esses fótons nada mais são que feixes de luz polarizados, sujeitos aos princípios da mecânica quântica. Esses feixes de luz polarizados conseguem armazenar informações de um qubit, já que ambos podem ser representados como um vetor. Ao realizar a medição dos fótons, observamos uma mudança nos dados originais, sem que seja possível prever o dado anterior, e, por isso, é possível saber se houve uma tentativa de ler os dados originais. Muitos protocolos de distribuição de chaves foram criados com base nesse efeito [7].

Pesquisas recentes têm demonstrado avanços nessa área. Em agosto de 2015, a *University of Geneva* e *Corning Inc* obtiveram a maior distância de fibra óptica (307 km) [17]. No mesmo experimento, uma chave secreta era gerada a uma velocidade de 12,7 kbit/s. Em junho desse ano, físicos liderados por Thomas Jennewein do *Institute for Quantum Computing* e a *University of Waterloo*, no Canadá, demonstraram pela primeira vez a distribuição de chaves quânticas de um transmissor em terra à uma aeronave em movimento. Eles relataram links ópticos com distâncias de 3 a 10 quilômetros e geraram chaves seguras de até 868 kB [18].

6. Perspectivas

- Já existem redes de distribuição de chaves quânticas. Dentre elas temos: Tokyo QKD Network, SwissQuantum, SECOQC, DARPA e Los Alamos National Laboratory; E, apesar de todas as vantagens que o meio quântico possa apresentar, com elas diversas formas de ataque aos protocolos *QKD* estão sendo descobertas [8].

- Atualmente uma grande empresa de tecnologia, D-Wave, vem produzindo uma série de computadores quânticos. O último modelo lançado, D-Wave 2000Q conta com 2048 qubits, 5600 couplers e consome 25kW de energia, enquanto que supercomputadores convencionais consomem em média 2500kW. Boa parte dessa energia é utilizada para manter o processador quântico a uma temperatura próxima ao zero absoluto, assim, eliminando interferências do ambiente e garantindo um bom funcionamento.

  Esse computador possui APIs em C/C++, Python e MATLAB, que podem ser acessadas por usuários como um recurso na nuvem. Também há ferramentas da própria D-Wave disponibilizadas, como a QSage, ToQ, qbsolv, dw, além disso, pode-se escrever diretamente em instruções de máquina quântica (QMI).

  Os primeiros computadores da empresa demoraram a ser considerados quânticos pela comunidade até um artigo científico publicado na

Figura 7: D-Wave 2000Q

Nature realmente reconhecer os computadores da D-Wave como quânticos. Porém, é importante ressaltar que seus computadores não são utilizados para propósito geral, apenas conseguem resolver problemas mais específicos, não processam o algoritmo de Shor, por exemplo [2].

- Semelhante à Lei de Moore, mas agora em contexto quântico, a Lei de Rose foi criada por Steve Jurvetson, diretor geral da Draper Fisher Jurvetson. A Lei de Rose diz que o poder computacional dos computadores quânticos deve dobrar a cada ano juntamente com o número de qubits emaranhados, sendo ainda mais rápida que a Lei de Moore [9].

- Criado com o propósito de ser o maior pólo de pesquisa quântica do mundo, os fundadores da BlackBerry, Mike Lazaridis and Doug Fregin criaram um fundo de investimento de 100 milhões de dólares para tecnologias que empregam aplicações práticas de física quântica, localizado na região de Waterloo, no Canadá. Em 2000, a *Perimeter Institute for Theoretical Physics* foi criada como um instituto independente de pesquisa em física teórica. A *Perimeter* cresceu e se expandiu, liderando globalmente em pesquisa teórica em física fundamental. Com ajuda de Mike, também, foi criada a *Institute for Quantum Computing* (IQC), na University of Waterloo. A IQC foi criada como um instituto de pesquisa focado em informação quântica e hoje lidera as pesquisas científicas no ramo [1].

- Até agora estamos falando de processadores quânticos, mas já existem

iniciativas para criar memórias quânticas. Em uma publicação na Nature, físicos demonstraram um armazenamento de um bit em somente um átomo. O átomo estudado foi o Hólmio, que possui diversos elétrons não pareados, assim gerando um campo magnético orientado que pode ser lido como 0 ou 1. A equipe que conseguiu provar a escrita e leitura em tal átomo incluía pesquisadores da IBM. Esse disco rígido é um sistema de dois bits apenas [6].

7. Considerações Finais

A computação quântica é campo do conhecimento relativamento novo, baseado nos conceitos da mecânica quântica. Estes conceitos são pouco intuitivos, de forma que é difícil projetar ou mesmo entender os algoritmos quânticos.

Ainda não se sabe exatamente qual a capacidade de processamento de um computador quântico, mas alguns algoritmos já descobertos impactam diretamente no nível de segurança de algoritmos criptográficos simétricos (busca de Grover) e em algoritmos assimétricos (algoritmo de Shor).

Contudo, computadores quânticos de propósito geral ainda estão longe de ter uma quantidade de qubits grande o suficiente para possuir utilidade prática.

Por fim, quando computadores quânticos foram idealizados ainda não existiam processadores multi-core e a Lei de Moore seguia sendo respeitada, atualmente conforme ela chega para seu limite é observável um aumento de investimento em outros campos, como a Computação Quântica, que começa a despontar como uma área de interesse crescente.

Referências

[1] Creating canada's 'quantum valley'. Disponível em: https://bits.blogs.nytimes.com/2013/03/19/creating-canadas-quantum-valley/ (Acesso em 19/06/2016).

[2] The d-wave 2000q™ quantum computer technology overview. Disponível em: https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_0117F2.pdf (Acesso em 23/06/2016).

[3] Deutsch–jozsa algorithm. Disponível em: https://en.wikipedia.org/wiki/Deutsch%E2%80%93Jozsa_algorithm (Acesso em 13/06/2016).

[4] Grover's algorithm. Disponível em: https://en.wikipedia.org/wiki/Grover%27s_algorithm (Acesso em 13/06/2016).

[5] Introduction to quantum algorithms. Disponível em: https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf (Acesso em: 13/06/2016).

[6] Magnetic hard drives go atomic. Disponível em: http://www.nature.com/news/magnetic-hard-drives-go-atomic-1.21599 (Acesso em 16/06/2016).

[7] Quantum computing and communication. Disponível em: https://pdfs.semanticscholar.org/db97/6452bc9388b9df3c9ea6b5c8228041dde395.pdf (Acesso em 17/06/2016).

[8] Quantum key distribution. Disponível em: https://en.wikipedia.org/wiki/Quantum_key_distribution (Acesso em 19/06/2016).

[9] Rose's law for quantum computers. Disponível em: http://www.33rdsquare.com/2012/10/roses-law-for-quantum-computers.html (Acesso em 19/06/2016).

[10] Scott Aaronson. Shor, i'll do it. Disponível em: http://www.scottaaronson.com/blog/?p=208 (Acesso em 12/06/2017).

[11] Charles Bennett. A founder of quantum information theory. Disponível em https://youtu.be/9q-qoeqVVD0 (Acesso em 13/06/2017).

[12] Stephanie Blanda. Shor's algorithm – breaking rsa encryption. Disponível em http://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/ (Acesso em 16/06/2017.

[13] Juan J. Díaz Bulnes. *Emaranhamento e Separabilidade de Estados em Computação Quântica por Ressonância Magnética Nuclear*. PhD thesis, Centro Brasileiro de Pesquisas Físicas, Rio de Janeiro, 9 2005. Disponível em: http://www.cbpf.br/~fmelo/thesis/tese_Juan_qig_2005.pdf (Acesso em: 14/06/2016).

[14] Felipe Fanchini. Aula sobre algoritmo de deutsch. Disponível em https://youtu.be/Sb5WRs8XUuU (Acesso em 14/06/2017).

[15] Neil Gershenfeld and Isaac L Chuang. Quantum computing with molecules. *Scientific American*, 278(6):66–71, 1998 (Acesso em 13/06/2017).

[16] IBM. IBM quantum experience full user guide. Disponível em https://quantumexperience.ng.bluemix.net/qx/user-guide (Acesso em 13/06/2017).

[17] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 9:163–168, February 2015.

[18] Christopher J Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Nigar Sultana, Sascha Agne, Elena Anisimova, Vadim Makarov, Eric Choi, Brendon L Higgins, and Thomas Jennewein. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, 2(2):024009, 2017.

[19] John A. Smolin, Graeme Smith, and Alexander Vargo. Oversimplifying quantum factoring. *Nature*, 499, 07 2013.