

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**

**MATHEUS GIOVANNI DIAS**

**ALGORITMOS QUÂNTICOS E O PROBLEMA DA CLIQUE MÁXIMA EM  
GRAFOS**

**CURITIBA**

**2022**

**MATHEUS GIOVANNI DIAS**

**ALGORITMOS QUÂNTICOS E O PROBLEMA DA CLIQUE MÁXIMA EM  
GRAFOS**

**Quantum Algorithms and the Maximum Clique Problem in Graphs**

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Computação do Curso de Graduação em Engenharia de Computação da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Leandro M. Zatesko

**CURITIBA**

**2022**



[4.0 Internacional](https://creativecommons.org/licenses/by/4.0/)

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

**MATHEUS GIOVANNI DIAS**

**ALGORITMOS QUÂNTICOS E O PROBLEMA DA CLIQUE MÁXIMA EM  
GRAFOS**

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia de Computação do Curso de Graduação em Engenharia de Computação da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 14 de setembro de 2022

---

Leandro Miranda Zatesko  
Doutorado em Ciência da Computação  
Universidade Tecnológica Federal do Paraná

---

Marina Esther Groshaus  
Doutorado em Ciência da Computação  
Universidade Tecnológica Federal do Paraná

---

Murilo Vicente Gonçalves da Silva  
Doutorado em Ciência da Computação  
Universidade Federal do Paraná

**CURITIBA**  
**2022**

## **AGRADECIMENTOS**

Aproveito esta oportunidade para oferecer os meus agradecimentos a todos aqueles que contribuíram para a minha formação. Agradeço aos meus pais, que me forneceram as oportunidades; agradeço aos meus professores, que me forneceram o conhecimento; agradeço ao meu orientador, que me guiou nesta trajetória e agradeço aos membros da banca, por avaliar este trabalho e por compartilhar sua expertise a fim de melhorar a qualidade deste e de meus futuros trabalhos.

## RESUMO

Determinar a cardinalidade da clique máxima em um grafo simples é um problema NP-difícil com diversas aplicações de interesse. O melhor algoritmo clássico conhecido para este problema tem complexidade de tempo  $\mathcal{O}(3^{n/3})$ . A computação clássica utiliza fenômenos da física clássica para modelar, armazenar e processar a informação. Consequentemente, todo o modelo de computação clássica é limitado superiormente pelos limites da física clássica. Como alternativa, a Computação Quântica foi desenvolvida para aproveitar os fenômenos quânticos e proporcionar a construção de circuitos capazes de realizar certas computações de forma mais eficiente. Neste trabalho serão propostas e analisadas duas soluções quânticas para o problema da clique máxima, baseadas nos algoritmos de Busca Quântica de Grover e no Algoritmo Quântico de Busca do Mínimo, comparando suas respectivas complexidades de tempo com a melhor solução clássica conhecida.

**Palavras-chave:** subconjuntos de vértices com propriedades especiais; algoritmos quânticos e complexidade na teoria da computação; algoritmos em grafos.

## ABSTRACT

Determining the cardinality of the maximum clique on a simple graph is a NP-hard problem with several applications of interest. The best known classical algorithm for this problem has  $\mathcal{O}(3^{n/3})$  time complexity. Classical computing uses phenomena from classical physics to model, store and process information. Consequently, the entire model of classical computing is bounded superiorly by the limits of classical physics. As an alternative, Quantum Computing has been developed to take advantage of quantum phenomena and provide the constructions of circuits capable of performing certain computations more efficiently. In this paper, two quantum solutions to the maximum clique problem will be proposed and analyzed, based on the Grover Quantum Search algorithms and the Quantum Minimal Search Algorithm, comparing their respective time complexities with the best known classical solution.

**Keywords:** vertex subsets with special properties; quantum algorithms and complexity in the theory of computation; graph algorithms.

## LISTA DE FIGURAS

Figura 1 – Clique máxima em um grafo simples . . . . .	7
Figura 2 – Divisor de feixe . . . . .	10
Figura 3 – Configuração com dois divisores de feixe . . . . .	11
Figura 4 – Colapso de uma sobreposição quântica de dois estados . . . . .	14
Figura 5 – Esfera de Bloch . . . . .	22
Figura 6 – Diagrama de circuito . . . . .	23
Figura 7 – Operação NOT na esfera de Bloch . . . . .	24
Figura 8 – Representação compacta de portas controladas por sinais negados . . . . .	25
Figura 9 – Representação do vetor de estado no círculo unitário . . . . .	31
Figura 10 – Efeito de $U_f$ . . . . .	32
Figura 11 – Bases $\{ \Psi_{bad}\rangle,  \Psi_{good}\rangle\}$ e $\{ \Psi\rangle,  \neg\Psi\rangle\}$ . . . . .	33
Figura 12 – Efeito de $G$ sobre $ \Psi\rangle$ . . . . .	33
Figura 13 – O oráculo de Wie . . . . .	37
Figura 14 – Contador de elementos na clique máxima (3 qubits) . . . . .	40
Figura 15 – Oráculo de Wie-Bojié (3 qubits) . . . . .	41
Figura 16 – Comparador Unário . . . . .	43

## SUMÁRIO

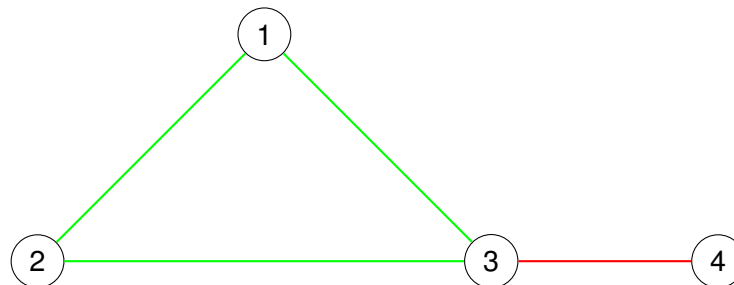
1	INTRODUÇÃO . . . . .	7
2	FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA . . . . .	10
2.1	Mecânica quântica e computação . . . . .	10
2.2	Vetores de estado, o espaço de Hilbert e o bit quântico . . . . .	13
2.3	Vetores duais e espaço dual . . . . .	15
2.4	Notação de Dirac . . . . .	16
2.5	Produto tensorial e registradores quânticos . . . . .	17
2.6	Base de Hadamard . . . . .	20
2.7	Estados equivalentes e esfera de Bloch . . . . .	21
2.8	Circuitos quânticos . . . . .	22
3	ALGORITMO DE GROVER . . . . .	27
3.1	O problema de busca cega . . . . .	27
3.2	Caixa preta quântica . . . . .	27
3.3	Aplicação do fenômeno da sobreposição . . . . .	28
3.4	Aplicação do fenômeno da interferência . . . . .	29
3.5	A iteração de Grover . . . . .	30
3.6	O algoritmo de busca quântica de Grover . . . . .	30
3.7	O efeito da iteração de Grover . . . . .	31
3.8	Complexidade do algoritmo . . . . .	34
4	ALGORITMOS QUÂNTICOS PARA CLIQUES . . . . .	36
4.1	O algoritmo de Wie . . . . .	36
4.2	O algoritmo de Bojié . . . . .	38
5	NOVAS PROPOSTAS . . . . .	39
5.1	Algoritmo de busca de Wie–Bojié . . . . .	39
5.2	Algoritmo quântico de otimização . . . . .	41
6	CONSIDERAÇÕES FINAIS . . . . .	45
	REFERÊNCIAS . . . . .	46



## 1 INTRODUÇÃO

Na teoria dos grafos uma clique em um grafo simples é um subconjunto de vértices onde cada par de vértices distintos são adjacentes (conectados por uma aresta), cliques são uma estrutura particularmente interessante e possuem aplicações em diversos problemas, como por exemplo análise de relacionamentos em redes sociais, diversos problemas da bioinformática, análise de redes de comunicação e estudo de estruturas químicas. Quando uma clique não está contida em uma outra clique, de maior cardinalidade, no mesmo grafo, ela é denominada clique maximal, as cliques maximais de maior cardinalidade em um grafo, são denominadas clique máximas. A Figura 1 ilustra um grafo simples com cinco cliques ( $\{1, 2\}$ ,  $\{1, 3\}$ ,  $\{2, 3\}$ ,  $\{1, 2, 3\}$  e  $\{3, 4\}$ ), sendo duas cliques maximais ( $\{1, 2, 3\}$  e  $\{3, 4\}$ ) e uma clique máxima ( $\{1, 2, 3\}$ ).

**Figura 1 – Clique máxima em um grafo simples**



**Fonte: A autoria própria (2022).**

Determinar a cardinalidade da clique máxima em um grafo é um problema NP-Difícil (KARP, 1972) com a melhor solução clássica conhecida para este problema tendo complexidade de tempo  $\mathcal{O}(3^{n/3})$ . O problema da clique máxima também é difícil de aproximar (HÅSTAD, 1999), isto é para qualquer  $\varepsilon > 0$ , não pode haver um algoritmo de aproximação em tempo polinomial para o problema, com um fator de aproximação de  $\mathcal{O}(n^{1-\varepsilon})$ , a menos que  $P = NP$ .

Diversos problemas de interesse são difíceis de se solucionar, ou até mesmo aproximar, utilizando os fundamentos da computação clássica. Isso incentivou a pesquisa em modelos de computação alternativos, dentre eles a computação quântica. Computadores são dispositivos físicos e como tais, estão sujeitos as limitações das leis da física. Enquanto os computadores clássicos são baseados e sujeitos às limitações dos modelos da física clássica, os computadores quânticos se baseiam nos modelos da física quântica, o que os permitem utilizar fenômenos quânticos para obter um ganho de performance em comparação ao seu equivalente clássico, para certos problemas.

O algoritmo de Busca Quântica de Grover é um algoritmo quântico que proporciona um ganho quadrático sobre a complexidade de tempo da melhor solução clássica para uma série de problemas importantes. O algoritmo utiliza os fenômenos de sobreposição e interferência quântica para buscar em um conjunto de possíveis soluções por um valor  $x$  que satisfaça uma função de caixa preta booleana  $f : \{0, 1\}^n \mapsto \{0, 1\}$ , denominado como o oráculo do problema, isto é,  $f(x) = 1$ , quando  $x$  é uma solução para o problema e  $f(x) = 0$ , caso contrário. Após

$\mathcal{O}(\sqrt{2^n})$  medições da função, a probabilidade de uma solução ser encontrada é  $1 - \mathcal{O}(1/n)$ . Diversos autores investigaram a possibilidade de utilizar algoritmos quânticos, como o algoritmo de Grover, a fim de obter um ganho de performance sobre a melhor solução clássica conhecida para diversos problemas computacionais.

Bojié propôs um algoritmo, baseado na busca quântica de Grover, para encontrar uma clique máxima em um grafo simples  $G$  (BOJIE, 2012). Utilizando uma abordagem iterativa, o algoritmo de Bojié percorre linearmente uma lista de possíveis cliques (subgrafos em  $G$ ) buscando cliques de cardinalidades cada vez maiores. Quando o algoritmo não é capaz de encontrar uma clique, assume-se que a última clique encontrada é uma clique máxima. No entanto, o autor não fornece a implementação do oráculo para a busca de Grover, nem sequer considera a complexidade de construção de tal oráculo, apenas sua descrição matemática é fornecida:

$$f(x) = \begin{cases} 1, & \text{se } x \text{ codifica uma clique maximal com pelo menos } k \text{ elementos;} \\ 0, & \text{caso contrário.} \end{cases}$$

Wie propôs um algoritmo, baseado na busca quântica de Grover, para encontrar todas as cliques maximais (não necessariamente máximas) em um grafo simples  $G$  (WIE, 2017). O algoritmo retorna uma superposição de todos os estados quânticos que descrevem uma clique maximal em  $G$ . Em seu trabalho, o autor inclui a descrição do oráculo, junto com as instruções para sua construção:

$$f(x) = \begin{cases} 1, & \text{se } x \text{ codifica uma clique maximal;} \\ 0, & \text{caso contrário.} \end{cases}$$

Neste trabalho, são propostas e analisadas duas soluções para o problema da clique máxima: a primeira, baseada nos algoritmos de Bojié e Wie, utiliza um oráculo de Wie modificado para atender aos critérios do algoritmo de Bojié, o algoritmo também é alterado para utilizar uma busca binária ao invés de uma linear ao procurar por cliques em  $G$  com cardinalidades incrementais. Tais modificações resultam em uma complexidade de tempo final de  $\mathcal{O}(\sqrt{2^n}(n \log n)^2)$ , representando um ganho de  $\mathcal{O}(\sqrt{2^n}(n \log n)^2 3^{-n/3})$  sobre a melhor solução clássica conhecida.

A segunda consiste em utilizar um algoritmo quântico de otimização para buscar um valor  $x$ , que codifica uma clique maximal em  $G$ , que maximiza o valor de uma função  $f : x \mapsto \alpha|x|$ , onde  $\alpha$  é um número real não negativo; assume-se que o valor encontrado é uma clique máxima em  $G$ . A complexidade de tempo desta proposta depende do algoritmo de otimização escolhido, no caso, utilizamos uma versão modificada do Algoritmo Quântico de Busca do Mínimo (DÜRR; HØYER, 1996) para encontrar o máximo, resultando em uma complexidade final de  $\mathcal{O}(\sqrt{n^2 2^n})$ , representando um ganho de  $\mathcal{O}(n\sqrt{2^n} 3^{-n/3})$  sobre a melhor solução clássica conhecida.

Este trabalho está dividido em seis capítulos, com o primeiro sendo esta introdução. No segundo capítulo é feita uma introdução aos fundamentos básicos da computação quântica necessários para o entendimento deste trabalho. No terceiro capítulo apresentamos o algoritmo de Grover, os fundamentos por trás de seu funcionamento e a análise de sua complexidade computacional. No quarto capítulo são apresentados os algoritmos de Wie e Bojié para busca de cliques maximais e máximas, respectivamente, em grafos simples. No quinto capítulo são apresentadas nossas propostas de solução para o problema da clique máxima, bem como suas análises de complexidade. Por fim, o sexto capítulo reúne as considerações finais dos autores deste trabalho.

## 2 FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA

Neste capítulo serão discutidos os fundamentos de Mecânica Quântica e Computação Quântica necessários para o entendimento do Algoritmo de Grover. Este capítulo está fundamentado na obra *An Introduction to Quantum Computing* (KAYE; LAFLAMME; MOSCA, 2007).

### 2.1 Mecânica quântica e computação

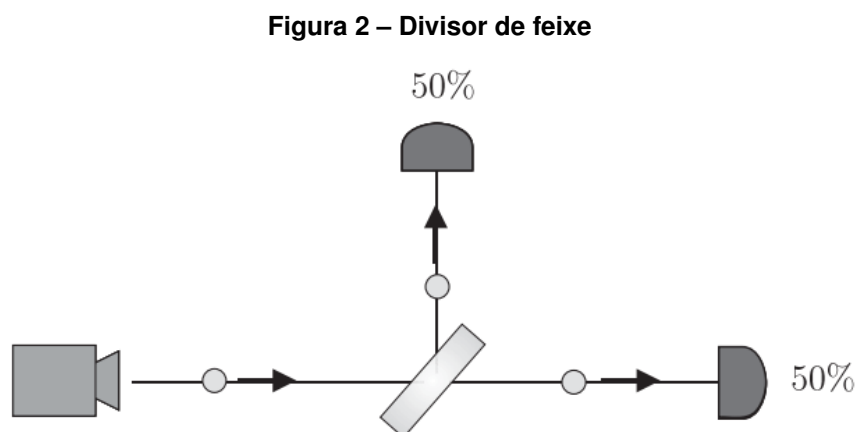
Para que a informação seja útil, deve ser armazenada e manipulada através de processos físicos. Como consequência, a capacidade computacional de qualquer máquina que processe informação é limitada pelas leis da física.

As máquinas de computação clássica foram desenvolvidas tendo como base os fenômenos descritos pela física clássica, a qual consegue descrever com alta precisão fenômenos que podem ser observados por humanos, no entanto falha quando a escala dos fenômenos torna-se subatômica.

Diversos fenômenos subatômicos não podem ser explicados através da física clássica e têm resultados contraintuitivos. Isso levou a necessidade da criação de uma nova física a fim de descrever os fenômenos quânticos.

A computação quântica se desenvolveu em uma tentativa de utilizar as propriedades dos sistemas quânticos a fim de criar dispositivos computacionais sem as limitações impostas pela mecânica clássica.

O seguinte experimento ilustra como fenômenos quânticos podem ser contraintuitivos e não podem ser expressos em termos da física clássica, mas tem uma explicação simples em termos da mecânica quântica. Suponha uma configuração experimental composta por uma fonte de fótons, um espelho semitransparente e um par de detectores de fótons posicionados, de tal forma que o espelho atue como um divisor de feixe e o feixe de fótons disparado pela fonte atinja os dois detectores simultaneamente, como ilustra a Figura 2.

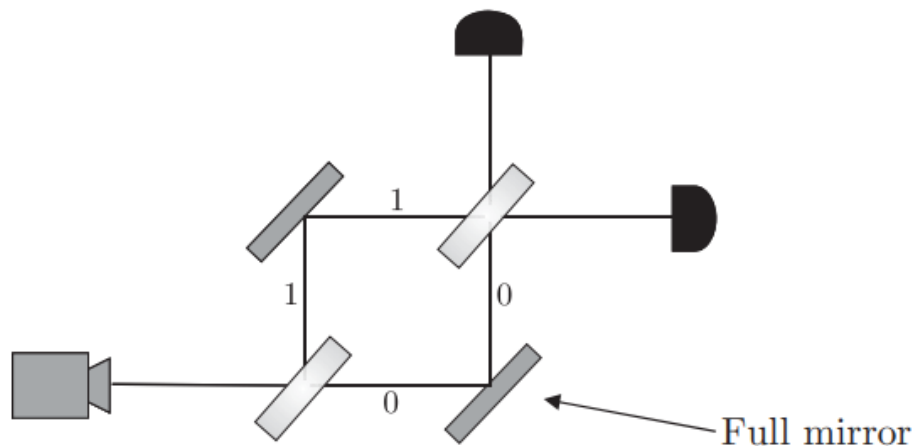


Fonte: Kaye, Laflamme e Mosca (2007).

Suponha que ao invés de um feixe, a fonte dispare uma série de fótons individuais, se observa que os fótons são detectados pelo primeiro detector (à direita) metade do tempo e pelo segundo (ao topo), pela outra metade. Em termos da física clássica pode-se dizer que o divisor atua como um “lançador de moedas”, refletindo ou deixando passar o fótons com probabilidades iguais.

Suponha agora que uma modificação seja feita à configuração, incluindo dois espelhos semi transparentes e dois espelhos completamente reflexivos, como ilustrado pela Figura 3.

**Figura 3 – Configuração com dois divisores de feixe**



**Fonte: Kaye, Laflamme e Mosca (2007).**

Tratando cada um dos divisores individualmente, a física clássica prevê que o resultado desta configuração permanece inalterado, com os fótons sendo captados por cada um dos detectores 50% do tempo. No entanto ao executar o experimento, observa-se que os fótons são captados pelo detector ao topo 100% do tempo.

A física clássica falha ao tentar prever o resultado deste experimento. Um simples modelo probabilístico não é suficiente para explicar os fenômenos que ocorrem neste sistema. A física quântica, no entanto, nos oferece uma nova ótica e fornece uma simples explicação para o resultado observado. Para isso introduz dois novos conceitos: a sobreposição e a interferência.

Na primeira configuração, o fóton pode seguir um de dois caminhos: atravessar o divisor e atingir o detector à direita, ou ser refletido e atingir o detector no topo. Podemos considerar esta configuração como um sistema de dois estados, onde a presença do fóton no caminho que leva ao detector à direita é denominado estado 0 e representado pelo vetor

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

e a presença do fóton no caminho que leva ao detector ao topo, denominado estado 1, representado pelo vetor

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

As razões pelas quais os estados são representados por vetores ficarão mais claras a seguir.

Ao ser disparado pela fonte, o fóton se encontra no estado 0; no entanto, ao atingir o divisor de feixe, o estado do fóton é alterado. Segundo o modelo da física clássica o fóton pode estar em apenas um dos dois estados em um dado instante de tempo, mas com a física quântica podemos modelar um sistema em que o fóton esteja em ambos os estados simultaneamente, fenômeno denominado *sobreposição*. Ao atingir o divisor o fóton entra em uma sobreposição dos estados 0 e 1 que pode ser descrita como uma combinação linear dos vetores dos estados básicos:

$$\alpha_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}. \quad (1)$$

O fóton permanece no estado de sobreposição até que sofra uma medição, o que ocorre ao atingir um dos detectores. A partir de então assume e permanece em um dos estados básicos, fenômeno denominado *colapso* do sistema. O estado após o colapso tem probabilidade  $|\alpha_0|^2$  de ser o estado 0 e  $|\alpha_1|^2$  de ser o estado 1.

Uma vez que os estados são representados por vetores, pode-se representar o efeito do divisor de feixe sobre o estado do fóton como um operador linear, representado por uma matriz. Pode-se descrever matematicamente o efeito do divisor como uma multiplicação matricial do operador pelo vetor de estado, que no caso deste experimento é dada por

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}. \quad (2)$$

Note que a probabilidade de o fóton ser encontrado no estado 0 é  $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$  e  $\left|\frac{i}{\sqrt{2}}\right|^2 = \frac{1}{2}$  para o estado 1. Note também que o modelo corresponde ao comportamento observado na primeira configuração.

Na segunda configuração, o sistema se inicia no estado 0. Assim como anteriormente, o fóton passa pelo primeiro divisor e então é redirecionado pelos espelhos reflexivos para um segundo espelho semitransparente. Matematicamente, o operador que descreve o divisor é aplicado no vetor de estado duas vezes. Ao aplicar novamente o operador ao vetor de estado,

$$\left( \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \right) \left( \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} \right) = \begin{bmatrix} 0 \\ i \end{bmatrix}, \quad (3)$$

prevê-se que o sistema passa a ter  $|0|^2 = 0\%$  de probabilidade de colapsar no estado 0 e  $|1|^2 = 100\%$  de colapsar no estado 1, ou seja, apenas o detector ao topo passa a captar os fótons, exatamente como observado.

O primeiro divisor deixa o sistema em uma sobreposição de dois estados de base, ambos os quais se encontram no segundo divisor onde interferem um com o outro, provocando o aumento da amplitude do estado 1 e redução da amplitude do estado 0 (fenômeno da interferência). Uma vez que a física clássica não permite sobreposições de estados, ela falha ao prever a interferência, e por consequência falha ao tentar prever o resultado deste experimento.

## 2.2 Vetores de estado, o espaço de Hilbert e o bit quântico

Os estados de um sistema quântico são representados por vetores unitários em um espaço vetorial  $n$ -dimensional com componentes complexas  $\mathbb{C}^n$ , onde  $n$  é o número de estados de base do sistema:

$$|\psi\rangle = \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_n \end{bmatrix}, \quad (4)$$

cada componente  $p_i$  do vetor é denominada amplitude de probabilidade e está associada à probabilidade de colapso do sistema no estado de base correspondente, de tal forma que  $|p_i|^2$  é a probabilidade do sistema colapsar no estado fundamental  $i$ . Para a mecânica quântica todo espaço vetorial em  $\mathbb{C}$  de dimensões finitas é um *espaço de Hilbert*  $\mathcal{H}$ .

Ao se realizar uma medição, o sistema quântico necessariamente colapsa em um dos seu estados de base de acordo com as probabilidades associadas; qualquer medição após o colapso retornará sempre o mesmo valor. A Figura 4 retrata o processo de colapso de um sistema quântico de dois estados. Note que apesar de possuir diferentes valores de amplitudes, os estados possuem a mesma probabilidade de colapso.

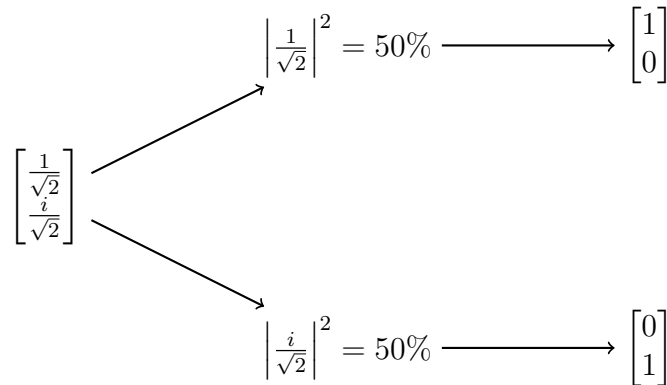
Uma vez que uma medição necessariamente provoca o colapso do sistema, a soma das probabilidades deve sempre ser igual a 1, ou seja:

$$\sum_{i=0}^n |p_i|^2 = \langle \psi, \psi \rangle = \|\psi\|^2 = 1. \quad (5)$$

Note que (5) implica que todos os vetores de estado são unitários.

Ao se trabalhar com vetores, deve-se ter uma base vetorial definida. Este conceito dá propriamente significado para os componentes do vetor. Na Computação Quântica, geralmente se utiliza a Base Computacional para expressar os vetores de estado, sendo tal base formada

**Figura 4 – Colapso de uma sobreposição quântica de dois estados**



**Fonte: Autoria própria (2022).**

pelos vetores  $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$  e  $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ , cada um representando um dos estados básicos de um sistema de dois estados. Um vetor de estado pode ser expresso como uma combinação linear dos vetores da base computacional:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (6)$$

Sistemas quânticos de dois estados são particularmente interessantes para a Computação Quântica pois representam a extensão quântica do elemento básico de informação da Computação Clássica, o bit.

O bit quântico ou *qubit* (do inglês *quantum bit*), de forma análoga ao bit, possui dois estados de base, porém, devido à natureza quântica do sistema, qubits podem assumir ambos os estados simultaneamente através de sobreposições, sendo representados por vetores de estados em um espaço de Hilbert de 2 dimensões.

Qubits são geralmente expressos como combinações lineares em termos da base computacional:

$$|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (7)$$

Da mesma forma que bits, qubits não estão restritos a uma implementação física específica. Qualquer sistema quântico de dois estados, incluindo o sistema descrito na Figura 2, pode ser considerado um qubit. Deve ser acordado previamente qual estado do sistema será associado aos estados de base, no experimento do divisor de feixe, considerou-se que a presença do fóton no caminho que leva ao detector à direita como sendo o estado de base  $|0\rangle$  e a presença no caminho que leva ao detector ao topo como o estado de base  $|1\rangle$ .

Outros exemplos de possíveis implementações físicas de qubits (DIVINCENZO, 2000) são:



- O spin de um elétron, onde um spin up é associado ao estado  $|0\rangle$  e um spin down ao estado  $|1\rangle$ ;
- Uma partícula com dois estados de excitação, onde o primeiro é associado a  $|0\rangle$  e o segundo a  $|1\rangle$ ;
- A polarização de um fóton, onde uma polarização horizontal é associada ao estado  $|0\rangle$  e uma vertical ao estado  $|1\rangle$ .

Um qubit no entanto não pode ser observado em um estado de sobreposição, uma vez que uma medição necessariamente provoca o colapso do sistema quântico, forçando-o a assumir e permanecer em um dos seus estados de base. Desta forma apenas o fenômeno da sobreposição não oferece qualquer ganho de performance sobre a Computação Clássica, uma vez que o comportamento pode ser simulado através de algoritmos pseudo-aleatórios ou verdadeiro-aleatórios, no entanto é possível explorar outros fenômenos e propriedades quânticas antes de se realizar a medição a fim de construir circuitos quânticos capazes de resolver certos problemas de forma extremamente eficiente quando comparados a circuitos clássicos.

### 2.3 Vetores duais e espaço dual

Assim como os espaços euclidianos (como espaços vetoriais finitos sobre os números reais), os espaços de Hilbert também possuem um produto interno  $\langle, \rangle$  definido, uma operação vetorial binária que relaciona um par de vetores a um único número complexo enquanto satisfaz as propriedades de:

- linearidade no segundo argumento:

$$\left\langle v, \sum_i \lambda_i w_i \right\rangle = \sum_i \lambda_i \langle v, w_i \rangle, \quad (8)$$

- comutatividade conjugada:

$$\langle v, w \rangle = \langle w, v \rangle^*, \quad (9)$$

- não negatividade:

$$\langle v, v \rangle \geq 0. \quad (10)$$

O produto interno padrão de um espaço de Hilbert é o produto escalar, definido por

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} v_1^* & v_2^* & \dots & v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \sum_{i=1}^n v_i^* w_i, \quad (11)$$

onde o símbolo de estrela (\*) representa o complexo conjugado do número complexo associado.

A matriz coluna obtida ao transpor um vetor  $v$  e tomar os complexos conjugados de suas componentes (transposto conjugado) é denominada dual de  $v$  ou vetor dual associado a  $v$ . Desta forma o produto escalar pode ser definido como a multiplicação matricial à esquerda do segundo vetor pelo dual do primeiro.

Os duais dos vetores de um determinado espaço de Hilbert  $\mathcal{H}$  também podem ser considerados vetores e, portanto, formam um segundo espaço de Hilbert denominado espaço dual  $\mathcal{H}^*$ . Assim tem-se que:

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathcal{H} \iff \begin{bmatrix} v_1^* & v_2^* & \dots & v_n^* \end{bmatrix} \in \mathcal{H}^*. \quad (12)$$

## 2.4 Notação de Dirac

Para representar o estado de um sistema quântico com  $n$  estados de base, é necessário um vetor de  $n$  dimensões. A notação vetorial de matriz coluna pode desperdiçar espaço ao representar sistemas resultantes da sobreposição de poucos estados de base. Uma forma mais objetiva de representar tais estados é através da notação de Dirac.

Também denominada notação bra-ket, a notação de Dirac foi criada como uma forma de representar vetores unitários em espaços de Hilbert e é amplamente utilizada na mecânica quântica para representar vetores de estado.

Os vetores de base são representados como símbolos dentro de kets  $| \rangle$ , os demais vetores são representados como combinação linear dos vetores de base. Desta forma, um vetor de estado bidimensional, em termos da base computacional, é representado como

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (13)$$

, onde  $\alpha$  e  $\beta$  são números complexos.

A notação de Dirac também permite representar sistemas mais complexos, com mais de dois estados de base. Todas as seguintes notações são formas válidas e equivalentes de retratar um sistema de quatro estados em termos da base computacional:

$$|r\rangle = \alpha |0\rangle \otimes |0\rangle + \beta |0\rangle \otimes |1\rangle + \gamma |1\rangle \otimes |0\rangle + \delta |1\rangle \otimes |1\rangle , \quad (14a)$$

$$|r\rangle = \alpha |0\rangle |0\rangle + \beta |0\rangle |1\rangle + \gamma |1\rangle |0\rangle + \delta |1\rangle |1\rangle , \quad (14b)$$

$$|r\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle . \quad (14c)$$

A notação de Dirac costuma economizar espaço, quando comparada à notação vetorial de matriz coluna, e permite representar sistemas resultantes da sobreposição de poucos estados de forma mais objetiva:

$$|r\rangle = \begin{bmatrix} \alpha \\ 0 \\ 0 \\ \delta \end{bmatrix} , \quad (15a)$$

$$|r\rangle = \alpha |00\rangle + 0 |01\rangle + 0 |10\rangle + \delta |11\rangle , \quad (15b)$$

$$|r\rangle = \alpha |00\rangle + \delta |11\rangle . \quad (15c)$$

Para representar o dual de um vetor, utiliza-se o mesmo símbolo que representa o vetor, porém dentro de um bra  $\langle |$ :

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} , \quad (16a)$$

$$\langle\psi| = \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} . \quad (16b)$$

Desta forma, a notação de Dirac permite representar produtos internos de forma bastante elegante ao combinar bras e kets em um bracket:

$$|\psi\rangle \cdot |\phi\rangle = \langle\psi|\phi\rangle . \quad (17)$$

## 2.5 Produto tensorial e registradores quânticos

Embora não seja exclusivo dos espaços de Hilbert, também está definido para espaços euclidianos, os produtos tensoriais são amplamente utilizados na Computação Quântica. O produto tensorial é uma operação binária de composição definida para diversos objetos mate-

máticos, detre os quais vetores, espaços vectoriais, e matrizes, que relaciona dois elementos do mesmo tipo a um terceiro de maiores dimensões.

Sejam dois espaços de Hilbert  $\mathcal{H}_1$  e  $\mathcal{H}_2$  de dimensões  $n$  e  $m$ , respectivamente, o produto tensorial  $\mathcal{H}_1 \otimes \mathcal{H}_2$  é um terceiro espaço de Hilbert de dimensões  $nm$  composto pelos produtos tensoriais entre os vetores pertencentes a  $\mathcal{H}_1$  e  $\mathcal{H}_2$ :

$$|\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2 \iff (|\psi\rangle \otimes |\phi\rangle) \in (\mathcal{H}_1 \otimes \mathcal{H}_2). \quad (18)$$

Sejam dois vetores de estado  $|\psi\rangle$  e  $|\phi\rangle$  de dimensões  $n$  e  $m$ , respectivamente, o produto tensorial  $|\psi\rangle \otimes |\phi\rangle$  é um terceiro vetor, de dimensões  $nm$ , cujas componentes são os produtos entre as componentes de  $|\psi\rangle$  e  $|\phi\rangle$ :

$$|\psi\rangle \otimes |\phi\rangle = |\psi\phi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{bmatrix} \otimes \begin{bmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_m \end{bmatrix} = \begin{bmatrix} \psi_1\phi_1 \\ \psi_1\phi_2 \\ \vdots \\ \psi_1\phi_m \\ \psi_2\phi_1 \\ \vdots \\ \vdots \\ \psi_n\phi_m \end{bmatrix}. \quad (19)$$

Sejam duas matrizes (ou operadores vectoriais)  $A$  e  $B$  de dimensões  $m \times n$  e  $p \times q$ , respectivamente, o produto tensorial  $A \otimes B$  é a matriz, de dimensões  $mp \times nq$ , expressa por

$$A \otimes B = \begin{bmatrix} A_{11}B_{11} & \dots & A_{11}B_{1q} & \dots & \dots & A_{1n}B_{11} & \dots & A_{1n}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{11}B_{p1} & \dots & A_{11}B_{pq} & \dots & \dots & A_{1n}B_{p1} & \dots & A_{1n}B_{pq} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{11} & \dots & A_{m1}B_{1q} & \dots & \dots & A_{mn}B_{11} & \dots & A_{mn}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{p1} & \dots & A_{m1}B_{pq} & \dots & \dots & A_{mn}B_{p1} & \dots & A_{mn}B_{pq} \end{bmatrix}, \quad (20)$$

uma representação mais compacta de (20) é a “forma de bloco”, expressa por

$$A \otimes B = \begin{bmatrix} A_{11}[B] & A_{12}[B] & \dots & A_{1n}[B] \\ A_{21}[B] & A_{22}[B] & \dots & A_{2n}[B] \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}[B] & A_{m2}[B] & \dots & A_{mn}[B] \end{bmatrix}, \quad (21)$$

onde  $[B]$  representa a submatriz  $B$ , cada valor  $A_{ij}[B]$  é a matriz  $[B]$  multiplicada pelo valor na linha  $i$ , coluna  $j$ , da matriz  $A$ .

No contexto da Computação Quântica, o produto tensorial é utilizado para representar sistemas quânticos complexos através da composição de qubits, formando registradores quânticos.

Enquanto um registrador clássico dobra a quantidade de valores a cada bit adicionado, um registrador quântico dobra a quantidade de estados de base, conseqüentemente as dimensões do espaço de Hilbert, a cada qubit adicionado. Como todos os sistemas quânticos considerados pela computação quântica são formados por qubits, todos os espaços de Hilbert considerados pela computação quântica têm dimensão  $2^n$ , sendo  $n$  é o número de qubits.

A base de um registrador quântico é dada pelo resultado do produto tensorial entre os estados de base dos qubits individuais. Se a base considerada para os qubits for a computacional, a base de um registrador de  $n$  qubits é dada por

$$\{|0\rangle, |1\rangle\}^{\otimes n} = \{|00\dots 0\rangle, |00\dots 1\rangle, \dots, |11\dots 0\rangle, |11\dots 1\rangle\}. \quad (22)$$

Pelo *postulado da composição de sistemas*, o estado de um sistema composto formado por dois ou mais subsistemas isolados é dado pelo produto tensorial dos subsistemas isolados:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \quad (23)$$

No entanto, o postulado somente é válido quando os subsistemas estão isolados entre si, caso contrário não há garantias que os subsistemas não vão interagir e assumir um estado que não pode ser decomposto em subsistemas. Quando isso ocorre diz-se que os qubits estão entrelaçados.

O Par EPR é um sistema de dois qubits que se encontram em um estado de entrelaçamento:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle. \quad (24)$$

É fácil demonstrar que tal sistema não pode ser analisado como 2 subsistemas isolados. Assume-se que os sistemas não estão entrelaçados, portanto deve ser possível representar o

vetor  $|\psi\rangle$  como um produto tensorial de dois sistemas isolados, portanto

$$|\psi\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle) \quad (25)$$

$$= \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle \quad (26)$$

com

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \quad (27)$$

$$\alpha\delta = 0, \quad (28)$$

$$\beta\gamma = 0, \quad (29)$$

$$\beta\delta = \frac{1}{\sqrt{2}}. \quad (30)$$

De (27) e (30) podemos afirmar que  $\alpha$ ,  $\beta$ ,  $\gamma$  e  $\delta$  são não nulos, no entanto de (28) e (29) podemos afirmar que ao menos um elemento dos pares  $\alpha$ ,  $\beta$  e  $\gamma$ ,  $\delta$  devem ser nulos.

Prova-se portanto, por contradição, que o par EPR não pode ser expresso como um produto tensorial de dois sistemas isolados, portanto ambos os qubits estão entrelaçados.

Uma mudança de estado em um dos subsistemas que compõem um entrelaçamento, provocada por um colapso, por exemplo, necessariamente provocará uma mudança de estado nos demais subsistemas entrelaçados. Suponha que uma medição seja realizada somente no primeiro qubit do par EPR, o qual colapsa para o estado  $|0\rangle$ . Note que, segundo (24), a única possibilidade para o segundo qubit, quando o primeiro assume o estado  $|0\rangle$ , é o estado  $|0\rangle$ . Mesmo que não tenha ocorrido qualquer interação direta com o segundo qubit, a medição do primeiro provocou um colapso no segundo.

## 2.6 Base de Hadamard

Os vetores de estado considerados pela computação quântica são geralmente expressos em termos da base computacional  $\{|0\rangle, |1\rangle\}$ , composta por dois vetores unitários sem componentes comuns (ortogonais), formando assim uma base ortonormal.

Para verificar se dois vetores são ortogonais basta calcular o produto interno entre os vetores. Caso resultado seja 0, os vetores são ortogonais:

$$\langle 0|1\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0. \quad (31)$$

Uma outra base ortonormal muito importante para a Computação Quântica é a base de Hadamard, cujos vetores de base são denotados pelos símbolos  $|+\rangle$  e  $|-\rangle$  e correspondem aos vetores

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (32)$$

e

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad (33)$$

expressos na base computacional.

Assim como na base computacional, o produto interno entre os vetores  $|0\rangle$  e  $|1\rangle$  é nulo:

$$\langle + | - \rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = 0. \quad (34)$$

A base de Hadamard tem algumas propriedades interessantes que serão abordadas na seção 2.8.

## 2.7 Estados equivalentes e esfera de Bloch

Dois vetores de estado  $\psi$  e  $\phi$  que diferem apenas por um fator de fase

$$|\psi\rangle = e^{i\theta} |\phi\rangle \quad (35)$$

são ditos equivalentes e são indistinguíveis um do outro. Ambos tem as mesmas probabilidades de colapso e se comportam da mesma forma quando utilizados em operações quânticas.

No entanto, diferenças de fase entre os estados de base são significativas:

$$\alpha |0\rangle + \beta |1\rangle \neq \alpha |0\rangle + e^{i\theta} \beta |1\rangle, \quad (36)$$

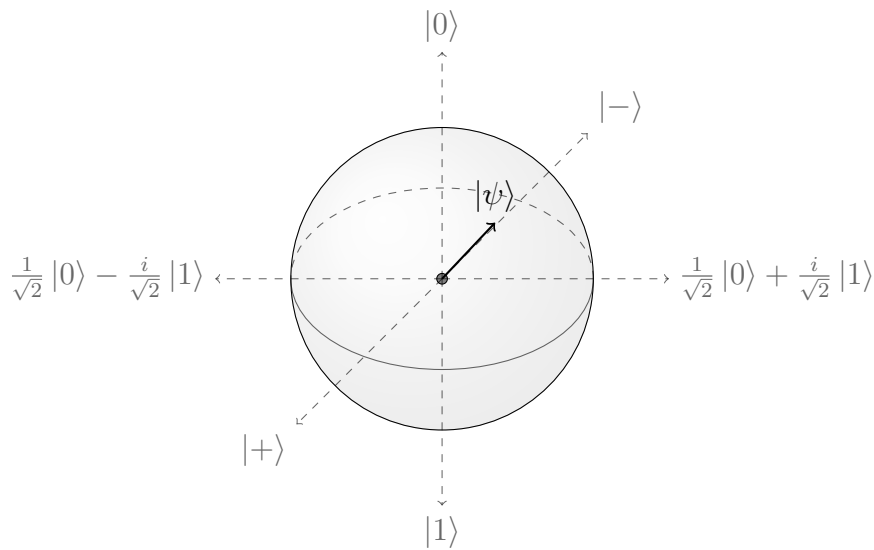
embora os qubits tenham as mesmas probabilidades de colapso, se comportam de forma distinta quando utilizados em operações quânticas.

Graças à equivalência de estados e ao fato de vetores de estado serem unitários, é possível descrever o estado de qualquer qubit pela expressão geral

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad (37)$$

sendo  $\theta$  e  $\phi$  são números reais. De (37), é possível mapear o estado de qualquer qubit a um ponto em uma superfície de uma esfera unitária em  $\mathbb{R}^3$ , denominada esfera de Bloch (Figura 5).

**Figura 5 – Esfera de Bloch**



**Fonte: Autoria própria (2022).**

$$x = \sin \theta \cos \phi$$

$$y = \sin \theta \sin \phi$$

$$z = \cos \theta$$

A esfera de Bloch nos permite visualizar as transformações dos sistemas quânticos como rotações de um vetor dentro de uma esfera unitária. No entanto é apenas uma ferramenta de visualização e pode induzir a falsas conclusões quando utilizada incorretamente. Por exemplo, a Figura 5 mostra os vetores  $|0\rangle$  e  $|1\rangle$  como opostos paralelos quando na realidade são ortogonais.

## 2.8 Circuitos quânticos

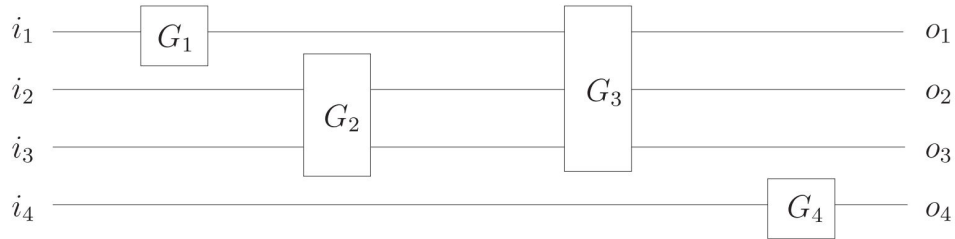
O modelo em circuito é uma forma de representar sistemas de computação através de redes formadas por fios e portas (Figura 6). Os fios são responsáveis por transportar a informação (bits no caso da computação clássica, qubits no caso da computação quântica) enquanto as portas (ou gates) transformam a informação realizando operações básicas.

Os bits (ou qubits) de entrada são escritos nos fios à esquerda do circuito, enquanto os bits de saída são lidos dos fios à direita do circuito. A cada unidade de tempo  $t$ , os bits são permitidos avançar uma passo à direita, com cada fio podendo entrar em no máximo um porta.

Matematicamente, uma operação quântica é representada por uma matriz  $n \times n$ , sendo  $n$  a dimensão do vetor de estado (número de estados de base). Por exemplo, a operação quântica



Figura 6 – Diagrama de circuito



Fonte: Kaye, Laflamme e Mosca (2007).

tica NOT, análoga à operação lógica clássica, é uma operação de 1 qubit que inverte as probabilidades de colapso do sistema, é representada pela matriz

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (38)$$

A operação (realizada pela porta) é aplicada ao qubit (carregado pelos fios), multiplicando a matriz correspondente pelo vetor de estado à esquerda, no caso da operação NOT:

$$\text{NOT} \begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix} = \begin{bmatrix} \psi_2 \\ \psi_1 \end{bmatrix}. \quad (39)$$

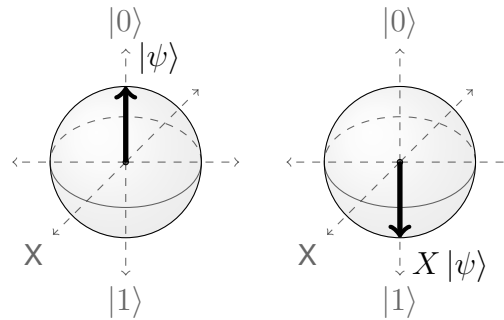
Observando o efeito da porta NOT em uma esfera de Bloch, nota-se que corresponde a uma rotação de  $180^\circ$  no eixo  $X$  (Figura 7), a porta NOT faz parte de um conjunto de portas denominado Portas de Pauli, que correspondem a operação Identidade  $I$  e rotações nos eixos  $X, Y$  e  $Z$  da esfera de Bloch:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Todas as operações sobre um único qubit podem ser vistas como rotações do vetor de estado na esfera de Bloch. Desta forma, é possível decompor qualquer operação de 1 qubit em

**Figura 7 – Operação NOT na esfera de Bloch**  
**(a) Estado psi**      **(b) Estado NOT psi**



**Fonte: Autoria própria (2022).**

uma série de portas de rotação, as quais são definidas em termos das Portas de Pauli:

$$R_x(\theta) = e^{-\frac{i\theta X}{2}}$$

$$R_y(\theta) = e^{-\frac{i\theta Y}{2}}$$

$$R_z(\theta) = e^{-\frac{i\theta Z}{2}}.$$

Um conjunto finito de portas é denominado universal caso seja possível construir um circuito para computar uma função  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ , onde  $m$  e  $n$  são dois inteiros positivos quaisquer, utilizando apenas portas deste conjunto. Um exemplo de conjunto universal para computação clássica é {NAND, FANOUT}, de forma que qualquer computação clássica pode ser computada por um circuito construído apenas por estas duas portas.

Um circuito é dito reversível caso seja possível computar os dados de entrada através dos dados de saída. Em outras palavras, um circuito  $C_n$ , de  $n$  fios, que computa uma função  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  é dito reversível se e somente se for possível construir um circuito  $C_n^{-1}$  capaz de computar  $f^{-1} : \{0, 1\}^m \rightarrow \{0, 1\}^n$ . Uma porta NOT é um exemplo de porta reversível.

Qualquer computação realizada por um circuito irreversível pode ser realizada por um circuito reversível equivalente com adição de uma ancila e traçando parte da saída. Pode-se considerar que todo circuito irreversível trate-se de um circuito reversível em que parte da informação foi descartada, embora não haja consequências pelo descarte destas informações extras em circuitos clássicos, o descarte dos “lixos” de dados em circuitos quânticos pode ocasionar erros.

Assim como vetores, portas podem ser combinados através do produto tensorial. Uma porta NOT que atua sobre um registrador de dois qubits é expressa como

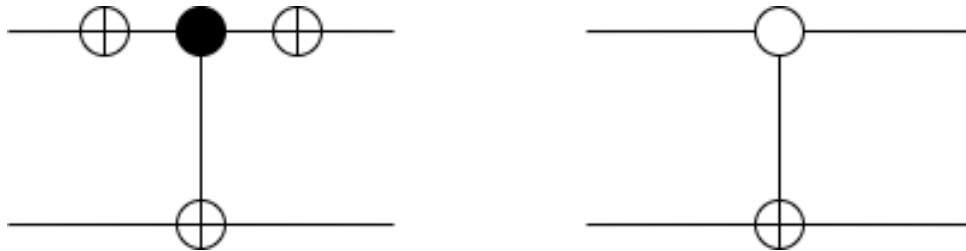
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad (40)$$

e seu efeito sobre o registrador é

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \\ \psi_4 \end{bmatrix} = \begin{bmatrix} \psi_4 \\ \psi_3 \\ \psi_2 \\ \psi_1 \end{bmatrix}. \quad (41)$$

A Tabela 1 ilustra as principais portas quânticas utilizadas para construir circuitos quânticos, junto as suas respectivas matrizes e os símbolos utilizados para representá-las. A Figura 8 ilustra uma representação compacta para circuitos em que um dos sinais deva passar por uma porta NOT imediatamente antes e imediatamente após passar por uma porta quântica.








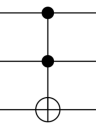
**Figura 8 – Representação compacta de portas controladas por sinais negativos**



**Fonte: Autoria própria (2022).**

Apesar de ser pesquisada por mais de quarenta anos (Benioff, 1980) e se demonstrado promissora para um grande número de problemas de interesse, os estudos em computação quântica permanecem maioritariamente no ambiente teórico. Limitações tecnológicas impedem a confecção e manutenção de um número significativo de qubits em um estado coerente (isolado de interações com o ambiente externo) para construir e utilizar circuitos quânticos para realizar computação.

Tabela 1 – Principais portas utilizadas para construir circuitos quânticos

Porta	Símbolo	Matriz
Pauli-X (NOT)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$
CZ		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Fonte: Autoria própria (2022).

### 3 ALGORITMO DE GROVER

Neste capítulo serão discutidos e analisados o funcionamento e o ganho de performance, quando comparado com alternativas clássicas, do Algoritmo de Busca Quântica de Grover. Tal algoritmo se utiliza dos fenômenos quânticos de sobreposição e interferência para produzir um estado quântico que codifique uma solução para o problema de busca cega em uma dada lista de valores. Este capítulo está fundamentado no artigo *A Fast Quantum Mechanical Algorithm for Database Search* (GROVER, 1996).

#### 3.1 O problema de busca cega

O Algoritmo de Grover visa fornecer uma solução ao problema de busca cega, assumindo que as soluções possam ser expressas como strings binárias de tamanho  $n$ . Define-se uma função  $f : \{0, 1\}^n \mapsto \{0, 1\}$  tal que  $f(x) = 1$ , se  $x$  codifica uma solução para o problema, podendo ser chamada de *good string*, e  $f(x) = 0$  caso contrário, onde  $x$  é chamada de *bad string*.

O problema de busca pode ser definido pela seguinte estrutura matemática:

##### O Problema de Busca

**Entrada:** Uma caixa preta  $U_f$  para computar uma função desconhecida  $f : \{0, 1\}^n \mapsto \{0, 1\}$

**Problema:** Encontrar uma entrada  $x \in \{0, 1\}^n$  tal que  $f(x) = 1$

onde  $\{0, 1\}^n$  é o espaço de busca de tamanho  $N$ , formado por strings binárias de tamanho  $n$ . Portanto o tamanho total do espaço de busca acaba sendo exponencial no tamanho da entrada,  $N = 2^n$ .

Em certas situações é possível extrair informações do problema e do espaço de busca para eliminar algumas não-soluções e acelerar a execução do algoritmo. No entanto, no caso onde não é possível extrair tais informações (Busca Cega), deve-se verificar cada um dos valores a fim de encontrar uma solução para  $f(x) = 1$ . Desta forma, no pior caso, onde não há solução ou a solução é o último valor consultado, a complexidade de tempo do algoritmo clássico é  $O(2^n)$ .

#### 3.2 Caixa preta quântica

A fim de utilizar os fenômenos quânticos para proporcionar um ganho de performance sobre o algoritmo de busca clássico, é necessário definir a função de caixa preta, também chamada de oráculo, em termos de circuitos quânticos.

Define-se uma versão quântica  $U_f$  da função de caixa preta da seguinte forma:

$$U_f : |x\rangle |b\rangle \mapsto |x\rangle |b \oplus f(x)\rangle, \quad (42)$$

onde o primeiro registrador  $|x\rangle$ , de  $n$  qubits, é chamado de registrador de consulta e o segundo  $|b\rangle$ , de 1 qubit, registrador alvo. Definindo o registrador alvo como  $|0\rangle$  e dado um valor de busca  $x$ , codificado como  $|x\rangle$ , o efeito da caixa preta quântica é:

$$U_f : |x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle , \quad (43)$$

desta forma, uma medição do qubit alvo retorna a resposta para a consulta  $f$ . No caso de a medição retornar o estado puro  $|1\rangle$ , então certamente uma medição no registrador de consulta  $|x\rangle$  retornará uma resposta ao problema.

Ao definir o registrador alvo como  $|-\rangle$  e dado um valor de busca  $x$ , codificado como  $|x\rangle$ , o efeito da caixa preta quântica é ligeiramente alterado, passando a ser:

$$U_f : |x\rangle |-\rangle \mapsto |x\rangle ((-1)^{f(x)} |-\rangle) . \quad (44)$$

Como o registrador de consulta e do qubit alvo fazem parte de um sistema composto, pode-se associar o fator de deslocamento de fase com o registrador. Desta forma têm-se:

$$U_f : |x\rangle |-\rangle \mapsto (-1)^{f(x)} |x\rangle |-\rangle . \quad (45)$$

A caixa preta quântica passa a codificar o resultado da função como um deslocamento de fase. Caso  $x$  codifique uma *bad string* ( $f(x) = 0$ ), a fase do registrador  $|x\rangle$  permanece inalterada, no entanto quando  $x$  codifica uma *good string* ( $f(x) = 1$ ), a fase do registrador  $|x\rangle$  é deslocada por um fator de  $-1$ .

### 3.3 Aplicação do fenômeno da sobreposição

O primeiro fenômeno utilizado pelo algoritmo é o da sobreposição quântica. O registrador de consulta é preparado em uma sobreposição de todos os valores de busca possíveis:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle , \quad (46)$$

onde  $N$  é o tamanho do espaço de busca; como as entradas são codificadas como strings binárias de tamanho  $n$ , o tamanho de espaço de busca geralmente é exponencial no tamanho da entrada ( $N = 2^n$ ).

A sobreposição de (46) pode ser facilmente obtida ao preparar um registrador de  $n$ -qubits no estado  $|00\dots 0\rangle$  e passá-lo por uma porta de Hadamard de  $n$ -qubits:

$$|x\rangle = H |00\dots 0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle. \quad (47)$$

Pode-se dividir a soma em (47) em duas partes, a primeira sobre todos os valores de  $x$  tais que  $f(x) = 0$ , o conjunto das *bad strings*  $X_{bad}$ , e a segunda sobre todos os valores tais que  $f(x) = 1$ , o conjunto das *good strings*  $X_{good}$ .

No caso particular onde há apenas uma solução  $w$  para o problema, ou seja  $X_{good} = \{w\}$ , tem-se

$$|x\rangle = \frac{1}{\sqrt{N}} |\Psi_{good}\rangle + \sqrt{\frac{N-1}{N}} |\Psi_{bad}\rangle, \quad (48)$$

desta forma uma medição no qubit alvo retorna  $|1\rangle$  com probabilidade  $\frac{1}{N}$  e, quando isso acontece, uma medição no registrador de consulta necessariamente retornará uma solução ao problema.

Note que, no entanto, a sobreposição não oferece qualquer ganho de performance sobre as soluções clássicas, uma vez que a medição provoca o colapso do sistema para um dos estados de base de forma aleatória. Considerando que há apenas uma solução  $w$ , a probabilidade do sistema colapsar para uma *good string* é  $\frac{1}{N}$ , sendo que o número esperado de consultas à caixa preta é  $N = 2^n$ .

### 3.4 Aplicação do fenômeno da interferência

Embora a sobreposição por si só não ofereça ganhos de performance, é fácil perceber que, se houver uma maneira de aumentar a amplitude do estado solução  $w$ , e conseqüentemente a probabilidade de o sistema colapsar neste estado, serão necessárias menos consultas à  $U_f$  para que, com alta probabilidade de sucesso, se obtenha uma solução ao problema. A amplificação da amplitude de um estado em uma sobreposição pode ser alcançada através do fenômeno quântico de interferência.

Com aplicação de diferentes portas quânticas é possível aumentar as amplitudes das *good strings* e reduzir, ao mesmo tempo, as amplitudes das *bad strings*. Para isso, considere a caixa preta quântica com codificação por deslocamento de fase. Note que  $|-\rangle$  é um autovetor de  $U_f$  e que, para fins de análise, pode-se ser desconsiderado:

$$U_f : |x\rangle |-\rangle \mapsto (-1)^{f(x)} |x\rangle |-\rangle, \quad (49a)$$

$$U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle. \quad (49b)$$

Além de  $U_f$ , vamos definir uma outra porta quântica  $U_{0\perp}$  que atua como deslocador de fase por  $-1$  para todos os estados ortogonais a  $|00\dots 0\rangle$ :

$$U_{0\perp} = \begin{cases} |x\rangle \mapsto -|x\rangle & \text{se } x \neq 00\dots 0 \\ |00\dots 0\rangle \mapsto |00\dots 0\rangle \end{cases} . \quad (50)$$

Com estes operadores pode-se definir um operador que incrementa a amplitude de  $|\Psi_{good}\rangle$  ao mesmo tempo que reduz a amplitude de  $|\Psi_{bad}\rangle$ . Tal operador é denominado de Iteração de Busca Quântica ou Iteração de Grover.

### 3.5 A iteração de Grover

A Iteração de Grover é definido pelas seguintes transformações:

1. Aplicar a Caixa Preta  $U_f$ ;
2. Aplicar a porta de Hadamard de  $n$ -qubits;
3. Aplicar a porta  $U_{0\perp}$ ;
4. Aplicar a inversa da porta de Hadamard de  $n$ -qubits.

A porta de Hadamard é auto-inversora, portanto a última transformação pode ser simplificada como um outra porta de Hadamard de  $n$ -qubits. Desta forma a iteração de Grover é definida como:

$$G = H U_{0\perp} H U_f . \quad (51)$$

### 3.6 O algoritmo de busca quântica de Grover

Definida a Iteração de Grover pode-se definir o Algoritmo de Busca Grover para encontrar, com alta probabilidade de sucesso, um valor de  $x$  tal que  $f(x) = 1$ , no modelo em circuito.

---

#### Algoritmo 1 – Algoritmo Quântico de Busca de Grover

---

- 1: Comece com o estado de  $n$ -qubits  $|00\dots 0\rangle$ ;
  - 2: Aplique a porta de Hadamard de  $n$ -qubits  $H$ ;
  - 3: Aplique a iteração de Grover  $G$  um total de  $\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \rfloor$  vezes;
  - 4: Meça o estado resultante.
- 

Fonte: Grover (1996).



### 3.7 O efeito da Iteração de Grover

Todo o processo de amplificação de resultado é realizado pela Iteração de Grover, para analisar seu efeito no sistema, considere o estado inicial  $|\Psi\rangle = H|00\dots 0\rangle$ . Assim como em (48), é possível dividir a sobreposição em duas partes:

$$|\Psi\rangle = H|00\dots 0\rangle = A|\Psi_{good}\rangle + B|\Psi_{bad}\rangle, \quad (52)$$

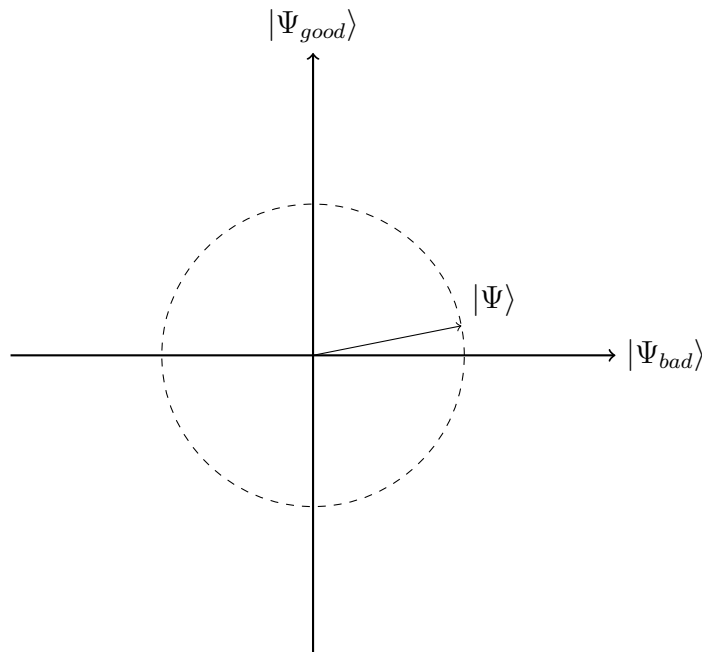
onde  $A$  e  $B$  são as amplitudes associadas aos estados  $|\Psi_{good}\rangle$  e  $|\Psi_{bad}\rangle$ , respectivamente. Neste caso específico, devido ao efeito de  $H$  no registrador  $|00\dots 0\rangle$ , as amplitudes  $A$  e  $B$  são números reais. Como qualquer outro vetor de estado,  $|\Psi\rangle$  é unitário, portanto as somas dos quadrados de  $A$  e  $B$  deve resultar em 1.

Pela identidade trigonométrica, pode-se encontrar um terceiro número real  $\theta \in (0, 2\pi)$  tal que:

$$|\Psi\rangle = \sin \theta |\Psi_{good}\rangle + \cos \theta |\Psi_{bad}\rangle. \quad (53)$$

Desta forma é possível representar o vetor de estado  $|\Psi\rangle$  como um ponto sobre uma circunferência de raio 1 nos eixos  $|\Psi_{good}\rangle$ , vertical e  $|\Psi_{bad}\rangle$ , horizontal (Figura 9). Todas as operações podem ser vistas como rotações do vetor de estado sobre a circunferência.

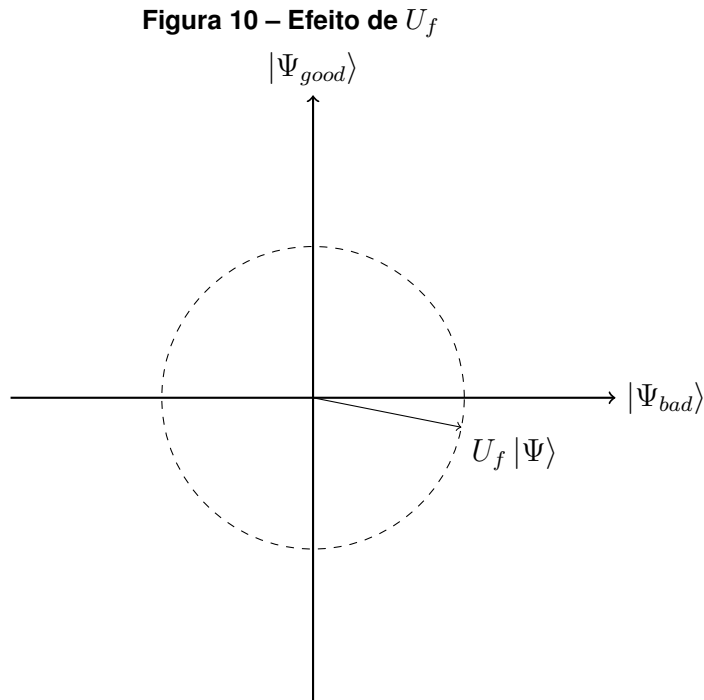
**Figura 9 – Representação do vetor de estado no círculo unitário**



**Fonte: Kaye, Laflamme e Mosca (2007).**

O primeiro passo da iteração de Grover é aplicar o oráculo quântico  $U_f$  ao vetor  $|\Psi\rangle$ . Como visto anteriormente, o oráculo desloca a fase das *good strings* por um fator de  $-1$  en-

quanto mantém as *bad strings* inalteradas. Na circunferência, o efeito de  $U_f$  pode ser visto como um espelhamento sobre o eixo  $|\Psi_{bad}\rangle$  (Figura 10).



Não há grandes benefícios em analisar as demais portas que compõem a iteração de Grover de forma individual, portanto vamos combiná-las em uma única operação quântica

$$U_{\psi\perp} = H U_{0\perp} H. \quad (54)$$

Para analisar o efeito de  $U_{\psi\perp}$ , é útil definir uma outra base para o sistema, representada por um par de eixos distintos sobre a circunferência de raio 1:

$$|\Psi\rangle = \sin \theta |\Psi_{good}\rangle + \cos \theta |\Psi_{bad}\rangle, \quad (55a)$$

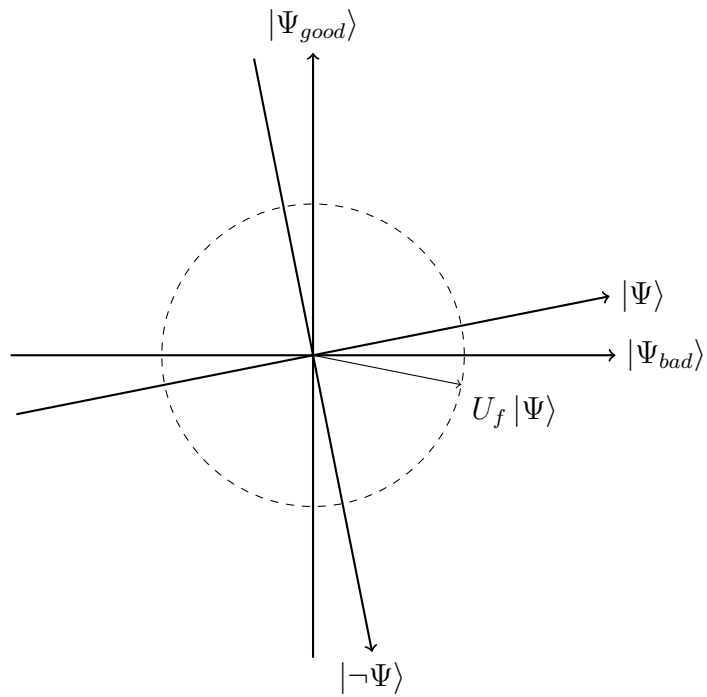
$$|\neg\Psi\rangle = \cos \theta |\Psi_{good}\rangle - \sin \theta |\Psi_{bad}\rangle. \quad (55b)$$

Note que  $|\Psi\rangle$  é o estado inicial do sistema e  $|\neg\Psi\rangle$  é ortogonal a  $|\Psi\rangle$ . A Figura 11 ilustra ambos os pares de eixos e o vetor  $U_f |\Psi\rangle$ .

A operação  $U_{\psi\perp}$  pode ser vista na base  $\{|\Psi\rangle, |\neg\Psi\rangle\}$  como uma reflexão sobre o eixo  $|\Psi\rangle$ . Combinando as operações  $U_f$  e  $U_{\psi\perp}$ , o efeito total da iteração de Grover  $G$  é ilustrado na Figura 12.

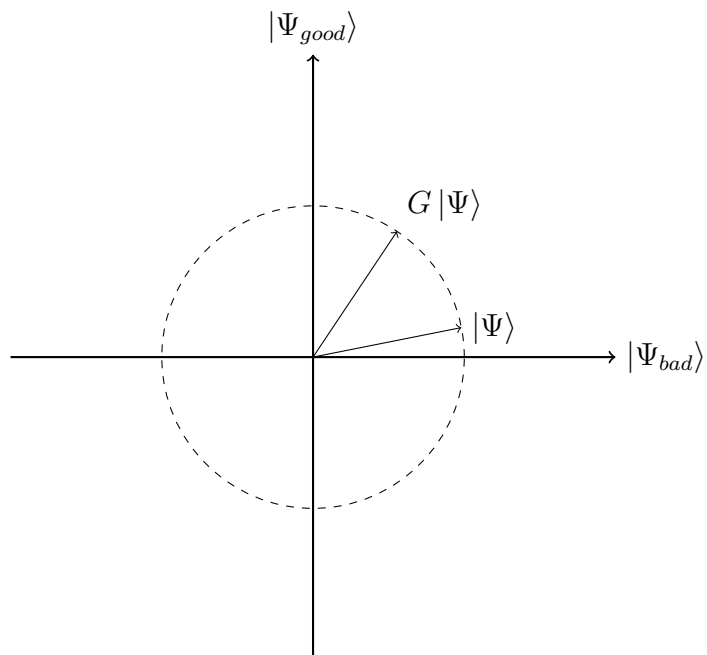
Após passar pela iteração de Grover, o vetor está mais próximo (a um menor ângulo) do eixo  $|\Psi_{good}\rangle$ , ou seja, o sistema tem uma maior probabilidade de colapsar em  $|\Psi_{good}\rangle$ .

**Figura 11 – Bases  $\{|\Psi_{bad}\rangle, |\Psi_{good}\rangle\}$  e  $\{|\Psi\rangle, |-\Psi\rangle\}$**



Fonte: Kaye, Laflamme e Mosca (2007).

**Figura 12 – Efeito de  $G$  sobre  $|\Psi\rangle$**



Fonte: Kaye, Laflamme e Mosca (2007).

Aplicando  $G$  um número suficiente de vezes, a probabilidade associada à  $|\Psi_{good}\rangle$  torna-se praticamente 1, assim uma medição resulta quase que certamente em um estado  $|x\rangle$  tal que  $f(x) = 1$ .

### 3.8 Complexidade do algoritmo

Pode-se facilmente deduzir que  $k$  aplicações de  $G$  deixam o sistema no estado

$$G^k |\Psi\rangle = \sin [(2k + 1)\theta] |\Psi_{good}\rangle + \cos [(2k + 1)\theta] |\Psi_{bad}\rangle . \quad (56)$$

Uma vez que  $\sin \frac{\pi}{2} = 1$ , para que a probabilidade associada a  $|\Psi_{good}\rangle$  seja 1, é necessário que:

$$(2k + 1)\theta = \frac{\pi}{2}, \quad (57a)$$

$$k = \frac{\pi}{4\theta} - \frac{1}{2}. \quad (57b)$$

No pior caso, onde há apenas uma *good string*  $|w\rangle$  e diversas *bad strings* sobrepostas em  $|\Psi_{bad}\rangle$ , tem-se:

$$|\Psi\rangle = \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |\Psi_{bad}\rangle , \quad (58)$$

portanto:

$$\sin \theta = \frac{1}{\sqrt{N}}, \quad (59a)$$

$$\cos \theta = \sqrt{\frac{N-1}{N}}. \quad (59b)$$

Quando  $N$  tende ao infinito,  $\frac{1}{\sqrt{N}}$  torna-se muito pequeno, desta forma pode-se utilizar a aproximação  $\sin \theta = \theta$ , quando  $\theta$  tende a zero. Uma vez que  $k$  deve obrigatoriamente ser um número inteiro, um número suficiente de aplicações de  $G$  para solucionar o problema de busca, com alta probabilidade, pode ser calculado por:

$$k = \lfloor \frac{\pi}{4} \sqrt{N} \rfloor \quad (60)$$

Assim a complexidade de pior caso do algoritmo é dada por  $O(\sqrt{N})$ , onde  $N$  é o tamanho do espaço de busca, geralmente exponencial no tamanho da entrada  $n$ . Portanto a complexidade do algoritmo em relação ao tamanho da entrada é dada por  $O(\sqrt{2^n})$ , o que representa um ganho de performance quadrático sobre a melhor solução clássica conhecida para o problema de busca cega, com complexidade  $O(2^n)$ .

Diferente de outros algoritmos quânticos, como o algoritmo de Shor para fatoração de números inteiros, o algoritmo de Grover não garante um ganho exponencial sobre a melhor solução clássica, mas sim um ganho polinomial. Enquanto outros algoritmos se concentram em fornecer uma solução para um problema mais específico, o algoritmo de Grover foi idealizado com um algoritmo de uso genérico, capaz de ser utilizado em uma grande variedade de problemas de busca. Dentre os problemas em que o algoritmo de Grover pode ser utilizado, encontram-se alguns problemas NP-Completo. Não se acredita que problemas NP-Completo possam ter ganhos exponenciais mesmo com o uso da computação quântica (AARONSON, 2013).

## 4 ALGORITMOS QUÂNTICOS PARA CLIQUES

Na teoria dos grafos, uma *clique* em um grafo simples é um subconjunto de vértices no qual todos os pares de vértices distintos são adjacentes (conectados por uma aresta). Ao longo deste texto, um grafo é sempre um grafo simples. Uma clique *maximal* é uma clique que não está contida em uma clique maior no mesmo grafo. Uma clique *máxima* é a maior das cliques maximais de um grafo.

Determinar a cardinalidade da clique máxima em um grafo é um problema NP-difícil. A melhor solução clássica determinística conhecida para este problema tem uma complexidade de tempo  $\mathcal{O}(3^{n/3})$ . O problema da clique máxima também é difícil de aproximar (HåSTAD, 1999). Isto é, para qualquer  $\varepsilon > 0$ , não pode haver um algoritmo de aproximação de tempo polinomial para o problema com um fator de aproximação  $\mathcal{O}(n^{1-\varepsilon})$ , a menos que  $P = NP$  (Ibid.).

Utilizando circuitos quânticos é possível construir um algoritmo com melhor complexidade de tempo comparada à melhor solução clássica. Os autores Wie e Bojie propõem em seus artigos algoritmos quânticos, baseados na Busca Quântica de Grover, para encontrar todos os cliques maximais (WIE, 2017) e a clique máxima (BOJIE, 2012) em um grafo, respectivamente.

Nesta seção serão estudados os algoritmos propostos por Wie e Bojie.

### 4.1 O algoritmo de Wie

Wie propôs um algoritmo quântico, baseado na Busca de Grover, que retorna uma sobreposição dos estados quânticos que representam todas as cliques maximais presentes em um grafo simples  $G(V, E)$ .

Em uma representação por matriz de adjacência de um grafo  $G(V, E)$ , cada linha  $i$  da matriz pode ser considerada como o conjunto dos vizinhos do  $i$ -ésimo vértice  $c \in V$ . Um algoritmo clássico para determinar se um conjunto de vértices  $Q$  é uma clique maximal em  $G$  consiste em verificar se a interseção dos vizinhos de todos os vértices  $q \in Q$  resulta no conjunto nulo  $\emptyset$ :

$$N_G(q_1) \cap N_G(q_2) \cap \dots \cap N_G(q_d) = \emptyset, \quad (61)$$

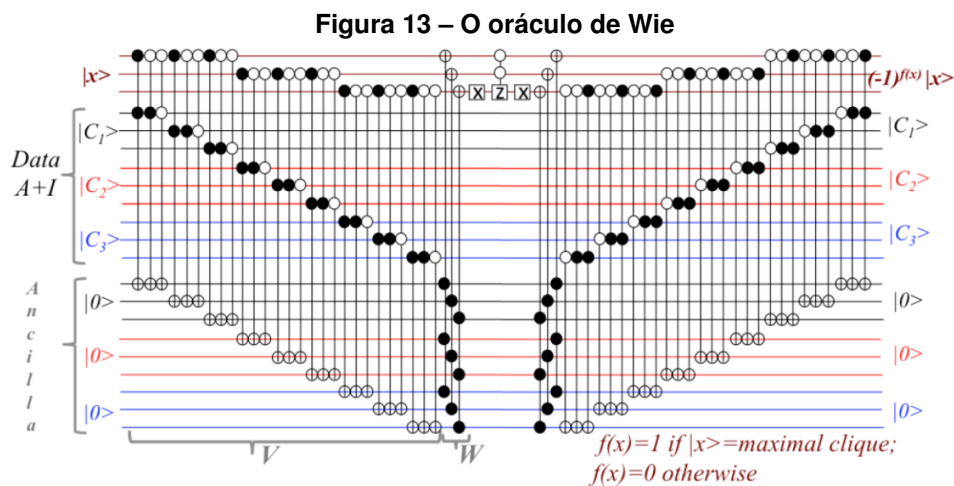
onde  $N_G(q_i)$ , representa o conjunto de vizinhos do vértice  $q_i$  em  $G$ . Alternativamente pode-se verificar se a interseção das uniões dos vértices em  $Q$  com seus vizinhos em  $G$  resulta no próprio conjunto  $Q$ :

$$(N_G(q_1) \cup \{q_1\}) \cap (N_G(q_2) \cup \{q_2\}) \cap \dots \cap (N_G(q_d) \cup \{q_d\}) = Q. \quad (62)$$

O oráculo de Wie implementa um versão quântica do algoritmo clássico descrito acima. O circuito recebe como entrada um candidato a clique (ou uma sobreposição de candidatos) e uma representação do grafo  $G$  na forma de matriz de adjacência. Caso o candidato testado

seja uma clique maximal em  $G$ , o circuito inverte a fase do estado que codifica a clique, caso contrário, o estado permanece inalterado (Figura 13). Um candidato a clique é um subgrafo em  $G$  representado por estado quântico  $|c_1 c_2 \dots c_n\rangle$ , onde  $n$  é o número de vértices em  $G$ , e:

$$|c_i\rangle = \begin{cases} |1\rangle, & \text{se } q_i \in Q; \\ |0\rangle, & \text{caso contrário.} \end{cases} \quad (63)$$



Fonte: WIE (2017).

É possível dividir o circuito em três partes: na primeira é implementada a versão quântica do circuito clássico para detecção de cliques maximais, após esta etapa, o registrador  $|x\rangle$  estará no estado  $|00 \dots 0\rangle$  caso o candidato seja um clique maximal em  $G$ ; na segunda parte utiliza-se um porta  $Z$  controlada para inverter a fase de  $|x\rangle$  caso todos os qubits de  $|x\rangle$  estejam no estado  $|0\rangle$  ( $|x\rangle$  codifica um clique maximal), uma vez que a porta  $Z$  inverte apenas a fase do estado  $|1\rangle$ , utiliza-se duas portas  $X$  para inverter o estado de um dos qubits de  $|x\rangle$  e reverter a operação; por fim a última parte corresponde ao circuito reverso das duas partes anteriores, desta forma o oráculo é um circuito reversível.

O circuito descrito na Figura 13 implementa o oráculo utilizado no algoritmo de Grover. Note que o circuito satisfaz a condição exigida de inverter a fase das “good strings” e manter inalterada a fase das “bad string”. O algoritmo de Grover amplifica a amplitudes dos estados quânticos que representam uma clique maximal em  $G$ , aumentando a probabilidade do estado resultante colapsar em uma representação de uma clique maximal. A complexidade de tempo total do algoritmo é dada por  $\mathcal{O}(\sqrt{n^2 2^n / M})$ , onde  $M$  é o número total de cliques maximais no grafo.

## 4.2 O algoritmo de Bojié

Bojié propôs um algoritmo quântico, baseado na Busca de Grover, capaz de retornar uma clique máxima em um grafo simples  $G(V, E)$ .

A proposta de Bojié consiste em buscar iterativamente em  $G$  por cliques cada vez maiores, até que a busca falhe por não haver uma clique de maior cardinalidade. Neste caso, a última clique encontrada é uma clique máxima e sua cardinalidade é a cardinalidade da clique máxima em  $G$ .

Em sua abordagem, Bojié utiliza a busca de Grover para iterativamente buscar, em uma lista de subgrafos em  $G$ , uma clique maximal com mais de  $k$  vértices, com o valor de  $k$  iniciando em 1 e sendo substituído pela cardinalidade da última clique encontrada. O algoritmo está descrito no Algoritmo 2.

---

### Algoritmo 2 – Algoritmo de Bojié

---

- 1: Inicialize a variável  $k = 1$  e o vetor  $|r\rangle = |00 \dots 0\rangle$ ;
  - 2: Defina uma função  $f(x)$  para um oráculo que será utilizado pelo algoritmo de Grover. A função  $f(x)$  retorna 1 se o estado  $x$  representa uma clique em  $G$  e sua cardinalidade for maior que  $k$ , caso contrário a função retorna 0;
  - 3: Inicialize um registrador quântico de tamanho  $n = \log_2 N$  no estado  $|00 \dots 0\rangle$  e utiliza a porta de Hadamard para colocar o registrador na sobreposição uniforme dos estados de base;
  - 4: Execute o algoritmo de Grover para um número desconhecido de soluções;
  - 5: Meça o registrador quântico. Se o resultado for uma clique e sua cardinalidade for maior que a variável  $k$ , então copie o resultado para o vetor  $|r\rangle$  e a cardinalidade da clique para a variável  $k$  e vá para o passo 2; caso contrário, vá para o passo 6;
  - 6: Retorne o registrador  $|r\rangle$ .
- 

Fonte: BOJIE (2012).

A proposta original de Bojié resulta em um algoritmo com complexidade de tempo  $\mathcal{O}(n\sqrt{2^n})$ , onde a abordagem iterativa adiciona um fator de  $\mathcal{O}(n)$ . No entanto, autor não considera a construção do oráculo utilizada na busca quântica, nem apresenta a implementação de tal oráculo.

Percebe-se que substituindo a abordagem iterativa por uma busca binária, pode-se reduzir a complexidade do algoritmo por um fator  $n/\log n$ , resultando em uma complexidade final, sem considerar a construção do oráculo, de  $\mathcal{O}(\log n\sqrt{2^n})$ . Tal modificação foi sugerida pelo autor como um possível ponto de melhoria em seu trabalho, porém, o impacto e o ganho de performance de tal modificação não foram analisados.



## 5 NOVAS PROPOSTAS

Neste capítulo serão apresentadas duas novas propostas para a resolução do problema da clique máxima.

### 5.1 Algoritmo de busca de Wie–Bojié

Em sua abordagem iterativa, Bojié apresenta um algoritmo, baseado na Busca Quântica de Grover, capaz de retornar a cardinalidade da clique máxima em um grafo simples. No entanto, o autor não apresenta em seu artigo a implementação do oráculo utilizado na busca quântica, nem ao menos considera a construção de tal oráculo na análise de complexidade do algoritmo, apenas sua descrição matemática é apresentada:

$$f(x) = \begin{cases} 1, & \text{se } x \text{ codifica uma clique maximal com mais de } k \text{ elementos;} \\ 0, & \text{caso contrário.} \end{cases} \quad (64)$$

Wie por sua vez propõe um algoritmo, baseado na Busca Quântica de Grover, capaz de retornar uma sobreposição de todos as cliques maximais presentes em um grafo simples. Em sua abordagem, Wie não apenas apresenta a descrição matemática do oráculo utilizado na busca quântica, como também as instruções para construção de tal oráculo.

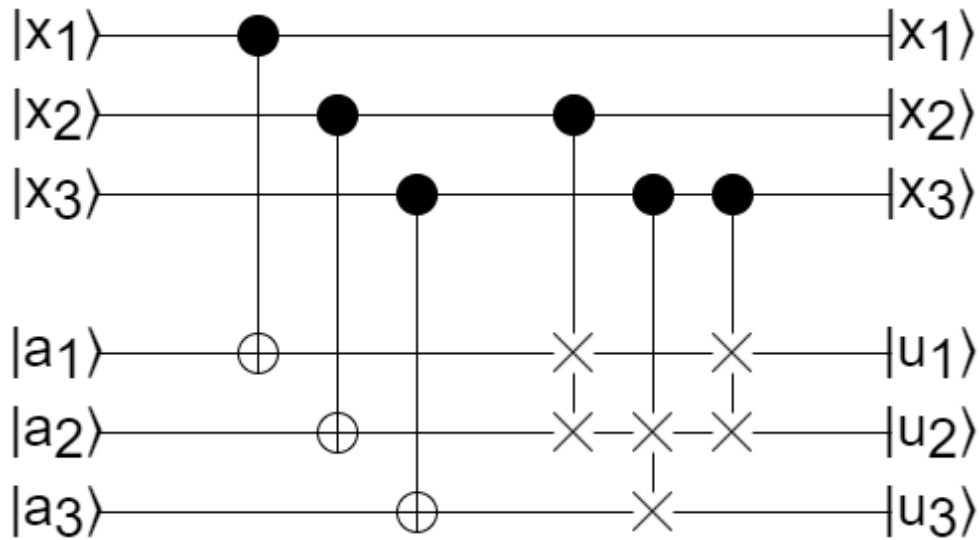
$$f(x) = \begin{cases} 1, & \text{se } x \text{ codifica uma clique maximal;} \\ 0, & \text{caso contrário.} \end{cases} \quad (65)$$

Uma vez que uma clique máxima é uma clique maximal, mais especificamente, a clique maximal de maior cardinalidade, investigamos a possibilidade de utilizar o oráculo de Wie no algoritmo de Bojié. Note por (64) e (65) que os oráculos diferem apenas por uma condição adicional em (64); o candidato a clique deve ter mais de  $k$  elementos.

No oráculo de Wie (Figura 13), uma porta Z controlada inverte a fase dos estados que codificam uma clique maximal. Adicionando um sinal de controle extra que assume o valor  $|1\rangle$  quando o candidato tem pelo menos  $k + 1$  vértices, e  $|0\rangle$  caso contrário, o circuito passa a atender aos critérios do oráculo de Bojié.

Note que na codificação utilizada para representar os candidatos a cliques maximais, a quantidade de elementos na clique é igual à quantidade de qubits no estado  $|1\rangle$ . Adicionalmente, note que, caso os qubits sejam ordenados de forma que todos os qubits  $|1\rangle$  estejam na parte menos significativa do registrador quântico, o registrador passa a conter o número de elementos

Figura 14 – Contador de elementos na clique máxima (3 qubits)



Fonte: Autoria própria (2022).

presentes na clique na base unária. Desta forma, o problema da contagem de elementos de reduz a uma ordenação dos qubits do estado quântico.

Para contar, na base unária, o número de elementos no candidato a clique maximal, foi desenvolvido um algoritmo quântico baseado no algoritmo clássico de ordenação *Insertion Sort*, tal algoritmo foi escolhido devido às suas características de escalabilidade e fácil construção do circuito quântico. Substrings são iterativamente ordenadas e expandidas inserindo os elementos restantes nas posições corretas. Cada elemento é inserido no fim da string (parte mais significativa), se o valor for  $|0\rangle$ , ou movido para o início (parte mais significativa) se o valor for  $|1\rangle$ . Este circuito pode ser construído com portas CNOT e CSWAP em tempo  $\mathcal{O}(n^2)$ , como descrito pelo Algoritmo 3 e representado na Figura 14.

#### Algoritmo 3 – Algoritmo de contagem de elementos na clique maximal

**requer** um estado  $|x\rangle$  codificando um candidato a clique  $Q$ ;

**requer** uma ancila  $|a\rangle = |00\dots 0\rangle$ .

1: **para**  $i \in [1, 2, \dots, n]$  **faça**

2: aplicar uma porta CNOT em  $|a_i\rangle$ , controlada por  $|x_i\rangle$ ;

3: **finaliza para**

4: **para**  $i \in [2, 3, \dots, n]$  **faça**

5: **para**  $j \in [i, i-1, \dots, 2]$  **faça**

6: aplicar uma porta CSWAP em  $|a_j\rangle$  e  $|a_{j-1}\rangle$ , controlada por  $|x_i\rangle$

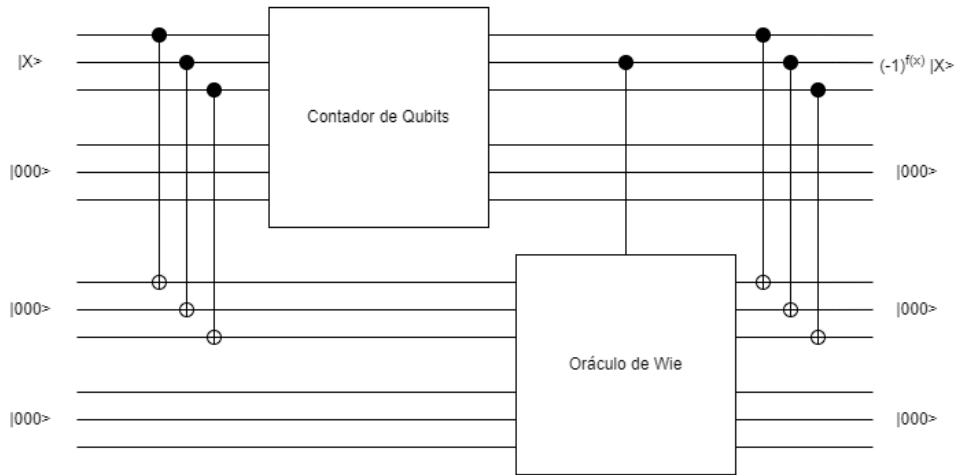
7: **finaliza para**

8: **finaliza para**

Fonte: Autoria própria (2022).

Note que, na base unária, caso o  $i$ -ésimo dígito menos significativo do número em unário for 1, então o número é maior ou igual a  $i$ . Desta forma, ao utilizar o qubit  $i+1$  como o controle adicional do oráculo de Wie, o circuito passa a satisfazer aos critérios do algoritmo de Bojié.

**Figura 15 – Oráculo de Wie-Bojié (3 qubits)**



**Fonte: Autoria própria (2022).**

A Figura 15 representa o oráculo modificado de Wie que pode ser utilizado pelo algoritmo de Bojié.

Nossa abordagem faz  $\mathcal{O}(\log n)$  tentativas para o valor de  $k$ , construindo, para cada suposição, um circuito em tempo  $\mathcal{O}(n^2)$  e executando a Busca de Grover com o circuito construído como o oráculo da busca. Isto resultaria em uma complexidade de tempo  $\mathcal{O}(\sqrt{2^n n^2 \log n})$ , mas, para garantir uma probabilidade de erro  $1 - \mathcal{O}(1/n)$  (alta probabilidade de sucesso), cada busca de Grover deve ser repetida algumas vezes.

A probabilidade  $p$  para que nossa abordagem seja bem sucedida é limitada inferiormente pela probabilidade que cada busca de Grover tenha sucesso de forma individual e independente. Seja  $p_i$  a probabilidade de sucesso da  $i$ -ésima busca de Grover, para  $1 \leq i \leq 2 \lceil \lg n \rceil$ . Para obter  $p \geq 1 - \mathcal{O}(1/n)$ , como desejado, basta que cada  $p_i \geq (1 - \mathcal{O}(1/n))^{1/(2 \lceil \lg n \rceil)}$ , que afirmamos ser alcançado ao executar cada busca de Grover  $\lceil \lg n \rceil$  vezes. Tal afirmação se sustenta ao observar que a probabilidade de que todas as  $\lceil \lg n \rceil$  iterações da busca de Grover falhem é  $\mathcal{O}((1/n)^{\lg n})$ , que é menor que  $1 - (1 - \mathcal{O}(1/n))^{1/(2 \lceil \lg n \rceil)}$  para um  $n$  suficientemente grande. Desta forma a complexidade de tempo final do algoritmo é dada por  $\mathcal{O}(\sqrt{2^n (n \log n)^2})$ .

É possível demonstrar que a complexidade do algoritmo é inferior à melhor solução clássica através do limite:

$$\lim_{n \rightarrow \infty} \frac{\sqrt{2^n (n \log n)^2}}{3^{n/3}} = 0. \quad (66)$$

## 5.2 Algoritmo quântico de otimização

Nesta seção o problema da clique máxima será analisado como um problema de otimização, a partir do qual um algoritmo quântico de otimização pode ser utilizado para obter a cardinalidade da clique máxima em um grafo simples.

Dada uma lista de cliques maximais em  $G$  e uma função  $T(x)$  que mapeia uma clique maximal à sua respectiva cardinalidade, é possível utilizar um algoritmo de otimização a fim de encontrar a clique maximal que maximiza o valor de  $T(x)$ . Uma vez que uma clique máxima é a clique maximal de maior cardinalidade, uma clique maximal que resulta no valor máximo de  $T(x)$ , é uma clique máxima em  $G$ .

O algoritmo de Wie pode ser utilizado para construir uma sobreposição de todos cliques maximais em  $G$  e o contador de qubits, descrito pelo Algoritmo 3 e ilustrado pela Figura 14 fornece uma maneira de realizar o mapeamento descrito pela função  $T$ . Para encontrar então uma clique máxima, basta aplicar um algoritmo de otimização tal como o Algoritmo Quântico de Busca do Mínimo (DÜRR; HØYER, 1996), descrito pelo Algoritmo 4.

---

**Algoritmo 4 – Algoritmo quântico de busca do mínimo**

---

- 1: Escolha um índice de limiar  $0 \leq y \leq N - 1$  de forma aleatória e uniforme;
  - 2: **enquanto** o tempo total de execução seja inferior que  $22.5\sqrt{N} + 1.4\log N^2$  **faça**
  - 3: Inicialize a memória como  $\sum_j \frac{1}{\sqrt{N}} |j\rangle |y\rangle$ ;
  - 4: Aplique o algoritmo de Grover para buscar um valor  $y'$  tal que  $T[y'] < T[y]$ ;
  - 5: Observe o primeiro registrador: seja  $y'$  o resultado. Se  $T[y'] < T[y]$ , então defina o limiar  $y$  como  $y'$ .
  - 6: **finaliza enquanto**
  - 7: **retorna**  $y$
- 

**Fonte: DÜRR e HØYER (1996).**

---

Apesar de ser originalmente desenvolvido para buscar o valor mínimo, o Algoritmo 4 pode ser facilmente modificado para buscar o máximo, bastando apenas modificar a condição 5 e desenvolver um circuito quântico que implemente a função de caixa preta, utilizada na busca de Grover,  $f(x)$  tal que:

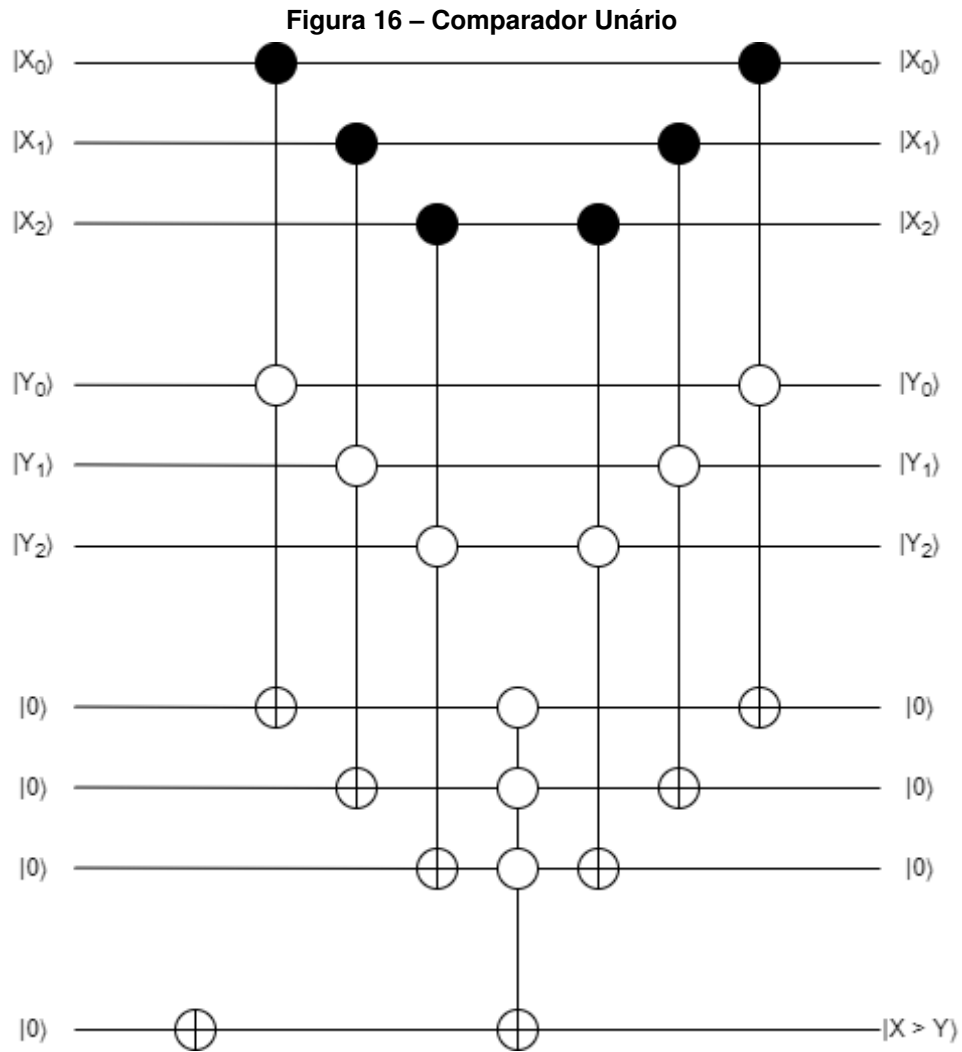
$$f(x) = \begin{cases} 1, & \text{Se } T(x) > T(y); \\ 0, & \text{Caso contrário} \end{cases} . \quad (67)$$

A Figura 16 ilustra a implementação desenvolvida de (67) para três qubits. O circuito considera valores de entrada na base unária, uma vez que o mapeamento  $T$  realizado pelo algoritmo Algoritmo 3 produz valores nesta base.

O Algoritmo 5 descreve o procedimento completo. Note que o algoritmo de Wie e o contador unário não fazem parte do iterador de Grover, estes circuitos podem ser construídos uma única vez e o resultado pode ser armazenado em um registrador auxiliar e reaproveitados para todas as iterações do algoritmo de otimização.

O algoritmo pode ser dividido em três partes, cujas complexidades podem ser analisadas de forma isolada e então contabilizadas para a complexidade total do algoritmo:

1. Obter todos as cliques maximais em  $G$ ;
2. Mapear cada clique maximal à sua respectiva cardinalidade;



Fonte: Autoria própria (2022).

### 3. Buscar a clique maximal de maior cardinalidade.

Na primeira parte utilizamos o algoritmo de Wie para obter uma sobreposição de todas as cliques maximais em  $G$ , sua complexidade de tempo é dada por  $\mathcal{O}(\sqrt{n^2 2^n / M})$ , onde  $n$  é o número de vértices em  $G$  e  $M$  o número total de cliques maximais em  $G$ .

A segunda parte utiliza o algoritmo de contagem unária de qubits para obter a cardinalidade de cada clique maximal, sua complexidade é dada por  $\mathcal{O}(n^2)$ .

Por fim, utilizamos o algoritmo de otimização para buscar a clique maximal de maior cardinalidade, a complexidade deste algoritmo é dada pela expressão  $\mathcal{O}(22.5\sqrt{2^n} + 1.4 \log^2 2^n)$ , a qual pode ser simplificada ao considerar apenas os termos dominantes, resultando em uma complexidade de  $\mathcal{O}(\sqrt{2^n})$ .

A complexidade total do algoritmo, sem considerar a probabilidade de sucesso, é dada pela soma dos três termos  $\mathcal{O}(\sqrt{\frac{n^2 2^n}{M}} + n^2 + \sqrt{2^n})$ , a expressão pode ser simplificada ao considerar apenas os termos dominantes, resultando em uma complexidade de tempo final de  $\mathcal{O}(n\sqrt{2^n})$ .

---

**Algoritmo 5 – Algoritmo Quântico de Otimização para Busca da Clique Máxima**


---

**requer** Um representação em matriz de adjacência de um grafo simples  $G$

- 1: Inicie o registrador  $|r\rangle$  no estado  $|00 \dots 0\rangle$ ;
  - 2: Aplique a porta de Hadamard de  $n$  qubits em  $|r\rangle$  para obter a sobreposição de todos os estados de  $n$  qubits (candidatos a cliques);
  - 3: Aplique o algoritmo de Wie para obter a sobreposição de todos os estados quânticos que codificam uma clique maximal em  $G$ ;
  - 4: Copie o valor do registrado  $|r\rangle$  para um registrador auxiliar  $|c\rangle$ ;
  - 5: Aplique o contador unário de qubits ao registrador  $|r\rangle$  para mapear cada candidato à clique à sua respectiva cardinalidade;
  - 6: Escolha uma clique maximal  $y$  em  $G$  de forma aleatória e uniforme;
  - 7: **enquanto** o tempo total de execução for inferior a  $22.5\sqrt{N} + 1.4 \log^2 N$ ; **faça**
  - 8:   Inicialize um registrador  $|w\rangle$  com o valor de  $|r\rangle$ ;
  - 9:   Aplique o algoritmo de Grover para buscar uma clique maximal  $y'$  tal que a cardinalidade de  $y'$  seja maior que a cardinalidade de  $y$ ;
  - 10:   Observe o registrador  $|w\rangle$ : seja  $y'$  o resultado. Se a cardinalidade de  $y'$  for maior que a cardinalidade de  $y$ , então defina  $y$  como  $y'$ ;
  - 11: **finaliza enquanto**
  - 12: **retorna**  $|c\rangle$ ;
- 

**Fonte: Autoria própria (2022).**

É possível demonstrar que a complexidade do algoritmo é inferior à melhor solução clássica através do limite:

$$\lim_{n \rightarrow \infty} \frac{n\sqrt{2^n}}{3^{n/3}} = 0. \quad (68)$$

## 6 CONSIDERAÇÕES FINAIS

Neste trabalho analisamos os ganhos teóricos de performance que podem ser obtidos ao utilizar algoritmos quânticos para buscar soluções para problemas de difícil resolução através de algoritmos clássicos, em particular o problema NP-difícil de Busca de Cliques Máximas em grafos simples.

Utilizamos duas abordagens para analisar o problema da clique máxima e determinar um algoritmo quântico adequado para oferecer uma solução ao problema em um tempo inferior ao da melhor solução clássica conhecida.

A Tabela 2 contém uma relação entre os algoritmos propostos e suas respectivas complexidades de tempo. A melhor solução clássica também foi incluída para fins de comparação.

**Tabela 2 – Complexidades dos Algoritmos**

Algoritmo	Complexidade de Tempo
Melhor Solução Clássica	$\mathcal{O}(3^{n/3})$
Busca de Wie-Bojié	$\mathcal{O}(\sqrt{2^n}(n \log n)^2)$
Algoritmo de Otimização	$\mathcal{O}(n\sqrt{2^n})$

**Fonte: Autoria própria (2022).**

Percebe-se pela Tabela 2 que o algoritmo de otimização é o que oferece o maior ganho de complexidade em comparação à melhor solução clássica conhecida, representando um ganho de  $\mathcal{O}[(n\sqrt{2^n})/(3^{n/3})]$  sobre a melhor solução clássica e  $\mathcal{O}[1/(n \log^2 n)]$  sobre o algoritmo de busca de Wie-Bojié. Ressalta-se, no entanto, que a complexidade em  $\mathcal{O}(n\sqrt{2^n})$  não considera a probabilidade de sucesso do algoritmo.

Quando o tempo de execução do algoritmo de otimização é superior a  $\mathcal{O}(22.5\sqrt{N} + 1.4 \log^2 N)$ , o algoritmo assume que a última clique maximal é a de maior cardinalidade. Caso não seja, o algoritmo falha e será necessário executar o algoritmo novamente. Repetindo a execução um número suficiente de vezes, a probabilidade que o algoritmo falhe em todas torna-se muito pequena e pode ser desprezada.

Por fim levantamos a possibilidade de, em futuros trabalhos, realizar uma análise mais aprofundada da complexidade do algoritmo de otimização incluindo a probabilidade de falha, bem como a análise do efeito de diferentes algoritmos de otimização e de contagem de qubits na complexidade do algoritmo para busca de cliques máximas.

## REFERÊNCIAS

- AARONSON, S. **Quantum computing since Democritus**. Cambridge, England: Cambridge University Press, 2013.
- Benioff, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. **Journal of Statistical Physics**, v. 22, n. 5, p. 563–591, maio 1980.
- BOJIE, A. Quantum algorithm for finding a maximum clique in an undirected graph. **JIOS**, v. 36, n. 2, p. 91–98, 2012. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/1521-3978%28200009%2948%3A9%3A11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E>.
- DIVINCENZO, D. P. The physical implementation of quantum computation. **Fortschritte der Physik**, v. 48, n. 9-11, p. 771–783, 2000. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/1521-3978%28200009%2948%3A9%3A11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E>.
- DÜRR, C.; HØYER, P. A quantum algorithm for finding the minimum. 1996. Disponível em: <https://arxiv.org/pdf/quant-ph/9607014.pdf>.
- GROVER, L. K. A fast quantum mechanical algorithm for database search. *In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. New York, NY, USA: Association for Computing Machinery, 1996. (STOC '96), p. 212–219. ISBN 0897917855. Disponível em: <https://doi.org/10.1145/237814.237866>.
- HÅSTAD, J. Clique is hard to approximate within  $n^{1-\epsilon}$ . **Acta Math**, v. 182, p. 105–142, 1999.
- KARP, R. M. Reducibility among combinatorial problems. **Complexity of Computer Computations**, p. 85–103, 1972.
- KAYE, P.; LAFLAMME, R.; MOSCA, M. **An Introduction to Quantum Computing**. [S.l.]: United States of America: Oxford University Press Inc., 2007.
- WIE, C. R. A quantum circuit to construct all maximal cliques using grover's search algorithm. **Fortschritte der Physik**, v. 48, n. 9-11, p. 1–13, 2017. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/1521-3978%28200009%2948%3A9%3A11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E>.