Introdução à Computaçã Quântica

Kaio Karam Galvão – 016480
MO401 - Arquitetura de Computadores I
Instituto de Computação
Universidade Estadual de Campinas
kaio.karam@students.ic.unicamp.br

Ian Liu Rodrigues – 061485
MO401 - Arquitetura de Computadores I
Instituto de Computação
Universidade Estadual de Campinas
ian.liu88@gmail.com

RESUMO
A computação quântica introduz um novo conceito em arquitetura de computadores abrindo portas para novos algoritmos. Muitos problemas atuais são bastante difíceis de serem resolvidos com computadores clássicos, como por exemplo a fatoração de números inteiros, devido à sua alta complexidade de tempo. Ao se utilizar propriedades quânticas, como superposição e emaranhamento, nos algoritmos, é possível reduzir drasticamente o tempo de execução de alguns destes problemas complexos .

Neste artigo apresentamos os conceitos básicos da computação quântica, uma introdução à arquitetura do computador quântico e os algoritmos mais famosos já criados.

Keywords
Computação Quântica, qubit, algoritmos quânticos

1. INTRODUÇÃO
As bases da ciência da computação foram lançadas por Alan Turing [5] em um artigo no qual ele descrevia abstratamente uma máquina programável, criando o modelo de computação atualmente conhecido como Máquina de Turing. Turing demonstrou que existe uma Máquina de Turing Universal que pode ser utilizada para simular qualquer outra máquina de Turing. Ele ainda afirmou que, dado um algoritmo executado em qualquer máquina real, existe um algoritmo equivalente para a máquina universal que executa exatamente a mesma tarefa que o algoritmo para a máquina real [4].

Pouco depois do artigo de Turing, o primeiro computador baseado em componentes eletrônicos foi contruído. Porém, foi a partir do advento do transistor, em 1947 [4], que o hardware dos computadores passou a ter uma evolução muito rápida. O crescimento do poder de computação foi muito grande e, em 1965, Gordon Moore observou que o número de transistores que podem ser acomodados em um único chip de circuito integrado aproximadamente dobra a cada período de tempo de 18 a 24 meses [1]. A afirmação de que o poder de computação dobra a aproximadamente cada 2 anos ficou então conhecida como Lei de Moore.

Tal crescimento do poder computacional é possível graças à miniaturização dos componentes eletrônicos. A construção de componentes como os transistores é uma aplicação da física quântica. Porém, a operação de tais componentes é realizada de acordo com as leis da física clássica. A diminuição nas dimensões logo atingirá um limite no qual os efeitos da física quântica irão interferir no funcionamento dos componentes eletrônicos de maneira a inviabilizar sua operação. A partir de então, a Lei de Moore, que até agora tem-se mostrado verdadeira, irá falhar. Uma maneira de resolver essa limitação causado pelo tamanho dos componentes é criar um novo paradigma para a construção de computadores. Passar a utilizar a mecânica quântica, no lugar da física clássica, para processar informação é uma possível maneira de alterar o modo como os computadores são construídos. A computação quântica baseia-se nesta ideia e é um possível novo paradigma para os sistemas de computação.

Por tratar-se de um assunto ainda muito novo, apesar do rápido desenvolvimento que vem experimentando, este texto tratará apenas dos conceitos fundamentais da computação quântica. Primeiramente, será apresentada uma breve contextualização histórica do desenvolvimento da computação quântica. Em seguida, será introduzido o conceito utilizado na representação de informação em computação quântica, análogo ao *bit* da computação clássica. Logo após, circuitos e computadores quânticos serão descritos. Por fim, serão apresentados alguns algoritmos quânticos.

2. O BIT QUÂNTICO
O bit é um conceito fundamental na computação clássica. De forma análoga, a computação quântica baseia-se no conceito do *bit quântico*, ou *qubit*. Assim como o bit clássico, o qubit possui uma implementação física, que pode ser feita de várias formas, através de sistemas quânticos, como, por exemplo: polarizações de um fóton, estados de um elétron orbitando um átomo, entre outras. Desconsideraremos aqui detalhes da realização física do qubit. Apenas supomos que um qubit é um sistema físico que obedece às leis da mecânica quântica.

Assim como um bit clássico está em um estado específico (0 ou 1), o qubit também tem um estado. Segundo o primeiro postulado da mecânica quântica, todo sistema físico

representa um espaço vetorial complexo com produto interno definido, chamado *espaço de estados* do sistema. O sistema é completamente descrito por seu *vetor de estado*, que é um vetor unitário do espaço de estados. Em mecânica quântica usa-se a *notação de* DIRAC, onde os vetores de estado são representados pelo símbolo $|\cdot\rangle$. Por exemplo, $|\psi\rangle$ denota um estado, onde ψ é o nome do estado.

Um qubit é um sistema simples com espaço de estados de dimensão igual a dois. Suponha que $|0\rangle$ e $|1\rangle$ sejam dois estados que formam uma base ortonormal desse espaço. Logo, qualquer outro vetor do espaço de estados pode ser escrito como uma combinação linear dos vetores da base,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde α e β são números complexos. Como $|\psi\rangle$ deve ser um vetor unitário, então temos que $|\alpha|^2 + |\beta|^2 = 1$. Os estados $|0\rangle$ e $|1\rangle$ do qubit são, intuitivamente, análogos aos estados 0 e 1 do bit clássico. O qubit difere do bit clássico por poder apresentar outros estados, que são superposições destes. Os estados $|0\rangle$ e $|1\rangle$ são ditos *estados base computacionais*.

Dizemos que uma combinação linear qualquer de estados é uma *superposição* dos estados que aparecem na combinação. Da equação acima, dizemos que $|\psi\rangle$ é uma superposição dos estados $|0\rangle$ e $|1\rangle$, com *amplitude* α para o estado $|0\rangle$ e amplitude β para o estado $|1\rangle$.

Ainda segundo os postulados fundamentais da mecânica quântica, a simples observação de um sistema físico altera o seu estado. No nosso caso, ao se medir um qubit, o estado de superposição $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ em que o qubit estiver colapsa para um dos estados $|0\rangle$ ou $|1\rangle$. Como resultado da medida, teremos ou 0, com probabilidade $|\alpha|^2$, ou 1, com probabilidade $|\beta|^2$. Como a soma das probabilidades deve ser igual a um, $|\alpha|^2 + |\beta|^2 = 1$. Logo, $|\psi\rangle$ é um vetor unitário, o que está de acordo com o primeiro postulado.

Considere um sistema com dois qubits. Os estados que podem ser observados no sistema são $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$. Estes são os estados base computacionais do espaço de estados definido pelo par de qubits. O par pode estar em uma superposição destes quatro estados base:

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle.$$

O resultado de uma medida do sistema é um valor x que pode ser igual $00, 01, 10$ ou 11, cada um com probabilidade $|\alpha_i|^2$. A restrição de que a soma das probabilidades deve ser igual a um (ou de que o vetor deve ser unitário) é expressada pela condição de *normalização*

$$\sum_{i=1}^{4} |\alpha_i|^2 = 1.$$

O número de estados base computacionais cresce exponencialmente conforme aumentamos o número de qubits. Em um sistema com n qubits, os estados base terão a forma $|x_1 x_2 \ldots x_n\rangle$, onde cada x_i pode ser igual a 0 ou 1. Portanto, o estado do sistema é dado por 2^n amplitudes. É como se houvessem 2^n números complexos armazenados neste sistema de n qubits.

2.1 Operações em qubits

Assim como os computares clássicos podem operar sobre os bits, alterando seus estados, deve ser possível, com um computador quântico, operar sobre os qubits. Seja $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ o estado de um sistema quântico. Este estado também pode ser representado em notação vetorial como

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix},$$

que é um vetor do espaço vetorial na base $\{|0\rangle, |1\rangle\}$. Diversas transformações podem ser efetuadas sobre um sistema físico. Aqui, vamos nos ater a transformações lineares que, num espaço vetorial, são representadas por uma multiplicação matricial.

Seja T uma transformação linear que pode ser aplicada em um qubit. Essa transformação pode ser escrita como um produto matricial:

$$T\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}t_{11} & t_{12}\\ t_{21} & t_{22}\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

A condição de normalização deve ser estar satisfeita pelo estado do sistema quântico antes e após a aplicação da transformação. Portanto, a transformação T deve preservar a magnitude do vetor que representa o estado ($T|\psi\rangle$ deve ter comprimento igual a 1). Assim, a matriz da transformação T deve ser uma matriz *unitária*.

Uma matriz quadrada U é unitária se e somente se $U^\dagger U = I$, onde $U^\dagger$ é a transposta conjugada de U. Isso significa que a transposta conjugada é também a matriz inversa de U, ou $U^\dagger = U^{-1}$. Estas matrizes tem a propriedade de preservar a magnitude do vetor. Sejam v, w dois vetores $n \times 1$ e U uma matriz $n \times n$. Se $Uv = w$, então $v = U^\dagger w$. Multiplicando ambos os lados por $v^\dagger$, temos

$$v^\dagger v = v^\dagger U^\dagger w$$

mas $v^\dagger v = |v|^2$ e aplicando a regra da transposta da multiplicação de matrizes, temos

$$\begin{aligned} |v|^2 &= (Uv)^\dagger w \\ &= w^\dagger w \\ &= |w|^2. \end{aligned}$$

No caso de 1 qubit, as matrizes são de tamanho 2×2. Um exmeplo de transformação que inverte as amplitudes do vetor de estado de um sistema quântico é

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}.$$

À medida que aumentamos o número de qubits, os estados base computacionais também aumentam e, por consequência, as matrizes devem se adequar. Se tivermos n qubits e quisermos operar em todos ao mesmo tempo, precisaremos de uma matriz unitária de dimensão $2^n \times 2^n$.

3. PORTAS E CIRCUITOS QUÂNTICOS

Assim como um computador hoje em dia é construído com fios e portas lógicas para, respectivamente, transportar e manipular a informação, um computador quântico é construído com fios e portas quânticas. Uma porta quântica sempre

aplica uma transformação linear sobre qubits. Tais portas são representadas por matrizes. A única restrição necessária a essas matrizes é que sejam unitárias. Portanto, qualquer matriz unitária representa uma porta quântica válida.

Existem inúmeras portas quânticas e suas implementações físicas não são o objetivo deste trabalho. Em computação clássica, existe apenas uma porta que atua em um único bit, o NOT. Um processo que leve um qubit do estado $|0\rangle$ ao estado $|1\rangle$ seria um bom cadidato ao NOT quântico. O exemplo de transformação linear da seção anterior faz isso. No caso mais geral em que temos superposição de estados, esta transformação inverte as amplitudes do vetor de estado. Definimos esta matriz como a porta quântica NOT,

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Como basta que a transformação seja uma matriz unitária, em computação quântica existem diversas portas que atuam em um único qubit. Outras duas portas importantes que atuam em um único bit são a porta Z e a porta de HADAMARD. A porta Z mantém o estado $|0\rangle$ inalterado e troca o sinal do estado $|1\rangle$:

$$\begin{aligned} Z|\psi\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |\psi\rangle \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}. \end{aligned}$$

A porta de HADAMARD é uma das mais utilizadas. Esta porta transforma o estado $|0\rangle$ em $(|0\rangle + |1\rangle)/\sqrt{2}$ e o estado $|1\rangle$ em $(|0\rangle - |1\rangle)/\sqrt{2}$. De forma geral:

$$\begin{aligned} H|\psi\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |\psi\rangle \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}. \end{aligned}$$

A Tabela 1 mostra algumas portas quânticas comumente utilizadas.

Uma porta quântica de múltiplos qubits simples e muito importante é a porta *NOT-controlado* ou CNOT. A porta recebe dois qubits de entrada, um é o qubit *controle* e outro é o qubit *alvo*. A matriz desta transformação é:

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

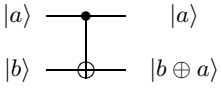
Se o qubit controle é $|0\rangle$, então o estado do qubit alvo é mantido. Se o qubit controle é $|1\rangle$, então o qubit alvo é trocado. Ou seja:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

Nome	Matriz	Símbolo
Hadamard	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
X (NOT)	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	
Pauli-Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	
Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	
SWAP	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	

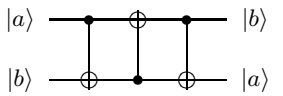
Table 1: Algumas portas quânticas importantes

A operação do CNOT também pode ser descrita como o XOR clássico. A transformação pode ser resumida como $|a, b\rangle \rightarrow |a, b \oplus a\rangle$. A representação gráfica de circuito da porta CNOT está a seguir.



Qualquer porta quântica de múltiplos qubits pode ser construída com portas CNOT e outras portas de um qubit. Este é um resultado importante para a construção de portas e circuitos quânticos. Uma prova deste resultado pode ser encontrada em [4].

Como um exemplo simples de circuito quântico, consideremos um circuito composto de três portas CNOT que permuta os estados de dois qubits. O diagrama



representa este circuito. Note que esta sequência de portas realiza a seguinte sequência de transformações no estado $|a, b\rangle$:

$$\begin{aligned} |a, b\rangle &\rightarrow |a, a \oplus b\rangle \\ &\rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\ &\rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle. \end{aligned}$$

A Tabela 1 mostra a matriz unitária e o símbolo equivalentes a este circuito.

Diferente dos circuitos clássicos, os circuitos quânticos não permitem laços, ou seja, realimentação de uma parte do circuito a outra. Outra operação muito comum nos circuitos clássicos, o *fanout*, onde vários fios são ligados juntos e são obtidas várias cópias de um bit, não é possível em circuitos quânticos. O **Teorema do no-cloning** afirma que não existe uma transformação unitária U tal que $U|\psi, 0\rangle = |\psi, \psi\rangle$

para um qubit qualquer $|\psi\rangle$. Uma prova deste teorema pode ser encontrada em [4].

4. PRODUTO TENSORIAL

Sejam $A_{m\times n}$ e $B_{r\times s}$ duas matrizes, então o produto tensorial (ou produto de Kronecker) é a matriz $C_{mr\times ns}$

$$C = A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots \\ a_{2,1}B & a_{2,2}B & \\ \vdots & & \ddots \end{pmatrix}$$

Para que o produto tensorial faça sentido, podemos representar os vetores de estado base computacional como vetores convencionais. Se temos 2-qubits, então a dimensão do nosso espaço é $2^2 = 4$ e podemos fazer uma relação de 1 para 1 da base deste espaço com a base canônica do $\mathbb{R}^4$

$$|00\rangle \to \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle \to \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle \to \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \text{ e } |11\rangle \to \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Com esta relação podemos aplicar o produto tensorial nos vetores e vemos uma propriedade interessante. O produto tensorial nos permite descrever o estado de um sistemas com múltiplos qubits em função do estado de cada qubit. Por exemplo, o estado $|01\rangle$ pode ser escrito como o produto tensorial $|0\rangle \otimes |1\rangle$. Por conveniência, as vezes omitimos o símbolo do produto tensorial, ficando apenas $|0\rangle|1\rangle$. Mas nem todo estado pode ser decomposto dessa maneira. Na sessão sobre emaranhamento, falaremos mais sobre isso.

O produto tensorial satisfaz várias propriedades interessantes, como associatividade e distributividade sobre a soma, entretanto ele não é comutativo. Além disso, o produto tensorial satisfaz as duas propriedades abaixo

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$
$$(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B).$$

Exemplo: com esta nova ferramenta em mãos, somos capazes de aplicar transformações com mais facilidade na notação de Dirac. Considere o seguinte estado de superposição

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Vamos aplicar a matriz de Hadamard no primeiro qubit, que é equivalente a multiplicar o vetor de estado pela matriz $H \otimes I$, onde a identidade I multiplicará o segundo qubit, deixando-o inalterado

$$\begin{aligned} H \otimes I|\psi\rangle &= H \otimes I\frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ &= \frac{H \otimes I|00\rangle + H \otimes I|11\rangle}{\sqrt{2}} \\ &= \frac{(H|0\rangle)(I|0\rangle) + (H|1\rangle)(I|1\rangle)}{\sqrt{2}} \\ &= \frac{\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle}{\sqrt{2}} \\ &= \frac{|00\rangle + |10\rangle + |01\rangle - |11\rangle}{2} \end{aligned}$$

5. EMARANHAMENTO

Na mecânica quântica existe o conceito de emaranhamento que, em poucas palavras, ocorre quando duas partículas interagem fisicamente e são separadas de uma maneira que seus estados quânticos são desconhecidos individualmente mas estão fortemente correlacionados. Quando uma partícula é medida e o seu estado passa a ser conhecido, imediatamente[2] saberemos o estado da outra partícula. Por exemplo, se uma possui *spin* no sentido horário, a outra terá *spin* no sentido anti-horário.

Matematicamente, duas partículas são consideradas emaranhadas quando o vetor de superposição das duas não pode ser fatorado como um produto tensorial de dois vetores. Por exemplo, o estado $|\psi\rangle = \frac{1}{4}|00\rangle + \frac{1}{4}|01\rangle + \frac{1}{4}|10\rangle + \frac{1}{4}|11\rangle$ pode ser escrito como $|\psi\rangle = (\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle) \otimes (\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle)$, logo $|\psi\rangle$ os qubits não estão emaranhados.

Agora veja o estado $|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ e suponha que ele possa ser escrito da forma

$$|\phi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha'|0\rangle + \beta'|1\rangle.$$

Então

$$|\phi\rangle = \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \alpha'\beta|01\rangle + \beta\beta'|11\rangle.$$

Igualando termo a termo, temos

$$\begin{aligned} \alpha\alpha' &= \frac{1}{\sqrt{2}} \\ \alpha\beta' &= 0 \\ \alpha'\beta &= 0 \\ \beta\beta' &= \frac{1}{\sqrt{2}}. \end{aligned}$$

Da segunda equação temos que $\alpha = 0$ ou $\beta' = 0$ vale zero. Se $\alpha = 0$, temos uma contradição, pois $\alpha\alpha' = \frac{1}{\sqrt{2}}$. Caso $\beta' = 0$ temos outra contradição, pois $\beta\beta' = \frac{1}{\sqrt{2}}$. Portanto $|\phi\rangle$ não pode ser escrito como um produto tensorial de dois vetores, logo os bits que o compõe estão emaranhados.

6. CODIFICAÇÃO SUPER DENSA

Dada uma superposição $|\psi\rangle$ de n-qubits, a quantidade de informação que podemos extrair dela é limitada pela quantidade de Holevo, isto é, n-qubits não podem conter mais informações do que n-bits clássicos[3].

Entretanto, se considerarmos que as partes que trocam informações compartilham qubits emaranhados, é possível re-

alizar a *codificação super densa*. Esta técnica permite transmitir 2-bits clássicos utilizando apenas 1-qubit.

Suponha que Alice quer enviar os bits a e b para Bob, e que cada um possui um qubit, ambos no estado emaranhado dado por

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A|1\rangle_B. \end{aligned}$$

Os qubits A e B são de Alice e Bob respectivamente.

Alice segue os seguintes passos para enviar os bits a e b para Bob:

1. Se $a = 1$, aplica a transformação unitária
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
no qubit A.
2. Se $b = 1$, aplica a transformação unitária
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
no qubit A.
3. Alice envia o qubit A para Bob.

Quando Bob recebe o qubit de Alice, ele segue os seguintes passos:

1. Aplica a matrix CNOT em ambos os qubits
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$
2. Aplica a matriz de HADAMARD no qubit A.
3. Mede os dois qubits, cujos valores serão a e b com probabilidade 1.

Exemplo: Imagine que Alice queira enviar os bits 01 para Bob. Como o bit $a = 1$, Alice pula o primeiro passo. Depois aplica a matriz unitária σ_x no qubit A, obtendo

$$\begin{aligned} |\psi'\rangle &= \sigma_x \otimes I|\psi\rangle \\ &= \frac{1}{\sqrt{2}}(\sigma_x|0\rangle_A)|0\rangle_B + \frac{1}{\sqrt{2}}(\sigma_x|1\rangle_A)|1\rangle_B \\ &= \frac{1}{\sqrt{2}}|1\rangle_A|0\rangle_B + \frac{1}{\sqrt{2}}|0\rangle_A|1\rangle_B, \end{aligned}$$

ou de maneira mais simplificada

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle.$$

Alice envia $|\psi'\rangle$ para Bob que, por sua vez, aplica a matriz CNOT em ambos os qubits, obtendo

$$\begin{aligned} U_{CN}|\psi'\rangle &= U_{CN}\left[\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|01\rangle\right] \\ &= \frac{1}{\sqrt{2}}U_{CN}|10\rangle + \frac{1}{\sqrt{2}}U_{CN}|01\rangle \\ &= \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|01\rangle. \end{aligned}$$

Por fim, Bob aplica a matriz de HADAMARD no qubit de Alice

$$\begin{aligned} H \otimes I|\psi'\rangle &= \frac{1}{\sqrt{2}}H|1\rangle|1\rangle + \frac{1}{\sqrt{2}}H|0\rangle|1\rangle \\ &= \frac{1}{2}(|0\rangle - |1\rangle)|1\rangle + \frac{1}{2}(|0\rangle + |1\rangle)|1\rangle \\ &= \frac{1}{2}(|01\rangle - |11\rangle) + \frac{1}{2}(|01\rangle + |11\rangle) \\ &= |01\rangle. \end{aligned}$$

Bob lê $H \otimes I|\psi'\rangle$ e obtém o resultado $|01\rangle$ com probabilidade 1, que é exatamente o valor enviado por Alice.

7. ALGORITMO DE DEUTSCH

Seja uma função $f : \{0, 1\} \to \{0, 1\}$. Chamamos ela de *caixa preta* pois não sabemos como ela funciona, isto é como ela mapeia os valores da entrada. Existem 4 tipos de funções desse tipo:

	f_0	f_1	f_2	f_3
Entradas 0	0	0	1	1
1	0	1	0	1

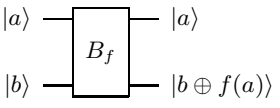
O problema é encontrar se a função que estamos lidando é constante ou não. No modelo clássico, podemos fazer isto executando a função duas vezes, $f(0)$ e $f(1)$ e avaliando se $f(0) = f(1)$. Caso afirmativo dizemos que a função é constante.

Agora vamos transformar o problema para ser resolvido no computador quântico. Para tanto é necessário alterar um pouco o problema, uma vez que a função f pode não ser uma matriz unitária. Por exemplo, se $f = f_0$ então a matriz que representa a transformação é

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

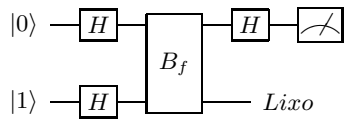
que não é unitária.

Defina a porta quântica B_f que atua em 2-qubits da seguinte maneira:



Esta porta é uma matriz de permutação para qualquer f, que sempre é uma matriz unitária.

O algoritmo de DEUTSCH é dado pelo seguinte circuito quântico



A leitura do primeiro qubit resulta no valor 0 quando f é constante e 1 caso contrário. A corretude do algoritmo se deve ao fato de que o resultado da medida do primeiro qubit vale $f(0) \oplus f(1)$ que vale 0 se $f(0) = f(1)$ ou 1 caso contrário.

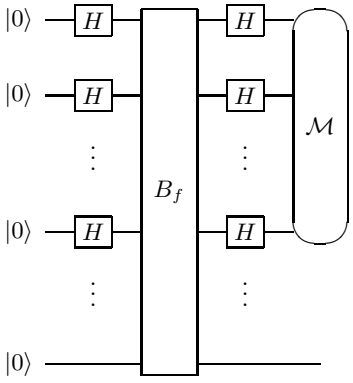
8. ALGORITMO DE SIMONS

O algoritmo de Simons resolve o problema da caixa-preta exponencialmente mais rápido que qualquer algoritmo clássico. O algoritmo executa $O(n)$ operações enquanto o melhor algoritmo clássico executa $O(2^{\frac{n}{2}})$.

O problema da caixa-preta que o algoritmo de Simons resolve é uma extensão do problema anterior, que usava uma função $f : \{0,1\} \to \{0,1\}$.

Neste problema, temos uma função $f : \{0,1\}^n \to \{0,1\}^n$ que satisfaz a seguinte propriedade: existe $s \in \{0,1\}^n$ tal que para todo $y, z \in \{0,1\}^n$, tem-se $f(y) = f(z)$ se e somente se $y \oplus z = s$. No caso em que $s = 0^n$ temos que f é uma bijeção, pois $s = 0$ implica que $f(y) = f(z)$ se e somente se $y = z$. Finalmente, o problema é encontrar o valor s.

O algoritmo de Simons consiste em aplicar o seguinte circuito quântico no estado inicial $|0^n\rangle$



A porta quântica B_f recebe $2n$ qubits de entrada, e realiza a seguinte operação

$$B_f |x\rangle |y\rangle = |x\rangle |f(x) \oplus y\rangle .$$

Afirmamos que o vetor resultante da medida dos n primeiros qubits, é um vetor y que satisfaz a propriedade $y \cdot s = 0$, e a distribuição de probabilidades é uniforme sobre todos os vetores que satisfazem esta propriedade.

Esta propriedade garante o resultado para o problema desde que o processo seja repetido várias vezes e com uma pequena probabilidade de falhar.

Se este circuito quântico é executado $n - 1$ vezes, teremos um sistema linear de equações do tipo

$$\begin{aligned} y_1 \quad &\cdot \quad s = 0 \\ y_2 \quad &\cdot \quad s = 0 \\ &\vdots \\ y_{n-1} \quad &\cdot \quad s = 0. \end{aligned}$$

A probabilidade de que este sistema tenha solução é pelo menos

$$\prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0.288788 \cdots > \frac{1}{4}.$$

Quando obtiver um sistema linear independente, procure uma solução $s' \neq 0$ e teste se $f(0^n) = f(s')$. Caso positivo temos a solução $s = s'$, senão a solução tem que ser $s = 0^n$.

Repetindo a aplicação do circuito $4m$ vezes, temos que a probabilidade de não encontrar um sistema linearmente independente, é

$$\left(1 - \frac{1}{4}\right)^{4m} < e^{-m}.$$

9. CONCLUSÕES

A computação quântica estabelece um novo paradigma na construção de computadores e na criação de algoritmos. Esta nova teoria traz profundas consequências, tanto para a arquitetura de computadores, quanto para as teorias de computabilidade e complexidade. Muito conjetura-se a respeito das potencialidades da computação quântica. A evolução desta teoria deve-se ao grande desenvolvimento da física quântica e da teoria da computação. Apesar do rápido desenvolvimento da área a partir dos anos 1990, ainda há muitas questões em aberto. A pesquisa na área tem-se desenvolvido pela investigação da viabilidade de se construir um computador seguindo o modelo quântico capaz de manipular números suficientemente grandes. Já foram construídos alguns computadores quânticos, porém todos de pequeno porte.

Por outro lado, as pesquisas buscam estabelecer relações entre as classes de complexidade tradicionais e novas classes de complexidade definidas segundo o modelo de computação quântica. Busca-se por algoritmos quânticos eficientes para problemas bem conhecidos, inclusive aqueles que não possuem algoritmos eficientes no modelo de computação tradicional. Já existem alguns algoritmos quânticos que resolvem de forma eficiente problemas difíceis na computação tradicional. Um exemplo notável é o algoritmo de Shor, não descrito neste trabalho, que realiza eficientemente a fatoração de inteiros em números primos. Tal algoritmo, se implementado em um computador quântico, quebraria sistemas conhecidos de criptografia que baseiam-se na dificuldade de se efetuar a fatoração de números inteiros muito grandes. Isso traz como consequência a busca por novos sistemas de criptografia. A própria computação quântica provê recursos para a criação de tais sistemas.

10. REFERÊNCIAS

[1] G. Benenti, G. Casati, and G. Strini. *Principles of Quantum Computation and Information*, volume 1. World Scientific, 2004.

[2] B. Greene. The fabric of the cosmos. page 11.

[3] A. Nayak. Holevo's theorem and its implications for quantum communication and computation, 2000.

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

[5] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937.