

Laboratório Nacional de Computação Científica

# **Modelo de Caminhadas Quânticas Escalonado**

Tharso Dominisini Fernandes

Petrópolis, RJ - Brasil

13 de setembro 2017

Tharso Dominisini Fernandes

## **Modelo de Caminhadas Quânticas Escalonado**

Tese submetida ao corpo docente do Laboratório Nacional de Computação Científica como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências em Modelagem Computacional.

Laboratório Nacional de Computação Científica

Orientador: Renato Portugal

Petrópolis, RJ - Brasil

13 de setembro 2017

F363m Fernandes, Tharso Dominisini  
Modelo de Caminhadas Quânticas Escalonado / Tharso Dominisini Fernandes. –  
Petrópolis, RJ - Brasil. Laboratório Nacional de Computação Científica , 2017.  
64 p. : il. ; 29 cm.

Orientador: Renato Portugal

Tese de Doutorado – Laboratório Nacional de Computação Científica ,  
2017.

1. Computadores quânticos 2. Caminhadas quânticas. 3. Modelo escalonado.  
4. Simulações. I. Portugal, Renato. II. LNCC/MCTI. III. Modelo de Caminhadas  
Quânticas Escalonado.

CDD: 004.1

Tharso Dominisini Fernandes

## **Modelo de Caminhadas Quânticas Escalonado**

Tese submetida ao corpo docente do Laboratório Nacional de Computação Científica como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências em Modelagem Computacional.

Aprovada por:

---

**Prof. Renato Portugal, D.Sc.**  
(Presidente)

---

**Gilson Antonio Giraldi, D.Sc. - LNCC**

---

**Carlile Campos Lavor, D.Sc. -**  
**UNICAMP**

---

**Franklin de Lima Marquezino, D.Sc. -**  
**COPPE -UFRJ**

Petrópolis, RJ - Brasil  
13 de setembro 2017

**Dedicatória**  
*A minha família.*

# Agradecimentos

A todos os meus familiares, em especial minha esposa Assunção e minha filha Laura por tudo que me proporcionaram nestes últimos anos. Ao meu orientador Renato Portugal, por toda a dedicação. Aos meus colegas do LNCC, Aaron, Aline, Alonso, Bruno, Caio, Fernandinho, Fortia, Secilia e Suelen pelo companheirismo e ajuda nos momentos difíceis. Ao LNCC pela recepção e acolhimento.

*“A imaginação é mais importante que o conhecimento.”  
(Albert Einstein)*

# Resumo

Os passeios quânticos desempenham um papel importante no desenvolvimento de novos algoritmos quânticos, e podem ser usados para resolver eficientemente problemas como: distinção de elementos, avaliação de fórmulas booleanas, verificação de produto de matrizes e comutatividade de grupos e, em especial, problemas de busca espacial em grafos. Falk exemplificou um modelo de passeios quânticos para malha bidimensional, que não necessita de um espaço adicional para representar a moeda, no qual o operador de evolução pode ser obtido via um processo de tesselação. Porém, não foi explicitada a definição do modelo para grafos genéricos e nem comprovada a sua eficiência. A ideia apresentada por Falk inspirou a criação do Passeio Quântico Escalonado (SQW). Sendo assim, as contribuições deste trabalho são (1) definir o modelo escalonado para grafos genéricos, (2) demonstrar que um importante passeio quântico já conhecido e explorado na literatura, o modelo de Szegedy, é um caso particular do modelo escalonado e (3) mostrar a eficiência do passeio quântico escalonado no problema de busca na malha bidimensional.

**Palavras-chave:** Computadores quânticos, Caminhadas Quânticas, Modelo Escalonado, Simulações.

# Abstract

Quantum walks play an important role in the development of quantum algorithms, they can be used to solve efficiently problems such as: elements distinct, boolean formulas evaluation, matrix product verification and group commutativity, and especially, spatial search problems. Falk exemplified a quantum walk model for two-dimensional lattice, that does not require an additional space to the coin, and the evolution operator can be obtained via a tessellation process. However, it was not explicit the definition of the model for generic graphs and nor proven its efficiency. The idea presented by Falk inspired the creation of Staggered Quantum Walk model (SQW). Therefore, the goal of this work is: (1) define the stepped model for generic graphs, (2) demonstrate that an important quantum walk already known and explored in the literature, the Szegedy model, is a particular case of the SQW, (3) show the efficiency of SQW in the search problem in the two-dimensional lattice.

**Keywords:** Quantum Algorithms, Quantum Walk, Simulations, Staggered Quantum Walk.

# Lista de figuras

|   |    |
|---|----|
| Figura 1 – Grafo $G$ . . . . .  | 20 |
| Figura 2 – Grafo $\Gamma$ . . . . .   | 21 |
| Figura 3 – Exemplo de um conjunto de tesselações no grafo de Hajós . . . . .  | 23 |
| Figura 4 – Exemplo de um conjunto de tesselações alternativas para o grafo de Hajós, omitindo os polígonos triviais. . . . .  | 26 |
| Figura 5 – Grafo roda estendido $E_{3,3}$ com 3 tesselações. . . . .  | 28 |
| Figura 6 – Exemplo de grafo bipartido $\Gamma$ . . . . .  | 31 |
| Figura 7 – Modelo Stegged definido no $L(\Gamma)$ . . . . .   | 31 |
| Figura 8 – Grafo $G$ com suas tesselações . . . . .   | 33 |
| Figura 9 – Grafo bipartido $\Gamma$ , onde é realizado o passeio quântico de Szegedy . . . . .  | 33 |
| Figura 10 – Grafo de acordo com as tesselações apresentadas por Ambainis et al. (2013) . . . . .  | 37 |
| Figura 11 – Malha 2D com 4 tesselações, $n = 2$ . . . . .   | 38 |
| Figura 12 – Probabilidade no elemento marcado em função do número de passos do algoritmo, para o operador de evolução $\mathcal{U}_0(\frac{\pi}{4})$ . . . . .                | 40 |
| Figura 13 – Probabilidade no elemento marcado em função do número de passos do algoritmo, para o operador de evolução $\mathcal{U}_0(\frac{\pi}{4})$ . . . . .                | 40 |
| Figura 14 – Tempo de execução do algoritmo usando o operador $\mathcal{U}'_0(\frac{\pi}{4})$ em função da quantidade de vértices na escala loglog . . . . .                   | 41 |
| Figura 15 – Inverso da probabilidade de sucesso do algoritmo usando o operador $\mathcal{U}'_0(\frac{\pi}{4})$ em função da quantidade de vértices na escala loglog . . . . . | 42 |
| Figura 16 – Comportamento de $\lambda$ e $\phi_{min}$ em relação ao número de vértices $N$ , quando $\theta = \pi/3$ . . . . .  | 49 |
| Figura 17 – Nove grafos proibidos de Beineke . . . . .  | 60 |

# Lista de tabelas

|  |    |
|--|----|
| Tabela 1 – Probabilidades não nulas que o caminhante quântico assume até os 3 primeiros passos da caminhada. . . . . | 18 |
| Tabela 2 – Probabilidades não nulas após a aplicação do operador $U_0$ . . . . .                                     | 24 |
| Tabela 3 – Probabilidades não nulas após a aplicação do operador $U_1U_0$ . . . . .                                  | 25 |
| Tabela 4 – Probabilidades não nulas após a aplicação do operador $U_2U_1U_0$ . . . . .                               | 25 |
| Tabela 5 – Autovalores e autovetores de $U$ . . . . .  | 44 |

# Lista de símbolos

$A \otimes B$ : Produto tensorial entre  $A$  e  $B$

$A^{\otimes n}$ : Produto tensorial entre  $A$  de  $A$  com  $A$  repetido  $n$  vezes

$|\psi\rangle$ : Vetor, também chamado *ket*

$\langle\psi|$ : Vetor dual, também chamado *bra*

$\langle\varphi|\psi\rangle$ : Produto escalar entre  $|\varphi\rangle$  e  $|\psi\rangle$

$|\varphi\rangle \otimes |\psi\rangle$ : Produto tensorial entre  $|\varphi\rangle$  e  $|\psi\rangle$

$|\varphi\rangle |\psi\rangle$ : Produto tensorial entre  $|\varphi\rangle$  e  $|\psi\rangle$

$\langle\varphi| A |\psi\rangle$ : Produto escalar entre  $|\varphi\rangle$  e  $A |\psi\rangle$

$\log(\cdot)$ : logaritmo na base 2

$\ln(\cdot)$ : logaritmo Neperiano

$O(\cdot)$ :  $f(x) = O(g(x))$  se existem  $C > 0, x_0$  tais que  $f(x) \leq Cg(x), \forall x > x_0$

$\Omega(\cdot)$ :  $f(x) = \Omega(g(x))$  se existem  $C > 0, x_0$  tais que  $Cg(x) \leq f(x), \forall x > x_0$

$\Theta(\cdot)$ :  $f(x) = \Theta(g(x))$  se  $f(x) = O(g(x))$  e  $f(x) = \Omega(g(x))$

$\mathbb{Z}_N$ : Conjunto dos inteiros  $\{0, 1, \dots, N - 1\}$  com a soma módulo  $N$

$\omega_N$ : Raiz principal da unidade, definida por  $\omega_N \equiv \exp \frac{2\pi i}{N}$

# Sumário

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introdução</b>  | <b>13</b> |
| 1.1      | Contribuições desta tese   | 14        |
| 1.2      | Organização do texto   | 15        |
| <b>2</b> | <b>Passeios quânticos a tempo discreto</b>                                   | <b>16</b> |
| 2.1      | Passeios quânticos com moeda   | 16        |
| 2.1.1    | Caminhada quântica unidimensional  | 17        |
| 2.1.2    | Caminhada quântica com moeda em grafos genéricos                             | 18        |
| 2.2      | Passeio quântico de Szegedy  | 19        |
| <b>3</b> | <b>Modelo de Caminhadas Quânticas Escalonado</b>                             | <b>22</b> |
| 3.1      | O problema de tesselação em um grafo   | 25        |
| 3.2      | Staggered Quantum Walk Generalizado  | 28        |
| 3.3      | Staggered Quantum Walk com Hamiltonianos                                     | 29        |
| 3.4      | Inclusão do passeio de Szegedy no SQW  | 29        |
| 3.4.1    | Todo passeio de Szegedy é um SQW   | 29        |
| 3.4.2    | Em quais condições o SQW é equivalente ao passeio quântico de Szegedy?       | 31        |
| 3.4.3    | O problema de busca usando passeios quânticos                                | 34        |
| <b>4</b> | <b>Problema de busca em grades bidimensionais via Staggered Quantum Walk</b> | <b>36</b> |
| 4.1      | Descrição dos algoritmos   | 37        |
| 4.2      | Resultados Numéricos   | 39        |
| 4.3      | Análise do algoritmo para o operador $\mathcal{U}_0(\frac{\pi}{4})$          | 42        |
| 4.3.1    | Autovalores e autovetores do operador $U$                                    | 43        |
| 4.3.2    | Probabilidade de sucesso e tempo de execução do algoritmo                    | 44        |
| 4.4      | Análise para valores de $\theta$ diferentes de $\frac{\pi}{4}$               | 49        |
| <b>5</b> | <b>Conclusões e perspectivas futuras</b>                                     | <b>50</b> |
|          | <b>Referências</b>   | <b>51</b> |
|          | <b>Apêndices</b>   | <b>55</b> |
|          | <b>APÊNDICE A Postulados da Mecânica Quântica</b>                            | <b>56</b> |
|          | <b>APÊNDICE B Grafos</b>   | <b>59</b> |
|          | <b>APÊNDICE C Prova <math>C</math> é <math>\Theta(\sqrt{\ln N})</math></b>   | <b>62</b> |

# 1 Introdução

A computação quântica mostrou-se ativa no desenvolvimento de algoritmos ao longo das últimas três décadas (JORDAN, 2017). O algoritmo de Deutsch e Jozsa (1992) foi o primeiro a apresentar um ganho exponencial sobre qualquer versão clássica determinística. Porém, os algoritmos que chamaram a atenção da comunidade científica foram os de Shor (1994) e Grover (1996). O primeiro faz a fatoração de número inteiro em tempo polinomial, um ganho exponencial sobre o clássico; o segundo realiza a busca em um banco de dados arbitrariamente ordenado em um tempo de execução quadraticamente mais rápido que o análogo clássico. Esses algoritmos impulsionaram não só o surgimento de outros (MOSCA, 2009; CHILDS; DAM, 2010), mas também a busca por tecnologias que permitam a criação do computador quântico.

Recentemente, a empresa IBM anunciou a criação de dois processadores quânticos universais, um de 16 qubits para uso público e outro de 17 qubits para uso comercial (IBMQ, 2017). Em março de 2017, em uma conferência da Sociedade Norte Americana de Física, o líder do grupo de pesquisas em computação quântica da empresa Google informou que, até o final do ano de 2017, será capaz de produzir um computador quântico universal de 49 qubits (FELDMAN, 2017).

Junto à criação do computador quântico, surge também a necessidade de desenvolver novos algoritmos para aproveitar ao máximo essa tecnologia. A técnica dos passeios aleatórios vem sendo aplicada com muito sucesso na elaboração de algoritmos quânticos, e descreve a trajetória de uma partícula que se move com sucessivos passos, cujas direções são baseadas no resultado de uma variável aleatória. Na computação clássica temos aplicações importantes como, por exemplo, soluções para o problema  $k$ -SAT e conectividade de grafos (MOTWANI; RAGHAVAN, 2010). O passeio aleatório foi adaptado às leis da mecânica quântica e vem sendo usado na criação de algoritmos quânticos eficientes em diversos problemas como: busca por triângulos (MAGNIEZ et al., 2007), verificação de produto de matrizes e comutatividade de grupos (SANTHA, 2008), distinção de elementos (*element distinctness*) (AMBAINIS, 2007), avaliação de fórmulas booleanas (FARHI et al., 2007), transporte em redes complexas (MÜLKEN; BLUMEN, 2011) e, em especial, problemas de busca espacial (SHENVI et al., 2003; AMBAINIS et al., 2005a; ABAL et al., 2010; MARQUEZINO et al., 2011).

Existem pelo menos quatro modelos de passeios quânticos descritos na literatura, os quais foram criados com diferentes objetivos e características. O primeiro é o Passeio Quântico com Moeda, introduzido por Aharonov et al. (1993). Os autores apresentaram um passeio quântico na reta discreta a tempo discreto e utilizaram um espaço para posição

da partícula e outro para a moeda. Este modelo foi estendido para grafos genéricos por [Aharonov et al. \(2001\)](#).

O segundo modelo, Passeio Quântico a Tempo Contínuo, que foi proposto por Farhi e Gutmann ([FARHI; GUTMANN, 1998](#)), e vem sendo amplamente explorado, tanto do ponto de vista teórico quanto do experimental ([ROSSI et al., 2017](#)).

O terceiro modelo foi proposto por [Szegedy \(2004\)](#) e na literatura é simplesmente referenciado como Passeio Quântico de Szegedy. Ele faz a quantização dos passeios aleatórios clássicos por meio da duplicação do grafo original, sem o uso do espaço moeda. Este modelo é obtido via quantização das cadeias de Markov clássicas a tempo discreto, o que permite uma definição natural para o tempo de alcance quântico. [Szegedy \(2004\)](#) mostrou que o tempo para a detecção de um elemento marcado é quadraticamente menor no passeio aleatório quantizado. O modelo de Szegedy já foi abordado nos problemas de busca em grafos por elementos marcados ([MAGNIEZ et al., 2011](#); [KROVI et al., 2010](#)), busca por triângulos ([MAGNIEZ et al., 2007](#)), verificação de produto de matrizes e comutatividade de grupos ([SANTHA, 2008](#)).

O quarto modelo, que será o principal objeto de estudo desta tese, é conhecido como Passeio Quântico Escalonado ou *Staggered Quantum Walk (SQW)* e não faz uso de um espaço adicional para determinar a direção da caminhada aleatória, por isso é considerado um modelo sem moeda. As ideias seminais para este modelo apareceram em um artigo de [Falk \(2013\)](#), no qual o autor mostrou que o operador de evolução na malha pode ser obtido através de um processo de difusão local da malha e que pode ser modelado por tesselações. Ele foi definido formalmente em [Portugal et al. \(2016\)](#) e [Portugal et al. \(2016\)](#) propuseram uma versão para modelo com o uso de Hamiltonianos.

## 1.1 Contribuições desta tese

Tanto o SQW quanto o modelo proposto por Szegedy não fazem uso do operador moeda. Portanto, fizemos questionamentos a respeito da relação entre esses dois modelos e verificamos que o modelo proposto por Szegedy é um caso particular do SQW. Este resultado e a definição formal do modelo SQW são contribuições inéditas desta tese. Eles compõem o artigo [Portugal et al. \(2016\)](#), o qual recebeu o prêmio *Howard E. Brandt Best Paper Award 2016* da revista *Quantum Information Processing*.

Obtivemos alguns resultados sobre o problema de tesselação em grafos, os quais fazem parte do artigo [Abreu et al. \(2017\)](#), que foram publicados na revista *Matemática Contemporânea*. Também indagamos sobre a eficiência do modelo SQW no problema de busca em grades bidimensionais e em resposta a esta indagação encontramos um algoritmo quântico, que faz uso da versão estendida do SQW usando Hamiltonianos, com mesma complexidade dos algoritmos quânticos mais eficientes para a solução do problema. Este

resultado foi publicado no periódico *Physical Review A* (PORTUGAL; FERNANDES, 2017) e alguns resultados numéricos relevantes para o problema que foram apresentados na *4th Conference of Computational Interdisciplinary Sciences* (FERNANDES; PORTUGAL, 2016).

Alcançamos resultados colaterais sobre a análise da eficiência de algoritmos quânticos para o problema de busca via grupo de renormalização. Eles fazem parte do artigo [Bottcher et al. \(2017\)](#), que foi submetido para publicação na revista *Nature Communications*.

## 1.2 Organização do texto

Este trabalho está organizado da seguinte forma. No capítulo 2, faremos uma breve revisão a respeito dos passeios quânticos com moeda e do modelo de Szegedy. No capítulo 3, definiremos formalmente o modelo SQW, abordaremos o problema de tesselação em grafos e mostraremos que o modelo de Szegedy pode ser incluído no SQW. No capítulo 4, abordaremos o problema de busca em grades bidimensionais via SQW. No capítulo 5, delineamos nossas considerações finais. No apêndice A, apresentaremos uma breve revisão sobre a computação quântica. No apêndice B, exibiremos algumas definições e resultados da teoria de grafos. No apêndice C, é mostraremos que o termo  $C$  definido no capítulo 4 é  $\Theta(\sqrt{\ln N})$ .

## 2 Passeios quânticos a tempo discreto

Um modelo de caminhada aleatória ou passeio aleatório descreve o movimento de uma partícula que se move por meio de sucessivos passos aleatórios, isto é, a cada instante de tempo, a direção a ser seguida é baseada no resultado de uma variável aleatória. Usualmente, um passeio aleatório é descrito por um grafo, uma matriz estocástica e um vértice inicial. O grafo representa as possíveis posições que a partícula pode assumir, a matriz estocástica descreve as probabilidades de deslocamento em cada vértice na direção de seus vizinhos e o vértice inicial é o ponto de partida do caminhante.

No caso quântico, um passeio aleatório é definido por um grafo, um operador unitário, chamado de operador de evolução, e um estado inicial. A caminhada quântica será realizada no espaço de Hilbert  $\mathcal{H}^p$ , onde  $p$  deve ser da mesma cardinalidade do conjunto de vértices do grafo, exceto na caminhada quântica com moeda, em que é adicionado um espaço de Hilbert extra para representação da moeda. O caminhante quântico é representado por um vetor normalizado em  $\mathcal{H}^p$  e cada vértice do grafo  $v$  é representado por um vetor da base computacional  $|v\rangle$  em  $\mathcal{H}^p$ . Em uma caminhada quântica, o sistema é inicializado no estado  $|\psi(0)\rangle$ , após  $t$  passos, o sistema vai para o estado:

$$|\psi(t)\rangle = U^t |\psi(0)\rangle, \quad (2.1)$$

onde  $U$  é o operador de evolução da caminhada. O operador  $U$  deve preservar a localidade, isto é, se aplicado a um vetor da base computacional  $|v\rangle$ , o vetor resultante, quando decomposto na base computacional, deve conter apenas vetores que representam vértices vizinhos a  $v$ . Note que, após  $t$  passos da caminhada, o estado do sistema é completamente determinístico, a aleatoriedade em um passeio quântico é adicionada quando efetuarmos uma medição na base computacional no estado do sistema. Tal medição terá como resultado um vetor da base computacional, que representa um vértice do grafo. Vale ressaltar que o estado inicial pode ser uma sobreposição dos elementos da base computacional.

Neste capítulo, vamos descrever os dois modelos de caminhadas quânticas a tempo discreto encontrados na literatura. Primeiramente veremos o modelo com moeda e, em seguida, apresentaremos o modelo proposto por Szegedy.

### 2.1 Passeios quânticos com moeda

Esta seção objetiva revisar brevemente os passeios quânticos a tempo discreto com moeda. Portanto, se for necessário obter maiores detalhes sobre esse assunto, basta consultar *Quantum Walks and search algorithms* (PORTUGAL, 2013). Agora, a fim de introduzir o modelo de caminhadas quânticas com moeda, veremos a definição do modelo

na reta unidimensional; em seguida, mostraremos como esse modelo pode ser estendido a grafos genéricos.

### 2.1.1 Caminhada quântica unidimensional

Um caso sobre caminhada aleatória comumente estudado pode ser descrito na reta unidimensional, onde consideramos o movimento de uma partícula que se move de forma aleatória em uma reta discreta infinita. A cada passo é lançada uma moeda, e de acordo com resultado do lançamento, a partícula se moverá para a direita ou para a esquerda. No caso quântico, cada posição que a partícula pode assumir é associada a um vetor da base computacional  $\{|p\rangle, p \in \mathbb{Z}\}$  do espaço de Hilbert  $\mathcal{H}_\infty$ . Adicionamos ao sistema um qubit extra para representar o espaço moeda, com isso a caminhada quântica ocorrerá no espaço de Hilbert  $\mathcal{H}_2 \otimes \mathcal{H}_\infty$ . A dinâmica do passeio é definida por dois operadores unitários, o primeiro atuará somente no espaço da moeda, ele agirá de forma análoga ao lançamento da moeda no caso clássico. Ele é da forma  $C \otimes I$ , onde  $C$  é um operador unitário  $2 \times 2$ , que pode ser escolhido livremente. O segundo, será o operador de deslocamento  $S$ , este atuará no espaço posição de acordo com estado da moeda. A definição do operador  $S$  na base computacional é dada por:

$$S |0\rangle |i\rangle = |0\rangle |i+1\rangle, \quad (2.2)$$

$$S |1\rangle |i\rangle = |1\rangle |i-1\rangle. \quad (2.3)$$

Dessa forma, se o estado da moeda for  $|0\rangle$ , o espaço posição "move-se" para a direita, e se o estado da moeda for  $|1\rangle$ , a partícula "move-se" para a esquerda. Portanto, pelas equações dadas em (2.2) e (2.3), podemos explicitar  $S$  como:

$$S = |0\rangle \langle 0| \otimes \sum_{i=-\infty}^{\infty} |i+1\rangle \langle i| + |1\rangle \langle 1| \otimes \sum_{i=-\infty}^{\infty} |i-1\rangle \langle i|. \quad (2.4)$$

O operador de evolução da caminhada quântica será:

$$U = S(H \otimes I). \quad (2.5)$$

Após  $t$  passos da caminhada, o sistema vai para o estado:

$$|\psi(t)\rangle = U^t \psi(0). \quad (2.6)$$

Podemos explicitar um exemplo de caminhada tomando como condição inicial o vetor

$$|\psi(0)\rangle = |0\rangle |0\rangle, \quad (2.7)$$

e, como operador moeda, o operador de Hadamard:

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

Assim, os três primeiros passos da caminhada quântica serão:

$$|\psi(1)\rangle = \frac{1}{\sqrt{2}} (|1\rangle |-1\rangle + |0\rangle |1\rangle), \quad (2.8)$$

$$|\psi(2)\rangle = \frac{1}{2} (|1\rangle |-2\rangle + (|0\rangle + |1\rangle) |0\rangle + |0\rangle |2\rangle), \quad (2.9)$$

$$|\psi(3)\rangle = \frac{1}{2\sqrt{2}} (|1\rangle |-3\rangle - |0\rangle |-1\rangle + (2|0\rangle + |1\rangle) |1\rangle + |0\rangle |3\rangle) \quad (2.10)$$

Em caso de medição na base computacional, o caminhante quântico assume as probabilidades em cada vértice da reta de acordo com a tabela.

Tabela 1 – Probabilidades não nulas que o caminhante quântico assume até os 3 primeiros passos da caminhada.

| t/p | -3            | -2            | -1            | 0             | 1             | 2             | 3             |
|-----|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| 0   |               |               |               | 1             |               |               |               |
| 1   |               |               | $\frac{1}{2}$ |               | $\frac{1}{2}$ |               |               |
| 2   |               | $\frac{1}{4}$ |               | $\frac{1}{2}$ |               | $\frac{1}{4}$ |               |
| 3   | $\frac{1}{8}$ |               | $\frac{1}{8}$ |               | $\frac{5}{8}$ |               | $\frac{1}{8}$ |

### 2.1.2 Caminhada quântica com moeda em grafos genéricos

Dado um grafo  $G(V, E)$ , onde  $V$  é o conjunto de vértices e  $E$ , o conjunto de arestas de  $G$ . A princípio, vamos assumir que  $G$  seja um grafo  $d$ -regular. Associamos o conjunto de vértices  $V$  ao espaço de Hilbert  $\mathcal{H}^{|V|}$ ,  $\mathcal{H}^d$  será o nosso espaço auxiliar referente à moeda. Em  $\mathcal{H}^{|V|}$ , consideramos a base computacional  $|v\rangle \in \mathcal{H}^{|V|}$ , com  $v \in V$ . No espaço moeda, vamos enumerar todas as aresta dos vértices de 1 a  $d$  e assumir a base computacional  $\{|1\rangle, |2\rangle, \dots, |d\rangle\}$ . A dinâmica do passeio quântico deverá ocorrer no espaço de Hilbert  $\mathcal{H}^d \otimes \mathcal{H}^{|V|}$ . O operador de evolução da caminhada quântica é definido como  $U = S(C \otimes I)$ , onde  $C$  é um operador unitário qualquer definido em  $\mathcal{H}^d$ , chamado de operador moeda,  $S$  é o operador de deslocamento definido na base computacional por  $S|a, v\rangle = |a, u\rangle$ , onde  $u$  é o  $a$ -ésimo vizinho de  $v$ .

Para a definição do modelo para grafos não regulares, vamos relaxar na informação exata do operador  $U$ , e somente exigir que  $U$  preserve a estrutura do grafo, isto é, para todos  $v \in V$  e  $a$ , a sobreposição  $U|a, u\rangle$  deve conter apenas elementos da base  $|a', u'\rangle$ , com  $u' = N(v) \cup \{v\}$ , onde  $N(v)$  são os vizinhos de  $v$  (AHARONOV et al., 2001).

## 2.2 Passeio quântico de Szegedy

Nesta seção, descreveremos o modelo de caminhadas quânticas proposto por [Szegedy \(2004\)](#). Primeiramente, apresentaremos o método de quantização de passeios clássicos em grafos bipartidos; e em seguida mostraremos como é feita a duplicação de um grafo qualquer para criar um passeio aleatório equivalente em um grafo bipartido.

Considere um grafo bipartido não direcionado  $\Gamma(X, Y, E)$ , onde  $X, Y$  são os conjuntos disjuntos de vértices e  $E$ , o conjunto de arestas. Dados  $x, y$  elementos quaisquer de  $X, Y$ , respectivamente, definimos  $p_{xy}$  a probabilidade de um caminhante sair de  $x$  em direção a  $y$ , e  $q_{yx}$ , o inverso. Com isso, temos as matrizes estocásticas  $P = [p_{xy}]$  e  $Q = [q_{yx}]$ , que permitem a definição dos seguintes vetores unitários:

$$|\psi_x\rangle := \sum_{y \in Y} \sqrt{p_{xy}} |x, y\rangle, \quad (2.11)$$

$$|\phi_y\rangle := \sum_{x \in X} \sqrt{q_{yx}} |x, y\rangle. \quad (2.12)$$

Onde  $|x, y\rangle$  são vetores da base computacional do espaço de Hilbert  $\mathcal{H}^N \otimes \mathcal{H}^M$ , com  $|X| = M$  e  $|Y| = N$ . Assim são definidos os refletores:

$$R_A := 2 \sum_x |\psi_x\rangle \langle \psi_x| - I, \quad (2.13)$$

$$R_B := 2 \sum_y |\phi_y\rangle \langle \phi_y| - I. \quad (2.14)$$

Podemos verificar que:

$$R_A R_A^\dagger = R_A R_A = (2 \sum_x |\psi_x\rangle \langle \psi_x| - I)(2 \sum_{x'} |\psi_{x'}\rangle \langle \psi_{x'}| - I) \quad (2.15)$$

$$= 4 \sum_x |\psi_x\rangle \langle \psi_x| - 2 \sum_x |\psi_x\rangle \langle \psi_x| - 2 \sum_x |\psi_x\rangle \langle \psi_x| + I \quad (2.16)$$

$$= I. \quad (2.17)$$

Analogamente,  $R_B R_B = R_B R_B^\dagger = I$ . Portanto,  $R_A$  e  $R_B$  são operadores hermitianos e unitários.

A partir dessa informação, tem-se a definição do operador de evolução do passeio quântico de Szegedy como sendo:

$$W := R_B R_A. \quad (2.18)$$

A princípio, pode-se observar que o passeio quântico de Szegedy é um passeio nas arestas do grafo  $\Gamma$ . No capítulo 3 mostraremos a equivalência entre os passeios quânticos de Szegedy e o SQW, o que nos permitirá uma interpretação adequada dos passeios.

Agora vamos ver como é feita a duplicação do grafo para criar um passeio aleatório equivalente em um grafo bipartido.

Seja  $G = (X, E)$  um grafo não direcionado e  $P$  uma matriz estocástica, tal que  $p_{x_1x_2}$  representa a probabilidade do caminhante sair de  $x_1$  em direção a  $x_2$ . A partir de  $G$ , podemos definir o grafo bipartido  $\Gamma = (X, Y, E')$ , onde  $Y$  é uma cópia de  $X$  (com *labels* distintos) com cada elemento  $x_k \in X$  representado por um elemento  $y_k \in Y$ . As arestas  $\{x_j, x_k\} \in E$  são transformadas em arestas  $\{x_j, y_k\} \in E'$ . A matriz estocástica do novo passeio aleatório é dada por:

$$\bar{P} = \begin{bmatrix} \overbrace{\mathbf{0}}^X & \overbrace{P}^Y \\ P & \mathbf{0} \end{bmatrix}.$$

Neste caso,  $Q = P$ .

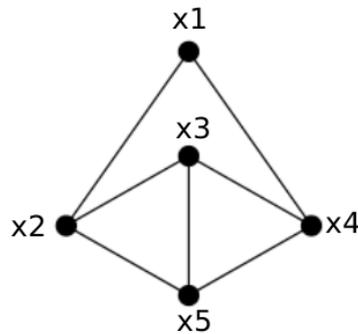


Figura 1 – Grafo G

**Exemplo 1.** Se tivermos um passeio aleatório definido em  $G$  (figura 1), assumindo transição equiprovável para todos os vizinhos, isto é, a matriz estocástica associada ao passeio definida por

$$P = \begin{bmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \end{bmatrix}.$$

O grafo bipartido  $\Gamma$  associado a  $G$  será o grafo da figura 2. E a matriz estocástica, associada

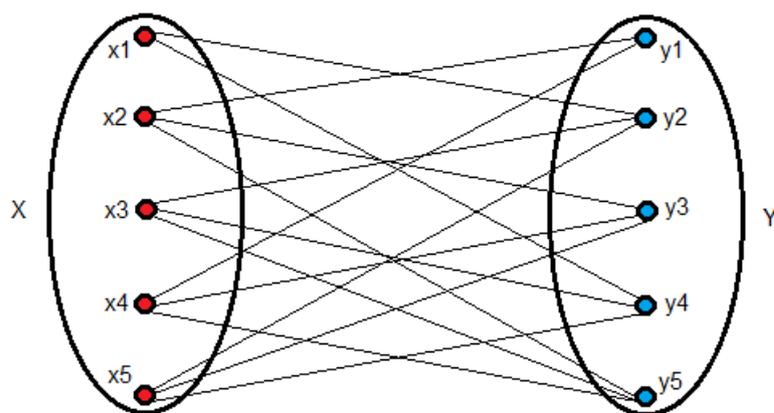


Figura 2 – Grafo  $\Gamma$

ao passeio aleatório, será

$$\bar{P} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

### 3 Modelo de Caminhadas Quânticas Escalonado

Neste capítulo, abordaremos o modelo de passeios quânticos escalonado (SQW). Primeiramente, faremos a definição formal do modelo em grafos genéricos. Na seção 3.1, discorreremos acerca do problema de tesselação em um grafo. Na seção 3.2, apresentaremos a generalização do modelo para englobar o problema de busca. Na seção 3.3, definiremos a versão do modelo proposta por Portugal et al. (2017), que faz o uso de hamiltonianos. Na seção 3.4, veremos como o modelo de Szegedy é incluído no SQW.

Vejamos a seguir a definição de tesselação, que é um conceito fundamental para o SQW.

**Definição 1.** *Dado um grafo não direcionado  $G = (V, E)$ , onde  $V$  é o conjunto de vértices e  $E$  um conjunto de arestas do grafo. Uma tesselação  $\mathcal{T}_k = \{\tau_{kj}\}$ , onde  $\tau_{kj} \subset V$ , satisfaz as seguintes condições:*

- $\cup_j \tau_{kj} = V$ ;
- $\tau_{kj} \cap \tau_{kl} = \emptyset, \forall j \neq l$ ;
- $\tau_{kj}$  é uma clique de  $G, \forall j$ .

Os subconjuntos  $\tau_{kj}$  são chamados de polígonos da tesselação  $\mathcal{T}_k$ .

De maneira um pouco mais informal, podemos dizer que um conjunto de polígonos  $\mathcal{T}_k$  de  $G$  é uma tesselação de  $G$ , se  $\mathcal{T}_k$  obedecer às seguintes condições:

- $\mathcal{T}_k$  cobre todo o conjunto de vértices de  $G$ ;
- não há sobreposição entre os polígonos de  $\mathcal{T}_k$ ;
- os polígonos de  $\mathcal{T}_k$  são subgrafos completos de  $G$ .

Na figura 3, exibimos o exemplo do grafo de Hajós com 3 tesselações: azul, verde e vermelha.

$$\mathcal{T}_0 = \{\{0, 4, 5\}; \{1\}; \{2\}; \{3\}\} \text{ (verde),} \quad (3.1)$$

$$\mathcal{T}_1 = \{\{1, 3, 4\}; \{0\}; \{2\}; \{5\}\} \text{ (vermelho),} \quad (3.2)$$

$$\mathcal{T}_2 = \{\{2, 3, 5\}; \{0\}; \{1\}; \{4\}\} \text{ (azul).} \quad (3.3)$$

Os polígonos triviais, que contém apenas um vértice, foram omitidos na figura 3.

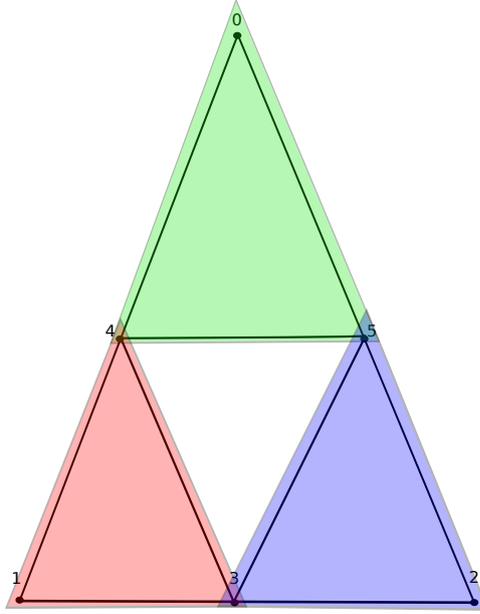


Figura 3 – Exemplo de um conjunto de tesselações no grafo de Hajós

A partir da tesselação podemos definir o operador de evolução do SQW. Dado um grafo não direcionado  $G = (V, E)$  e um conjunto de tesselações  $\mathcal{T} = \{\mathcal{T}_k\}$  de  $G$ , que cobrem todas as arestas de  $G$ ; neste caso, dizemos que uma tesselação  $\mathcal{T}_k$  cobre uma aresta de  $G$  se os dois vértices que a compõem pertencerem a um mesmo polígono de  $\mathcal{T}_k$ . Associado a  $G$ , temos o espaço de Hilbert  $\mathcal{H}^N$ , onde  $N = |V|$  e cada vértice  $v \in V$  é relacionado a um vetor da base computacional em  $\mathcal{H}^N$ , o qual denotaremos por  $|v\rangle$  de  $\mathcal{H}^N$ . Para cada subconjunto  $\tau_{kj} = \{l\}$ , definimos os seguintes vetores:

$$|\tau_{kj}\rangle := \sum_{l \in \tau_{kj}} \alpha_{k,j,l} |l\rangle. \quad (3.4)$$

Os coeficientes complexos  $\{\alpha_{k,j,l}\}$  não podem ser nulos e devem ser escolhidos de forma que  $\sum_{l \in \tau_{kj}} |\alpha_{k,j,l}|^2 = 1$ , logo  $|\tau_{kj}\rangle$  são unitários. Com isto, definimos os operadores de reflexão:

$$U_k := 2 \sum_j |\tau_{kj}\rangle \langle \tau_{kj}| - I, \quad (3.5)$$

Podemos verificar que:

$$U_k U_k = (2 \sum_j |\tau_{kj}\rangle \langle \tau_{kj}| - I)(2 \sum_l |\tau_{kl}\rangle \langle \tau_{kl}| - I) \quad (3.6)$$

$$= 4 \sum_j |\tau_{kj}\rangle \langle \tau_{kj}| - 2 \sum_j |\tau_{kj}\rangle \langle \tau_{kj}| - 2 \sum_j |\tau_{kj}\rangle \langle \tau_{kj}| + I \quad (3.7)$$

$$= I. \quad (3.8)$$

Portanto,  $U_k$  são operadores hermitianos e unitários.

Assim, podemos definir o operador de evolução

$$U := U_n \dots U_1 U_0 \quad (3.9)$$

No caso geral, dados um grafo  $G$ , um operador de evolução  $U$  e um estado inicial  $|\psi_0\rangle$ , evoluímos o passeio quântico durante um tempo  $t$ ,

$$|\psi(t)\rangle := U^t |\psi_0\rangle, \quad (3.10)$$

então efetuamos uma medição, geralmente na base computacional, no estado final  $|\psi(t)\rangle$ . Com a medição, obtemos como resultado um vértice do grafo.

**Exemplo 2.** *Se consideramos que o caminhante esteja no estado inicial  $|0\rangle$  e que o grafo em questão seja o grafo de Hajós da figura 3, com as tesselações:*

*Admitindo que os coeficientes das tesselações sejam reais positivos e uniformemente distribuídos, isto é,  $\alpha_{k,j,l} = \frac{1}{\sqrt{3}}$  para todos  $k, j, l$ , a atuação do operador  $U_0$  sobre o estado inicial será:*

$$U_0 |0\rangle = -\frac{1}{3} |0\rangle + \frac{2}{3} |4\rangle + \frac{2}{3} |5\rangle. \quad (3.11)$$

*Em caso de medição na base computacional, após a aplicação do operador de reflexão  $U_0$ , o caminhante assume as probabilidades (em caso de medição na base computacional) nos vértices de acordo com a tabela 2.*

Tabela 2 – Probabilidades não nulas após a aplicação do operador  $U_0$ .

| Vértice | Probabilidade |
|---------|---------------|
| 0       | 1/9           |
| 4       | 4/9           |
| 5       | 4/9           |

*As demais probabilidades serão nulas.*

*Ao aplicar o operador de reflexão  $U_1$ , no resultado anterior, temos*

$$U_1 U_0 |0\rangle = \frac{1}{3} |0\rangle + \frac{4}{9} |1\rangle + \frac{4}{9} |3\rangle - \frac{2}{9} |4\rangle - \frac{2}{3} |5\rangle. \quad (3.12)$$

*Em caso de medição na base computacional, após a aplicação do operador de reflexão  $U_1 U_0$ , o caminhante assume as probabilidades nos vértices de acordo com a tabela 3.*

*Ao aplicar o operador  $U_2$ , o sistema vai para o estado:*

$$U_2 U_1 U_0 |0\rangle = -\frac{1}{3} |0\rangle - \frac{4}{9} |1\rangle - \frac{4}{27} |2\rangle - \frac{16}{27} |3\rangle + \frac{2}{9} |4\rangle - \frac{14}{27} |5\rangle. \quad (3.13)$$

*Em caso de medição na base computacional, as probabilidades são distribuídas de acordo com a tabela 4. E assim, a probabilidade, em caso de medição, se distribui ao longo do grafo.*

Tabela 3 – Probabilidades não nulas após a aplicação do operador  $U_1U_0$ .

| Vértice | Probabilidade |
|---------|---------------|
| 0       | 1/9           |
| 1       | 16/81         |
| 3       | 16/81         |
| 4       | 4/81          |
| 5       | 4/9           |

Tabela 4 – Probabilidades não nulas após a aplicação do operador  $U_2U_1U_0$ .

| Vértice | Probabilidade |
|---------|---------------|
| 0       | 1/9           |
| 1       | 16/81         |
| 2       | 16/729        |
| 3       | 256/729       |
| 4       | 4/81          |
| 5       | 196/729       |

### 3.1 O problema de tesselação em um grafo

Um conjunto de tesselações para um dado grafo que cobre todo o conjunto de arestas de um dado grafo  $\Gamma$  não é único, podemos escolher diferentes cliques para compor um conjunto de tesselações. Tomamos como exemplo o grafo de Hajós, e criaremos um conjunto alternativo de tesselações para ele, o resultado será como o apresentado na figura 4. Para a implementação física do modelo, é desejável uma quantidade mínima de tesselações; sendo assim, uma questão natural que surge é: dado um grafo  $\Gamma$ , qual quantidade mínima de tesselações será necessária para cobrir todas as arestas de  $\Gamma$ ? Nesta seção, abordaremos alguns questionamentos sobre o número mínimo de tesselações de um grafo. Antes, porém, é importante dar algumas definições, o que possibilitará uma posterior discussão sobre o problema. Também faremos uso de algumas definições usadas na teoria de grafos e que podem ser encontradas no apêndice B. Com fins de definição, vamos dizer que um grafo  $\Gamma$  é  $k$ -tesselável se existe um conjunto de tesselações  $\mathcal{T}$  com  $k$  elementos que cobrem todo o conjunto de arestas de  $\Gamma$ . O número de tesselação do grafo  $\Gamma$  é definido pela cardinalidade do menor conjunto de tesselações que cobre todo o conjunto de arestas de  $\Gamma$ , denotaremos este número por  $T(\Gamma)$ . Portugal (2016) mostrou que os grafos 2-tesseláveis são caracterizados pelo número cromático do seu grafo clique (teorema 1).

**Teorema 1.** (PORTUGAL, 2016) Dado um grafo  $\Gamma$ ,  $T(\Gamma) = 2$ , se e somente se,  $K(\Gamma)$  é 2-colorível.

Este teorema não pode ser trivialmente generalizado, uma vez que o grafo de Hajós,

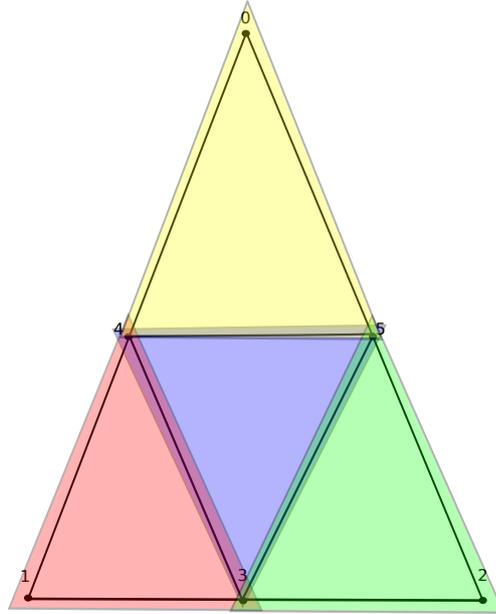


Figura 4 – Exemplo de um conjunto de tesselações alternativas para o grafo de Hajós, omitindo os polígonos triviais.

já apresentado em exemplos anteriores, é 3-tesselável; porém, o número cromático do seu grafo clique (grafo completo com 4 vértices) é 4. O número cromático do grafo clique nos dá um limite superior para a quantidade mínima de tesselações para um grafo, como pode ser visto no teorema 2.

**Teorema 2.** *Dado um grafo  $\Gamma$  conexo, se o grafo clique de  $\Gamma$  não é 2-colorível, então  $3 \leq T(\Gamma) \leq \chi(K(\Gamma))$ .*

*Demonstração.* Dado um grafo  $\Gamma$  conexo. O limite inferior fica bem estabelecido pelo teorema 1. Para provar o limite superior, vamos criar um conjunto de tesselações para  $\Gamma$  baseado na coloração do seu grafo clique. Considere  $C = \{g\}$  um conjunto mínimo de cores para  $K(\Gamma)$ , seja  $M_g$  um conjunto de cliques coloridos por  $g$ , definimos  $\mathcal{T}_g$  a tesselação formada pelas cliques de cor  $g$  união com os conjuntos com somente um vértice do complementar de  $M_g$  em relação aos nós de  $\Gamma$ . Desta forma, todos os vértices de  $\Gamma$  estão em  $\mathcal{T}_g$  e o conjunto de tesselações  $\{\mathcal{T}_g\}$  cobre todo o conjunto de arestas de  $\Gamma$ .  $\square$

Temos um limite superior e inferior para o número mínimo de tesselações de um grafo, daí surge uma questão: como a quantidade mínima de tesselações para um grafo cresce à medida que o número cromático de seu grafo aumenta? Isto é, qual a relação de  $\chi(K(\Gamma))$  com  $T(\Gamma)$ ? A fim de responder a este questionamento, definimos a classe de grafos roda estendido de acordo com a definição 2, ou seja, uma classe de grafos cujo número cromático de seu grafo clique aumenta, porém o seu número mínimo de tesselações permanece sempre em 3 unidades. O grafo definido abaixo bem com os

resultados das proposições 1 e 2 são partes das contribuições inéditas desta tese e fazem parte do artigo [Abreu et al. \(2017\)](#), que está sendo confeccionado para submissão.

**Definição 2.** O grafo  $(3, n)$  - **Roda Estendido**  $(E_{3,n})$ , para  $n \geq 2$ , é definido adicionando as arestas  $\{3i, 3j\}$ ,  $\{3i + 1, 3j + 1\}$ ,  $\{3i + 2, 3j + 2\}$  para  $0 \leq i, j < n$  ao grafo roda  $W_{3n}$ .

**Proposição 1.** O grafo  $E_{3,n}$  possui 3 cliques com  $n + 1$  elementos e  $3n$  cliques com 3 elementos, ambos contêm o vértice  $3n$ .

*Demonstração.* Dado  $i$  no intervalo  $0 \leq i < 3n$  e considerando a aritmética módulo  $3n$ , os conjuntos  $\{i, i + 1, 3n\}$  formam uma clique maximal de  $E_{3,n}$ , pois os vértices  $i, i + 1$  são vizinhos e todos os vértices estão ligados ao vértice  $3n$  no grafo roda original, variando o  $i$  de 0 a  $3n - 1$  teremos  $3n$  cliques maximais com esse formato. As novas arestas inseridas no grafo  $\{3i, 3j\}$ ,  $\{3i + 1, 3j + 1\}$ ,  $\{3i + 2, 3j + 2\}$  induzem as seguintes cliques  $\{0, 3, 6, \dots, 3n - 3, 3n\}$ ,  $\{1, 4, 7, \dots, 3n - 2, 3n\}$  e  $\{2, 5, 8, \dots, 3n - 1, 3n\}$ , respectivamente. A clique  $\{0, 3, 6, \dots, 3n - 3, 3n\}$  é maximal, pois os vértices que não estão presentes nesta clique são da forma  $3i + 1$  ou  $3i + 2$  e não são adjacentes aos vértices  $3i + 3$  e  $3i$  respectivamente, logo  $\{0, 3, 6, \dots, 3n - 3, 3n\}$  é maximal. De forma análoga, podemos mostrar que  $\{1, 4, 7, \dots, 3n - 2, 3n\}$  e  $\{2, 5, 8, \dots, 3n - 1, 3n\}$  são maximais. As  $3n$  cliques maximais da forma  $\{i, i + 1, 3n\}$  e as 3 cliques  $\{0, 3, 6, \dots, 3n - 3, 3n\}$ ,  $\{1, 4, 7, \dots, 3n - 2, 3n\}$  e  $\{2, 5, 8, \dots, 3n - 1, 3n\}$  são as únicas cliques maximais do grafo  $E(3, n)$ .  $\square$

Usando-se a proposição anterior, podemos concluir que  $K(E_{3,n})$  é um grafo completo com  $3n + 3$  vértices.

**Proposição 2.**  $T(E_{3,n}) = 3$  para  $n \geq 2$ .

*Demonstração.* Vamos mostrar que  $E_{3,n}$  é 3-tesselável exibindo explicitamente um conjunto de tesselações para  $E_{3,n}$  com 3 elementos. Considere as tesselações:

$$\mathcal{T}_0 = \{\{0, 3, 6, \dots, 3n - 3, 3n\}, \{3i + 1, 3i + 2\}, \text{ para } 0 \leq i \leq n - 1\},$$

$$\mathcal{T}_1 = \{\{1, 4, 7, \dots, 3n - 2, 3n\}, \{3i + 2, 3i + 3\}, \text{ para } 0 \leq i \leq n - 1\},$$

$$\mathcal{T}_2 = \{\{2, 5, 8, \dots, 3n - 1, 3n\}, \{3i + 3, 3i + 4\}, \text{ para } 0 \leq i \leq n - 1\}.$$

Onde a aritmética sobre  $i$  é considerada módulo  $3n$ . Os polígonos de  $\mathcal{T}_0$ ,  $\mathcal{T}_1$  e  $\mathcal{T}_2$  são cliques de  $E_{3,n}$ , pois  $\{0, 3, 6, \dots, 3n - 3, 3n\}$ ,  $\{1, 4, 7, \dots, 3n - 2, 3n\}$  e  $\{2, 5, 8, \dots, 3n - 1, 3n\}$  são cliques maximais de  $E_{3,n}$ , conforme demonstrado na proposição 1, e os vértices  $3i + k$ ,  $3i + k + 1$  são adjacentes no grafo roda original de  $E_{3,n}$ , para  $k = 1, 2, 3$  e  $0 \leq i \leq n - 1$ . Todos os vértices de  $E_{3,n}$  estão presentes nas tesselações  $\mathcal{T}_0$ ,  $\mathcal{T}_1$  e  $\mathcal{T}_2$ . Nos falta verificar se o conjunto de tesselações apresentado cobre todas as arestas de  $E_{3,n}$ , note que as arestas do grafo roda original de  $E_{3,n}$  são cobertas pelos polígonos  $\{0, 3, 6, \dots, 3n - 3, 3n\}$ ,  $\{1, 4, 7, \dots, 3n - 2, 3n\}$ ,

$\{2, 5, 8, \dots, 3n - 1, 3n\}$  e  $\{3i + k, 3i + k + 1\}$  com  $k = 1, 2, 3$  e  $0 \leq i \leq n - 1$ . Já as aresta adicionadas ao grafo;  $\{3i, 3j\}$ ,  $\{3i+1, 3j+1\}$ ,  $\{3i+2, 3j+2\}$  para  $0 \leq i, j < n$ ; são cobertas pelos polígonos  $\{0, 3, 6, \dots, 3n - 3, 3n\}$ ,  $\{1, 4, 7, \dots, 3n - 2, 3n\}$ ,  $\{2, 5, 8, \dots, 3n - 1, 3n\}$ .

Pelos argumentos expostos acima,  $E_{3,n}$  é 3-tesselável, como o número cromático de  $K(E_{3,n})$  é  $3n + 3$ . De acordo com o teorema 1,  $K(E_{3,n})$  não é 2-tesselável, logo  $T(E_{3,n}) = 3$ .  $\square$

A figura 5 mostra um exemplo do grafo  $E_{3,3}$  com suas tesselações. Neste exemplo, os polígonos que compõe cada tesselação foram representados pela coloração das arestas que eles cobrem.

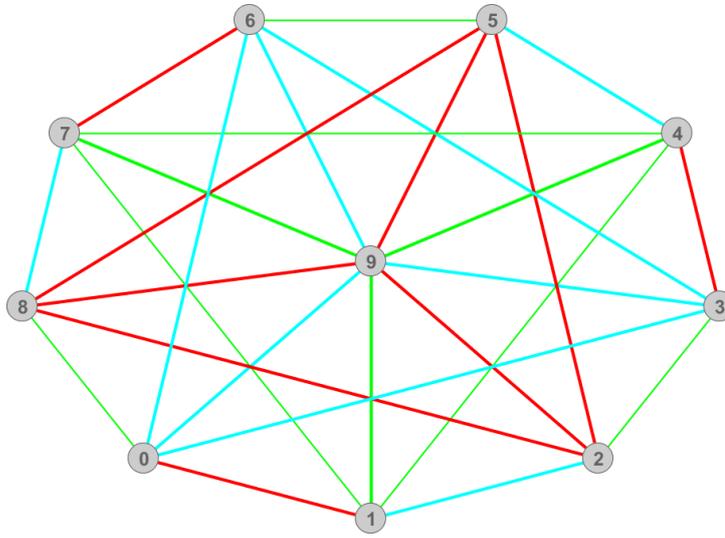


Figura 5 – Grafo roda estendido  $E_{3,3}$  com 3 tesselações.

## 3.2 Staggered Quantum Walk Generalizado

Geralmente, os passeios quânticos são definidos sem elementos marcados. Neste caso, a dinâmica do sistema não privilegia nenhum vértice, aumentando a sua probabilidade em caso de medição. Porém, a definição geral do passeio quântico pode ser alterada para o problema de busca. No caso do passeio quântico discreto com moeda, é feita uma alteração no operador moeda dos elementos marcados (SHENVI et al., 2003).

O SQW pode ser estendido, a fim de contemplar algoritmos para o problema de busca. Vamos excluir a necessidade de cada tesselação cobrir todo o conjunto de vértices, permitindo assim uma tesselação parcial dos vértices. Os vértices que não estiverem em uma tesselação serão marcados. Dessa forma, algoritmos como o de Grover (1996) passam a ser contemplados pelo modelo generalizado. Para verificar essa afirmação, basta considerar um grafo completo com as tesselações  $\alpha$  com todos os elementos, e a tesselação  $\beta$  com cada

elemento isoladamente, exceto os elementos marcados. Isto posto, o operador de evolução do algoritmo de Grover é igual ao do SQW.

### 3.3 Staggered Quantum Walk com Hamiltonianos

Uma outra generalização do modelo SQW foi proposta por [Portugal et al. \(2017\)](#). Visando a uma proposta para implementação física do modelo, os autores apresentaram uma extensão em que o operador de evolução do passeio quântico é produto de operadores Hamiltonianos. Nesta nova definição do modelo, usando-se o fato de que  $U_k$  (3.5) são hermitianos, tais operadores serão substituídos por  $e^{i\theta_k U_k}$ , onde os novos ângulos inseridos  $\theta_k$ , representam energias específicas do sistema e intervalos de tempo (divididos pela constante de Planck  $\hbar$ ).

Os autores que apresentaram a generalização do modelo também propuseram a sua implementação via ressonadores de micro-ondas com supercondutores, onde as operações locais são fornecidas pela interação com o vizinho mais próximo dos ressonadores acoplados através de dispositivos de interferência quântica ([MOQADAM et al., 2017](#)).

A generalização do modelo com hamiltonianos permite a criação de algoritmos quânticos mais eficientes que os correspondentes clássicos. No capítulo 4 apresentaremos um algoritmo quântico para o problema de busca em grades bidimensionais mais eficaz que os equivalentes clássicos. A construção desse algoritmo só foi possível, em nossos experimentos, quando foi adotada a versão do modelo escalonado com hamiltonianos.

### 3.4 Inclusão do passeio de Szegedy no SQW

Mostraremos a seguir que todo passeio quântico de Szegedy é um SQW e que o oposto nem sempre é verdade. Para isso, exibiremos as condições necessárias e suficientes para verificar essa equivalência, também abordaremos as consequências da equivalência no problema de busca.

#### 3.4.1 Todo passeio de Szegedy é um SQW

Como se pôde ver na seção 2.2, o passeio quântico de Szegedy ocorre nas arestas do grafo bipartido, então, vamos analisá-lo em seu grafo linha.

Dado um grafo bipartido  $\Gamma(X, Y, E)$  e matrizes estocásticas  $P, Q$ , considere os polígonos definidos no grafo linha de  $\Gamma$ ,  $L(\Gamma)$ :

$$\tau_{0x} := \{e_{xy}, y \in Y\}, \quad (3.14)$$

$$\tau_{1y} := \{e_{xy}, x \in X\}. \quad (3.15)$$

Onde  $e_{xy}$  é o vértice que representa a aresta  $\{x, y\}$ . Os polígonos  $\alpha_x, \beta_x$  formam duas tesselações em  $L(\Gamma)$ . Com isso, definimos os vetores unitários:

$$|\tau_{0x}\rangle := \sum_{y \in Y} \sqrt{p_{xy}} |e_{xy}\rangle, \quad (3.16)$$

$$|\tau_{1y}\rangle := \sum_{x \in X} \sqrt{q_{yx}} |e_{xy}\rangle. \quad (3.17)$$

Os vetores  $|e_{xy}\rangle$  formam a base computacional do espaço de Hilbert associado a  $L(\Gamma)$ . E como foi feito no princípio do capítulo, obteremos os operadores de reflexão  $U_0, U_1$  e o de evolução

$$U := U_1 U_0. \quad (3.18)$$

Dessa forma, criamos um passeio SQW associado a um grafo bipartido, mas ainda é necessário mostrar que este passeio é equivalente ao passeio de Szegedy, criado para o mesmo grafo. Para tanto, considere a aplicação linear

$$f : \mathcal{H}^P \longrightarrow \mathcal{H}^N \otimes \mathcal{H}^M, \quad (3.19)$$

definida na base computacional por  $f(|e_{xy}\rangle) = |x, y\rangle$ . Onde  $P = |L(\Gamma)|$ . A função  $f$ , assim definida, gera um isomorfismo de  $\mathcal{H}^P$  em um subespaço de  $\mathcal{H}^N \otimes \mathcal{H}^M$ , que é o espaço onde o passeio quântico de Szegedy atua. Com isso,

$$f(|\tau_{0x}\rangle) = |\psi_x\rangle, \quad (3.20)$$

$$f(|\tau_{1y}\rangle) = |\phi_y\rangle. \quad (3.21)$$

Logo os operadores  $U_0, U_1$  são reflexões ortogonais em subespaços isomorfos aos subespaços de reflexão dos operadores  $R_A, R_B$ , respectivamente. O que nos leva a concluir que  $f(U |e_{xy}\rangle) = W |x, y\rangle$ , para todo  $\{x, y\} \in E$ , e os operadores de evolução são os mesmos, a menos de um isomorfismo.

Os argumentos expostos acima provam a seguinte proposição.

**Proposição 3.** *Todo passeio quântico de Szegedy em um grafo bipartido  $\Gamma$  é equivalente a um SQW definido em  $L(\Gamma)$ .*

**Exemplo 3.** *Considere o grafo bipartido  $\Gamma$  exibido na figura 6, o grafo linha de  $\Gamma$  é apresentado na figura 7. Para construção do grafo linha de  $\Gamma$ , suas arestas foram enumeradas de 1 a 8 e cada aresta deve ser associada a um vértice em  $L(\Gamma)$ . Cada vértice do conjunto de arestas  $X$  induzirá uma clique em  $L(\Gamma)$ , cliques estas que irão ser associadas aos polígonos da tesselação  $\alpha$ , cujas arestas estão coloridas de azul na figura 7. De forma análoga, os vértices de  $Y$  formarão cliques que serão associadas à tesselação  $\beta$  e suas arestas foram coloridas de vermelho na figura 7. Tomando como coeficientes para cada elemento de cada polígono de  $\alpha$  e  $\beta$ , os coeficientes apresentados nas equações 3.16, 3.17, respectivamente, o operador de evolução do SQW em  $L(\Gamma)$  será equivalente ao operador de evolução de Szegedy definido em  $\Gamma$ , a menos de um isomorfismo.*

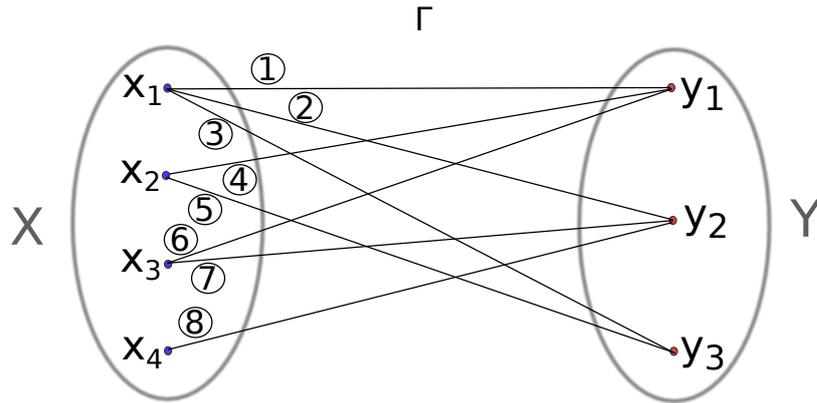


Figura 6 – Exemplo de grafo bipartido  $\Gamma$

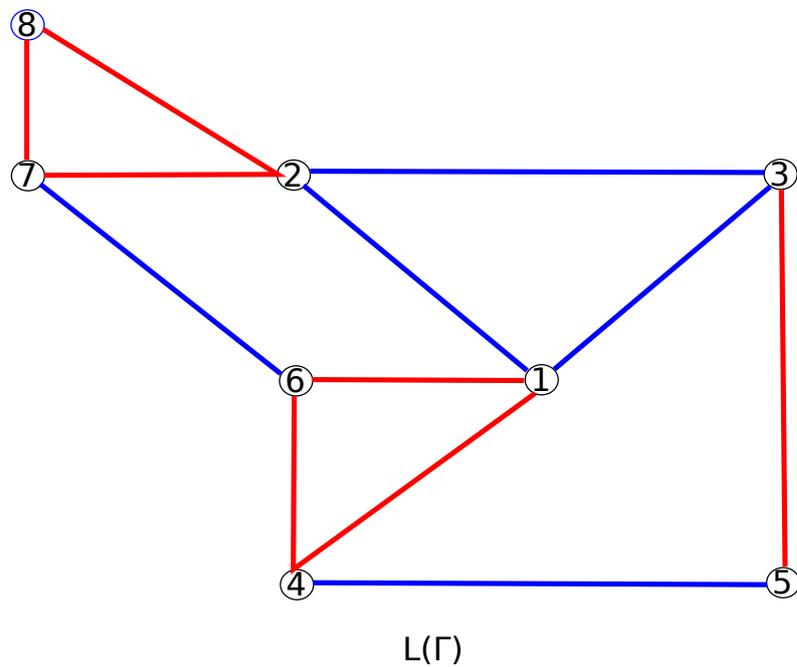


Figura 7 – Modelo Stegged definido no  $L(\Gamma)$

### 3.4.2 Em quais condições o SQW é equivalente ao passeio quântico de Szegedy?

A princípio, considere um SQW em um grafo  $\Gamma'$ , duas tesselações  $\mathcal{T}_0, \mathcal{T}_1$  e com a seguinte restrição: os polígonos  $\tau_{0j}$  e  $\tau_{1k}$  possuem no máximo um elemento em comum, para todos  $j, k$ .

Com as duas tesselações, criamos os conjuntos de vértices  $X = \{\tau_{0j}\}$  e  $Y = \{\tau_{1k}\}$ , onde cada polígono  $\tau_{0j}, \tau_{1k}$  das tesselações é associado a um vértices de  $X, Y$ , respectivamente. Os elementos da interseção  $e_{jk} = \tau_{0j} \cap \tau_{1k}$  irão compor o conjunto de arestas  $E = \{\{\tau_{0j}, \tau_{1k}\}, \tau_{0j} \in X, \tau_{1k} \in Y\}$ . Obtendo assim um grafo bipartido  $\Gamma(X, Y, E)$ . Para obter a descrição completa de um passeio aleatório em  $\Gamma$ , falta a definição das

matrizes estocásticas  $P, Q$ . A fim de obtê-las, os vetores unitários

$$|\tau_{0j}\rangle := \sum_{l \in \tau_{0j}} \alpha_{0,j,l} |l\rangle, \quad (3.22)$$

$$|\tau_{1k}\rangle := \sum_{m \in \tau_{1k}} \alpha_{1,k,m} |m\rangle, \quad (3.23)$$

com o uso da restrição anterior, serão renomeados para:

$$|\tau_{0j}\rangle := \sum_{l \in \tau_{0j}} \alpha_{0,j,l} |e_{jl}\rangle, \quad (3.24)$$

$$|\tau_{1k}\rangle := \sum_{m \in \tau_{1k}} \alpha_{1,k,m} |e_{km}\rangle. \quad (3.25)$$

Iremos impor uma segunda restrição: os coeficientes  $\alpha_{0,j,l}, \alpha_{1,k,m}$  devem ser números reais positivos. Dessa forma, definimos  $p_{jl} = |\alpha_{0,j,l}|^2$  e  $p_{km} = |\alpha_{1,k,m}|^2$ . Com isso,  $f$  definida em 3.19 é um isomorfismo, o SWQ em  $\Gamma'$ , com as restrições impostas, é equivalente ao passeio quântico de Szegedy em  $\Gamma$ .

Os argumentos anteriores comprovam a proposição seguinte.

**Proposição 4.** *Todo passeio SQW com duas tesselações  $\mathcal{T}_0$  e  $\mathcal{T}_1$ , em que a interseção dos polígonos  $\tau_{0j}$  com os polígonos  $\tau_{1k}$  tenha no máximo um elemento e que faça uso de coeficientes reais positivos, é equivalente a um passeio quântico de Szegedy em um grafo bipartido.*

A segunda restrição pode ser eliminada, se considerarmos uma pequena extensão no modelo de Szegedy, permitindo fases nos vetores:

$$|\psi_x\rangle := \sum_{y \in Y} \sqrt{p_{xy}} e^{i\theta_{xy}} |x, y\rangle, \quad (3.26)$$

$$|\phi_y\rangle := \sum_{x \in X} \sqrt{q_{yx}} e^{i\gamma_{xy}} |x, y\rangle. \quad (3.27)$$

Com isso, podemos reescrever a proposição 4 da seguinte forma:

**Proposição 5.** *Todo passeio SQW com duas tesselações  $\mathcal{T}_0$  e  $\mathcal{T}_1$  em que a interseção dos polígonos  $\tau_{0j}$  com os polígonos  $\tau_{1k}$  tenha no máximo um elemento, é equivalente a um passeio quântico de Szegedy estendido em um grafo bipartido.*

**Exemplo 4.** *Considere o SQW definido em  $G$ , de acordo com as tesselações apresentadas na figura 8. Criaremos um grafo bipartido  $\Gamma$  com dois subconjuntos de vértices  $X$  e  $Y$ , cada polígono da tesselação azul será associado a um vértice de  $X$ , assim como cada polígono da tesselação vermelha será associado a um vértice de  $Y$ . As arestas de  $\Gamma$  serão criadas de acordo com os vértices na interseção dos polígonos, como pode ser visto na figura 9. Desta forma, o passeio quântico de Szegedy em  $\Gamma$  é equivalente ao SQW em  $G$ .*

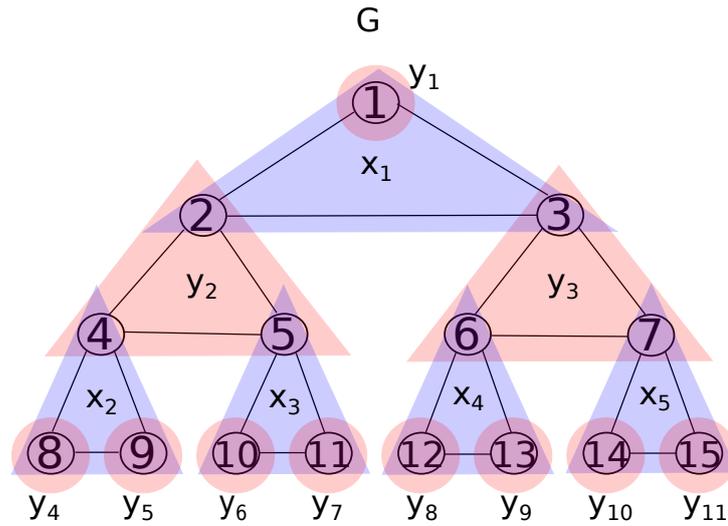


Figura 8 – Grafo  $G$  com suas tesselações

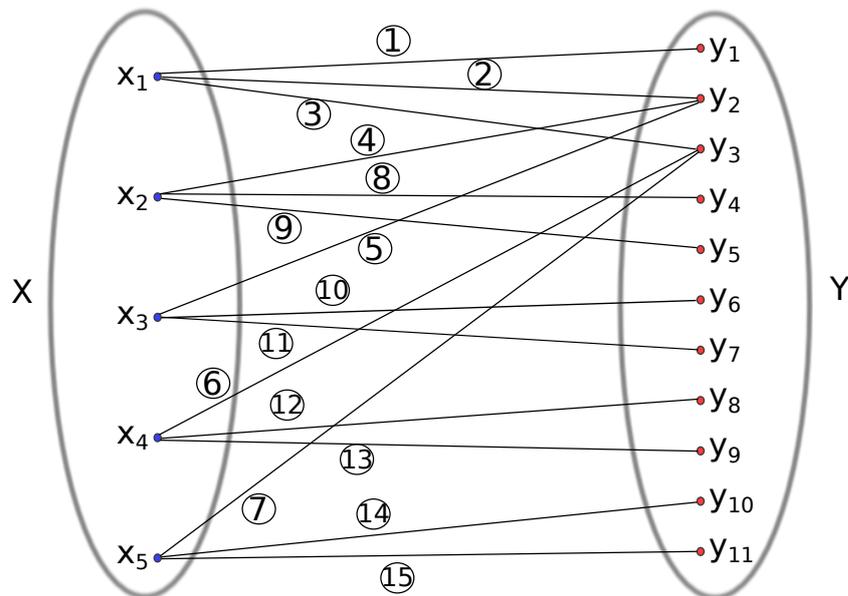


Figura 9 – Grafo bipartido  $\Gamma$ , onde é realizado o passeio quântico de Szegedy

A condição de que deve haver no máximo um elemento na interseção de cada polígono faz-se necessária e para justificar este argumento vamos, usar alguns resultados da teoria de grafos, que podem ser encontrados no apêndice B.

Dado um grafo  $\Gamma$ , se  $\Gamma$  não é um grafo linha de outro grafo, ele contém os subgrafos proibidos de Beineke, neste caso, verifica-se que, ou ele possui mais de duas tesselações, ou as tesselações possuem dois ou mais elementos em comum na interseção de elementos de tesselações distintas.

Por um lado, se  $\Gamma$  é um grafo linha de outro grafo, ele é Krausz particionável, e se a partição de Krausz é 2-colorível, então ele será um grafo linha de um grafo bipartido. E assim podemos usar as equações 3.24 e 3.23 para criar um passeio quântico de Szegedy

equivalente. Por outro lado, se a partição de Krausz não é 2-colorível, então  $\Gamma$  requer mais de duas tesselações ou existem mais de dois elementos na interseção de elementos de tesselações distintas. Dessa forma, teremos a seguinte proposição.

**Proposição 6.** *Instâncias do SQW com duas tesselações, que possuem dois ou mais elementos em comum na interseção de elementos de tesselações distintas não são equivalentes a um passeio quântico de Szegedy.*

Sendo assim, podemos concluir que as instâncias do passeio quântico de Szegedy são um subconjunto próprio de instâncias do SWQ, a menos de um isomorfismo.

### 3.4.3 O problema de busca usando passeios quânticos

O problema de busca espacial quântica pode ser definido como exposto a seguir. Suponha que exista um grafo com  $N$  vértices que representam os lugares que um robô possa percorrer. As arestas desempenham o papel de direções que o robô pode escolher. O objetivo é encontrar um determinado vértice (ou elemento de um conjunto de vértices) com a menor quantidade de passos possível, assumindo que o robô pode se mover somente para vértices vizinhos, e que cada passo equivale a uma unidade de tempo (AMBAINIS et al., 2013).

O modelo proposto por Szegedy pode ser usado para o problema de busca em um grafo  $\Gamma$ , utilizando uma estratégia do método clássico para cálculo do tempo de alcance. O tempo de alcance em um passeio aleatório é o tempo médio que o caminhante leva para passar por um determinado vértice pela primeira vez. Uma maneira de calcular o tempo de alcance é dada a seguir.

Dado um passeio aleatório em um grafo não direcionado  $\Gamma$ , com uma matriz estocástica  $P$  e um estado inicial qualquer, podemos converter o grafo original em um grafo direcionado  $\Gamma'$  removendo as arestas que saem dos elementos marcados, criando assim uma nova matriz estocástica  $P'$ . Dessa forma, os elementos marcados se converterão em acumuladores de probabilidade e quando o caminhante passar por um vértice marcado pela primeira vez, não seguirá adiante. Se o caminhante encontra-se em um vértice não marcado, certamente ele ainda não passou por nenhum elemento marcado. Assim sendo,  $P'$  pode ser usada para o cálculo do tempo de alcance. Os detalhes desse mecanismo podem ser encontrados em Portugal (2013).

Szegedy propôs uma versão quântica para este procedimento. Dado passeio aleatório em um grafo  $G = (X, E)$  com matriz estocástica  $P$ , defina um grafo bipartido  $\Gamma(X, Y, E')$  conforme foi definido na seção 2.2. Se a matriz  $P$  for substituída por  $P'$ , matriz que converte os vértices marcados em acumuladores de probabilidade, obteremos um novo

passeio quântico no grafo bipartido  $\Gamma(X, Y', E')$ . Se definirmos o vetor

$$|\psi_0\rangle := \frac{1}{\sqrt{n}} \sum_{x,y \in Y} \sqrt{p_{xy}} |x, y\rangle, \quad (3.28)$$

como condição inicial, Szegedy mostrou que neste contexto o passeio quântico terá um ganho quadrático sobre passeio o aleatório clássico, no que diz respeito ao tempo de alcance. O método de converter instâncias do passeio de Szegedy para instâncias do SQW, com pequenas modificações pode ser usado para o problema de busca. Seja  $L(\Gamma)$  um grafo linha de um grafo bipartido  $\Gamma(X, Y, E')$ , vamos definir os polígonos das eq. 3.16, 3.17 para todo  $x \in X$  e  $y \in Y$  que não pertençam ao conjunto de elementos marcados. Esses polígonos definem tesselações parciais e podem ser usadas para busca no SQW generalizado, que é equivalente ao passeio quântico de Szegedy em  $\Gamma'(X, Y, E')$ . Neste caso, a condição inicial deve ser

$$|\psi_0\rangle := \frac{1}{\sqrt{n}} \sum_{x,y \in Y} \sqrt{p_{xy}} |e_{xy}\rangle, \quad (3.29)$$

onde  $e_{xy}$  são os vértices do grafo  $L(\Gamma)$ , que estão associados à aresta  $\{x, y\}$ .

O último componente do passeio quântico de Szegedy é a medição, que é feita na base computacional de  $X$ ; neste momento, é feita uma medida parcial  $Y$ . Se for feita a medição no momento exato, que neste caso é próximo do tempo de alcance, a probabilidade de encontrar um elemento marcado é suficientemente alta. Essa versão pode ser transcrita para o SQW como segue: para todo  $x \in X$ , defina os projetores:

$$\Pi_x = \sum_{x' \in \alpha_x} |x'\rangle \langle x'|. \quad (3.30)$$

Desta forma,  $\sum_x \Pi_x = I$ . Efetuando uma medição com observável

$$\mathcal{O} = \sum_{x \in X} x \Pi_x, \quad (3.31)$$

teremos como resultado um elemento  $x_0 \in X$ , que esperamos ser um elemento marcado, caso a medição seja efetuada no tempo de alcance.

## 4 Problema de busca em grades bidimensionais via Staggered Quantum Walk

Na década de 1990, [Grover \(1996\)](#) propôs um algoritmo quântico que despertou a atenção da comunidade científica para o real potencial da computação quântica; tratava-se de um algoritmo para busca em um banco de dados não ordenado de  $O(\sqrt{N})$ . Em 2002, [Benioff \(2002\)](#) observou que a aplicação direta do algoritmo de Grover em uma malha bidimensional com  $\sqrt{N} \times \sqrt{N}$  vértices não apresenta ganhos se comparado com algoritmo clássico de busca, usando caminhada aleatória, que neste caso é  $O(N \ln N)$ . Porém, [Ambainis et al. \(2005a\)](#) (AKR) perceberam que, com uma mera alteração no operador de *shift* juntamente com o método de amplificação de amplitude, é possível obter um algoritmo quântico com complexidade  $O(\sqrt{N} \ln N)$ . [Tulsi \(TULSI, 2008\)](#) apresentou um algoritmo de complexidade  $O(\sqrt{N \ln N})$ , com a adição de um *q-bit* extra no sistema. Por fim, [Ambainis et al. \(2012a\)](#) mostraram como o método de amplificação de amplitude pode ser eliminado do algoritmo AKR usando um pós-processamento clássico, obtendo assim um algoritmo  $O(\sqrt{N \ln N})$  sem a necessidade de um *q-bit* extra.

Os algoritmos citados anteriormente para o problema de busca em grafos bidimensionais fazem uso do espaço adicional da moeda na caminhada aleatória quântica. O primeiro trabalho com objetivo de resolver o problema sem a utilização desse espaço foi o de [Patel et al. \(2005\)](#). Com argumentações baseadas em implementações numéricas, concluiu-se que o algoritmo proposto é  $O(\sqrt{N} \ln N)$ , caso o método de amplificação de amplitude seja usado. Usando SQW e também baseado em implementações numéricas, [Falk \(2013\)](#) concluiu equivocadamente que o algoritmo de busca leva  $O(\sqrt{N})$  passos para encontrar o elemento marcado com probabilidade de sucesso constante.

O único trabalho a apresentar uma prova analítica da complexidade do SQW em grafos bidimensionais foi o de [Ambainis et al. \(2013\)](#), no qual foi mostrado que o algoritmo de Falk leva  $O(\sqrt{N \ln N})$  passos para encontrar um elemento marcado com uma probabilidade de sucesso  $O(1/\ln N)$ . O que implica em um algoritmo  $O(\sqrt{N \ln N})$ , se for usado o método de pós-processamento proposto por [Ambainis et al. \(2012a\)](#). Porém, tal algoritmo apresenta um equívoco na construção das tesselações, usando a correta definição de SQW, o grafo correto para as tesselações descritas em [Ambainis et al. \(2013\)](#) é o grafo exibido na figura 10.

Neste capítulo, apresentaremos alguns resultados numéricos sobre o problema de busca em grades bidimensionais usando o SQW. Variando alguns parâmetros no operador de evolução do passeio quântico, foi obtido um algoritmo com a mesma ordem

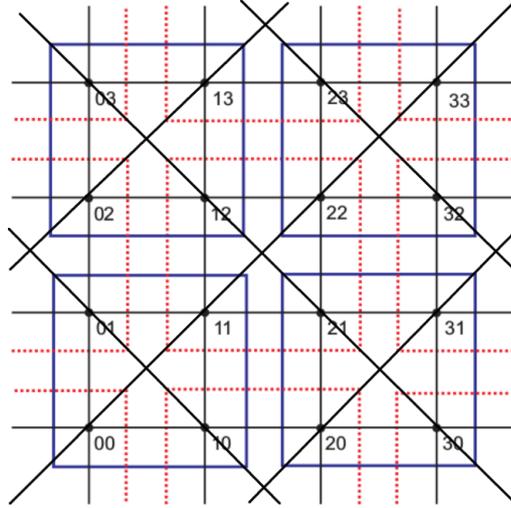


Figura 10 – Grafo de acordo com as tesselações apresentadas por [Ambainis et al. \(2013\)](#)

no número de passo que o AKR; para este algoritmo, faremos uma prova analítica de sua complexidade. Os resultados numéricos apresentados neste capítulo são partes do artigo *Quantum search on two-dimensional lattice with the staggered model* ([FERNANDES; PORTUGAL, 2016](#)), a prova analítica de complexidade do melhor algoritmo encontrado compõe o artigo *Quantum search on the two-dimensional lattice using the staggered model with hamiltonians* ([PORTUGAL; FERNANDES, 2017](#)) e ambos são partes das contribuições inéditas desta tese.

## 4.1 Descrição dos algoritmos

Considere a malha bidimensional  $2D$  com condições de bordas cíclicas, isto é, os vértices das bordas são conectados. Vamos assumir que temos  $2n$  coordenadas nos eixos  $x, y$ , para algum inteiro  $n > 1$ , totalizando  $4n^2$  vértices. Vamos denotar os vértices de acordo com suas coordenadas  $x, y$  (vide figura 11) e associa-los a um vetor da base computacional  $\{|x, y\rangle, 0 \leq x, y < 2n\}$ , onde  $|x, y\rangle$  pertencem ao espaço de Hilbert  $\mathcal{H}^N = \mathcal{H}^{2n} \otimes \mathcal{H}^{2n}$ . Com as condições de contornos cíclicos, vamos considerar a aritmética sobre os labels dos vértices módulo  $2n$ .

A quantidade mínima de tesselações para cobrir todas as arestas da malha bidimensional é quatro, vamos defini-las por:

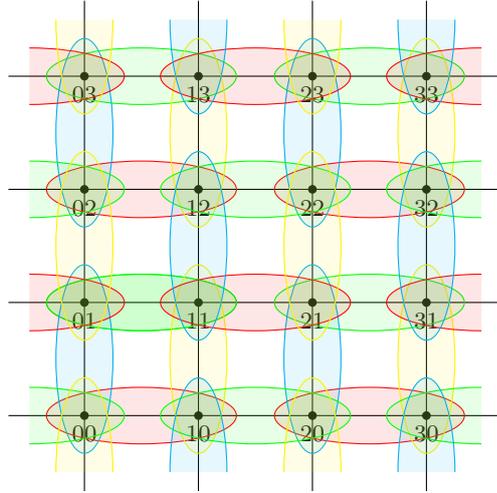
$$\mathcal{T}_{00} = \{\{(x, y), (x + 1, y)\}, x + y \text{ par}, 0 \leq x, y < 2n\}, \quad (4.1)$$

$$\mathcal{T}_{01} = \{\{(x, y), (x, y + 1)\}, x + y \text{ par}, 0 \leq x, y < 2n\}, \quad (4.2)$$

$$\mathcal{T}_{10} = \{\{(x, y), (x - 1, y)\}, x + y \text{ par}, 0 \leq x, y < 2n\}, \quad (4.3)$$

$$\mathcal{T}_{11} = \{\{(x, y), (x, y - 1)\}, x + y \text{ par}, 0 \leq x, y < 2n\}. \quad (4.4)$$

Na figura 11 apresentamos o exemplo da malha  $2D$  com  $n = 2$ , a tesselação  $\mathcal{T}_{00}$  tem seus


 Figura 11 – Malha 2D com 4 tesselações,  $n = 2$ 

polígonos coloridos de vermelho,  $\mathcal{T}_{01}$  azul,  $\mathcal{T}_{10}$  verde; e  $\mathcal{T}_{11}$  amarelo. Tais tesselações podem ser expressas por  $\mathcal{T}_{ab} = \{(x, y), (x + (-1)^a \delta_{b0}, y + (-1)^a \delta_{b1})\}, x + y \text{ par}, 0 \leq x, y < 2n\}$ , sendo assim, criamos os operadores de reflexão:

$$H_{ab} = 2 \sum_{\substack{x,y=0 \\ x+y \text{ par}}}^{2n-1} |u_{xy}^{ab}\rangle \langle u_{xy}^{ab}| - I, \quad (4.5)$$

onde

$$|u_{xy}^{ab}\rangle = \frac{|x, y\rangle + |x + (-1)^a \delta_{b0}, y + (-1)^a \delta_{b1}\rangle}{\sqrt{2}}. \quad (4.6)$$

O modelo usado para o problema de busca será SQW com hamiltonianos (PORTUGAL et al., 2017); logo os operadores unitários associados às tesselações são definidos por  $U_{ab}(\theta) = \exp(i\theta H_{ab})$ . Os operadores de evolução para o passeio quântico analisados foram:

$$U(\theta) = -U_{11}(\theta)U_{10}(\theta)U_{01}(\theta)U_{00}(\theta), \quad (4.7)$$

$$U'(\theta) = -U_{11}(\theta)U_{01}(\theta)U_{10}(\theta)U_{00}(\theta). \quad (4.8)$$

Os operadores de evolução descritos acima não privilegiam nenhum elemento do grafo. Interessados no problema de busca, devemos modificar tais operadores para que a probabilidade, no caso de medição em um determinado passo do algoritmo seja maior no elemento procurado. Para tanto, usaremos o método proposto por Grover e já usado nos algoritmos quânticos de busca citados no início do capítulo. Inseriremos um operador de reflexão sobre o elemento marcado no operador de evolução do passeio quântico. Então, definiremos o operador de reflexão como:

$$R_m = I - 2|m\rangle \langle m|, \quad (4.9)$$

onde  $m$  é o elemento marcado. Note que  $R_m|m\rangle = -|m\rangle$ ,  $R_m|i\rangle = |i\rangle$ , se  $i \neq m$  e  $R_m^2 = I$ .

Sem perda de generalidade, vamos considerar o elemento marcado  $(0, 0)$ . Denotaremos por  $R_0$  a reflexão  $R_{(0,0)}$ , os operadores de evolução do passeio quântico para a busca serão:

$$\mathcal{U}_0(\theta) = U(\theta)R_0, \quad (4.10)$$

$$\mathcal{U}'_0(\theta) = U'(\theta)R_0. \quad (4.11)$$

Como condição inicial tomamos o vetor,

$$|\psi_0\rangle = \frac{1}{\sqrt{2n}} \sum_{\substack{x,y=0 \\ x+y \text{ par}}}^{2n-1} |x, y\rangle. \quad (4.12)$$

Após  $t$  passos o estado do sistema será dado por  $|\psi(t)\rangle = \mathcal{U}_0(\theta)^t |\psi(0)\rangle$ . Por se tratar de uma evolução *quasi-periodica*, a probabilidade sobre o elemento marcado, em caso de medição, deve oscilar como uma função senoidal. Executaremos o nosso algoritmo até primeiro ponto de máximo desta função, tomaremos como tempo de execução o tempo  $t$  e a probabilidade de sucesso será dada por  $p_0(t) = |\langle 0, 0 | \mathcal{U}_0(\theta)^t |\psi(0)\rangle|^2$ , onde  $\mathcal{U}_0$  é o operador de evolução escolhido.

## 4.2 Resultados Numéricos

Foram analisadas as simulações para o algoritmo de busca usando os operadores  $\mathcal{U}_0(\theta)$  e  $\mathcal{U}'_0(\theta)$ , com  $\theta$  assumindo valores discretos entre 0 e  $\frac{\pi}{2}$ . Os algoritmos que tiveram melhor desempenho foram no caso em que  $\theta = \frac{\pi}{4}$ . Os caso em que os valores de  $\theta$  são distintos de  $\frac{\pi}{4}$  serão abordados na seção 4.4. Também foram analisados os casos  $\mathcal{U}_0(\pi/2)$ , que é equivalente a SQW sem o uso de hamiltonianos, variando os coeficientes de cada uma das 4 tesselações, porém nenhum algoritmo obteve ganho satisfatório.

A metodologia adotada nas simulações foi a seguinte: para cada operador de evolução iniciamos o sistema no estado  $|\psi_0\rangle$ . Foi feita a evolução do sistema e analisada a probabilidade no elemento marcado, em caso de medição na base computacional. A quantidade de passos até o primeiro ponto de máximo da probabilidade é considerada a quantidade de passos do algoritmo, e o valor máximo que a probabilidade assume é considerada a probabilidade de sucesso do algoritmo. Esse mesmo procedimento foi realizado para diferentes valores de  $N$ , com objetivo de obter o comportamento do tempo de execução do algoritmo e a probabilidade de sucesso do mesmo em função de  $N$ . Todas as simulações começavam com  $N = 1.000$  e terminavam com  $N$  próximo de 1.000.000. Para chegar a valores tão expressivos de  $N$  foi usada computação de alto desempenho via programa Hiperwalk (LARA et al., 2015) em placas Nvidia Tesla K20 e K40.

O algoritmo que obteve melhor desempenho foi quando consideramos o operador de evolução  $\mathcal{U}_0(\frac{\pi}{4})$ . Tomando  $N = 10.000$ , o comportamento da probabilidade de sucesso em função do número de passo, para  $N = 10.000$ , é mostrado na figura 12.

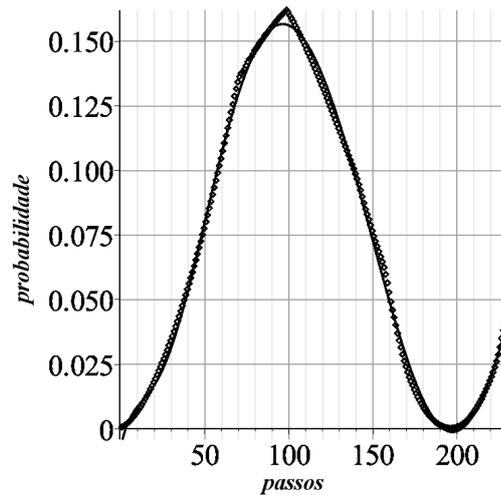


Figura 12 – Probabilidade no elemento marcado em função do número de passos do algoritmo, para o operador de evolução  $\mathcal{U}_0(\frac{\pi}{4})$

Por  $\mathcal{U}_0(\frac{\pi}{4})$  ser considerado o algoritmo de melhor desempenho nos experimentos numéricos foi feita uma prova analítica de sua complexidade. Na seção 4.3 mostraremos que o tempo de execução do algoritmo em função do número de elementos na malha é  $O(\sqrt{N \ln N})$  e que a probabilidade de sucesso do algoritmo decresce em função do número de elementos  $O(1/\ln N)$ . Neste caso o tempo de execução e a probabilidade de sucesso do algoritmo são da mesma ordem do algoritmo AKR.

Outro algoritmo que se destacou na análise numérica foi quando usamos o operador de evolução  $\mathcal{U}'_0(\frac{\pi}{4})$ , o comportamento da probabilidade de sucesso em função do número de passo, para  $N = 10.000$ , é mostrado na figura 13.

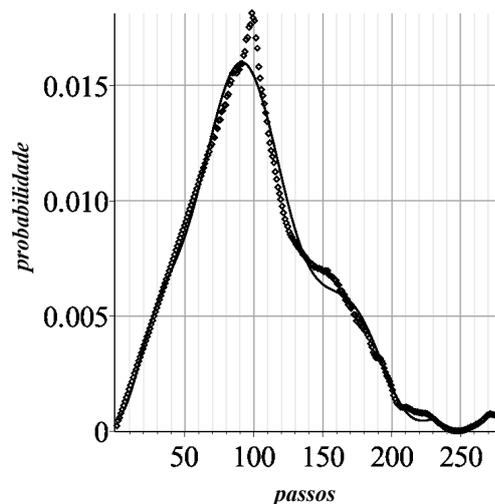


Figura 13 – Probabilidade no elemento marcado em função do número de passos do algoritmo, para o operador de evolução  $\mathcal{U}'_0(\frac{\pi}{4})$

Foi feita a análise numérica do comportamento do tempo de execução do algoritmo

em função da quantidade de vértices da malha e o resultado obtido pode ser visto na figura 14. A reta de interpolação dos dados obtidos sugere um comportamento aproximado de  $276N^{0.5}$  o que significa um tempo de execução  $O(\sqrt{N})$ , que é mais eficiente que os resultados dos demais modelos para a malha. O que torna esse operador de evolução menos atrativo é a forma com que a probabilidade de sucesso do algoritmo decai em relação à quantidade de vértices da malha.

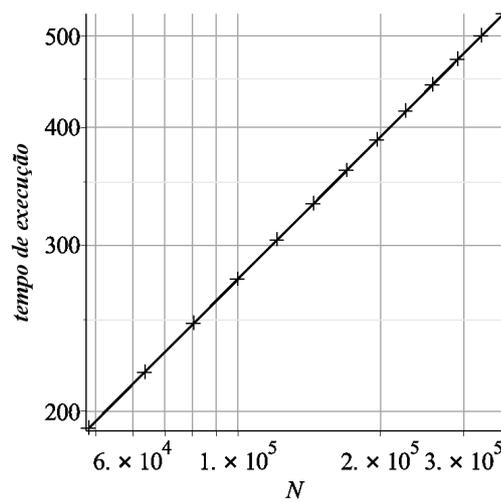


Figura 14 – Tempo de execução do algoritmo usando o operador  $\mathcal{U}'_0(\frac{\pi}{4})$  em função da quantidade de vértices na escala loglog

Na figura 15 é apresentado o comportamento de  $1/p$  em relação ao número de vértices da malha. Na escala loglog,  $p$  é a probabilidade de sucesso do algoritmo. O comportamento da reta de interpolação é aproximadamente  $175N^{0.499}$ , o que sugere que a probabilidade de sucesso do algoritmo decresce em função da quantidade de vértices da malha  $O(1/N^{0.5})$ . Caso o método de amplificação de amplitude seja usado temos um algoritmo com tempo de execução  $O(N^{3/4})$ , com probabilidade de sucesso constante. Neste caso temos um ganho de desempenho em relação aos algoritmos clássicos para o problema de busca na malha bidimensional, porém não melhor que o algoritmo que faz uso do operador  $\mathcal{U}_0(\frac{\pi}{4})$ .

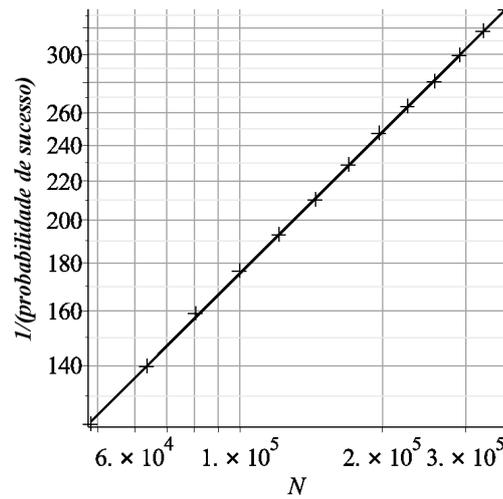


Figura 15 – Inverso da probabilidade de sucesso do algoritmo usando o operador  $\mathcal{U}'_0(\frac{\pi}{4})$  em função da quantidade de vértices na escala loglog

### 4.3 Análise do algoritmo para o operador $\mathcal{U}_0(\frac{\pi}{4})$

Para a análise do algoritmo é necessário encontrar o comportamento da probabilidade, em caso de medição na base computacional, sobre o elemento marcado em função da quantidade de passos do algoritmo, isto é,  $p_{00}(t) = |\langle 00 | \mathcal{U}_0^t | 00 \rangle|^2$ . Sem perda de generalidade, será considerado o elemento marcado 00; nesta seção, será denotado por  $\mathcal{U}_0$  o operador  $\mathcal{U}_0(\frac{\pi}{4})$  e por  $U$ , o operador  $U(\frac{\pi}{4})$ .

Para a análise do comportamento de  $p_{00}(t)$ , tanto o elemento marcado quanto a condição inicial devem ser descritos na base de autovetores de  $\mathcal{U}_0$ . Verificaremos nesta seção que os autovetores associados ao autovalor de menor argumento são os únicos autovetores relevantes na dinâmica do sistema, como ocorre na análise de outros problemas de busca (PORTUGAL, 2013; AMBAINIS et al., 2005b; AMBAINIS et al., 2015). Com objetivo de descrever o elemento marcado e a condição inicial em uma base de autovetores de  $\mathcal{U}_0$ , vamos encontrar uma base ortonormal de autovetores do operador  $U$ . Para esta tarefa, vamos lançar mão da análise Fourier, uma técnica já usada para encontrar autovalores e autovetores de operadores associados a passeios quânticos em grafos com simetrias (PORTUGAL, 2013; AMBAINIS et al., 2015), ou seja, grafos cuja atuação do operador de evolução sobre um conjunto de vetores é invariante. Em seguida será feita a decomposição do elemento marcado e da condição inicial na base de autovetores de  $\mathcal{U}_0$ ; e por fim, será feita a análise do comportamento de  $p_{00}(t)$ .

### 4.3.1 Autovalores e autovetores do operador $U$

Considere os seguintes vetores:

$$|\psi_{kl}^0\rangle = \frac{1}{\sqrt{2}n} \sum_{x,y=0}^{n-1} \left( \omega^{2xk+2yl} |2x, 2y\rangle + \omega^{(2x+1)k+(2y+1)l} |2x+1, 2y+1\rangle \right) \quad (4.13)$$

$$|\psi_{kl}^1\rangle = \frac{1}{\sqrt{2}n} \sum_{x,y=0}^{n-1} \left( \omega^{2xk+(2y+1)l} |2x, 2y+1\rangle + \omega^{(2x+1)k+2yl} |2x+1, 2y\rangle \right) \quad (4.14)$$

com  $\omega = \exp(\pi i/n)$  e  $0 \leq k, l < 2n$ . Note que os vetores  $|\psi_{kl}^i\rangle$  são unitários e ortogonais para valores distintos de  $i, k, l$ .

Fixados  $k, l$ , a atuação de  $U$  sobre os vetores  $|\psi_{kl}^0\rangle$  e  $|\psi_{kl}^1\rangle$  é dada por:

$$U |\psi_{kl}^0\rangle = A_{kl} |\psi_{kl}^0\rangle - B_{kl}^* |\psi_{kl}^1\rangle, \quad (4.15)$$

$$U |\psi_{kl}^1\rangle = B_{kl} |\psi_{kl}^0\rangle + A_{kl}^* |\psi_{kl}^1\rangle, \quad (4.16)$$

onde  $A_{kl} = a_{kl} + i b_{kl}$ ,  $B_{kl} = c_{kl} + i d_{kl}$  e

$$a_{kl} = \frac{1}{2} \left( \cos \tilde{k} + \cos \tilde{l} \right)^2 - 1, \quad (4.17)$$

$$b_{kl} = -\frac{1}{2} \left( \sin \tilde{k} + \sin \tilde{l} \right) \left( \cos \tilde{k} + \cos \tilde{l} \right), \quad (4.18)$$

$$c_{kl} = \frac{1}{2} \sin(\tilde{l} - \tilde{k}) \left( \cos \tilde{k} + \cos \tilde{l} \right), \quad (4.19)$$

$$d_{kl} = \frac{1}{2} \left( \cos(\tilde{k} - \tilde{l}) - 1 \right) \left( \cos \tilde{k} + \cos \tilde{l} \right). \quad (4.20)$$

Inserimos também as novas variáveis  $\tilde{k} = \pi k/n$  e  $\tilde{l} = \pi l/n$ . Portanto a matriz  $U$ , no subespaço gerado por  $|\psi_{kl}^0\rangle$  e  $|\psi_{kl}^1\rangle$ , pode ser reduzida à matriz  $2 \times 2$ :

$$U_{red} = \begin{bmatrix} A_{kl} & B_{kl} \\ -B_{kl} & A_{kl} \end{bmatrix}. \quad (4.21)$$

Se  $\alpha_{kl}$  for um autovalor de  $U_{red}$  com autovetor associado  $|\psi_{\alpha_{kl}}\rangle$  então  $\alpha_{kl}$  também é um autovalor de  $U$  com autovetor associado  $|\psi_{kl}\rangle = \langle 0 | \psi_{\alpha_{kl}} \rangle |\psi_{kl}^0\rangle + \langle 1 | \psi_{\alpha_{kl}} \rangle |\psi_{kl}^1\rangle$ . A próxima tarefa será encontrar todos os autovalores com seus respectivos autovetores de  $U$  usando a matriz  $U_{red}$ . A matriz  $U_{red}$  é uma matriz unitária seus autovalores são dados por  $e^{i\phi_{kl}}$ , onde:

$$\phi_{kl} = \begin{cases} \pi, & \text{se } k+l \equiv n \pmod{2n}, \\ 2\pi k/n, & \text{se } k=l, \\ \arccos a_{kl}, & \text{caso contrário;} \end{cases} \quad (4.22)$$

vamos considerar os seguintes autovetores associados já normalizados:

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ , se  $k=l$  ou  $k+l \equiv n \pmod{2n}$  para  $0 \leq k < n$ ;

- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ , se  $k = l$  ou  $k + l \equiv n \pmod{2n}$  para  $n \leq k < 2n$ ;
- $|v_{kl}^\phi\rangle = \frac{1}{\sqrt{2 \operatorname{sen} \phi_{kl}}} \begin{bmatrix} \sqrt{\operatorname{sen} \phi_{kl} + b_{kl}} \\ \frac{d_{kl} + ic_{kl}}{\sqrt{\operatorname{sen} \phi_{kl} + b_{kl}}} \end{bmatrix}$ , nos casos não listados acima, para  $0 \leq k < n$ ; e  $|v_{kl}^{-\phi}\rangle$ , para  $n \leq k < 2n$ .

Um conjunto completo de autovalores e autovetores para o operador  $U$  pode ser obtido de acordo com a tabela 5.

 Tabela 5 – Autovalores e autovetores de  $U$ .

| Autovalores              | Autovetores              | $(kl)$                                      |
|--------------------------|--------------------------|---|
| -1                       | $ \psi_{kl}^0\rangle$    | $k \pm l = n$ e $k < n$                     |
| -1                       | $ \psi_{kl}^1\rangle$    | $k \pm l = n$ e $k \geq n$                  |
| $e^{-\frac{2\pi ki}{n}}$ | $ \psi_{kl}^0\rangle$    | $k = l$ , $k \pm l \neq n$ e $0 \leq k < n$ |
| $e^{\frac{2\pi ki}{n}}$  | $ \psi_{kl}^1\rangle$    | $k = l$ , $k \pm l \neq n$ e $k \geq n$     |
| $e^{i\phi_{kl}}$         | $ \psi_{kl}^\phi\rangle$ | $k \neq l$ , $k \pm l \neq n$               |

### 4.3.2 Probabilidade de sucesso e tempo de execução do algoritmo

Nesta subseção, vamos obter o comportamento assintótico do tempo de execução e da probabilidade de sucesso do algoritmo; para isso, mostraremos que os únicos autovalores e autovetores que influenciam nestes cálculos são os relacionados aos autovalores de menor argumento do operador  $\mathcal{U}_0$ . Pelo fato de estarmos interessados no comportamento assintótico, algumas vezes será abusado o uso do sinal de “=” . E os termos que não influenciam no comportamento assintótico dos cálculos serão desprezados. Considere  $e^{i\lambda}$  o autovalor de  $\mathcal{U}_0$  de menor argumento (positivo e não nulo), com autovetor associado  $|\lambda\rangle$ , isto é,  $\mathcal{U}_0 |\lambda\rangle = e^{i\lambda} |\lambda\rangle$ . Escrevendo  $|\lambda\rangle$  na base de autovetores de  $U$ , temos:

$$|\lambda\rangle = \sum_{kl} \langle \psi_{kl}^\phi | \lambda \rangle |\psi_{kl}^\phi\rangle \quad (4.23)$$

Na equação 4.23, a notação foi usada em excesso e considerado  $|\psi_{kl}^\phi\rangle$  como um vetor genérico da tabela 5. Multiplicando ambos os lados da igualdade 4.23 pela esquerda, por  $\langle 00|$ , obtemos:

$$\langle 00 | \lambda \rangle = \sum_{kl} \langle \psi_{kl}^\phi | \lambda \rangle \langle 00 | \psi_{kl}^\phi \rangle. \quad (4.24)$$

Usando a definição de  $\mathcal{U}_0$  e o fato que  $\mathcal{U}_0 |\lambda\rangle = e^{i\lambda} |\lambda\rangle$ , a equação

$$\langle \psi_{kl}^\phi | \mathcal{U}_0 | \lambda \rangle = \langle \psi_{kl}^\phi | U R_0 | \lambda \rangle \quad (4.25)$$

pode ser reescrita como:

$$\langle \psi_{kl}^\phi | \lambda \rangle = \frac{2 \langle 00 | \lambda \rangle \langle \psi_{kl}^\phi | 00 \rangle}{1 - e^{i(\lambda - \phi_{kl})}}. \quad (4.26)$$

Substituindo a equação 4.26 em 4.24,

$$\langle 00|\lambda\rangle = 2 \langle 00|\lambda\rangle \sum_{kl} \frac{|\langle 00|\psi_{kl}^\phi\rangle|^2}{1 - e^{i(\lambda - \psi_{kl}^\phi)}}, \quad (4.27)$$

que é equivalente a

$$\frac{1}{2} = \sum_{kl} \frac{|\langle 00|\psi_{kl}^\phi\rangle|^2}{1 - e^{i(\lambda - \phi_{kl})}}. \quad (4.28)$$

Usando o fato de que  $\langle 00|\psi_{kl}^\phi\rangle = 1/(\sqrt{2n}) \langle 0|v_{kl}^\phi\rangle$  na equação (4.28), obtemos:

$$n^2 = \sum_{kl} \frac{|\langle 0|v_{kl}^\phi\rangle|^2}{1 - e^{i(\lambda - \phi_{kl})}}. \quad (4.29)$$

Abrindo mão da igualdade  $(1 - e^{ix})^{-1} = 1/2(1 + i \cotg(x/2))$  e tomando somente a parte imaginária de 4.29, obtemos:

$$\sum_{kl} |\langle 0|v_{kl}^\phi\rangle|^2 \cotg \frac{\lambda - \phi_{kl}}{2} = 0. \quad (4.30)$$

Substituindo os valores de  $\phi_{kl}$  4.22 na equação acima teremos:

$$(2n - 1) \cotg \frac{\lambda - \pi}{2} + \sum_{\substack{k=0 \\ 2k \neq n}}^{n-1} \cotg \frac{\lambda_j + 2\tilde{k}}{2} + \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{kl}^\phi\rangle|^2 \cotg \frac{\lambda - \phi_{kl}}{2} = 0. \quad (4.31)$$

A equação 4.31 pode ser usada para calcular os valores de  $\lambda$  via métodos numéricos, estamos interessados no comportamento assintótico de  $\lambda$ , faremos algumas suposições e ignoraremos termos que não influenciam nesta análise. A primeira suposição que será feita é considerar  $\lambda \ll \phi_{min}$ , para  $1 \ll n$ , onde  $\phi_{min}$  o menor argumento positivo dos autovalores do operador  $U$ . Essa suposição será confirmada assim que tivermos o valor de  $\lambda$ . Usando a expansão em séries de Taylor e ignorando os termos  $O(\lambda^2)$ ,

$$\cotg \frac{\lambda - \phi_{kl}}{2} = -\cotg \frac{\phi_{kl}}{2} - \frac{\lambda}{2} \left( 1 + \cotg^2 \frac{\phi_{kl}}{2} \right). \quad (4.32)$$

Com isso, a equação 4.31 pode ser reescrita como:

$$\begin{aligned} & -(2n - 1) \frac{\lambda}{2} + \cotg \frac{\lambda}{2} + \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \cotg \tilde{k} - \frac{\lambda}{2} \left( 1 + \cotg^2 \tilde{k} \right) + \\ & \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{kl}^\phi\rangle|^2 \left[ -\cotg \frac{\phi_{kl}}{2} - \frac{\lambda}{2} \left( 1 + \cotg^2 \frac{\phi_{kl}}{2} \right) \right] = 0 \end{aligned} \quad (4.33)$$

Usando a aproximação  $\cotg \frac{\lambda}{2} \approx \frac{2}{\lambda} - \frac{\lambda}{6}$ ,

$$\begin{aligned} & -(2n - 1) \frac{\lambda}{2} + \frac{2}{\lambda} - \frac{\lambda}{6} + \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \cotg \tilde{k} - \frac{\lambda}{2} \left( 1 + \cotg^2 \tilde{k} \right) + \\ & \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{kl}^\phi\rangle|^2 \left[ -\cotg \frac{\phi_{kl}}{2} - \frac{\lambda}{2} \left( 1 + \cotg^2 \frac{\phi_{kl}}{2} \right) \right] = 0 \end{aligned} \quad (4.34)$$

Rearrmando a equação (4.34):

$$\frac{2}{\lambda} - \lambda n^2 C^2 + \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \cotg \tilde{k} - \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0 | v_{kl}^\phi \rangle|^2 \cotg \frac{\phi_{kl}}{2} = 0 \quad (4.35)$$

onde,

$$C^2 = \frac{1}{2n^2} \left[ (2n-1) + \frac{1}{3} + \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} (1 + \cotg^2 \tilde{k}) + \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0 | v_{kl}^\phi \rangle|^2 \left( 1 + \cotg^2 \frac{\phi_{kl}}{2} \right) \right]. \quad (4.36)$$

Usando os fatos  $\cotg \frac{k\pi}{n} = -\cotg \frac{(n-k)\pi}{n}$  e

$$\sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0 | v_{kl}^\phi \rangle|^2 \cotg \frac{\phi_{kl}}{2} = 0 \quad (4.37)$$

a equação 4.35 se reduz a:

$$\frac{2}{\lambda} - \lambda n^2 C^2 = 0 \quad (4.38)$$

Desta forma,

$$\lambda = \pm \frac{\sqrt{2}}{nC} \quad (4.39)$$

Isto mostra que  $e^{\pm i\lambda}$  são autovalores de  $\mathcal{U}_0$ . No apêndice C, mostramos que  $C = \Theta(\sqrt{\ln n})$  e portanto  $1/\lambda = \Theta(\sqrt{N \ln N})$ . Para verificar se a suposição  $\lambda \ll \phi_{min}$  está correta, falta obter o comportamento de  $\phi_{min}$ . Pela equação 4.22, o menor valor de positivo para  $\phi_{kl}$  ocorre quando  $k = 1$  e  $l = 0$ , ou vice-versa, em ambos os casos:

$$\phi_{min} = \arccos \left( \frac{1}{2} \left( \cos \frac{\pi}{n} + 1 \right)^2 - 1 \right) \quad (4.40)$$

possui expansão assintótica

$$\phi_{min} = \frac{\sqrt{2}\pi}{n} + O\left(\frac{1}{n^3}\right). \quad (4.41)$$

Logo  $\phi_{min} = \Theta(1/\sqrt{N})$  e a suposição feita é verdadeira.

Agora faremos a decomposição do estado inicial e do elemento marcado na base de autovetores de  $\mathcal{U}_0$ . Começaremos pelo elemento marcado, que pode ser escrito como:

$$|00\rangle = \langle \lambda | 00 \rangle |\lambda\rangle + \langle \lambda^- | 00 \rangle |\lambda^-\rangle + |\lambda^\perp\rangle. \quad (4.42)$$

Onde  $|\lambda^-\rangle$  é o autovetor associado a  $e^{-i\lambda}$ , e  $|\lambda^\perp\rangle$  é a componente ortogonal ao subespaço gerado por  $|\lambda\rangle$  e  $|\lambda^-\rangle$ . Para a análise do comportamento assintótico do tempo de execução

do algoritmo e probabilidade de sucesso não será necessário obter as expressões de  $|\lambda\rangle$ ,  $|\lambda^-\rangle$  e  $|\lambda^\perp\rangle$ . Substituindo a equação 4.26 e o fato  $|\langle 00|\psi_{kl}^\phi\rangle|^2 = |\langle 0|v_{kl}^\phi\rangle|^2 / 2n^2$  na condição de normalidade  $\sum_{kl} |\langle \psi_{kl}^\phi|\lambda\rangle|^2 = 1$ ,

$$\frac{1}{|\langle 00|\lambda\rangle|^2} = \frac{1}{n^2} \sum_{kl} \frac{|\langle 0|v_{kl}^\phi\rangle|^2}{1 - e^{i(\lambda - \psi_{kl}^\phi)}} \quad (4.43)$$

Usando novamente a igualdade  $(1 - e^{ix})^{-1} = 1/2(1 + i \cotg(x/2))$ ,

$$\frac{1}{|\langle 00|\lambda\rangle|^2} = \frac{1}{2n^2} \sum_{k,l} |\langle 0|v_{k,l}^\phi\rangle|^2 \operatorname{cosec}^2 \frac{\lambda - \phi_{k,l}}{2}. \quad (4.44)$$

Substituindo os valores de  $\phi_{k,l}$  (4.22) e separando os somatórios em 4 casos,

$$\begin{aligned} \frac{1}{|\langle 00|\lambda\rangle|^2} &= \frac{2n-1}{2n^2} \operatorname{cosec}^2 \frac{\lambda - \pi}{2} + \frac{1}{2n^2} \operatorname{cosec}^2 \frac{\lambda}{2} + \\ &\frac{1}{2n^2} \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \operatorname{cosec}^2 \frac{\lambda + 2\tilde{k}}{2} + \frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{k,l}^\phi\rangle|^2 \operatorname{cosec}^2 \frac{\lambda - \phi_{k,l}}{2} \end{aligned} \quad (4.45)$$

Observe que, para  $1 \ll n$ ,

$$\frac{1}{2n^2} \operatorname{cosec}^2 \frac{\lambda}{2} \approx \frac{2}{n^2 \lambda^2} = C^2. \quad (4.46)$$

Usando a expansão em séries  $\operatorname{cosec}^2 \frac{\lambda - \phi_{k,l}}{2} = \operatorname{cosec}^2 \left( \frac{\phi_{k,l}}{2} \right) \left( 1 + \lambda \cotg \frac{\phi_{k,l}}{2} \right) + O(\lambda^2)$  e ignorando os termos  $O(\lambda^2)$ :

$$\begin{aligned} \frac{1}{|\langle 00|\lambda\rangle|^2} &= C^2 + \frac{2n-1}{2n^2} + \frac{1}{2n^2} \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \operatorname{cosec}^2 k (1 - \lambda \cotg k) + \\ &\frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{k,l}^\phi\rangle|^2 \operatorname{cosec}^2 \frac{\phi_{k,l}}{2} \left( 1 + \lambda \cotg \frac{\phi_{k,l}}{2} \right) \end{aligned} \quad (4.47)$$

Observe que o termo  $C^2 - 1/6n^2$  aparece na equação acima, sendo assim:

$$\begin{aligned} \frac{1}{|\langle 00|\lambda\rangle|^2} &= 2C^2 - \frac{1}{6n^2} - \frac{\lambda}{2n^2} \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} \cotg^3 k + \\ &\frac{\lambda}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0|v_{k,l}^\phi\rangle|^2 \cotg^3 \frac{\phi_{k,l}}{2}. \end{aligned} \quad (4.48)$$

Usando argumentos similares aos que foram usados em 4.37 e ignorando os termos  $O(1/n^2)$ ,

$$\frac{1}{|\langle 00|\lambda\rangle|^2} = 2C^2 = \frac{4}{n^2 \lambda^2} \quad (4.49)$$

Sem perda de generalidade, vamos assumir que  $\langle 00|\lambda \rangle$  é um número real e positivo. Se  $\langle 00|\lambda \rangle = ae^{ib}$  com  $a, b$  números reais e  $a$  positivo, como temos liberdade de escolha de  $|\lambda \rangle$ , podemos redefini-lo por  $|\lambda \rangle = e^{-ib} |\lambda \rangle$ . Dessa forma,  $\langle 00|\lambda \rangle = 1/(\sqrt{2}C)$ .

Agora, vamos escrever a condição inicial na base de autores de  $\mathcal{U}_0$  como:

$$|\psi_0^\perp \rangle = \langle \psi_0|\lambda \rangle |\lambda \rangle + \langle \psi_0|\lambda^- \rangle |\lambda^- \rangle + |\psi_0^\perp \rangle. \quad (4.50)$$

Onde  $|\psi_0^\perp \rangle$  é a decomposição de  $|\psi_0 \rangle$  ortogonal ao subespaço gerado por  $|\lambda \rangle$  e  $|\lambda^- \rangle$ . Note que  $|\psi_0 \rangle = |\psi_{00}^0 \rangle$ , usando novamente a equação 4.26 para  $|\psi_0 \rangle$ ,

$$\langle \psi_0|\lambda \rangle = \frac{2 \langle 00|\lambda \rangle \langle \psi_{00}^0|00 \rangle}{1 - e^{i\lambda}} = \frac{\lambda}{\sqrt{2}(1 - e^{i\lambda})}. \quad (4.51)$$

Usando novamente  $(1 - e^{ix})^{-1} = 1/2(1 + i \cotg(x/2))$  e ignorando os termos de ordem  $O(\lambda^2)$ , teremos:

$$\langle \psi_0|\lambda \rangle = -\frac{ie^{\frac{\lambda}{2}}}{\sqrt{2}} \quad (4.52)$$

Usando os mesmos procedimentos para o cálculo de  $\langle \psi_0|\lambda^- \rangle$ , chegamos em:

$$\langle \psi_0|\lambda^- \rangle = -\frac{ie^{\frac{\lambda}{2}}}{\sqrt{2}}. \quad (4.53)$$

O que é suficiente para checarmos que:

$$|\langle \psi_0|\lambda \rangle|^2 + |\langle \psi_0|\lambda^- \rangle|^2 = 1, \quad (4.54)$$

logo, a menos de termos  $O(\lambda^2)$ ,  $|\psi_0^\perp \rangle$  não influenciará na dinâmica do sistema, que é dada por

$$(\mathcal{U}_0)^t |\psi_0 \rangle = -\frac{ie^{i\lambda(t+\frac{1}{2})}}{\sqrt{2}} |\lambda \rangle + \frac{ie^{-i\lambda(t+\frac{1}{2})}}{\sqrt{2}} |\lambda^- \rangle. \quad (4.55)$$

Usando as equações 4.42 e 4.49 a probabilidade de sucesso em um instante  $t$  é dada por:

$$p_0(t) = |\langle 0, 0 | (\mathcal{U}_0)^t |\psi_0 \rangle|^2 = \frac{n^2 \lambda^2}{2} \text{sen}^2 \lambda \left( t + \frac{1}{2} \right). \quad (4.56)$$

O primeiro ponto de máximo da função  $p_0(t)$  ocorre quando

$$t = \frac{\pi}{2\lambda}, \quad (4.57)$$

e a probabilidade máxima será:

$$P = \frac{n^2 \lambda^2}{2} \quad (4.58)$$

No apêndice C será mostrado que  $C = \Theta(\sqrt{\ln n})$ , logo  $1/\lambda = \Theta(\sqrt{N \ln N})$ ; com isso, a probabilidade de sucesso do algoritmo decresce  $P = \Theta(1/\ln N)$  e o tempo de execução será  $t = \Theta(\sqrt{N \ln N})$ . Temos duas possibilidades para obter um algoritmo  $\Theta(\sqrt{N \ln N})$  com probabilidade de sucesso  $O(1)$ : podemos usar o método proposto por [Tulsi \(2012\)](#) e incluir um qubit extra no sistema, ou usar o método proposto por [Ambainis et al. \(2012b\)](#) que faz um pós-processamento clássico de  $O(\sqrt{N})$  para encontrar o elemento marcado.

#### 4.4 Análise para valores de $\theta$ diferentes de $\frac{\pi}{4}$

Foi feita uma análise numérica do comportamento dos algoritmos de busca para  $\mathcal{U}_0(\theta)$ , com  $\theta \neq \pi/4$ . Em todos os casos, a probabilidade de sucesso do algoritmo decresce em função do número de vértices  $O(1/N)$ , ou seja, o algoritmo não “distingue” o elemento marcado dos demais vértices do grafo. Com objetivo de entender este problema, analisamos como os menores argumentos dos operadores  $\mathcal{U}(\theta)$  e  $U_0(\theta)$  se comportam em relação ao número de elementos do grafo, tanto  $\lambda$  quanto  $\phi_{min}$  tendem à mesma constante,  $|4\theta - \pi|$ . Na figura 16 temos o comportamento de  $\lambda$  e  $\phi_{min}$  em relação ao número de vértices  $N$  para o caso  $\theta = \pi/3$ . Isso nos leva a conjecturar que a imposição  $\lambda \ll \phi_{min}$  para  $1 \ll n$  é uma condição necessária para que o algoritmo quântico “encontre” o elemento marcado eficientemente.

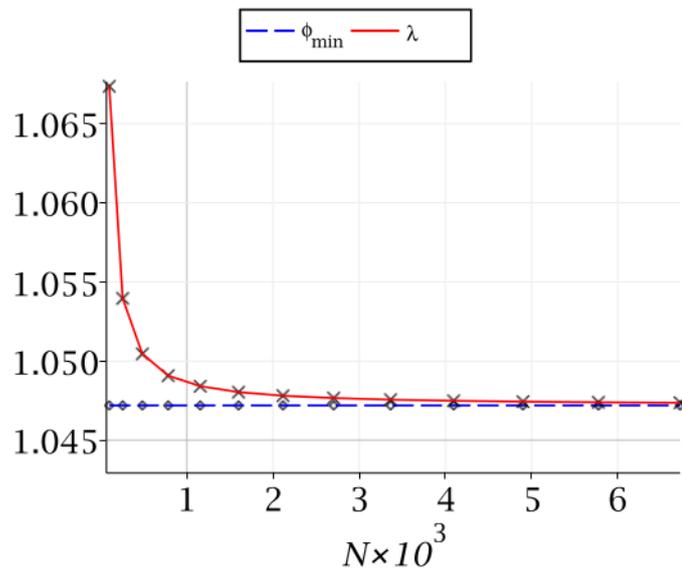


Figura 16 – Comportamento de  $\lambda$  e  $\phi_{min}$  em relação ao número de vértices  $N$ , quando  $\theta = \pi/3$

## 5 Conclusões e perspectivas futuras

O uso dos passeios quânticos tem contribuído para a descoberta de algoritmos quânticos eficientes, e o entendimento cada vez maior dos modelos de caminhadas quânticas tem facilitado essa descoberta. Portanto, neste trabalho, definimos o modelo de Passeios Quânticos Escalonado (SQW) para grafos genéricos e demonstramos que o modelo de passeios quânticos proposto por Szegedy pode ser incluído no SQW, o que possibilita não somente uma melhor compreensão para o modelo de Szegedy, mas também o uso dos resultados já obtidos para o modelo de Szegedy no SWQ. A definição do modelo SQW trouxe um conceito novo para a teoria dos grafos, o de tesselação. E com este conceito surge um novo problema, como estabelecer o número mínimo de tesselações que cobrem todas as arestas de um grafo? Este problema cria uma nova perspectiva de pesquisa na área de teoria dos grafos.

Também foi apresentado um algoritmo de  $O(\sqrt{N \ln N})$  para o problema de busca em grades bidimensionais, usando a versão do SQW com Hamiltonianos. O operador de busca  $\mathcal{U}_0(\theta)$  mostrou-se mais eficiente quando tomamos  $\theta = \pi/4$ , neste caso obtivemos um algoritmo  $O(\sqrt{N \ln N})$ . Para os demais valores de  $\theta$ , os algoritmos de busca não apresentaram resultados com ganhos em relação aos equivalentes clássicos. Uma mera alteração na ordem dos operadores que compõem o operador de busca nos permitiu encontrar um algoritmo  $O(N^{3/4})$ . Isso mostra que o modelo pode ser usado para obtenção de algoritmos quânticos eficientes em problemas práticos.

Porém, alguns questionamentos ainda precisam ser respondidos. Por exemplo, a variação do ângulo  $\theta$  também afetará as propriedades do passeio quântico como: desvio padrão, tempo de mistura ou tempo de alcance? E os algoritmos de busca que apresentam melhores desempenhos são os que possuem maior desvio padrão para o passeio quântico sem a inclusão da busca? Uma outra possibilidade de trabalho futuro consiste em analisarmos o comportamento do modelo SQW nos casos não contemplados pelo modelo de Szegedy. Para esses grafos, examinaremos o desvio padrão, o tempo de mistura e o tempo de alcance. E, por fim, verificaremos a eficiência do modelo para o problema de busca em outros grafos.

## Referências

- ABAL, G.; DONANGELO, R.; MARQUEZINO, F. L.; PORTUGAL, R. Spatial search on a honeycomb network. *Mathematical Structures in Computer Science*, Cambridge University Press, v. 20, n. 6, p. 999–1009, 2010. Citado na página 13.
- ABREU, A.; CUNHA, L.; FERNANDES, T.; FIGUEIREDO, C. de; KOWADA, L.; MARQUEZINO, F.; POSNER, D.; PORTUGAL, R. Bounds and complexity for the tessellation problem. *Matemática Contemporânea*, 2017. Citado 2 vezes nas páginas 14 e 27.
- AHARONOV, D.; AMBAINIS, A.; KEMPE, J.; VAZIRANI, U. Quantum walks on graphs. In: ACM. *Proceedings of the thirty-third annual ACM symposium on Theory of computing*. [S.l.], 2001. p. 50–59. Citado 2 vezes nas páginas 14 e 18.
- AHARONOV, Y.; DAVIDOVICH, L.; ZAGURY, N. Quantum random walks. *Physical Review A*, APS, v. 48, n. 2, p. 1687, 1993. Citado na página 13.
- AMBAINIS, A. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, SIAM, v. 37, n. 1, p. 210–239, 2007. Citado na página 13.
- AMBAINIS, A.; BACKURS, A.; NAHIMOV, N.; OZOLS, R.; RIVOSH, A. Search by quantum walks on two-dimensional grid without amplitude amplification. In: *Theory of Quantum Computation, Communication, and Cryptography, 7th Conference, TQC 2012, Tokyo, Japan, May 17-19, 2012, Revised Selected Papers*. [s.n.], 2012. p. 87–97. Disponível em: <[http://dx.doi.org/10.1007/978-3-642-35656-8\\_7](http://dx.doi.org/10.1007/978-3-642-35656-8_7)>. Citado na página 36.
- AMBAINIS, A.; BACKURS, A.; NAHIMOV, N.; OZOLS, R.; RIVOSH, A. Search by quantum walks on two-dimensional grid without amplitude amplification. In: SPRINGER. *TQC*. [S.l.], 2012. p. 87–97. Citado na página 48.
- AMBAINIS, A.; KEMPE, J.; RIVOSH, A. Coins make quantum walks faster. In: SOCIETY FOR INDUSTRIAL AND APPLIED MATHEMATICS. *Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*. [S.l.], 2005. p. 1099–1108. Citado 2 vezes nas páginas 13 e 36.
- AMBAINIS, A.; KEMPE, J.; RIVOSH, A. Coins make quantum walks faster. In: *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms*. [S.l.: s.n.], 2005. p. 1099–1108. Citado na página 42.
- AMBAINIS, A.; PORTUGAL, R.; NAHIMOV, N. Spatial search on grids with minimum memory. *Quantum Information & Computation (Aceito)*, *arXiv preprint arXiv:1312.0172*, 2013. Citado 4 vezes nas páginas 9, 34, 36 e 37.
- AMBAINIS, A.; PORTUGAL, R.; NAHIMOV, N. Spatial search on grids with minimum memory. *Quantum Information & Computation*, v. 15, p. 1233–1247, 2015. Citado na página 42.
- BEINEKE, L. W. Characterizations of derived graphs. *Journal of Combinatorial Theory*, Elsevier, v. 9, n. 2, p. 129–135, 1970. Citado na página 60.

BENIOFF, P. Space searches with a quantum robot. *AMS Contemporary Math Series*, v. 305, 2002. Citado na página 36.

BOETTCHER, S.; LI, S.; FERNANDES, T. D.; PORTUGAL, R. Determining the efficiency of quantum search algorithms with the renormalization group. *arXiv preprint arXiv:1708.05339*, 2017. Citado na página 15.

CHARTRAND, G.; ZHANG, P. *Chromatic graph theory*. [S.l.]: CRC press, 2008. Citado na página 61.

CHILDS, A. M.; DAM, W. V. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, APS, v. 82, n. 1, p. 1, 2010. Citado na página 13.

DEUTSCH, D.; JOZSA, R. Rapid solution of problems by quantum computation. In: THE ROYAL SOCIETY. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. [S.l.], 1992. v. 439, n. 1907, p. 553–558. Citado na página 13.

FALK, M. Quantum search on the spatial grid. *arXiv preprint arXiv:1303.4127*, 2013. Citado 2 vezes nas páginas 14 e 36.

FARHI, E.; GOLDSTONE, J.; GUTMANN, S. A quantum algorithm for the hamiltonian nand tree. *arXiv preprint quant-ph/0702144*, 2007. Citado na página 13.

FARHI, E.; GUTMANN, S. Quantum computation and decision trees. *Physical Review A*, APS, v. 58, n. 2, p. 915, 1998. Citado na página 14.

FELDMAN, M. *Google and IBM Battle for Quantum Supremacy*. 2017. Disponível em: <<https://www.top500.org/news/google-and-ibm-battle-for-quantum-supremacy>>. Citado na página 13.

FERNANDES, T. D.; PORTUGAL, R. Quantum search on two-dimensional lattice with the staggered model. In: PACIS. *4th Conference of Computational Interdisciplinary Science*. [S.l.], 2016. Citado 2 vezes nas páginas 15 e 37.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: *Proceedings of the 28th ACM Symposium on the Theory of Computing*. [S.l.: s.n.], 1996. p. 212–219. Citado 3 vezes nas páginas 13, 28 e 36.

HARARY, F. *Graph Theory*. [S.l.]: Addison-Wesley, Series in Mathematics, 1994. Citado na página 59.

IBMQ. 2017. <<https://www.research.ibm.com/ibm-q/>>. Acessado em 07/07/2017. Citado na página 13.

JORDAN, S. *Quantum Algorithm Zoo*. 2017. Disponível em: <<http://math.nist.gov/quantum/zoo/>>. Citado na página 13.

KROVI, H.; MAGNIEZ, F.; OZOLS, M.; ROLAND, J. Finding is as easy as detecting for quantum walks. In: *Automata, Languages and Programming*. [S.l.]: Springer, 2010. p. 540–551. Citado na página 14.

LARA, P.; LEÃO, A.; PORTUGAL, R. Simulation of quantum walks using hpc. *J. Comp. Int. Sci*, v. 6, n. 1, p. 21–29, 2015. Citado na página 39.

- MAGNIEZ, F.; NAYAK, A.; ROLAND, J.; SANTHA, M. Search via quantum walk. *SIAM Journal on Computing*, SIAM, v. 40, n. 1, p. 142–164, 2011. Citado na página 14.
- MAGNIEZ, F.; SANTHA, M.; SZEGEDY, M. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, SIAM, v. 37, n. 2, p. 413–424, 2007. Citado 2 vezes nas páginas 13 e 14.
- MARQUEZINO, F. de L.; PORTUGAL, R.; BOETTCHER, S. Quantum search algorithms on hierarchical networks. In: IEEE. *Information Theory Workshop (ITW), 2011 IEEE*. [S.l.], 2011. p. 247–251. Citado na página 13.
- MOQADAM, J. K.; OLIVEIRA, M. C. de; PORTUGAL, R. Staggered quantum walks with superconducting microwave resonators. *Physical Review B*, APS, v. 95, n. 14, p. 144506, 2017. Citado na página 29.
- MOSCA, M. Quantum algorithms. In: *Encyclopedia of Complexity and Systems Science*. [S.l.]: Springer, 2009. p. 7088–7118. Citado na página 13.
- MOTWANI, R.; RAGHAVAN, P. *Randomized algorithms*. [S.l.]: Chapman & Hall/CRC, 2010. Citado na página 13.
- MÜLKEN, O.; BLUMEN, A. Continuous-time quantum walks: Models for coherent transport on complex networks. *Physics Reports*, Elsevier, v. 502, n. 2, p. 37–87, 2011. Citado na página 13.
- PATEL, A.; RAGHUNATHAN, K.; RUNGTA, P. Quantum random walks without a coin toss. *arXiv preprint quant-ph/0506221*, 2005. Citado na página 36.
- PORTUGAL, R. *Quantum walks and search algorithms*. [S.l.]: Springer Science & Business Media, 2013. Citado 4 vezes nas páginas 16, 34, 42 e 64.
- PORTUGAL, R. Staggered quantum walks on graphs. *Phys. Rev. A*, American Physical Society, v. 93, p. 062335, Jun 2016. Disponível em: <<http://link.aps.org/doi/10.1103/PhysRevA.93.062335>>. Citado na página 25.
- PORTUGAL, R.; FERNANDES, T. D. Quantum search on the two-dimensional lattice using the staggered model with hamiltonians. *Physical Review A*, APS, v. 95, n. 4, p. 042341, 2017. Citado 2 vezes nas páginas 15 e 37.
- PORTUGAL, R.; OLIVEIRA, M. C. de; MOQADAM, J. K. Staggered quantum walks with hamiltonians. *arXiv preprint arXiv:1605.02774*, 2016. Citado na página 14.
- PORTUGAL, R.; OLIVEIRA, M. de; MOQADAM, J. Staggered quantum walks with hamiltonians. *Physical Review A*, APS, v. 95, n. 1, p. 012328, 2017. Citado 3 vezes nas páginas 22, 29 e 38.
- PORTUGAL, R.; SANTOS, R. A.; FERNANDES, T. D.; GONÇALVES, D. N. The staggered quantum walk model. *Quantum Information Processing*, Springer, v. 15, n. 1, p. 85–101, 2016. Citado na página 14.
- ROSSI, M. A.; BENEDETTI, C.; BORRELLI, M.; MANISCALCO, S.; PARIS, M. G. Continuous-time quantum walk on spatially correlated noisy lattices. *arXiv preprint arXiv:1707.01441*, 2017. Citado na página 14.

- SANTHA, M. Quantum walk based search algorithms. In: *Theory and Applications of Models of Computation*. [S.l.]: Springer, 2008. p. 31–46. Citado 2 vezes nas páginas 13 e 14.
- SHENVI, N.; KEMPE, J.; WHALEY, K. B. Quantum random-walk search algorithm. *Physical Review A*, APS, v. 67, n. 5, p. 052307, 2003. Citado 2 vezes nas páginas 13 e 28.
- SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, SIAM, v. 41, n. 2, p. 303–332, 1994. Citado na página 13.
- SZEGEDY, M. Quantum speed-up of markov chain based algorithms. In: IEEE. *Foundations of Computer Science, 2004. Proceedings. 45th Annual IEEE Symposium on*. [S.l.], 2004. p. 32–41. Citado 2 vezes nas páginas 14 e 19.
- TULSI, A. Faster quantum-walk algorithm for the two-dimensional spatial search. *Physical Review A*, APS, v. 78, n. 1, p. 012310, 2008. Citado na página 36.
- TULSI, A. General framework for quantum search algorithms. *Physical Review A*, APS, v. 86, n. 4, p. 042331, 2012. Citado na página 48.

# Apêndices

# APÊNDICE A – Postulados da Mecânica Quântica

Neste apêndice são descritos os quatro postulados da Mecânica Quântica. O primeiro postulado faz a descrição matemática de um sistema quântico isolado, o segundo descreve como os sistemas quânticos evoluem, já o terceiro descreve a forma como se pode extrair informações de um sistema quântico através do processo de medição, e o quarto descreve a forma como sistemas quânticos diferentes podem ser combinados.

Um sistema quântico isolado é associado a um espaço linear complexo  $\mathbb{C}^n$  com produto interno, num espaço de Hilbert, que é chamado de espaço de estados.

**Postulado 1.** *A qualquer sistema físico isolado existe associado um espaço vetorial de Hilbert complexo, conhecido como espaço de estado do sistema. O sistema é completamente descrito pelo seu vetor de estado, que é um vetor unitário no espaço de estados.*

Por analogia a um sistema físico clássico de dois níveis capaz de representar um bit, pode-se pensar em um sistema quântico de dois níveis capaz de representar um *bit* quântico, o que se define por qubit (quantum bit). Um bit clássico assume o valor “0” ou “1”, já o qubit pode assumir os valores “0”, “1” ou qualquer superposição deles, o que é visto como combinação linear.

**Definição 1.** *Um qubit é um vetor unitário de  $\mathbb{C}^2$ .*

Um qubit  $|\psi\rangle \in \mathbb{C}^2$  pode ser visto como combinação dos elementos da base computacional  $|\psi\rangle = a|0\rangle + b|1\rangle$ . Onde  $a, b \in \mathbb{C}$  são chamados de amplitudes e obedecem à equação  $|a|^2 + |b|^2 = 1$ . Diz-se que  $|\psi\rangle$  está em superposição de  $|0\rangle$  e  $|1\rangle$ .

O próximo postulado diz como ocorre a evolução temporal de um sistema, que é dada por uma transformação linear no espaço de Hilbert em questão. Como o vetor que representa o sistema deve ser sempre um vetor unitário, a transformação também deve ser sempre unitária, ou seja, a transformação deve levar vetores unitários a vetores unitários.

**Postulado 2.** *A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado  $|\psi\rangle$  de um sistema em um tempo  $t_1$  está relacionado ao estado  $|\psi'\rangle$  do sistema em  $t_2$  por um operador unitário que depende somente de  $t_1$  e  $t_2$ :*

$$|\psi'\rangle = U|\psi\rangle.$$

**Exemplo 1.** *Um operador unitário muito usado é a porta de Hadamard, sendo denotado por  $H$ . Definido pela matriz:*

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

A porta de Hadamard atua sobre os vetores da base computacional da seguinte forma:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ e } H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

A evolução dos estados na Mecânica Quântica é um processo determinístico, porém a forma de extrair informações de um sistema quântico introduz um caráter probabilístico à Mecânica Quântica. O terceiro postulado é o da medida, que determina como as informações são extraídas de um sistema quântico e será exibido a seguir.

**Postulado 3.** *As medidas quânticas são descritas por determinados operadores de medida  $M_m$ , os quais atuam sobre os estados do sistema. O índice  $m$  refere-se aos possíveis resultados da medida, onde  $m \in \mathbb{N}$ . Se o estado quântico for  $|\psi\rangle$ , imediatamente antes da medida, a probabilidade de um resultado ocorrer é dada por:*

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle,$$

e o estado do sistema após a medida será:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}},$$

Os operadores de medida satisfazem a relação de completude:

$$\sum_m M_m^\dagger M_m = I.$$

Onde  $M^\dagger$  é a matriz transposta conjugada da matriz  $M$ .

A relação de completude deve-se ao fato de que a soma das probabilidades deve ser igual a 1, para todo estado  $|\psi\rangle$ .

**Exemplo 2.** *Um exemplo de medida é a medida de um estado na base computacional, que é um tipo de medida muito utilizada na Computação Quântica.*

*Defini-se  $M_0 := |0\rangle\langle 0|$ ,  $M_1 := |1\rangle\langle 1|$ , seja  $M = \{M_0, M_1\}$  os operadores de medida, observe que  $M_0^2 = M_0 M_0 = (|0\rangle\langle 0|)(|0\rangle\langle 0|) = |0\rangle\langle 0| = M_0$ , o mesmo acontecendo a  $M_1^2 = M_1$ . Também observe que  $M_0^\dagger = M_0$  e  $M_1^\dagger = M_1$ . Com isso,  $M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 M_0 + M_1 M_1 = I$ ; portanto, a relação de completude é satisfeita.*

*Dado um estado  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , a probabilidade de se ter o resultado 0 é dada por:*

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = |\alpha|^2.$$

A probabilidade de se ter o resultado 1 é dada por:

$$p(1) = \langle \psi | M_1^\dagger M_1 | \psi \rangle = \langle \psi | M_1 | \psi \rangle = |\beta|^2.$$

O estado do sistema após a medida será:

$$\begin{aligned} \frac{M_0|\psi\rangle}{|\alpha|} &= \frac{\alpha|0\rangle}{|\alpha|}, \text{ se o resultado da medida for } 0. \\ \frac{M_1|\psi\rangle}{|\beta|} &= \frac{\beta|1\rangle}{|\beta|}, \text{ se o resultado da medida for } 1. \end{aligned}$$

**Exemplo 3.** Pode-se generalizar esses operadores de medida para um espaço de dimensão  $n$ . Com  $M_i := |i\rangle\langle i|$ , com  $i = 0, 1, \dots, n-1$  e o conjunto de operadores de medida  $M = \{M_i\}$ .

$$M_i = [m_{jk}^i], m_{jk}^i = \begin{cases} 1, & \text{se } j = k = i \\ 0, & \text{caso contrário.} \end{cases}$$

Pode-se ver que  $M_i^\dagger = M_i$  e que  $M_i^2 = M_i$ ; com isso, a relação de completude é satisfeita.

$$\sum_i M_i^\dagger M_i = \sum_i M_i^2 = \sum_i M_i = I.$$

No estado  $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \dots + \alpha_{n-1}|n-1\rangle$ , a probabilidade de se medir e obter o resultado  $i$  é:

$$p(i) = \langle \psi | M_i^\dagger M_i | \psi \rangle = |\alpha_i|^2.$$

E o estado do sistema após a medida será:

$$\frac{M_i|\psi\rangle}{|\alpha_i|} = \frac{\alpha_i}{|\alpha_i|} |i\rangle.$$

O último postulado propõe a combinação de estados. Um estado composto é formado pelo produto tensorial de seus sistemas individuais.

**Postulado 4.** O espaço de um sistema físico composto é produto tensorial dos espaços de estados dos sistemas físicos individuais. Se os sistemas forem de 1 até  $n$ , e o sistema  $i$  estiver no estado  $|\psi_i\rangle$ , o estado do sistema composto será  $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle$ .

## APÊNDICE B – Grafos

Este apêndice contém algumas definições e resultados da teoria de grafos que foram usados no decorrer desta tese e não pretende ser exaustivo. Uma referência com maiores detalhes encontra-se em [Harary \(1994\)](#).

Um **grafo não direcionado**  $\Gamma(V, E)$  é definido por um conjunto de vértices  $V$  e um conjunto de arestas  $E = \{\{v_i, v_j\}, v_i, v_j \in V\}$ , onde cada elemento  $\{v_i, v_j\}$  representa a ligação do vértice  $v_i$  com o vértice  $v_j$ . Dois vértices ligados por uma aresta são chamados de **adjacentes** ou **vizinhos**. Um grafo  $\Gamma(V, E)$  será chamado de **completo** se para todo par de vértices de  $V$ , existir uma aresta em  $E$  que os ligue.

Um subgrafo  $\Gamma'(V', E')$ , onde  $V' \subset V$  e  $E' \subset E$  é um **subgrafo induzido** de  $\Gamma(V, E)$ , se todo vértice adjacente em  $\Gamma$ , que compõe  $\Gamma'$ , for adjacente em  $\Gamma'$ .

Uma **clique** é um subconjunto de vértices  $C \subset V$ , tal que o subgrafo induzido de  $C$  é um grafo completo, e uma **clique maximal** é uma clique que não pode ser estendida ao se adicionar um ou mais vértices adjacentes, isto é, é uma clique que não existe exclusivamente dentro de um conjunto de vértices de uma clique maior. Deve-se ressaltar que neste texto considera-se uma clique composta apenas um vértice.

Um **grafo bipartido** é um grafo em que seu conjunto de vértices é a união disjunta de dois conjuntos  $X, Y$ , tais que toda aresta conecta um vértice em  $X$  a um vértice em  $Y$ . Neste caso denotaremos por  $\Gamma(X, Y, E)$ .

O **grafo linha** de um grafo  $\Gamma(V, E)$  (grafo raiz) é um grafo que denotaremos por  $L(\Gamma)$ , cujo conjunto de vértices é formado pelas arestas de  $\Gamma$  e dois vértices de  $L(\Gamma)$  serão adjacentes, se e somente se, suas arestas correspondentes compartilharem um mesmo vértice em  $\Gamma$ . Nas figuras 6,7 é apresentado um exemplo de um grafo linha de um grafo bipartido, e pode-se notar que cada vértice do grafo bipartido gera uma clique em seu grafo linha e cada clique gerada por elementos de  $X$  terá no máximo um elemento na interseção com uma clique gerada por um elemento de  $Y$ .

Dado um grafo qualquer, sempre conseguimos obter seu grafo linha. Um questionamento natural é: quando um grafo é raiz de outro? A partição de Krausz e os nove grafos proibidos de Beineke desempenham um papel importante na resposta a este questionamento.

Uma coleção  $K$  de subgrafos de um grafo  $\Gamma$  é chamada de **partição de Krausz** se,

- todos os elementos de  $K$  forem grafos completos,

- cada vértice de  $\Gamma$  pertencer a exatamente dois elementos de  $K$ .

Os nove grafos proibidos de Beineke são os grafos apresentados na figura 17

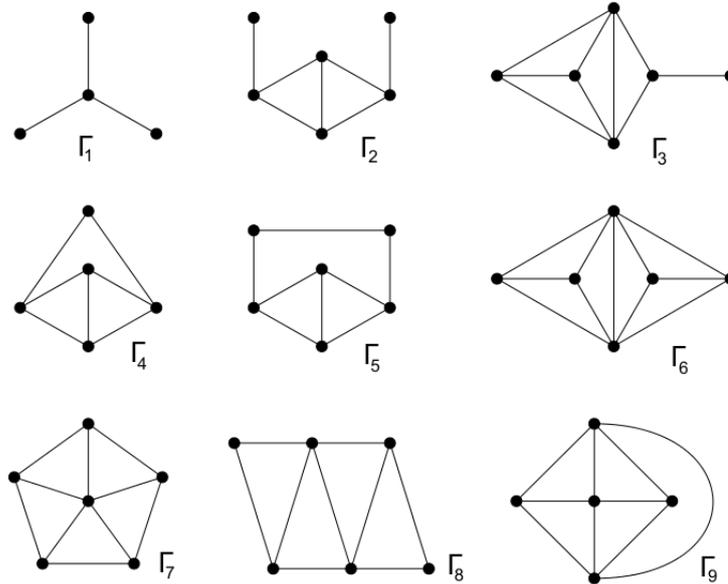


Figura 17 – Nove grafos proibidos de Beineke

Assim, temos o seguinte resultado.

**Teorema 3.** (BEINEKE, 1970) *As afirmações a seguir são equivalentes,*

1. Um grafo  $\Gamma$  é um grafo linha de um outro grafo.
2.  $\Gamma$  admite uma partição de Krausz.
3. Nenhum dos nove grafos proibidos de Beineke (figura 17) é um subgrafo de  $\Gamma$ .

O **grafo clique** de  $\Gamma$  é definido de acordo com as cliques maximais do grafo e será denotado por  $K(\Gamma)$ , cada clique maximal de  $\Gamma$  é associada a um vértice em  $K(\Gamma)$  e dois vértices estarão ligados em  $K(\Gamma)$ , se as cliques associadas aos mesmos possuírem um elemento em comum em  $\Gamma$ .

Uma  **$k$ -coloração** de um grafo  $\Gamma(X, E)$  é uma função de rotulamento  $f : X \rightarrow S$ , onde  $S$  corresponde a um conjunto de cores e  $|S| = k$ . Os vértices associados a uma cor formam uma classe de cores. Uma  **$k$ -coloração** é **própria** se os vértices adjacentes do grafo tiverem rótulos (cores) diferentes.

Um grafo é  **$k$ -colorível** se ele tiver uma  $k$ -coloração própria. O número mínimo de cores para se colorir um grafo  $\Gamma$  é chamado de número cromático de  $\Gamma$ , geralmente denotamos por  $\chi(\Gamma)$ .

---

**Proposição 7.** (*CHARTRAND; ZHANG, 2008*) *Um grafo não trivial  $\Gamma$  é 2-colorível, se e somente se,  $\Gamma$  for um grafo bipartido.*

# APÊNDICE C – Prova $C$ é $\Theta(\sqrt{\ln N})$

Neste apêndice mostraremos que  $C$ , definido em 4.36, é  $\Theta(\sqrt{\ln n})$ .

$$C^2 = \frac{1}{2n^2} \left[ (2n-1) + \frac{1}{3} + \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} (1 + \cotg^2 \tilde{k}) + \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0 | v_{kl}^\phi \rangle|^2 \left( 1 + \cotg^2 \frac{\theta_{k,l}}{2} \right) \right]. \quad (\text{C.1})$$

Os dois primeiros termos de  $(2n-1)/2n^2$  e  $1/6n^2$  são  $O(1/n)$  e  $O(1/n^2)$ , respectivamente. O termo

$$\frac{1}{2n^2} \sum_{\substack{k=1 \\ 2k \neq n}}^{n-1} (1 + \cotg^2 \tilde{k}) = O(1). \quad (\text{C.2})$$

Dessa forma, podemos expressar

$$C^2 = \frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} |\langle 0 | v_{kl}^\phi \rangle|^2 \left( 1 + \cotg^2 \frac{\theta_{k,l}}{2} \right) + O(1). \quad (\text{C.3})$$

Usando a definição de  $|v_{kl}^\phi\rangle$  e a igualdade  $1 + \cotg^2(x/2) = 2/(1 - \cos x)$ ,

$$C^2 = \frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} \frac{\text{sen} \phi_{k,l} + b_{kl}}{\text{sen} \phi_{k,l} (1 - \cos \phi_{kl})} + O(1). \quad (\text{C.4})$$

Sabendo que,

$$\frac{b_{kl}}{\text{sen} \phi_{k,l} (1 - \cos \phi_{kl})} = - \frac{b_{n+k,n+l}}{\text{sen} \phi_{n+k,n+l} (1 - \cos \phi_{n+k,n+l})}, \quad (\text{C.5})$$

$$\frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} \frac{b_{kl}}{\text{sen} \phi_{k,l} (1 - \cos \phi_{kl})} = 0. \quad (\text{C.6})$$

Logo,

$$C^2 = \frac{1}{2n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} \frac{1}{1 - \cos \phi_{kl}} + O(1). \quad (\text{C.7})$$

Pela definição de  $\phi_{kl}$  (4.22),  $\cos(\phi_{kl}) = \frac{1}{2} (\cos(k\pi/n) + \cos(l\pi/n))^2 - 1$ , com isso:

$$C^2 = \frac{1}{n^2} \sum_{\substack{k,l=0 \\ k \neq l \\ k \pm l \neq n}}^{2n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + O(1). \quad (\text{C.8})$$

Os somatórios,

$$\frac{1}{n^2} \sum_{\substack{k=1 \\ k \neq n}}^{2n-1} \frac{1}{4 - 4 \cos^2(k\pi/n)}, \quad (\text{C.9})$$

$$\frac{1}{n^2} \sum_{\substack{k+l=n \\ k \neq l}}^{2n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2}, \quad (\text{C.10})$$

são ambos  $O(1)$ , com isso podemos reescrever

$$C^2 = \frac{1}{n^2} \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{2n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + O(1). \quad (\text{C.11})$$

O somatório acima pode ser dividido em 4 partes

$$C^2 = \frac{1}{n^2} \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0)}}^{n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} \quad (\text{C.12})$$

$$\frac{1}{n^2} \sum_{k=0, l=n}^{n-1, 2n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + \quad (\text{C.13})$$

$$\frac{1}{n^2} \sum_{k=n, l=0}^{2n-1, n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + \quad (\text{C.14})$$

$$\frac{1}{n^2} \sum_{\substack{k=n, l=n \\ (k,l) \neq (n,n)}}^{2n-1, 2n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + \quad (\text{C.15})$$

$$+ O(1). \quad (\text{C.16})$$

Usando o fato de que  $(\cos(k\pi/n) + \cos(l\pi/n))^2 = (\cos[(n+k)\pi/n] + \cos[(n+l)\pi/n])^2$ ,

$$C^2 = \frac{4}{n^2} \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{4 - (\cos(k\pi/n) + \cos(l\pi/n))^2} + O(1). \quad (\text{C.17})$$

Podemos usar a igualdade  $1/(4 - a^2) = 1/[4(2 - a)] + 1/[4(2 + a)]$  para reescrever

$$C^2 = \frac{1}{n^2} \left( \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{2 - (\cos(k\pi/n) + \cos(l\pi/n))} + \right. \quad (\text{C.18})$$

$$\left. \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{2 + (\cos(k\pi/n) + \cos(l\pi/n))} \right) + O(1). \quad (\text{C.19})$$

Agora vamos usar a relação entre os somatórios,

$$\frac{2n^2}{3} - \frac{n}{\sqrt{2}} + \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{2 + (\cos(k\pi/n) + \cos(l\pi/n))} = \quad (\text{C.20})$$

$$\sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{2 - (\cos(k\pi/n) + \cos(l\pi/n))} + O(1), \quad (\text{C.21})$$

para obter

$$C^2 = \frac{1}{n^2} \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0) \\ (k,l) \neq (n,n)}}^{n-1} \frac{1}{2 - (\cos(k\pi/n) + \cos(l\pi/n))} + O(1). \quad (\text{C.22})$$

Usando a desigualdade,

$$1 - \frac{\pi^2 k^2}{2n^2} \leq \cos\left(\frac{\pi k}{n}\right) \leq 1 - \frac{2k^2}{n^2} \quad (\text{C.23})$$

para  $0 \leq k < n$ , obtemos, esquecendo os termos de  $O(1)$ ,

$$\frac{2I(n)}{\pi^2} \leq C^2 \leq \frac{I(n)}{2}, \quad (\text{C.24})$$

onde

$$I(n) = \sum_{\substack{k,l=0 \\ (k,l) \neq (0,0)}}^{n-1} \frac{1}{k^2 + l^2}, \quad (\text{C.25})$$

O termo  $I(n)$  da equação C.25 já é conhecido na literatura (PORTUGAL, 2013), neste caso  $I(n) = \Theta(\ln n)$ , o que mostra  $C = \Theta(\sqrt{\ln N})$ .