Revista Eletrônica
Paulista de Matemática

ISSN 2316-9664
Volume 19, dez. 2020
Edição Iniciação Científica

Um estudo passo a passo dos algoritmos de Grover e Shor

A step-by-step study of Grover and Shor algorithms

Luciano Alves Vieira
Centro de Ciência e Tecnologia
UFCA - Universidade Federal do Cariri
luciano.alves.vieira@gmail.com

Clarice Dias de Albuquerque
Centro de Ciência e Tecnologia
UFCA - Universidade Federal do Cariri
clarice.albuquerque@ufca.edu.br

Resumo

Os algoritmos de Grover e de Shor são duas das principais descobertas da computação quântica no início das pesquisas nessa área. O primeiro é um algoritmo de busca com um ganho de velocidade significativo em relação aos algoritmos clássicos e com grande aplicação na resolução de diversos outros problemas. O segundo é capaz de resolver o problema da fatoração de um número C em tempo polinomial, o que foi responsável por um grande impulso na pesquisa em computação e criptografia quântica. Neste trabalho de Iniciação Científica apresentamos os algoritmos quânticos de Grover e Shor, amplamente utilizados na computação quântica, com uma proposta original focada nos estados quânticos obtidos após cada passo na evolução do circuito. Dessa forma, exercita-se a aplicação das portas quânticas e a percepção das propriedades quânticas, bem como o funcionamento desses dois algoritmos. No circuito de Grover destacamos a fundamental propriedade de emaranhamento quântico que permite executar tarefas de processamento de informação.
Palavras-chave: Algoritmos Quânticos. Algoritmo de Grover. Algoritmo de Shor. Emaranhamento.

Abstract

The Grover's and Shor's algorithms are two of the main discoveries in quantum computing. The first is a search algorithm with a significant speed gain over the classic algorithms and with great application in solving several other problems. The second is able to solve the problem of factoring an C number in polynomial time, which was responsible for a major boost in research in quantum computing and quantum cryptography. In this Scientific Initiation work we present the quantum algorithms of Grover and Shor, largely used in quantum computing, with an original proposal focused on the quantum states obtained after each step in the evolution of the circuit. In this way, the application of quantum gates and the perception of quantum properties are exercised, as well as the operation of these two algorithms. In the Grover circuit we highlight the fundamental property of quantum entanglement that allows to perform information processing tasks.
Keywords: Quantum Algorithms. Grover's Algorithm. Shor's Algorithm. Entanglement.

Artigo recebido em abr. 2020 e aceito em jul. 2020

1 Introdução

Devido às propriedades da Mecânica Quântica, espera-se que um computador quântico possa ser mais eficiente que um computador convencional, ou seja, que o número de passos computacionais básicos para se resolver um determinado problema seja menor em um computador quântico. Além disso, a necessidade de simulações de sistemas quânticos, protocolos de criptografia mais seguros e a limitação física para a miniaturização dos transistores usados nos computadores clássicos justificam a busca pelo computador quântico.

Duas propriedades se destacam em Mecânica Quântica por serem responsáveis pelo ganho de velocidade na computação quântica diante da computação clássica, a *Superposição* e o *Emaranhamento* de estados. Diferentemente da física clássica, as partículas quânticas apresentam comportamentos de partículas e ondas. Assim, na Mecânica Quântica as partículas podem ser vistas como estados e amplitudes. Uma partícula está em uma superposição de estados quando se consideram todas as amplitudes, como se a partícula estivesse em todas as posições possíveis simultaneamente. Por outro lado, o emaranhamento é uma propriedade de forte correlação entre dois ou mais sistemas quânticos, independente da distância entre os sistemas. Em termos de estados quânticos, as propriedades ficam definidas no estado emaranhado de forma global e não nas partículas individualmente, ou seja, uma interação nesse estado afeta simultaneamente tudo que está emaranhado. O emaranhamento é um recurso físico fundamental na computação e informação quântica. Para maior aprofundamento nesse assunto, sugerimos as referências (BARNETT, 2009; KAYE; LAFLAMME; MOSCA, 2007; NIELSEN; CHUANG, 2005; VEDRAL, 2006).

Em contrapartida às vantagens proporcionadas pelas propriedades quânticas, um dos grandes desafios a ser superado para a realização de uma computação quântica é o decaimento dos estados em superposição, conhecido como *decoerência*. Um sistema em superposição de estados colapsa para uma única possibilidade, assim como um sistema clássico, se houver qualquer interação (observação ou medida) com o meio em volta. No sentido de transpor esse obstáculo, muitas pesquisas são desenvolvidas em códigos quânticos corretores de erros e computação tolerante a falhas[1], além das pesquisas em modelos diversos de computador quântico. Sugerimos as referências (NIELSEN; CHUANG, 2005; PALER; DEVITT, 2015; PORTUGAL; GONÇALVES, 2012; PRESKILL, 1997; VEDRAL, 2006) para os leitores ávidos por mais informações nesse contexto.

Neste trabalho, apresentamos dois importantes algoritmos quânticos que muito contribuíram para o impulso nas pesquisas sobre computação quântica, a saber, o Algoritmo de Grover e o Algoritmo de Shor.

Lov Grover demonstrou, em 1996, que o problema de se realizar uma busca em um banco de dados desordenado poderia ser resolvido mais rapidamente em um computador quântico do que em um computador clássico (GROVER, 1996). O algoritmo de Grover foi o primeiro de uma série de algoritmos quânticos de busca (PORTUGAL, 2010). Enquanto um computador clássico precisa de cerca de N operações para encontrar um determinado elemento em uma lista com N elementos, em um computador quântico o algoritmo de Grover consegue resolver o mesmo problema com $\sqrt{N}$ operações. Esse ganho quadrático de velocidade é obtido devido à propriedade conhecida como *paralelismo quântico*, que permite que uma função $f(x)$ seja avaliada simultaneamente em vários valores de x (PORTUGAL *et al*, 2012; VEDRAL, 2006).

Em 1994, Peter Shor descreveu um algoritmo baseado em propriedades da Mecânica Quântica que resolvia o problema de fatoração de um número C em tempo polinomial (SHOR, 1994). O trabalho estimulou enormemente a pesquisa em computação e criptografia quântica (NIELSEN;

[1]Sistema de computação que funciona satisfatoriamente na presença de falhas, sejam elas em hardware, software, operador ou ruído.

CHUANG, 2005), uma vez que uma das técnicas criptográficas mais utilizadas hoje em dia é a RSA, um método de chave pública no qual o cálculo da chave privada é equivalente ao problema de fatorar um número inteiro muito grande. O sucesso do método até o momento se deve ao fato de que tal problema não pode ser resolvido em tempo polinomial por um computador clássico. No algoritmo de Shor, o problema de fatorar um número composto C é reduzido ao cálculo da ordem de um número menor do que C, escolhido aleatoriamente (PORTUGAL *et al*, 2012; VEDRAL, 2006). O algoritmo baseia-se especialmente nas características do paralelismo quântico e na Transformada de Fourier Quântica Discreta (COPPERSMITH, 1994) para a realização do cálculo.

Neste artigo serão estudados os dois algoritmos, Grover e Shor, com o uso de exemplos práticos. No primeiro caso, do algoritmo de Grover, será considerada uma lista com $N = 4$ elementos, e no algoritmo de Shor usaremos como exemplo a fatoração do número $C = 15$. Em cada exemplo será exibida uma representação do circuito quântico utilizado para a implementação do algoritmo em questão. Nesses circuitos serão definidos os estados quânticos intermediários para facilitar o entendimento da aplicação das portas quânticas utilizadas. Para o algoritmo de Grover será verificado ainda o emaranhamento nos estados intermediários e exposta uma interpretação geométrica para o seu funcionamento. Antes, porém, serão apresentados os conceitos básicos de Mecânica Quântica necessários para a compreensão do texto a seguir.

Partes deste trabalho foram apresentadas nos eventos IX Bienal da Matemática e XXXIX Congresso Nacional de Matemática Aplicada e Computacional (CNMAC 2019).

2 Preliminares

Na Computação Quântica a unidade fundamental da informação é o *bit quântico* ou *qubit*. Diferentemente do *bit* da computação clássica, que só possui dois estados distintos, 0 e 1, o qubit pode assumir os estados intermediários entre 0 e 1, ou seja, as combinações lineares dos dois estados. É conveniente na Mecânica Quântica utilizar a notação de Dirac para vetores, nesse caso os estados (NIELSEN; CHUANG, 2005; VEDRAL, 2006). A notação "$|\cdot\rangle$", conhecida como *ket*, irá indicar o vetor correspondente ao estado, por exemplo o estado $|0\rangle$ e o estado $|1\rangle$.

Os qubits são objetos físicos, como, por exemplo, elétrons onde um *spin-up* representa o estado $|1\rangle$ e um *spin-down* representa o estado $|0\rangle$. Porém, estamos interessados em vê-los como objetos matemáticos, dessa forma suas propriedades não dependerão de sistemas específicos.

Um estado de um qubit pode ser visto como um vetor unitário (vetor de estado) em um espaço vetorial complexo completo bidimensional com produto interno $\mathbb{C}^2$, ou espaço de Hilbert $\mathcal{H}^2$, que é o espaço de estados do sistema físico. O sistema fica completamente descrito pelo seu vetor de estado. Esse é o primeiro postulado da mecânica quântica.

O segundo postulado afirma que a evolução de um sistema quântico fechado é descrita por uma transformação unitária. Enquanto as medidas quânticas são descritas por operadores de medidas atuando sobre o espaço de estados do sistema, pelo terceiro postulado. Por fim, o quarto postulado estabelece que o espaço de estados de um sistema composto é obtido pelo produto tensorial dos espaços de estados dos sistemas individuais.

Assim, um estado arbitrário de um qubit pode ser representado por

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

em que $\alpha, \beta \in \mathbb{C}$ são, respectivamente, as amplitudes associadas aos estados $|0\rangle$ e $|1\rangle$. É necessário que α e β satisfação a condição

$$|\alpha|^2 + |\beta|^2 = 1.$$

Outra representação equivalente a 1 é dada através da matriz coluna

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

A base ortonormal (uma base cujos vetores são unitários e ortogonais entre si) para o espaço vetorial $\mathbb{C}^2$ composta pelos estados $|0\rangle$ e $|1\rangle$ é chamada de *base computacional*. Outra base ortonormal importante para o espaço vetorial $\mathbb{C}^2$ é formada pelos estados $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, conhecida como *base conjugada*.

Para relembrar os conceitos de álgebra linear como vetores linearmente independentes, vetores unitários, vetores ortogonais, base, dimensão, protudo interno, vetor dual, transformações unitárias e operadores, sugerimos, além dos livros básicos de Álgebra Linear, as referências (KAYE; LAFLAMME; MOSCA, 2007; NIELSEN; CHUANG, 2005; VEDRAL, 2006), que definem os conceitos usando a notação de Dirac, própria para Mecânica Quântica.

Para a representação de estados com mais de um qubit é necessário a introdução do *produto tensorial*. Sejam $|v\rangle$ e $|w\rangle$ vetores pertencentes aos espaços vetoriais V e W, respectivamente, cujas representações matriciais são dadas por

$$|v\rangle = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \quad \text{e} \quad |w\rangle = \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}.$$

O resultado do produto tensorial entre $|v\rangle$ e $|w\rangle$, denotado $|v\rangle \otimes |w\rangle$, é o estado $|\chi\rangle$, que possui $n \cdot m$ linhas, e é definido por

$$|\chi\rangle = \begin{bmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \\ \vdots \\ v_n w_1 \\ v_n w_2 \\ \vdots \\ v_n w_m \end{bmatrix},$$

sendo $v_i w_j$ o produto usual entre números complexos (PORTUGAL *et al*, 2012).

Outras notações para o produto tensorial $|v\rangle \otimes |w\rangle$ são $|v\rangle\,|w\rangle$ e $|vw\rangle$.

O produto tensorial também se aplica a matrizes (ou operadores). Seja A uma matriz $m \times n$ e B uma matriz $p \times q$, o produto tensorial de A por B é a matriz $A \otimes B$ com dimensões $mp \times nq$:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

em que A_{ij} é o elemento de A da linha i e coluna j e $A_{ij}B$ é produto do elemento A_{ij} de A pela matriz B.

Como mencionado anteriormente, o quarto postulado estabelece como espaços de estados de sistemas individuais devem ser combinados através do produto tensorial para formar espaços de sistemas compostos. Então, o espaço de estados de 2 qubits deve ser $\mathcal{H}^4$, cuja base computacional é $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Assim, o vetor de estado arbitrário que descreve dois qubits é

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

com $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.

Para sistemas compostos por n qubits, o espaço de estados é o espaço de Hilbert n-dimensional $\mathcal{H}^n$, cuja base computacional é $\{|00\ldots0\rangle, |00\ldots1\rangle, \ldots |11\ldots1\rangle\}$. A sequência que aparece nos *kets*, $|\cdot\rangle$, é equivalente à representação binária dos números $0, 1, \ldots, 2^n - 1$, o que permite escrever de modo mais simples: $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$. Um estado geral $|\psi\rangle \in \mathcal{H}^n$ é dado por

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

sujeito à condição

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Em circuitos computacionais as portas lógicas transformam a informação, ou seja, atuam nos estados causando mudanças neles (NIELSEN; CHUANG, 2005). Na Computação Quântica, as *portas quânticas* possuem alguma analogia com as portas lógicas da Computação Clássica. Uma porta quântica U transforma um estado quântico $|\psi\rangle$ em um estado $U|\psi\rangle$. Como vimos no segundo postulado, a evolução do sistema quântico é descrita por transformações unitárias, então toda porta quântica é equivalente a uma transformação unitária (ou matriz unitária, uma vez que existe uma associação entre matrizes e transformações lineares) U, ou seja, $UU^\dagger = I$, em que $U^\dagger$ representa a matriz adjunta de U (obtida por meio da transposição do complexo conjugado de U).

Dessa forma, portas quânticas que atuam sobre um qubit são representadas matematicamente por matrizes unitárias 2×2. Entre as portas quânticas sobre um qubit, possuem grande aplicabilidade as *Matrizes de Pauli*,

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Uma das razões para a grande importância das matrizes de Pauli é que elas formam uma base para o espaço vetorial das operações sobre um qubit. Ou seja, todo operador unitário (ou transformação unitária) sobre um qubit pode ser expresso como uma combinação linear das matrizes de Pauli (KAYE; LAFLAMME; MOSCA, 2007).

A aplicação de I sobre o estado de um qubit não o altera, ou seja: $I|\psi\rangle = |\psi\rangle$. Exibiremos o resultado das aplicações das portas X, Y e Z sobre um estado genérico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$$
$$Y|\psi\rangle = -\beta i|0\rangle + \alpha i|1\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

Vejamos alguns exemplos das ações das portas lógicas sobre 2 e 3 qubits. Considere um estado arbitrário de dois qubits $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, com $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Consideremos então o operador $X \otimes X$, cuja representação matricial é

$$X \otimes X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

A ação de $X \otimes X$ sobre o estado $|\psi\rangle$, ou seja, $(X \otimes X)|\psi\rangle$, é

$$(X \otimes X)|\psi\rangle = \alpha_{11}|00\rangle + \alpha_{10}|01\rangle + \alpha_{01}|10\rangle + \alpha_{00}|11\rangle.$$

Observe que o resultado é equivalente à aplicação de um porta X sobre cada qubit.
Da mesma forma, a aplicação do operador $(X \otimes Z)$, cuja representação matricial é

$$X \otimes Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

sobre o estado arbitrário $|\psi\rangle$ é equivalente à ação de uma porta lógica X sobre o primeiro qubit e uma porta lógica Z sobre o segundo:

$$(X \otimes Z)|\psi\rangle = \alpha_{10}|00\rangle - \alpha_{11}|01\rangle + \alpha_{00}|10\rangle - \alpha_{01}|11\rangle.$$

Tomemos agora o exemplo de um operador $X \otimes I \otimes Z$ sobre três qubits,

$$X \otimes I \otimes Z = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

A ação de $X \otimes I \otimes Z$ sobre o estado genérico de três qubits $|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$ é:

$$\begin{aligned}(X \otimes I \otimes Z)|\psi\rangle = {} & \alpha_{100}|000\rangle - \alpha_{101}|001\rangle + \alpha_{110}|010\rangle - \alpha_{111}|011\rangle \\ & + \alpha_{000}|100\rangle - \alpha_{001}|101\rangle + \alpha_{010}|110\rangle - \alpha_{011}|111\rangle.\end{aligned}$$

Como feito nesses exemplos, pode-se construir operadores sobre vários qubits através da combinação de operadores menores, fazendo uso do produto tensorial.

A porta de Hadamard H, dada por (2), é outra porta quântica sobre um qubit com grande aplicabilidade, cuja ação promove a mudança da base computacional $\{|0\rangle, |1\rangle\}$ para a base conjugada $\{|+\rangle, |-\rangle\}$:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2}$$

As portas R_k, com grande importância na implementação do circuito quântico do algoritmo de Shor, sãos representadas por

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}. \tag{3}$$

A aplicação de R_k sobre um estado $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ resulta em

$$R_k |\psi\rangle = \alpha |0\rangle + e^{2\pi i/2^k} \beta |1\rangle .$$

Também merece destaque o grupo de portas que representa *operações controladas*. Nesse tipo de porta existem dois grupos de qubits entrada: os qubits de controle e os qubits-alvo. Quando os qubits de controle são todos iguais a $|1\rangle$, um operador U qualquer é aplicado sobre os qubits-alvo. Veremos a seguir duas dessas portas que serão utilizadas nos circuitos do algoritmos de Grover e Shor.

A porta CNOT, ou NÃO-CONTROLADA, representada matricialmente por

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

possui um qubit de controle e um alvo. Quando o qubit de controle é $|1\rangle$, o qubit-alvo tem seu estado trocado de $|0\rangle$ para $|1\rangle$ e vice-versa. Por exemplo, para o estado arbitrário de dois qubits, $|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$, a aplicação da CNOT resulta em:

$$CNOT |\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{11} |10\rangle + \alpha_{10} |11\rangle .$$

A porta Toffoli é uma porta controlada que possui dois qubits de controle e um qubit-alvo, que tem seu estado alterado apenas quando os dois primeiros são iguais a $|1\rangle$. A forma matricial para a porta Toffoli é

$$Toffoli = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Considere um estado arbitrário de três qubits $|\psi\rangle = \alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \alpha_{010} |010\rangle + \alpha_{011} |011\rangle + \alpha_{100} |100\rangle + \alpha_{101} |101\rangle + \alpha_{110} |110\rangle + \alpha_{111} |111\rangle$. O uso da porta Toffoli sobre ele resulta em

$$Toffoli\,|\psi\rangle = \alpha_{000}\,|000\rangle + \alpha_{001}\,|001\rangle + \alpha_{010}\,|010\rangle + \alpha_{011}\,|011\rangle \\ +\alpha_{100}\,|100\rangle + \alpha_{101}\,|101\rangle + \alpha_{111}\,|110\rangle + \alpha_{110}\,|111\rangle\,.$$

Além da forma matricial, os operadores lineares também podem ser representados utilizando a chamada *representação de produto externo*.

Seja $|v\rangle \in V$ e $|w\rangle \in W$, onde V e W são espaços vetoriais. O produto externo $|v\rangle\langle w|$ representa o produto matricial de $|v\rangle$ por $\langle w|$, no qual $\langle w|$ é o *vetor dual* de $|w\rangle$, ou seja, $\langle w| = (|w\rangle)^\dagger$, (em que $\dagger$ representa o complexo conjugado transposto). O produto externo $|v\rangle\langle w|$ representa um operador linear de V para W, cuja ação é:

$$|v\rangle\langle w|\,(|x\rangle) = |v\rangle\langle w|x\rangle = \langle w|x\rangle\,|v\rangle\,. \tag{4}$$

Na equação (4), $\langle w|x\rangle$ denota o produto interno entre os vetores $|w\rangle$ e $|x\rangle$, equivalente ao produto matricial entre $\langle w|$ e $|x\rangle$.

3 Circuito do algoritmo de Grover

Suponha que se queira encontrar um determinado item em uma lista de N itens desordenados. Em média são necessários $\frac{N}{2}$ consultas à lista e, na pior das hipóteses, N consultas. Usando o Algoritmo de Grover o número de passos cai para $\sqrt{N}$.

Podemos reformular o problema da seguinte maneira: suponha que se deseje encontrar um determinado item i_0 em uma lista que contém $N = 2^n$ itens, $\{0, 1, 2, \ldots, N-1\}$, em que $n \in \mathbb{N}$, e que para o reconhecimento de i_0 pode-se utilizar uma função $f : \{0, 1, 2, \ldots, N-1\} \to \{0, 1\}$, tal que

$$f(i) = \begin{cases} 1, & \text{se } i = i_0, \\ 0, & \text{se } i \neq i_0. \end{cases}$$

A função f recebe o nome de *oráculo*, e o custo computacional dessa busca está relacionado ao número de vezes em que essa função é empregada.

O algoritmo de Grover possui dois registradores quânticos, o primeiro com n qubits, que está associado aos itens da lista em que é feita a busca e que inicia o algoritmo no estado $|00\ldots0\rangle$. O segundo registrador é composto por apenas um qubit, inicializado no estado $|1\rangle$, sendo necessário para a identificação do elemento i_0.

O algoritmo se inicia com a aplicação da porta de Hadamard, H, sobre todos os qubits dos dois registradores, como pode ser visto na Figura 1. Com essa aplicação, o primeiro registrador é colocado em um estado de superposição com 2^n estados, relacionados aos 2^n elementos da lista, ou seja,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle\,. \tag{5}$$

O resultado da aplicação da porta H sobre o segundo registrador também leva a um estado de superposição, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A função f será utilizada no algoritmo através de um operador linear unitário U_f, tal que

$$U_f(|i\rangle\,|j\rangle) = |i\rangle\,|j \oplus f(i)\rangle\,,$$

em que $|i\rangle$ e $|j\rangle$ são, respectivamente, o primeiro e o segundo registradores e $\oplus$ é a soma módulo 2.

A adição módulo 2, presente no operador U_f, funciona alterando o estado do segundo registrador quando o primeiro corresponde ao item procurado, i_0, ou seja, $U_f(|i_0\rangle\,|0\rangle) = |i_0\rangle\,|1\rangle$ e $U_f(|i_0\rangle\,|1\rangle) = |i_0\rangle\,|0\rangle$. Nos casos em que o elemento do primeiro registrador não é i_0, o estado do segundo registrador não se altera, isto é, $U_f(|i\rangle\,|j\rangle) = |i\rangle\,|j\rangle$, para $i \neq i_0$ e $j \in \{0, 1\}$.

Estando os dois operadores preparados, ou seja, no estado $|\psi\rangle\,|-\rangle$, aplica-se o operador U_f. Com o uso da distributividade do produto tensorial em relação à adição de vetores, da linearidade do operador U_f e das definições de $|-\rangle$ e da função $f(i)$, chega-se a

$$U_f(|\psi\rangle\,|-\rangle) = \left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{f(i)}\,|i\rangle\right)|-\rangle\,.$$

Para mais detalhes sobre o desenvolvimento da expressão acima pode-se consultar (KAYE; LAFLAMME; MOSCA, 2007; NIELSEN; CHUANG, 2005; PORTUGAL *et al*, 2012; VEDRAL, 2006).

Durante a aplicação do operador U_f acontece o fenômeno do *paralelismo quântico*, o qual permite que com apenas uma aplicação de U_f todos os elementos da lista sejam avaliados, sendo alterada apenas a amplitude associada ao elemento i_0, que passa a ser $-\frac{1}{\sqrt{N}}$. Portanto, o estado do primeiro registrador continua sendo uma superposição de todos os elementos da lista, e o estado do segundo registrador continua sendo $|-\rangle$.

Na sequência, o algoritmo aumenta a amplitude do elemento i_0. Para isso é aplicado o operador $2\,|\psi\rangle\,\langle\psi| - I$ sobre o primeiro registrador, em que $|\psi\rangle$ é o estado apresentado na equação (5). O estado do primeiro registrador após a aplicação do operador $2\,|\psi\rangle\,\langle\psi| - I$ passa a ser

$$|\psi_G\rangle = \frac{N-4}{N}\,|\psi\rangle + \frac{2}{\sqrt{N}}\,|i_0\rangle\,.$$

No estado $|\psi_G\rangle$, a amplitude do elemento procurado, i_0, passa a ser $\frac{1}{\sqrt{N}}\left(\frac{N-4}{N}\right)+\frac{2}{\sqrt{N}} = \frac{3N-4}{N\sqrt{N}}$. Novamente sugerimos as referências (KAYE; LAFLAMME; MOSCA, 2007; NIELSEN; CHUANG, 2005; PORTUGAL *et al*, 2012; VEDRAL, 2006) para mais detalhes sobre o desenvolvimento.

A composição dos dois operadores, U_f e $2\,|\psi\rangle\,\langle\psi| - I$ recebe o nome de *operador de Grover G*,

$$G = ((2\,|\psi\rangle\,\langle\psi|) \otimes I)U_f.$$

Dependendo do tamanho da lista, mesmo no estado $|\psi_G\rangle$ a amplitude do elemento i_0 ainda pode ser pequena. Com base no valor de N, ou seja, do número de elementos da lista, é possível calcular o número de aplicações consecutivas de G, denotado aqui pelo valor κ, necessárias para que ao fim do algoritmo a amplitude do estado $|i_0\rangle$ seja a maior possível.

$$\kappa = \frac{\arccos\left(\frac{1}{\sqrt{N}}\right)}{\arccos\left(\frac{N-2}{N}\right)}. \tag{6}$$

Como o número de aplicações do operador G deve ser um número inteiro, arredonda-se o valor de κ para o inteiro mais próximo.

Façamos agora um exemplo prático da aplicação do algoritmo de Grover em uma lista com $N = 4$ elementos, em que o elemento procurado é $i_0 = 10$.

Como foi explicado no início desta seção, o circuito possui dois registradores. O primeiro registrador deve ter n qubits, neste caso $n = 2$, uma vez que $N = 2^2$, e é inicializado no estado $|00\rangle$. O segundo registrador, com um qubit, é inicializado no estado $|1\rangle$.

Para esse caso, a equação (6) mostra que é necessária uma única aplicação do operador G, que consegue aumentar a probabilidade de uma medida do sistema e retornar o elemento i_0 de 25% para 100%. No circuito quântico da Figura 1 estão explicitadas as portas quânticas que compõem o operador $2|\psi\rangle\langle\psi| - I$.

Ao longo do circuito da Figura 1 foram calculados todos os estados intermediários, anteriores à medida realizada ao final, ou seja, $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{11}\rangle$. Esses estados identificam as aplicações das portas quânticas sobre os qubits do sistema.

A Figura 1 mostra o circuito do algoritmo de Grover para $N = 4$. Os qubits de entrada estão no extremo esquerdo da figura. Após a aplicação de cada porta quântica, as setas verticais apontadas para cima indicam o estado associado àquela etapa. Os quadrados com as letras H e X significam as portas de Hadamard e X, respectivamente. Observe que a porta Hadamard, ou a porta X, está sendo aplicada no qubit correspondente à linha na qual está desenhada a porta. As caixas pontilhadas destacam os operadores U_f e $(2|\psi\rangle\langle\psi| - I) \otimes I$. Após o estado $|\psi_{11}\rangle$ temos o símbolo da medida.

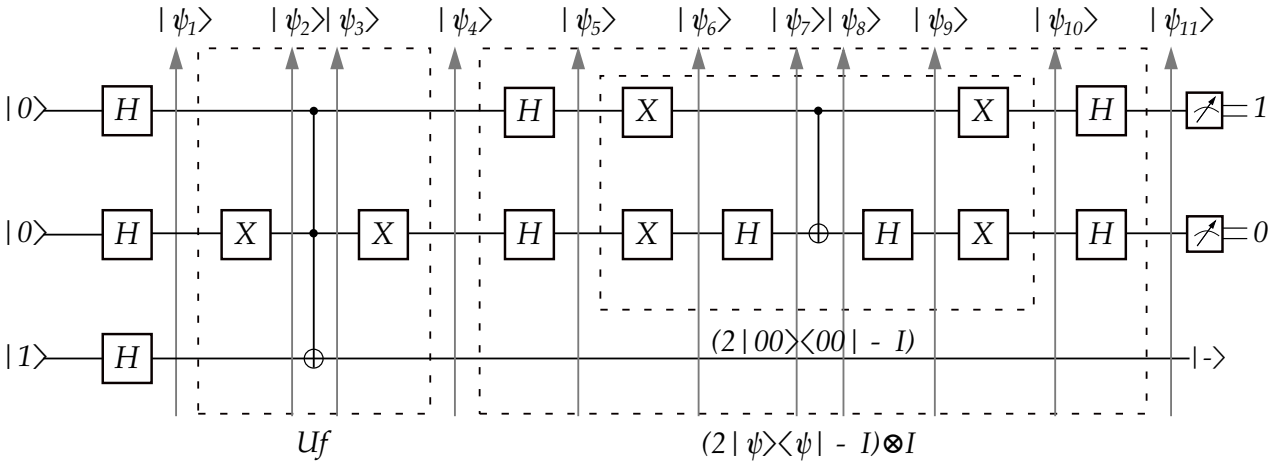

Figura 1 – Circuito de Grover para N = 4
Fonte: Elaborado pelos autores.

As representações das portas CNOT e Toffoli no circuito são destacadas na Figura 2. Perceba que os pontos pretos correspondem aos qubits de controle, enquanto o círculo corresponde ao qubit alvo.

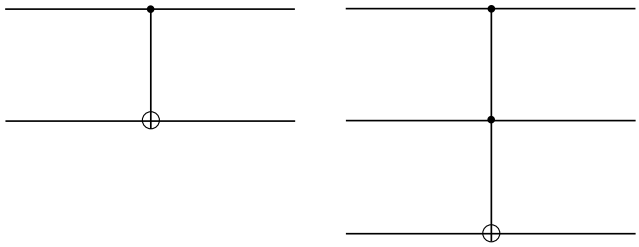

Figura 2 – Circuito das portas lógicas CNOT e Toffoli
Fonte: Elaborado pelos autores.

A seguir serão calculados os estados $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{11}\rangle$.

$$\begin{aligned}|\psi_1\rangle &= (H \otimes H \otimes H)\,|001\rangle \\ &= \frac{1}{2\sqrt{2}}[|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle].\end{aligned}$$

$$\begin{aligned}|\psi_2\rangle &= (I \otimes X \otimes I)\,|\psi_1\rangle \\ &= \frac{1}{2\sqrt{2}}[|010\rangle - |011\rangle + |000\rangle - |001\rangle + |110\rangle - |111\rangle + |100\rangle - |101\rangle].\end{aligned}$$

O estado $|\psi_3\rangle$ é resultado da aplicação da porta Toffoli sobre $|\psi_2\rangle$:

$$|\psi_3\rangle = \frac{1}{2\sqrt{2}}[|010\rangle - |011\rangle + |000\rangle - |001\rangle + |111\rangle - |110\rangle + |100\rangle - |101\rangle].$$

$$\begin{aligned}|\psi_4\rangle &= (I \otimes X \otimes I)\,|\psi_3\rangle \\ &= \frac{1}{2\sqrt{2}}[|000\rangle - |001\rangle + |010\rangle - |011\rangle + |101\rangle - |100\rangle + |110\rangle - |111\rangle].\end{aligned}$$

$$\begin{aligned}|\psi_5\rangle &= (H \otimes H \otimes I)\,|\psi_4\rangle \\ &= \frac{1}{2\sqrt{2}}[|000\rangle - |001\rangle - |010\rangle + |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle].\end{aligned}$$

$$\begin{aligned}|\psi_6\rangle &= (X \otimes X \otimes I)\,|\psi_5\rangle \\ &= \frac{1}{2\sqrt{2}}[|110\rangle - |111\rangle - |100\rangle + |101\rangle + |010\rangle - |011\rangle + |000\rangle - |001\rangle].\end{aligned}$$

$$|\psi_7\rangle = (I \otimes H \otimes I)\,|\psi_6\rangle = \frac{1}{2}[|000\rangle - |001\rangle - |110\rangle + |111\rangle].$$

O estado $|\psi_8\rangle$ é resultado da aplicação da porta CNOT sobre os dois primeiros qubits e a porta I sobre o terceiro qubit de $|\psi_7\rangle$:

$$|\psi_8\rangle = \frac{1}{2}[|000\rangle - |001\rangle - |100\rangle + |101\rangle].$$

$$\begin{aligned}|\psi_9\rangle &= (I \otimes H \otimes I)\,|\psi_8\rangle \\ &= \frac{1}{2\sqrt{2}}[|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle].\end{aligned}$$

$$|\psi_{10}\rangle = (X \otimes X \otimes I)\,|\psi_9\rangle$$
$$= \frac{1}{2\sqrt{2}}[|110\rangle - |111\rangle + |100\rangle - |101\rangle - |010\rangle + |011\rangle - |000\rangle + |001\rangle].$$
$$|\psi_{11}\rangle = (H \otimes H \otimes I)\,|\psi_{10}\rangle = -|101\rangle\,.$$

Na Seção 3.1 os estados $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{11}\rangle$ serão verificados quanto ao *emaranhamento*, mostrando em quais pontos essa propriedade quântica está presente no algoritmo de Grover.

O funcionamento do algoritmo de Grover permite ainda uma interpretação sob um ponto de vista geométrico. Para isso, considere a Figura 3, referente ao mesmo exemplo, ou seja, $N = 4$ e $i_0 = 10$. Na figura são registradas as amplitudes referentes ao primeiro registrador: o eixo vertical representa a amplitude do estado $|i_0\rangle$ e o eixo horizontal é a amplitude do vetor unitário $|u\rangle$, que é ortogonal a $|i_0\rangle$, sendo gerado por todos os elementos da base computacional diferentes de i_0, $|u\rangle = \frac{1}{\sqrt{N-1}} \sum_{i=0, i\neq i_0}^{N-1} |i\rangle$.

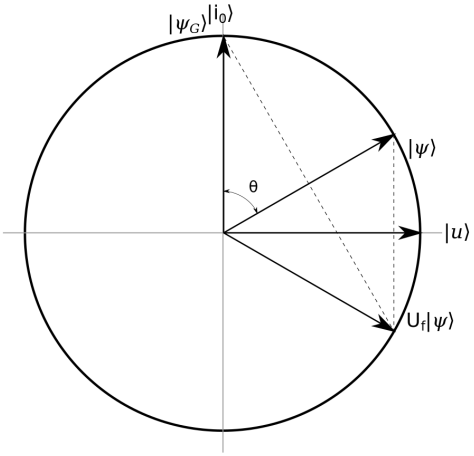

Figura 3 – Interpretação Geométrica do Operador G para N = 4
Fonte: Elaborado pelos autores.

Como dito, o estado do primeiro registrador após a aplicação da porta H sobre todos os qubits é $|\psi\rangle$, apresentado na equação (5). Nessa superposição de estados, todos os elementos da lista possuem a mesma probabilidade de serem retornados após a realização de uma medida.

A aplicação do operador U_f causa uma reflexão do vetor $|\psi\rangle$ em relação ao vetor $|u\rangle$. O resultado é apresentado na Figura 3 como $U_f\,|\psi\rangle$. Já o operador $2\,|\psi\rangle\,\langle\psi| - I$ reflete o vetor $U_f\,|\psi\rangle$ em relação a $|\psi\rangle$, aproximando o resultado $|\psi_G\rangle$ do eixo vertical, ou seja, aumentando a amplitude do elemento $|i_0\rangle$.

Para ajudar na visualização da interpretação geométrica, apresentamos mais um caso, $N = 8$, cujo operador G deve ser aplicado duas vezes, de acordo com a equação (6). Veja a Figura 4.

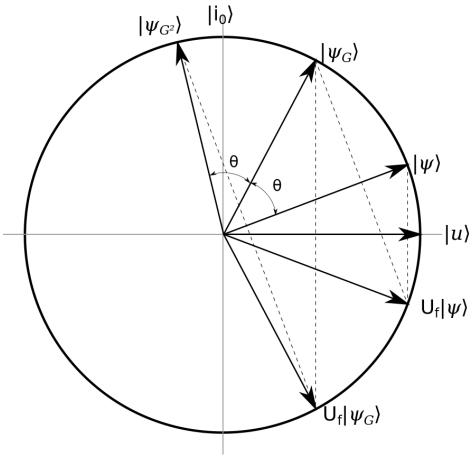

Figura 4 – Interpretação Geométrica do Operador G para N = 8
Fonte: Adaptado de Portugal *et al* (2012).

Percebe-se na Figura 4 que, ao final das aplicações do operador G, o estado final, $|\psi_{G^2}\rangle$, ainda é uma superposição de estados, já que ele não está sobre o eixo associado ao vetor $|i_0\rangle$. Assim, não é possível garantir que uma medida realizada sobre $|\psi_{G^2}\rangle$ retornará o elemento i_0, porém a probabilidade que a resposta dessa medida seja o elemento procurado é muito maior do que se a mesma medida fosse realizada sobre o estado inicial $|\psi\rangle$. Na verdade, para o caso $N = 8$, ao final do algoritmo o elemento procurado é obtido com probabilidade $\left(\frac{11}{4\sqrt{8}}\right)^2 \approx 94,53\%$ (PORTUGAL *et al*, 2012).

3.1 Emaranhamento no algoritmo de Grover

Como mencionado anteriormente, o *emaranhamento* é uma das propriedades fundamentais da Mecânica Quântica, sendo responsável pela aceleração da computação quântica em relação à computação clássica (VEDRAL, 2006).

Estados emaranhados possuem as suas propriedades armazenadas nas características globais do estado e não nas partículas individuais que as compõem. Dessa forma, uma medida realizada sobre uma dessas partículas é capaz de afetar todas as demais que formam o estado.

Vejamos um importante estado emaranhado de dois qubits, conhecido como *Estado de Bell* ou *Par EPR* (iniciais de Einstein, Podolsky e Rose)[2],

$$|\phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{7}$$

Se medirmos o primeiro qubit teremos 0 com probabilidade 1/2 e o estado após a medida ficará em $|\psi'\rangle = |00\rangle$, ou 1 com probabilidade 1/2 e o estado após a medida ficará em $|\psi'\rangle = |11\rangle$. O mesmo ocorre se medirmos o segundo qubit. Ou seja, os resultados são correlacionados e isso independe da medida utilizada (NIELSEN; CHUANG, 2005).

Estados emaranhados se caracterizam pela impossibilidade de escrevê-los como produtos tensoriais de estados individuais do sistema. Por exemplo, se tentarmos escrever o estado de Bell (7)

[2]Existem outros estados de Bell (ou pares EPR) $|\phi_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}; |\phi_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}; |\phi_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. Esses estados são fundamentais em aplicações de criptografia quântica, teleporte e codificação super-densa (NIELSEN; CHUANG, 2005; VEDRAL, 2006).

como $\frac{(\alpha|0\rangle+\beta|1\rangle)(\gamma|0\rangle+\delta|1\rangle)}{\sqrt{2}}$ chegaremos em uma contradição onde $\beta = 0$ ou $\gamma = 0$, porém $\alpha\gamma = 1$ e $\beta\delta = 1$.

Quando for possível representar um estado puro[3] arbitrário $|\psi\rangle = \alpha_1|00\ldots0\rangle + \alpha_2|00\ldots1\rangle + \cdots + \alpha_n|11\ldots1\rangle$, sujeito à condição $\sum_{i=1}^{n}|\alpha_i|^2 = 1$, como produto tensorial de estados de um qubit, diz-se que o estado é separável.

Para avaliar os estados intermediários $|\psi_1\rangle, \ldots, |\psi_{11}\rangle$ do algoritimo de Grover, quanto a serem emaranhados ou não, faremos uso de um critério de separabilidade apresentado em Gazzoni (2008).

Considere um estado arbitrário $|\psi\rangle$ composto por 3 qubits, definido por

$$\begin{aligned}|\psi\rangle =&\alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle \\ &+\alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle\end{aligned}',$$

em que $\alpha_0, \ldots, \alpha_7 \in \mathbb{C}$ e $\sum_{i=0}^{7}|\alpha_i|^2 = 1$. Segundo Gazzoni (2008), o estado $|\psi\rangle$ é separável se, e somente se, as equações em 8 forem simultaneamente satisfeitas.

$$\begin{aligned}&\alpha_0\alpha_3 = \alpha_1\alpha_2, && \alpha_1\alpha_7 = \alpha_3\alpha_5,\\ &\alpha_0\alpha_5 = \alpha_1\alpha_4, && \alpha_0\alpha_7 = \alpha_2\alpha_5,\\ &\alpha_2\alpha_7 = \alpha_3\alpha_6, && \alpha_0\alpha_7 = \alpha_1\alpha_6,\\ &\alpha_4\alpha_7 = \alpha_5\alpha_6, && \alpha_0\alpha_7 = \alpha_3\alpha_4.\\ &\alpha_0\alpha_6 = \alpha_2\alpha_4,\end{aligned} \tag{8}$$

A partir desse resultado verificaremos quais dos estados intermediários do algoritmo de Grover para $N = 4$ estão emaranhados.

Para os estados $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_8\rangle$, $|\psi_9\rangle$, $|\psi_{10}\rangle$ e $|\psi_{11}\rangle$ temos que todas as igualdades de 8 são satisfeitas. Logo, esses estados não estão emaranhados.

Para o estado $|\psi_3\rangle$ temos os coeficientes: $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = 1, \alpha_3 = -1, \alpha_4 = 1, \alpha_5 = -1, \alpha_6 = -1, \alpha_7 = 1$. Verifica-se que $\alpha_0\alpha_6 = -1 \neq 1 = \alpha_2\alpha_4$, portanto $|\psi_3\rangle$ está emaranhado.

Para os estados $|\psi_4\rangle$ e $|\psi_6\rangle$ os coeficientes são iguais: $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = 1, \alpha_3 = -1, \alpha_4 = -1, \alpha_5 = 1, \alpha_6 = 1, \alpha_7 = -1$. Analisando as igualdades em (8), observa-se que $\alpha_0\alpha_7 = -1 \neq 1 = \alpha_2\alpha_5$. Assim, $|\psi_4\rangle$ e $|\psi_6\rangle$ estão emaranhados.

No estado $|\psi_5\rangle$ temos: $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = -1, \alpha_3 = 1, \alpha_4 = 1, \alpha_5 = -1, \alpha_6 = 1, \alpha_7 = -1$. Portando, $\alpha_0\alpha_6 = 1 \neq -1 = \alpha_2\alpha_4$, logo $|\psi_5\rangle$ é um estado emaranhado.

Por fim, para o estado $|\psi_7\rangle$ temos: $\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = 0, \alpha_3 = 0, \alpha_4 = 0, \alpha_5 = 0, \alpha_6 = -1, \alpha_7 = 1$. Segue disso que $\alpha_0\alpha_6 = -1 \neq 0 = \alpha_2\alpha_4$, portanto $|\psi_7\rangle$ está emaranhado.

Observa-se que o emaranhamento dos estados acontece após a passagem pela porta Toffoli e que o desemaranhamento acontece após a porta CNOT.

4 Circuito do algoritmo de Shor

A primeira técnica de chave pública é a RSA, inventada em 1977, e ainda é um dos métodos mais utilizados atualmente (FALEIROS, 2011). Nesta técnica, o cálculo do valor da chave privada a partir da chave pública é equivalente ao problema de fatorar um número inteiro muito grande. Tal

[3]Dize-se que um sistema quântico cujo vetor de estado $|\psi\rangle$ é conhecido exatamente está em um estado puro (NIELSEN; CHUANG, 2005).

problema não pode ser resolvido em tempo polinomial por um computador clássico, e isso é o que motiva a utilização desse sistema criptográfico.

Contudo, em 1994 Peter Shor descreveu um algoritmo baseado em propriedades da Mecânica Quântica que resolve o problema da fatoração de um número C em tempo polinomial (SHOR, 1994), o que põe em cheque a segurança do sistema RSA. Esse trabalho apresenta um ganho de velocidade exponencial na solução do problema e reforça a crença de que os computadores quânticos sejam de fato muito mais eficientes do que os clássicos, aumentando a pesquisa na área.

Como mencionado na Introdução, no algoritmo de Shor o problema de fatorar um número C composto é reduzido ao cálculo da ordem de um número menor do que C, escolhido aleatoriamente. Seja x um número coprimo com C, tal que $1 < x < C$ (pois se x e C não forem relativamente primos já teremos que x é um fator de C). Deve-se calcular a ordem de x, ou seja, o menor inteiro r tal que

$$x^r \equiv 1 \bmod C. \tag{9}$$

Nosso interesse é encontrar um fator de C. De (9), segue que $x^r - 1 = pC$, e, assim, $(x^{r/2} - 1)(x^{r/2} + 1) = pC$, para $p \in Z$. Se r for ímpar ou se $x^{r/2} - 1$ ou $x^{r/2} + 1$ forem múltiplos de C, deve-se supor outro valor para x. Do contrário, podemos continuar e teremos que $x^{r/2} - 1$ e $x^{r/2} + 1$ possuem um divisor comum não trivial com C e ele poderá ser encontrado a partir do algoritmo de Euclides.

Aparentemente não há dificuldade para um computador clássico efetuar essas etapas, exceto determinar a ordem de x. Nesse ponto, as características quânticas, em especial a Transformada Quântica de Fourier, fazem a diferença.

Para mais informação sobre o algoritmo de Shor sugerimos as referências (BARNETT, 2009; JAEGER, 2007; NIELSEN; CHUANG, 2005; PORTUGAL *et al*, 2012; VEDRAL, 2006).

Para descrever o funcionamento do algoritmo de Shor e o passo a passo de como o circuito quântico acha a ordem do inteiro x módulo C será utilizado o exemplo $C = 15$, que é o menor número composto não trivial. Apesar de 15 ser um valor muito baixo, para o qual é evidente sua fatoração, é um valor em que podemos fazer os cálculos manualmente e demonstrar como o algoritmo trabalha.

Tomando $C = 15$, iremos escolher x sob as condições apresentadas acima. Sem perda, podemos supor $x = 2$ (consequentemente, sabemos que $r = 4$, mas obteremos essa ordem a partir do circuito).

Agora devemos determinar as entradas no circuito. O número de qubits do segundo registrador, n, deve ser igual a $\lceil \log_2 C \rceil$ (JAEGER, 2007). Já o número de qubits do primeiro registrador, t, deve ser escolhido de forma que $2^t \geq C^2$ (BARNETT, 2009). Porém, se a ordem do elemento x for uma potência de 2 é suficiente tomar $t = n$ (PORTUGAL *et al*, 2012). O conjunto dos números que são coprimos com 15 e são menores que 15 é $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Os elementos 4, 11 e 14 possuem ordem 2 e os elementos 2, 7, 8 e 13 possuem ordem 4. Assim, para o caso $C = 15$ sempre é possível fazer um circuito com $t = n$, independente do valor de x escolhido. No exemplo $n = \lceil \log_2 15 \rceil = 4$, tomamos $t = n = 4$. Então, teremos 4 qubits no primeiro registrador inicializando com $|0000\rangle$ e 4 qubits no segundo registrador inicializando com $|0000\rangle$.

O computador quântico é inicializado no estado $|\psi_0\rangle = |0000\rangle\,|0000\rangle$, conforme Figura 5. Em seguida, são aplicadas as portas de Hadamard nos primeiros 4 qubits, deixando o primeiro registrador em uma superposição de estados da base computacional com amplitude $\dfrac{1}{\sqrt{2^4}}$.

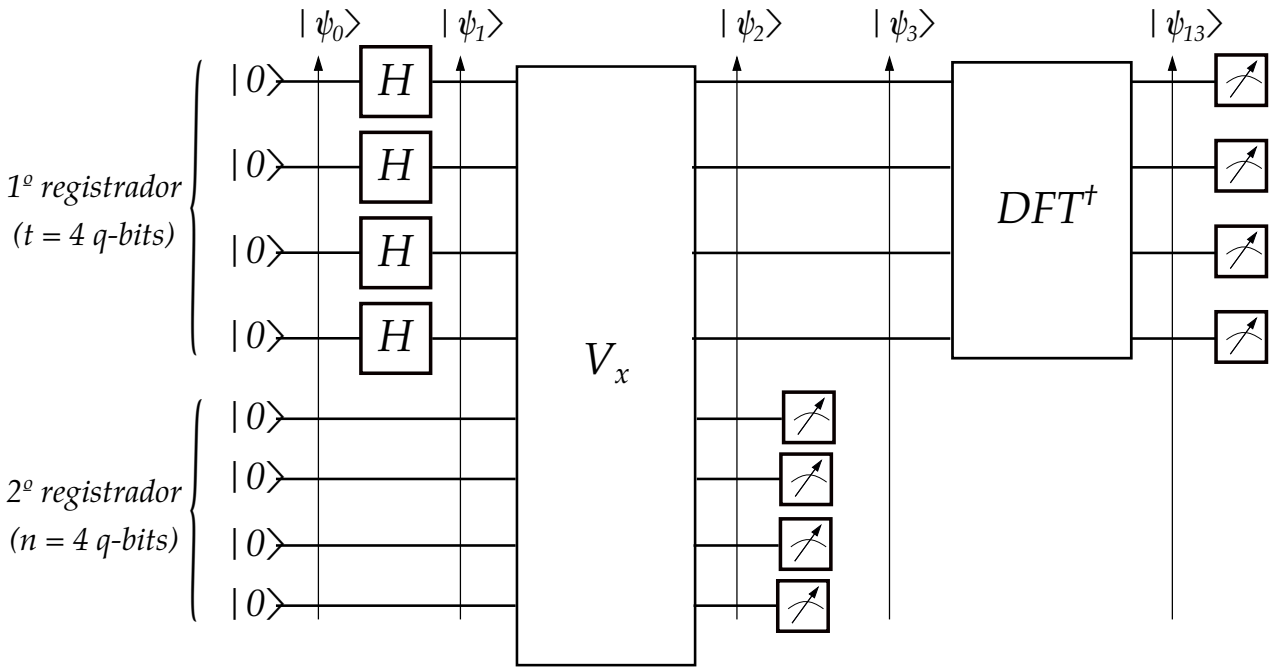

Figura 5 – Circuito do Algoritmo de Shor para N = 15
Fonte: Adaptado de Portugal *et al* (2012).

Depois é aplicado V_x, que é um operador linear unitário dado por $V_x(|j\rangle\,|k\rangle) = |j\rangle\left|k + x^j\right\rangle$, em que $|j\rangle$ e $|k\rangle$ são os estados do primeiro e do segundo registrador, respectivamente. V_x age simultaneamente em todos os termos e gera todas as potências de x. É feita uma medida no segundo registrador, gerando um dos números $\{1, 2, 4, 8\}$ com igual probabilidade. Com a realização da medida do segundo registrador, o primeiro será levado a uma superposição dos estados $|j\rangle$ para os quais 2^j mod 15 é igual à potência medida. Sem perda, consideremos que o resultado da medida sobre o segundo registrador gere 2.

O próximo passo é a aplicação da Transformada de Fourier Inversa $DFT^{-1} = DFT^{\dagger}$ no primeiro registrador, conforme Figura 6.

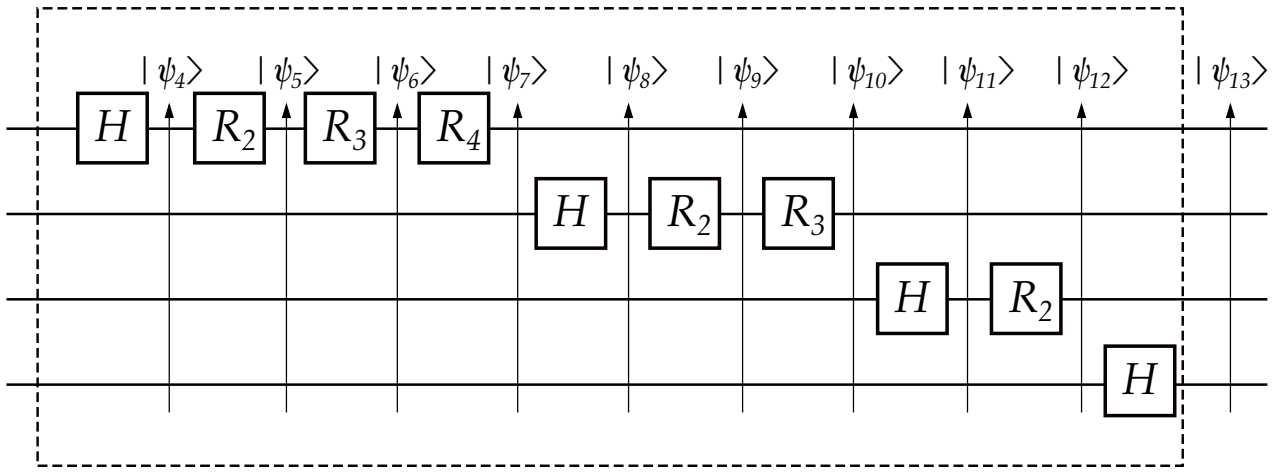

Figura 6 – Circuito da DFT^{-1}
Fonte: Elaborado pelos autores.

Neste momento existem várias etapas que são calculadas uma a uma. O resultado após a $DFT^{\dagger}$ é

$\frac{1}{2}[|0000\rangle - |0001\rangle + i\,|0010\rangle - i\,|0011\rangle]\,|2\rangle$, assim, os estados são equiprováveis com probabilidade $\frac{1}{4}$. É feita, então, uma medida no primeiro registrador. Se o resultado da medida não for coprimo com 2^t, então é preciso rodar o algoritmo novamente. Do contrário, resolve-se por frações contínuas para encontrar o valor de r.

Nas Figuras 5 e 6 as setas verticais apontadas para cima indicam os estados obtidos após cada porta ou operador e os quadrados com H correspondem às portas de Hadamard aplicadas no qubit em que a porta está desenhada. A caixa com $DFT^{\dagger}$ indica a Transformada Quântica de Fourier inversa e seu circuito é apresentado na Figura 6. Na Figura 6 as portas R_2, R_3 e R_4 são dadas pela matriz da Equação 3, para k igual a 2, 3 e 4, respectivamente. Ao final do circuito da Figura 5 temos a representação da medida.

Os estados apresentados nas Figuras 5 e 6 são calculados a seguir:

$$|\psi_0\rangle = |0000\rangle\,|0000\rangle\,.$$

$$\begin{aligned}
|\psi_1\rangle &= (H\otimes H\otimes H\otimes H\otimes I\otimes I\otimes I\otimes I)\,|\psi_0\rangle \\
&= 1/4[|0000\rangle\,|0000\rangle + |0001\rangle\,|0000\rangle + |0010\rangle\,|0000\rangle + |0011\rangle\,|0000\rangle + \\
&\quad |0100\rangle\,|0000\rangle + |0101\rangle\,|0000\rangle + |0110\rangle\,|0000\rangle + |0111\rangle\,|0000\rangle + \\
&\quad |1000\rangle\,|0000\rangle + |1001\rangle\,|0000\rangle + |1010\rangle\,|0000\rangle + |1011\rangle\,|0000\rangle + \\
&\quad |1100\rangle\,|0000\rangle + |1101\rangle\,|0000\rangle + |1110\rangle\,|0000\rangle + |1111\rangle\,|0000\rangle].
\end{aligned}$$

$$\begin{aligned}
|\psi_2\rangle &= V_x\,|\psi_1\rangle \\
&= 1/4[|0000\rangle\,|0001\rangle + |0001\rangle\,|0010\rangle + |0010\rangle\,|0100\rangle + |0011\rangle\,|1000\rangle + \\
&\quad |0100\rangle\,|0001\rangle + |0101\rangle\,|0010\rangle + |0110\rangle\,|0100\rangle + |0111\rangle\,|1000\rangle + \\
&\quad |1000\rangle\,|0001\rangle + |1001\rangle\,|0010\rangle + |1010\rangle\,|0100\rangle + |1011\rangle\,|1000\rangle + \\
&\quad |1100\rangle\,|0001\rangle + |1101\rangle\,|0010\rangle + |1110\rangle\,|0100\rangle + |1111\rangle\,|1000\rangle].
\end{aligned}$$

$$|\psi_3\rangle = 1/2[|0001\rangle + |0101\rangle + |1001\rangle + |1101\rangle]\,|0010\rangle\,.$$

$$\begin{aligned}
|\psi_4\rangle &= (H\otimes I\otimes I\otimes I)\,|\psi_3\rangle \\
&= 1/\sqrt{2}[|0001\rangle + |0101\rangle]\,|0010\rangle
\end{aligned}$$

$$|\psi_5\rangle = (R_2\otimes I\otimes I\otimes I)\,|\psi_4\rangle = |\psi_4\rangle$$

$$|\psi_6\rangle = (R_3\otimes I\otimes I\otimes I)\,|\psi_5\rangle = |\psi_5\rangle$$

$$|\psi_7\rangle = (R_4\otimes I\otimes I\otimes I)\,|\psi_6\rangle = |\psi_6\rangle$$

$$\begin{aligned}
|\psi_8\rangle &= (I\otimes H\otimes I\otimes I)\,|\psi_7\rangle \\
&= |0001\rangle\,|0010\rangle
\end{aligned}$$

$$|\psi_9\rangle = (I\otimes R_2\otimes I\otimes I)\,|\psi_8\rangle = |\psi_8\rangle$$

$$|\psi_{10}\rangle = (I\otimes R_3\otimes I\otimes I)\,|\psi_9\rangle = |\psi_9\rangle$$

$$\begin{aligned}
|\psi_{11}\rangle &= (I\otimes I\otimes H\otimes I)\,|\psi_{10}\rangle \\
&= 1/\sqrt{2}[|0001\rangle + |0011\rangle]\,|0010\rangle
\end{aligned}$$

$$
\begin{aligned}
|\psi_{12}\rangle &= (I \otimes I \otimes R_2 \otimes I)\,|\psi_{11}\rangle \\
&= 1/\sqrt{2}[|0001\rangle + e^{\frac{\pi i}{2}}\,|0011\rangle]\,|0010\rangle \\
|\psi_{13}\rangle &= (I \otimes I \otimes I \otimes H)\,|\psi_{12}\rangle \\
&= 1/2[|0000\rangle - |0001\rangle + i\,|0010\rangle - i\,|0011\rangle]\,|0010\rangle
\end{aligned}
$$

Saindo a medida do primeiro registrador igual a 3, a partir de $3/2^t$ obtemos r (PORTUGAL *et al*, 2012). Então, temos $r = 4$. Por fim, calculamos $(x^{r/2} - 1)$ e $(x^{r/2} + 1)$ para obtermos os fatores de C. Temos para esse exemplo, que $(2^{4/2} - 1) = 3$ e $(2^{4/2} + 1) = 5$. Obtemos, assim, que $15 = 3 \cdot 5$.

5 Conclusões

Grandes empresas na área de computação, tais como IBM, Microsoft e Google, estão investindo fortemente em modelos de computadores quânticos. Nos últimos anos muitos avanços têm confirmado a potencialidade dessas máquinas. Os computadores quânticos apresentados por essas marcas permitem a realização de cálculos e simulações que seriam impossíveis de serem efetuadas em um tempos razoável por computadores clássicos. O uso desses computadores tem sido destinado especialmente a experimentos científicos e pesquisas acadêmicas e governamentais, mas também existem parcerias com empresas de tecnologia, empresas aéreas e outras interessadas em usar os recursos. Atualmente, o computador quântico ocupa muito espaço e precisa ser resfriado em baixas temperaturas. Contudo, suas aplicações podem colaborar para grandes melhorias em setores bancários e financeiros, simulações químicas, eficiência energética, companhias aéreas, entre outros (GIBNEY, 2019; IBM COMUNICA, 2020; LANGSTON, 2019).

Nesse sentido, a pesquisa acerca de computação e informação quântica se faz extremamente necessária. Uma das áreas importantes nesse tema é a de algoritmos quânticos. Os algoritmos de Grover e Shor são dois dos mais conhecidos algoritmos quânticos devido à grande importância dos problemas que conseguem resolver: a busca em um banco de dados desordenado e a fatoração de um número, respectivamente. Além disso, possuem grandes aplicações e são mais eficientes do que os algoritmos para computadores clássicos conhecidos.

Este trabalho proporcionou um aprofundamento no estudo desses algoritmos através do cálculo explícito de cada estado quântico na evolução dos seus circuitos. Dessa forma, é possível compreender melhor a atuação das portas quânticas e também as propriedades de superposição e emaranhamento quântico no momento em que elas aparecem nos circuitos.

Para alguns algoritmos é possível ainda fazer uso de uma interpretação geométrica para o entendimento de seu funcionamento, como no caso do algoritmo de Grover. Para esse algoritmo a interpretação ajuda a entender como a amplitude do elemento procurado vai sendo aumentada ao longo do algoritmo.

Para a execução deste trabalho foi necessário um estudo introdutório de Mecânica Quântica, Portas Quânticas e Algoritmos Quânticos. Além disso, exercitou-se a construção do circuito de Grover por meio do programa IBM Q Cloud para simular circuitos quânticos.

6 Agradecimentos

Agradecemos à Luzinete Cristina Bonani de Faria por disponibilizar parte dos dados que serviram para a realização deste trabalho.

Agradecemos ao revisor por todas as sugestões e considerações que contribuíram sobremaneira para a melhoria do texto.

Este trabalho teve o suporte do CNPq através do projeto 425224/2016-3 e da UFCA.

Referências

BARNETT, S. M. **Quantum information**. New York: Oxford University Press, 2009.

COPPERSMITH, D. **An approximate Fourier transform useful in quantum factoring**. IBM Research Report RC 19642. New York: IBM Research Division, 1994.

FALEIROS, A. C. **Criptografia**. São Carlos: SBMAC, 2011. (Notas em Matemática Aplicada).

GAZZONI, W. C. **Estudo do emaranhamento quântico com base na teoria da codificação clássica**. Tese (Doutorado em Engenharia Elétrica) — Faculdade de Engenharia Elétrica e Computação, Universidade Estadual de Campinas, Campinas, 2008.

GIBNEY, E. **Hello quantum world! Google publishes landmark quantum supremacy claim**. 2019. Disponível em: https://www.nature.com/articles/d41586-019-03213-z. Acesso em: 21 jun. 2020.

GROVER, L. K. A fast quantum mechanical algorithm for database search. *In*: ANNUAL SYMPOSIUM ON THE THEORY OF COMPUTING, 28., 1996, Philadelphia, PA, USA. **Proceedings [...]**. New York, NY, USA: Association for Computing Machinery, 1996. p. 212–219.

IBM COMUNICA. **Do laboratório para a indústria: IBM anuncia últimos avanços em computação quântica**. 2020. Disponível em: https://www.ibm.com/blogs/ibm-comunica/do-laboratorio-para-a-industria-ibm-anuncia-ultimos-avancos-em-computacao-quantica/. Acesso em: 21 jun. 2020.

JAEGER, G. **Quantum information**: an overview. New York: Springer, 2007.

KAYE, P.; LAFLAMME, R.; MOSCA, M. **An introduction to quantum computing**. New York: Oxford University Press, 2007.

LANGSTON, J. **Como a busca pelo computador quântico escalável ajuda a combater o câncer**. 2019. Disponível em: https://news.microsoft.com/pt-br/features/como-a-busca-pelo-computador-quantico-escalavel-ajuda-a-combater-o-cancer/. Acesso em: 21 jun. 2020.

NIELSEN, M. A.; CHUANG, I. L. **Computação quântica e informação quântica**. Porto Alegre: Bookman, 2005.

PALER, A.; DEVITT, S. J. **An introduction to fault-tolerant quantum computing**. 2015. Disponível em: https://arxiv.org/abs/1508.03695. Acesso em: 21 jun. 2020.

PORTUGAL, R. **Algoritmos quânticos de busca**. São Carlos: SBMAC, 2010. (Notas em Matemática Aplicada).

PORTUGAL, R.; GONÇALVES, D. N. **Códigos quânticos corretores de erros**. São Carlos: SBMAC, 2012. (Notas em Matemática Aplicada).

PORTUGAL, R. *et al*. **Uma introdução à computação quântica**. São Carlos: SBMAC, 2012. (Notas em Matemática Aplicada).

PRESKILL, J. **Fault-tolerant quantum computation**. 1997. Disponível em: https://arxiv.org/abs/quant-ph/9712048. Acesso em: 21 jun. 2020.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *In*: ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, 35., 1994, Santa Fé, NM, USA. **Proceedings [...]**. Santa Fé: [*s.n.*], 1994. p. 124–134.

VEDRAL, V. **Introduction to quantum information science**. New York: Oxford University Press, 2006.