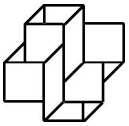


Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Algoritmos baseados em cadeias de Markov quânticas

Por

Raqueline Azevedo Medeiros Santos

PETRÓPOLIS, RJ - BRASIL

MARÇO DE 2014

ALGORITMOS BASEADOS EM CADEIAS DE MARKOV QUÂNTICAS

Raqueline Azevedo Medeiros Santos

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)

Prof. Gilson Antônio Giraldi, D.Sc.

Prof. Franklin de Lima Marquezino, D.Sc.

Prof. Marcelo de Oliveira Terra Cunha, D.Sc.

Prof. Roberto Imbuzeiro Moraes Felinto de Oliveira, Ph.D.

PETRÓPOLIS, RJ - BRASIL
MARÇO DE 2014

Santos, Raqueline Azevedo Medeiros

S237a Algoritmos baseados em cadeias de Markov quânticas / Raqueline Azevedo Medeiros Santos. Petropólis, RJ. : Laboratório Nacional de Computação Científica, 2014.

xvii, 86 p. : il.; 29 cm

Orientador: Renato Portugal

Tese (D.Sc.) – Laboratório Nacional de Computação Científica, 2014.

1. COMPUTADORES QUÂNTICOS. 2. cadeias de Markov quânticas. 3. passeios quânticos. I. Portugal, Renato. II. LNCC/MCT. III. Título.

CDD 004.1

e.pí.gra.fe

...
castanhas queimam,
com tirnas de sal,
no fundo de uma
lata primitiva.
re-
nascem
da casca óleos,
temperos, sementes, vírgulas.

(Iara Maria Carvalho)

Dedicatória

Aos meus pais.

Agradecimentos

A Deus.

A minha família, por toda torcida, carinho e apoio incondicional.

Ao Prof. Renato Portugal pela excelente orientação, apoio, paciência, confiança e ajuda essencial para o desenvolvimento dessa tese.

Ao Prof. Marcelo Fragoso por sua ajuda e apoio.

Ao grupo de computação quântica do LNCC, pelas proveitosas discussões durante os seminários.

Paldies e спасибо ao Prof. Andris Ambainis e ao grupo de computação quântica da Universidade da Letônia, pela recepção e ajuda durante o período do meu doutorado sanduíche. Em especial ao Alexander Rivosh, por toda ajuda na minha chegada em Riga. Ao Denis, por seu apoio e torcida, mesmo a distância, na fase final do doutorado.

Aos professores e funcionários do LNCC, por todo suporte, ajuda e agradável convivência durante esses anos.

Aos amigos e colegas por toda ajuda e torcida.

A CAPES e a FAPERJ pelo suporte financeiro.

Resumo da Tese apresentada ao LNCC/MCT como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

ALGORITMOS BASEADOS EM CADEIAS DE MARKOV QUÂNTICAS

Raqueline Azevedo Medeiros Santos

Março , 2014

Orientador: Renato Portugal, D.Sc

Co-orientador: Marcelo Dutra Fragoso, Ph.D

As cadeias de Markov quânticas ou passeios quânticos têm desempenhado um papel importante no desenvolvimento de algoritmos quânticos eficientes. Dessa forma, estudar suas propriedades, analisar o seu comportamento em diferentes topologias, e ver o impacto da descoerência sob esses passeios e seus algoritmos é fundamental para o desenvolvimento da área. Nesse contexto, contribuímos com a análise das seguintes questões. Para o passeio quântico de Szegedy, estudamos analiticamente o seu comportamento no ciclo; descrevemos como calcular a distribuição limite apresentando exemplos para a malha bidimensional, grafo completo e ciclo; estudamos um modelo de descoerência inspirado em percolação, em que definimos o tempo de alcance quântico descoerente e estabelecemos um intervalo da intensidade de descoerência em que o tempo de alcance quântico descoerente é quadraticamente menor que o clássico; o algoritmo de detecção sob ação da descoerência continua com ganho quadrático para o mesmo intervalo. Para o passeio quântico com moeda, apresentamos simulações do algoritmo para avaliar fórmulas booleanas, também considerando um modelo de oráculo defeituoso.

Abstract of Thesis presented to LNCC/MCT as a partial fulfillment of the requirements for the degree of Doctor of Sciences (D.Sc.)

ALGORITHMS BASED ON QUANTUM MARKOV CHAINS

Raqueline Azevedo Medeiros Santos

March, 2014

Advisor: Renato Portugal, D.Sc

Co-advisor: Marcelo Dutra Fragoso, Ph.D

Quantum Markov chains or quantum walks have been playing an important role in the development of efficient quantum algorithms. Therefore, studying its properties, analyzing its behavior in different topologies, and seeing the impact of decoherence on these walks and its algorithms is fundamental to the development of the area. In this context, we contribute through the analysis of the following issues. For Szegedy's quantum walk, we analytically study its behavior in the cycle; we describe how to calculate the limit distribution by providing examples for the two-dimensional grid, cycle and complete graph; we study a model of decoherence inspired by percolation, where we define the decoherent quantum hitting time and we establish a intensity range of decoherence where the decoherent quantum hitting time is quadratically smaller than the classic; the detection algorithm has a quadratic gain for the same range, under the action of decoherence. For the coined quantum walk, we present simulations of the algorithm for evaluating boolean formulas, also considering a faulty oracle model.

Sumário

Introdução **1**

1 Cadeias de Markov quânticas 4

1.1 Passeio quântico com moeda 5

1.2 Passeio quântico a tempo contínuo 7

1.3 Passeio quântico de Szegedy 8

2 Tempo de alcance quântico 13

2.1 Definição 13

2.2 Expressão para $F(T)$ em termos do espectro de $U_{P'}$ 15

2.3 Limiar para o tempo de alcance quântico 17

3 Passeio quântico de Szegedy no ciclo 18

3.1 Valores e vetores singulares da matriz discriminante 19

3.2 Espectro do operador de evolução 20

3.3 Tempo de alcance quântico 21

3.4 Probabilidade de encontrar um elemento marcado 24

3.5 Conclusões 26

4 Distribuição limite 28

4.1 Distribuição limite no passeio quântico de Szegedy 29

4.1.1 Autovalores com multiplicidade 1 30

4.1.2 Limite na malha bidimensional 31

4.1.3 O caso P' . . . 33
4.1.4 Limite no grafo completo . . . 35
4.1.5 Limite no ciclo . . . 37
4.2 Conclusões . . . 38

5 Tempo de alcance quântico descoerente 39
5.1 Modelo . . . 41
5.1.1 O que é percolação? . . . 41
5.1.2 Descoerência inspirada em percolação . . . 42
5.2 Limiar para o tempo de alcance quântico descoerente . . . 45
5.3 O problema de detecção . . . 51
5.3.1 Descoerência no algoritmo de detecção de Szegedy . . . 52
5.4 Simulações . . . 56
5.4.1 Distribuição de probabilidade no ciclo . . . 59
5.5 Conclusões . . . 60

6 Avaliação de fórmulas booleanas 63
6.1 Modelo . . . 64
6.2 Ideia dos algoritmos . . . 65
6.2.1 Tempo contínuo . . . 65
6.2.2 Tempo discreto . . . 66
6.3 Simulações do algoritmo de Childs et al. (2007a) . . . 68
6.3.1 Oráculo com falha . . . 69
6.4 Conclusões . . . 72

Considerações Finais **74**

Referências Bibliográficas 77

Apêndice

A Cadeias de Markov 84

A.1 Distribuição estacionária 85

A.2 Irredutibilidade 85

A.3 Periodicidade 85

A.4 Reversibilidade 86

A.5 Ergodicidade 86

Lista de Figuras

Figura

1.1 *Grafo bipartido cujo conjunto de vértices é dado por* $V = X \cup Y$ *onde,* $X = \{1, 2\}$ *e* $Y = \{1, 2, 3\}$. 10

1.2 *Exemplo de um grafo com 3 vértices e seu grafo bipartido gerado pelo processo de duplicação.* 11

2.1 *Exemplo de um grafo com 3 vértices, o grafo direcionado associado a* P' *e seu grafo bipartido gerado pelo processo de duplicação. Nesse caso,* $M = \{3\}$. 14

3.1 *Ciclo com 5 vértices. O grafo* (a) *não possui vértice marcado e está associado a matriz* P*. O grafo* (b) *possui um vértice marcado,* $M = \{5\}$*, e está associado a matriz* P'. 18

3.2 *Função* $F(T)$ *(linha sólida) e* $1 - \frac{m}{n}$ *(linha tracejada) para* $n = 100$ *e* $m = 13$*. O tempo de alcance quântico pode ser visto no gráfico como o instante* T *tal que* $F(T) = 1 - \frac{m}{n}$*, que é aproximadamente* 21.75 *nesse caso.* 22

3.3 *Função* $f(t)$ *(linha sólida) e sua aproximação (linha tracejada). Nesse caso,* $k = 10$ *e podemos observar a diferença entre as duas funções. A medida que aumentarmos* k*, essa diferença será menos perceptível.* 23

4.1 *Malha bidimensional* 4×4 *com condições de contorno periódicas.* . 31

4.2 *Limite inferior para a distribuição limite na malha bidimensional com condição inicial* $\left|\psi(0)\right\rangle$. 33

4.3 *Soma das probabilidades em todos os vértices, para* $n = 10 \ldots 50$ *e* $m = 1 \ldots 5$. 37

5.1 *Esboço em duas dimensões da estrutura de uma pedra porosa. Quando imersa na água, o vértice* x *será molhado pela invasão da água, enquanto que o vértice* y *permanecerá seco (Grimmett, 1999).* 41

5.2 *Exemplo da dinâmica da descoerência. O grafo original encontra-se a esquerda. Em* $t = 0$*, a aresta* $(2, 4)$ *foi inserida no grafo, após realizado o processo de descoerência. Em* $t = 1$*, o grafo é reiniciado e aplicamos novamente a remoção ou inserção de arestas dependendo da probabilidade* p*. Nesse passo, a aresta* $(3, 4)$ *foi removida e a aresta* $(2, 5)$ *inserida.* 42

5.3 *Ilustração da aplicação de duas reflexões* $R1$ *e* $R2$ *no vetor* $V1$*. O ângulo entre os eixos de rotação é* Ω*. A aplicação das duas reflexões em* $V1$ *faz uma rotação de* 2Ω*. Podemos observar que o ângulo entre* $V1^{\perp}$ *e* $(R2.R1)V1$ *é o mesmo ângulo formado entre* $-V1^{\perp}$ *e* $(R1.R2)V1$. 48

5.4 *Grafos de Johnson,* $J_{4,2,1}$*. No grafo da esquerda, os vértices são subconjuntos de tamanho* 2 *do seguinte conjunto* $\{1, 2, 3, 4\}$*. No grafo da direita, os vértices são subconjuntos de tamanho* 2 *do seguinte conjunto* $\{1, 2, 2, 4\}$ *e o vértice* $(2, 2')$ *é marcado, utilizamos* $2'$ *para distinguir no grafo os dois elementos que são iguais. Dois vértices estão conectados se a intersecção entre eles possui 1 elemento apenas.* 52

5.5 *Média dos tempos de alcance quântico,* HT_{avg}*, para o grafo completo, hipercubo, malha bidimensional e ciclo, variando os valores de* n*. A probabilidade de descoerência* $p \in [0, 0.1]$. 57

5.6 *Média dos tempos de alcance quântico,* HT_{avg}*, para o ciclo.* 58

5.7 *Probabilidade nos elementos marcados, $p_M(t)$, para o ciclo com $n = 100$ e $m = 1$.* 60

6.1 *Árvore representando a fórmula booleana: $\sigma(x_1, x_2, x_3, x_4) = (x_1 \barwedge x_2) \barwedge (x_3 \barwedge x_4)$. Nas folhas da árvore, temos as variáveis. Os nós internos representam o resultado ao aplicar o operador $\barwedge$ nos seus filhos.* 64

6.2 *Árvore aumentada por uma reta infinita e arestas extras nas folhas.* 65

6.3 *Árvore aumentada por uma reta finita e arestas extras nas folhas.* . 66

6.4 *Árvore aumentada pelos vértices r' e r'' conectados a raiz.* 67

6.5 *Média de $|\langle\psi(t)|\psi(0)\rangle|$ sobre 100 casos em que $\sigma(x) = 0$ (linha contínua) e 100 casos em que $\sigma(x) = 1$ (linha tracejada).* 69

6.6 *Média do produto interno sobre 1000 passos para diferentes profundidades quando $\sigma(x) = 0$.* 69

6.7 *Gráficos de $|\langle\psi(t)|\psi(0)\rangle|$ para 1000 passos com profundidade $d = 12$.* 71

6.8 *Produto interno com a condição inicial, $|\langle\psi(t)|\psi(0)\rangle|$, para 1000 passos com profundidade $d = 13$ e $\sigma(x) = 0$.* 72

6.9 *Produto interno com a condição inicial, $|\langle\psi(t)|\psi(0)\rangle|$, para 1000 passos com profundidade $d = 14$ e $\sigma(x) = 0$.* 72

Lista de Tabelas

Tabela

3.1 *Valores e vetores singulares da matriz discriminante C, associada a matriz estocástica P', para um ciclo com n vértices e m vértices marcados.* 20

3.2 *Autovalores e autovetores do operador de evolução $U_{P'}$. Os vetores $\left|v_j\right\rangle$ são dados pela Eq.* (3.4)*. No autoespaço de autovalor 1, temos $n^2 - 2n + m$ autovetores sem expressão.* 21

Lista de Siglas e Abreviaturas

- $\Pr(\cdot)$: probabilidade
- $\Pr(\cdot|\cdot)$: probabilidade condicional
- A_{ij}: elemento da linha i e coluna j de uma matriz A
- v_i: elemento da posição i de um vetor v
- $(\cdot)^\dagger$: transposto conjugado (no caso em que o vetor ou matriz é real, temos apenas o transposto)
- $G = (V, E)$: grafo descrito pelo conjunto de vértices V e pelo conjunto de arestas E ($|V| = n$ e $|E| = a$)
- d_i: grau do vértice i de um grafo
- $\deg_P(i)$: grau do vértice i do grafo P
- $O(\cdot)$: complexidade do pior caso - $f(n)$ é $O(g(n))$ se existem constantes c e n_0 tais que $f(n) \leq cg(n)\ \forall\ n \geq n_0$
- $\Omega(\cdot)$: complexidade do melhor caso - $f(n)$ é $\Omega(g(n))$ se existem constantes c e n_0 tais que $f(n) \geq cg(n)\ \forall\ n \geq n_0$
- $\Theta(\cdot)$: complexidade do caso médio - $f(n)$ é $\Theta(g(n))$ se $f(n)$ é $O(g(n))$ e $\Omega(g(n))$
- $\mathbf{1}$: vetor cujos elementos são todos iguais a 1 - $\mathbf{1}^T = (1\ 1 \cdots 1)$
- $\mathbb{C}$: conjunto dos números complexos
- $\mathbb{Z}$: conjunto dos números inteiros
- $\Gamma(i)$: vizinhança do vértice i de um grafo
- M: conjunto de elementos marcados - $|M| = m$
- P_M: matriz obtida de P eliminando as linhas e colunas indexadas pelos elementos de M
- P': matriz obtida de P, fazendo $p'_{xy} = \delta_{xy}$ para cada $x \in M$

- $\lambda(A)$: maior autovalor, em módulo, da matriz A (norma espectral de A)
- $\big|\cdot\big\rangle$: vetor no espaço de Hilbert na notação de Dirac
- $\big\langle\cdot\big|$: vetor dual (transposto conjugado) na notação de Dirac
- $\big|\psi_i\big\rangle \otimes \big|\psi_j\big\rangle$: produto tensorial entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$
- $\big|\psi_i\big\rangle\big|\psi_j\big\rangle$: produto tensorial entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$ (notação compacta)
- $\big|\psi_i, \psi_j\big\rangle$: produto tensorial entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$ (notação compacta)
- $\big|\psi_i\psi_j\big\rangle$: produto tensorial entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$ (notação compacta)
- $\big|\psi_i\big\rangle\big\langle\psi_j\big|$: produto externo entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$
- $\big\langle\psi_i\big|\psi_j\big\rangle$: produto interno entre $\big|\psi_i\big\rangle$ e $\big|\psi_j\big\rangle$
- $\big\langle\psi_i\big|A\big|\psi_j\big\rangle$: produto interno entre $\big|\psi_i\big\rangle$ e $A\big|\psi_j\big\rangle$
- $\text{ref}_{\mathcal{K}}$: reflexão em relação a $\mathcal{K}$
- $||\cdot||$: norma de um vetor - $||\cdot||^2 = \big\langle\cdot\big|\cdot\big\rangle$
- $(\cdot)^{\perp}$: ortogonal
- $H_{P,M}$: tempo de alcance quântico para o subconjunto M
- $H_{P,M}^{\text{dec}}$: tempo de alcance quântico descoerente para o subconjunto M
- $T_n(\cos\alpha)$: polinômio de Chebyshev do primeiro tipo - $T_n(\cos\alpha) = \cos(n\alpha)$
- $U_n(\cos\alpha)$: polinômio de Chebyshev do segundo tipo - $U_n(\cos\alpha) = \dfrac{\sin((n+1)\alpha)}{\sin\alpha}$

Introdução

Baseada nas leis da mecânica quântica, a computação quântica é uma área de pesquisa que vem crescendo nas últimas décadas (Nielsen e Chuang, 2000) e mostrando potencial para o desenvolvimento de algoritmos mais eficientes que seus correspondentes clássicos. Por exemplo, o algoritmo de Shor (1994) resolve o problema da fatoração de números inteiros e do cálculo de logaritmo discreto exponencialmente mais rápido que os melhores algoritmos clássicos conhecidos. Esse algoritmo apresenta um dos resultados mais importantes da computação quântica e foi o principal motivo que impulsionou o estudo da computação quântica ao redor do mundo. Além disso, o algoritmo de Shor se baseia na técnica conhecida como *transformada de Fourier quântica*, que também foi aplicada no desenvolvimento de outros algoritmos quânticos, como os algoritmos para estimação de fase (Mosca e Ekert, 1998) e para o problema do subgrupo oculto (Lomont, 2004). Uma segunda técnica utilizada para o desenvolvimento de algoritmos quânticos é a técnica que ficou conhecida como *amplificação de amplitude* e que surgiu com o algoritmo de Grover (1996), que faz uma busca num banco de dados quadraticamente mais rápido que uma busca clássica.

Mais recentemente, uma terceira técnica que tem tido sucesso no desenvolvimento de algoritmos quânticos eficientes são os *passeios quânticos* ou *cadeias de Markov quânticas*. Inspirados nos passeios aleatórios (*random walks*) que, por sua vez, são cadeias de Markov, diferentes formalismos de passeios quânticos surgiram na literatura (Aharonov et al., 1993; Farhi e Gutmann, 1998; Szegedy, 2004). Consequentemente, vários algoritmos foram desenvolvidos. Como exemplo, podemos citar o algoritmo de Childs et al. (2002), que utiliza um passeio quântico contínuo

num grafo obtido pela junção de duas árvores binárias cheias. Partindo de uma das raízes, o algoritmo consegue alcançar a outra raiz exponencialmente mais rápido que o algoritmo clássico. O algoritmo de Ambainis (2004), que utiliza um passeio quântico no grafo de Johnson, resolve o problema da distinção de elementos em $\Theta(n^{\frac{2}{3}})$ contra $\Theta(n \log n)$ do algoritmo clássico. Vários outros algoritmos com ganhos quadráticos para o problema de busca espacial em grafos foram desenvolvidos (Shenvi et al., 2003; Ambainis et al., 2005; Szegedy, 2004; Krovi et al., 2010). Dessa forma, estudar as propriedades dos passeios quânticos, analisar o seu comportamento em diferentes topologias, e ver o impacto da descoerência sob esses passeios e seus algoritmos é fundamental para o desenvolvimento da área. Nesse contexto, contribuímos com a análise das questões descritas a seguir.

Tratando de topologias particulares, o passeio quântico de Szegedy foi estudado apenas para o grafo completo (Santos e Portugal, 2010a). Analisamos o seu comportamento no ciclo. Szegedy (2004) mostrou que para cadeias de Markov ergódicas e simétricas, o tempo de alcance quântico possui ganho quadrático com relação ao clássico. O ciclo ímpar é ergódico, enquanto o ciclo par não é ergódico e, portanto, não podemos utilizar esse resultado. No Capítulo 3, responderemos se o tempo de alcance quântico continua com ganho quadrático e se existe diferença para os ciclos par e ímpar.

A distribuição limite ou distribuição estacionária foi calculada para os passeios quânticos contínuo e discreto com moeda (Aharonov et al., 2000; Moore e Russell, 2002; Marquezino et al., 2008). No Capítulo 4, veremos como calcular essa distribuição para o passeio quântico de Szegedy. Consideraremos a evolução do passeio com e sem elementos marcados e veremos o comportamento dessa distribuição para a malha bidimensional, grafo completo e ciclo.

No Capítulo 5, responderemos qual o impacto da descoerência no passeio quântico de Szegedy e no seu algoritmo de detecção. Utilizamos um modelo de descoerência baseado em percolação que é analisado pela primeira vez nesse passeio quântico. Na literatura, apenas Chiang (2010) analisou a descoerência no

passeio de Szegedy, considerando um modelo diferente, que está associado ao erro na precisão numérica do sistema.

O algoritmo de Childs et al. (2007a) avalia uma fórmula booleana utilizando um passeio quântico com moeda numa árvore aumentada. No Capítulo 6, vamos analisar o comportamento desse algoritmo através de simulações computacionais. Além disso, vamos considerar um modelo de oráculo defeituoso, permitindo que alguma variável tenha o seu valor invertido com uma determinada probabilidade. Esse modelo foi previamente analisado para o algoritmo de Grover (1996), por (Regev e Schiff, 2008) e (Ambainis et al., 2013).

Esta tese encontra-se organizada da seguinte forma. No Capítulo 1, fazemos uma breve revisão sobre as cadeias de Markov quânticas ou passeios quânticos, descrevendo os modelos de tempo discreto e de tempo contínuo. No Capítulo 2, apresentamos como Szegedy descreve o tempo de alcance quântico e sua relação com o tempo de alcance clássico. As contribuições originais desta tese são apresentadas nos Capítulos 3 ao 6. No Capítulo 3, estudamos analiticamente o passeio quântico de Szegedy no ciclo, calculando expressões para o tempo de alcance quântico e para a probabilidade de encontrar vértices marcados. No Capítulo 4, apresentamos como a distribuição limite é calculada para o passeio quântico de Szegedy. No Capítulo 5, analisamos o impacto de um modelo de descoerência inspirado em percolação no passeio quântico de Szegedy. No Capítulo 6, realizamos simulações numéricas para o algoritmo de avaliação de fórmulas booleanas, considerando um modelo com oráculo defeituoso. No Apêndice A, apresentamos algumas definições e propriedades úteis das cadeias de Markov.

Capítulo 1

Cadeias de Markov quânticas

Os passeios aleatórios clássicos são usados, em Ciência da Computação, no desenvolvimento de algoritmos probabilísticos, especialmente em algoritmos de busca por um vértice marcado num grafo. Os passeios aleatórios clássicos podem ser vistos como cadeias de Markov. De maneira informal, uma cadeia de Markov, homogênea, está definida sobre um conjunto de estados, X, e possui uma matriz de probabilidade, P. A cada passo de tempo se o estado em que ela se encontra é x_i, existe uma probabilidade fixa p_{ij} dela ir para o estado x_j. Para uma descrição mais detalhada, veja o Apêndice A. Podemos ver aplicações dos passeios aleatórios clássicos em problemas como o k-SAT e da conectividade em grafos (Motwani e Raghavan, 1995; Venegas-Andraca, 2008).

De acordo com Liu e Petulante (2011), a teoria de cadeias de Markov, quando adequadamente generalizada, fornece um paradigma potente para analisar a evolução estocástica de sistemas quânticos. Ao longo da última década, motivado em grande parte pela perspectiva de algoritmos supereficientes, a teoria das chamadas cadeias de Markov quânticas, especialmente sob o disfarce de passeios quânticos, tem gerado um grande volume de pesquisas, incluindo muitas descobertas de fundamental importância e numerosos avanços recentes (por exemplo, veja (Portugal, 2013)).

Esses modelos quânticos são obtidos através de um processo chamado de *quantização*, onde descrevemos o estado do sistema quântico por um vetor no

espaço de Hilbert e a evolução do sistema é governada por uma operação unitária se o sistema estiver totalmente isolado de interações com o mundo macroscópico ao redor. Como a evolução do sistema é unitária, não há nenhum espaço para fenômenos aleatórios. Apenas quando fizermos uma medição no sistema quântico, para obter informações sobre ele, é onde estaremos lidando com uma distribuição de probabilidades.

Os passeios quânticos são os análogos quânticos dos passeios aleatórios e vêm sendo usados no desenvolvimento de algoritmos mais eficientes que seus correspondentes clássicos. Eles foram introduzidos por Aharonov et al. (1993), nesse caso, a tempo discreto. Esse modelo é conhecido como passeio quântico com moeda. O passeio quântico a tempo contínuo foi desenvolvido por Farhi e Gutmann (1998). Em seguida, Szegedy (2004) desenvolveu um outro formalismo de passeio quântico a tempo discreto. Apresentaremos uma breve descrição de cada um desses modelos, a seguir. Mais detalhes também podem ser encontrados em (Kempe, 2003b; Marquezino, 2010; Santos, 2010; Portugal, 2013).

1.1 Passeio quântico com moeda

Como exemplo, vamos descrever o passeio quântico na reta. A posição n do caminhante deve ser um vetor em um espaço de Hilbert $\mathcal{H}_{\mathcal{P}}$ de dimensão infinita, cuja base computacional é $\{|n\rangle : n \in \mathbb{Z}\}$.[1] Além disso, a evolução do passeio quântico deve depender de uma "moeda" quântica. Logo, devemos associar um espaço de Hilbert bidimensional, $\mathcal{H}_{\mathcal{C}}$, que está associado a moeda e cuja base computacional é $\{|0\rangle, |1\rangle\}$. O espaço de Hilbert do sistema conjunto é $\mathcal{H} = \mathcal{H}_{\mathcal{C}} \otimes \mathcal{H}_{\mathcal{P}}$.

No início do passeio quântico, devemos aplicar o operador moeda C no estado inicial, que é análogo ao papel de jogar a moeda no caso clássico. O operador moeda pode ser definido como qualquer matriz 2×2 unitária. Usualmente, para o passeio

[1] Em computação quântica utilizamos a notação de Dirac: $|\cdot\rangle$ é um vetor no espaço de Hilbert nessa notação; $\langle \cdot |$ é o vetor dual (transposto conjugado); $|x, y\rangle = |x\rangle|y\rangle = |x\rangle \otimes |y\rangle$ é o produto tensorial entre $|x\rangle$ e $|y\rangle$.

quântico na reta é utilizado o operador de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.1}$$

Depois de aplicar a moeda devemos fazer o deslocamento de $\big|n\big\rangle$ para $\big|n+1\big\rangle$ ou para $\big|n-1\big\rangle$. Esse deslocamento é descrito pelo operador unitário S, que opera da seguinte forma:

$$S\big|0\big\rangle\big|n\big\rangle = \big|0\big\rangle\big|n+1\big\rangle, \tag{1.2}$$

$$S\big|1\big\rangle\big|n\big\rangle = \big|1\big\rangle\big|n-1\big\rangle. \tag{1.3}$$

Portanto, o operador de evolução para o passeio quântico é

$$U = S(C \otimes I). \tag{1.4}$$

No instante t, o estado do passeio quântico é dado por

$$\big|\psi(t)\big\rangle = U^t\big|\psi(0)\big\rangle, \tag{1.5}$$

onde $\big|\psi(0)\big\rangle$ é o estado inicial. Esse mesmo processo é utilizado para definir o passeio quântico em outros grafos.

Esses passeios quânticos aplicam-se especialmente a problemas de busca espacial quântica, onde procuramos por um vértice marcado no grafo. Shenvi et al. (2003) desenvolveram um algoritmo quântico de busca para o hipercubo com complexidade de tempo $O(\sqrt{N})$, onde N é o número de vértices do grafo, contra $O(N)$ do algoritmo clássico. Ambainis et al. (2005) usaram um método similar para desenvolver um algoritmo de busca quântico na malha bidimensional em tempo $O(\sqrt{N}\log N)$, contra $O(N)$ do algoritmo clássico, usando o método de amplificação de amplitude. Tulsi (2008) introduziu um *qubit* extra no sistema e melhorou a complexidade desse algoritmo sem utilizar o método de amplificação de amplitude.

Ambainis et al. (2011) também mostraram como eliminar o método de amplificação de amplitude fazendo um pós-processamento com busca clássica. Além disso, nas referências (Abal et al., 2010; Hein e Tanner, 2010; Abal et al., 2011) podemos ver sua aplicação em vários outros grafos gerando algoritmos eficientes.

1.2 Passeio quântico a tempo contínuo

Assim como no caso discreto, as *cadeias de Markov contínuas* serviram de inspiração para a quantização que gerou o passeio quântico contínuo. No caso em que o tempo é uma variável contínua, o caminhante pode ir do vértice x_i para um vértice adjacente x_j em qualquer instante. No início, o caminhante provavelmente será encontrado ainda em x_i. A medida que o tempo passa, a probabilidade de ser encontrado em um dos vértices vizinhos aumenta e a probabilidade de permanecer em x_i diminui. Nesse caso, temos uma taxa de transição, γ, que é a probabilidade de ocorrer a transição entre vértices vizinhos por unidade de tempo. A matriz de probabilidade é dada por

$$M(t) = e^{-Ht}, \tag{1.6}$$

onde H é uma matriz auxiliar, chamada de matriz geradora, dada por

$$H_{ij} = \begin{cases} d_i\gamma, & \text{se } i = j; \\ -\gamma, & \text{se } i \neq j \text{ e adjacentes;} \\ 0, & \text{se } i \neq j \text{ e não-adjacentes;} \end{cases} \tag{1.7}$$

onde d_i é o grau do vértice i. Essa expressão para a matriz $M(t)$ é a solução de uma equação diferencial que pode ser vista com mais detalhes em (Kempe, 2003b).

A ideia de Farhi e Gutmann (1998) foi trazer essa construção para o caso quântico, tratando H como o hamiltoniano do sistema. Dessa forma, temos o nosso operador de evolução sendo dado por

$$U(t) = e^{-iHt}. \tag{1.8}$$

Se a condição inicial for $\big|\psi(0)\big\rangle$, o estado quântico no instante t será

$$\big|\psi(t)\big\rangle = U(t)\big|\psi(0)\big\rangle. \tag{1.9}$$

Childs et al. (2002) mostraram que um passeio quântico contínuo num grafo G particular, descrito pela junção de duas árvores binárias cheias de altura d e raízes A e B, consegue alcançar B a partir de A em $O(d^2)$ passos, enquanto que o algoritmo clássico necessita de, pelo menos, $\Omega(2^d)$ passos para atingir B. Mais tarde, Farhi et al. (2008) desenvolveram um algoritmo que resolve o problema da árvore NAND em tempo $O(\sqrt{N})$, enquanto que o melhor algoritmo clássico conhecido é $O(N^{0.753\cdots})$, sendo N o número de folhas da árvore. Strauch (2006) apresenta uma conexão entre os modelos a tempo discreto e contínuo.

1.3 Passeio quântico de Szegedy

Szegedy (2004) propôs um passeio quântico que é descrito por operadores de reflexão num grafo bipartido. Essa noção de passeio quântico foi inspirada no algoritmo desenvolvido por Ambainis (2004) para resolver o problema de distinção de elementos.

Considere X e Y os conjuntos de vértices de um grafo bipartido[2] . Vamos denotar por x e y vértices genéricos dos conjuntos X e Y. P e Q são matrizes estocásticas descrevendo as probabilidades de X para Y e Y para X, respectivamente. As componentes dessas matrizes p_{xy} e q_{yx} satisfazem a

$$\sum_{y\in Y} p_{xy} = 1 \quad \forall x \in X, \tag{1.10}$$

$$\sum_{x\in X} q_{yx} = 1 \quad \forall y \in Y. \tag{1.11}$$

Para definir um passeio quântico nesse grafo bipartido, associamos ao grafo o espaço de Hilbert $\mathcal{H}^{n_X n_Y} = \mathcal{H}^{n_X} \otimes \mathcal{H}^{n_Y}$, onde $n_X = |X|$ e $n_Y = |Y|$. A base computacional

[2] Um *grafo bipartido* é um grafo cujos vértices podem ser divididos em dois conjuntos disjuntos U e V tais que toda aresta conecta um vértice em U a um vértice em V.

da primeira componente é $\{|x\rangle : x \in X\}$ e $\{|y\rangle : y \in Y\}$ é a base para a segunda componente. Dessa forma, a base computacional de $\mathcal{H}^{n_X n_Y}$ é $\{|x, y\rangle : x \in X, y \in Y\}$. Vamos definir os operadores $A : \mathcal{H}^{n_X} \to \mathcal{H}^{n_X n_Y}$ e $B : \mathcal{H}^{n_Y} \to \mathcal{H}^{n_X n_Y}$ da seguinte forma:

$$A = \sum_{x \in X} |\Phi_x\rangle\langle x|, \tag{1.12}$$

$$B = \sum_{y \in Y} |\Psi_y\rangle\langle y|, \tag{1.13}$$

onde

$$|\Phi_x\rangle = |x\rangle \otimes \left(\sum_{y \in Y} \sqrt{p_{xy}} |y\rangle \right), \tag{1.14}$$

$$|\Psi_y\rangle = \left(\sum_{x \in X} \sqrt{q_{yx}} |x\rangle \right) \otimes |y\rangle. \tag{1.15}$$

Podemos interpretar o vetor $|\Phi_x\rangle$ como uma superposição de todas as arestas que saem do vértice x. Analogamente $|\Psi_y\rangle$ é a superposição de todas as arestas que saem do vértice y.

O operador de evolução $U_{P,Q}$ é dado por

$$U_{P,Q} := \mathcal{R}_B \mathcal{R}_A. \tag{1.16}$$

onde

$$\mathcal{R}_A = 2 \sum_{x \in X} |\Phi_x\rangle\langle\Phi_x| - I_{n_X n_Y}, \tag{1.17}$$

$$\mathcal{R}_B = 2 \sum_{y \in Y} |\Psi_y\rangle\langle\Psi_y| - I_{n_X n_Y}, \tag{1.18}$$

são operadores de reflexão. $\mathcal{R}_A$ reflete um vetor genérico de $\mathcal{H}^{n_X n_Y}$ em torno do subespaço $\mathcal{H}_A$, que é gerado pelos vetores $|\Phi_x\rangle$. Um vetor genérico de $\mathcal{H}^{n_X n_Y}$ pode ser escrito como uma combinação linear de um vetor de $\mathcal{H}_A$ com um vetor de $\mathcal{H}_A^{\perp}$. A ação de $\mathcal{R}_A$ faz com que a componente em $\mathcal{H}_A$ fique inalterada e com que a

componente em $\mathcal{H}_A^{\perp}$ tenha o sinal invertido. O mesmo vale para $\mathcal{R}_B$ em relação ao subespaço $\mathcal{H}_B$.

Como exemplo, considere o grafo apresentado na Figura 1.1 com as seguintes

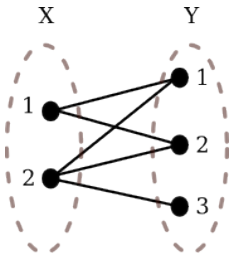


Figura 1.1: *Grafo bipartido cujo conjunto de vértices é dado por* $V = X \cup Y$ *onde,* $X = \{1, 2\}$ *e* $Y = \{1, 2, 3\}$.

matrizes de probabilidade

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{bmatrix} \text{ e } Q = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \\ 0 & 1 \end{bmatrix}, \tag{1.19}$$

que mapeiam as probabilidades do conjunto X para o Y, e do Y para o X, respectivamente. Nesse caso, a base computacional do nosso espaço de Hilbert é

$$\left\{|1\rangle|1\rangle, |1\rangle|2\rangle, |1\rangle|3\rangle, |2\rangle|1\rangle, |2\rangle|2\rangle, |2\rangle|3\rangle\right\}. \tag{1.20}$$

Os estados $\left|\Phi_x\right\rangle$ são descritos como:

$$\left|\Phi_1\right\rangle = \sqrt{\frac{1}{2}}|1\rangle|1\rangle + \sqrt{\frac{1}{2}}|1\rangle|2\rangle, \tag{1.21}$$

$$\left|\Phi_2\right\rangle = \sqrt{\frac{1}{4}}|2\rangle|1\rangle + \sqrt{\frac{1}{4}}|2\rangle|2\rangle + \sqrt{\frac{1}{2}}|2\rangle|3\rangle. \tag{1.22}$$

E os estados $\left|\Psi_y\right\rangle$:

$$\left|\psi_1\right\rangle = \sqrt{\frac{1}{2}}|1\rangle|1\rangle + \sqrt{\frac{1}{2}}|2\rangle|1\rangle, \tag{1.23}$$

$$\left|\psi_2\right\rangle = \sqrt{\frac{1}{3}}|1\rangle|2\rangle + \sqrt{\frac{2}{3}}|2\rangle|2\rangle, \tag{1.24}$$

$$|\psi_3\rangle = |2\rangle|3\rangle. \tag{1.25}$$

A partir disso, é possível obter as matrizes A e B e, consequentemente, o operador de evolução $U_{P,Q}$. Se aplicarmos o operador de evolução no estado $|1\rangle|1\rangle$, por exemplo, veremos que

$$U_{P,Q}|1\rangle|1\rangle = -\frac{1}{3}|1\rangle|2\rangle + \frac{2\sqrt{2}}{3}|2\rangle|2\rangle. \tag{1.26}$$

Então, se fizermos uma medição no primeiro registrador, teremos probabilidade $\frac{1}{9}$ de encontrar o caminhante no vértice 1 e probabilidade $\frac{8}{9}$ de encontrar o caminhante no vértice 2.

É importante ressaltar que todo grafo pode ser convertido num grafo bipartido através de um simples processo de duplicação. Seja $\Gamma(X, E)$ um grafo conexo e não-direcionado e P a matriz de probabilidade associada a esse grafo, o processo de duplicação é obtido fazendo $X = Y$ e $P = Q$. Dessa forma, cada aresta $\{x_i, x_j\}$ em E do grafo original é convertida em duas arestas no grafo bipartido $\{x_i, y_j\}$ e $\{y_i, x_j\}$. Na Figura 1.2, vemos um exemplo dessa duplicação para um grafo com 3 vértices. Nesse caso, denotaremos o operador de evolução por U_P.

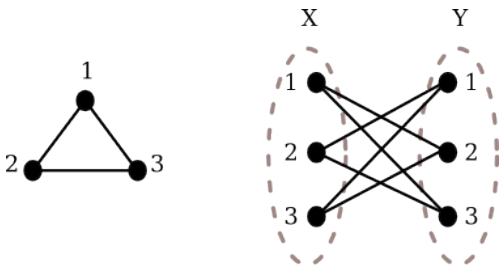


Figura 1.2: *Exemplo de um grafo com 3 vértices e seu grafo bipartido gerado pelo processo de duplicação.*

Esse passeio tem uma estrutura diferente do passeio quântico com moeda. Ele pode ser visto como um passeio nas arestas do grafo. Para isso, basta interpretar o estado $|x\rangle|y\rangle$ como uma aresta (x, y) representando que o caminhante encontra-se no vértice x tendo vindo do vértice y. Szegedy mostrou como obter parte da decomposição espectral do operador de evolução a partir da decomposição singular

da matriz $C = A^{\dagger}B$, chamada de matriz discriminante. Segue o teorema.

Teorema 1.3.1 (Szegedy (2004)) Sejam $\cos\theta_1, \ldots, \cos\theta_l$ os valores singulares de C em $[0, 1)$ e seus vetores singulares associados $\big|v_k\big\rangle$ e $\big|w_k\big\rangle (1 \leq k \leq l)$, temos a seguinte decomposição espectral para o operador de evolução $U = \mathcal{R}_B\mathcal{R}_A$:

(1) Os autovalores de U associados aos valores singulares de C em $[0, 1)$ são $e^{\pm 2i\theta_1}, \ldots, e^{\pm 2i\theta_l}$ e seus respectivos autovetores:

$$A\big|w_1\big\rangle - e^{\pm i\theta_1}B\big|v_1\big\rangle, \ldots, A\big|w_l\big\rangle - e^{\pm i\theta_l}B\big|v_l\big\rangle;$$

(2) Em $\mathcal{H}_A \cap \mathcal{H}_B$, U atua como I. $\mathcal{H}_A \cap \mathcal{H}_B$ coincide com o conjunto de vetores singulares de C com valor singular 1;

(3) Em $\mathcal{H}_A^{\perp} \cap \mathcal{H}_B^{\perp}$, U atua como I.

O formalismo de Szegedy apresenta resultados mais gerais para o problema de busca espacial em certas classes de grafos. Szegedy (2004) mostrou que o tempo de alcance quântico apresenta ganho quadrático com relação ao clássico na detecção de um conjunto de vértices marcados, para cadeias de Markov ergódicas e simétricas. Santos e Portugal (2010a) analisaram o problema de busca no grafo completo. Apresentando diferentes propostas, Magniez et al. (2009) e Krovi et al. (2010) desenvolveram algoritmos quânticos quadraticamente mais rápidos que seus correspondente clássicos, para encontrar um vértice marcado em cadeias de Markov ergódicas e reversíveis.

Capítulo 2

Tempo de alcance quântico

O *tempo de alcance* é uma medida que está associada a complexidade de algoritmos de busca que usam passeios aleatórios clássicos. Seja $M \subseteq X$ um subconjunto de vértices marcados num grafo, o tempo de alcance (*hitting time*) é o *tempo esperado* para o caminhante atingir um dos vértices de M pela primeira vez.

No caso quântico, podemos encontrar várias contribuições a respeito do tempo de alcance para o passeio quântico com moeda. Kempe (2003a) e Krovi e Brun (2006) definem maneiras diferentes para calcular o tempo de alcance, que variam entre deixar o passeio quântico evoluir até que a probabilidade de atingir um elemento marcado ultrapasse um determinado valor; ou fazer uma medição parcial a cada passo, checando se o caminhante atingiu o vértice marcado. Já em (Kempf e Portugal, 2009), temos uma noção que se baseia na definição da velocidade do caminhante enquanto o visualizamos como uma onda.

Neste capítulo, iremos descrever como (Szegedy, 2004) define o tempo de alcance quântico. Esta definição é uma generalização natural do tempo de alcance clássico.

2.1 Definição

É possível mostrar, como em (Santos, 2010), que o cálculo do tempo de alcance num grafo com matriz estocástica P é equivalente ao tempo de alcance

calculado num grafo direcionado modificado, cuja matriz estocástica associada é uma matriz P', descrita por

$$p'_{xy} = \begin{cases} p_{xy}, & x \notin M; \\ \delta_{xy}, & x \in M. \end{cases} \tag{2.1}$$

Classicamente, P' é chamada de caminhada absorvente (*absorbing walk*). Essa matriz estocástisca faz com que ao encontrar um elemento marcado, o caminhante permaneça nesse estado. Na Fig. 2.1 podemos ver um exemplo de um grafo com 3 vértices e os grafos associados a matriz modificada P'.

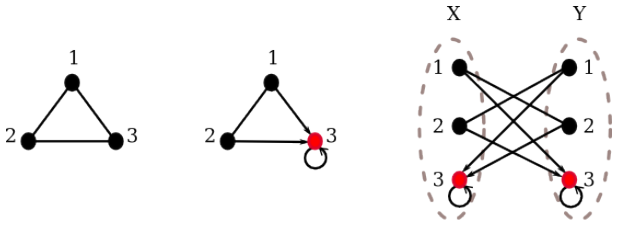


Figura 2.1: *Exemplo de um grafo com 3 vértices, o grafo direcionado associado a P' e seu grafo bipartido gerado pelo processo de duplicação. Nesse caso, $M = \{3\}$.*

É importante mencionar que o tempo de alcance clássico, partindo da distribuição estacionária π, coincide com o primeiro t em que a norma em L_1 de $\pi^\dagger P'^t - \pi^\dagger$ se torna suficientemente grande. Pois, somente a partir de um determinado instante t, o caminhante terá alcançado um dos elementos marcados.

De maneira análoga, para definir o *tempo de alcance quântico* iremos utilizar um operador de evolução modificado $U_{P'}$, associado a matriz estocástica P'. Esse novo operador não será uma caminhada absorvente como acontece no caso clássico, mas possivelmente permitirá que a probabilidade nos elementos marcados aumente durante a evolução do sistema. A condição inicial do passeio quântico é uma superposição sobre todas as arestas do grafo:

$$\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y \in X} \sqrt{p_{xy}} \big|x, y\big\rangle. \tag{2.2}$$

Definição 2.1.1 (Szegedy (2004)) O *tempo de alcance quântico* $H_{P,M}$ de um

passeio quântico com operador de evolução U_P, dado pela Eq. (1.16), e condição inicial $\big|\psi(0)\big\rangle$, é o menor número de passos, T, tal que

$$F(T) \geq 1 - \frac{m}{n}, \tag{2.3}$$

onde m é o número de vértices marcados, n o número de vértices do grafo original e $F(T)$ é definido como

$$F(T) = \frac{1}{T+1} \sum_{t=0}^{T} \Big\| \big|\psi(t)\big\rangle - \big|\psi(0)\big\rangle \Big\|^2, \tag{2.4}$$

onde $\big|\psi(t)\big\rangle = U_{P'}^t \big|\psi(0)\big\rangle$ e $U_{P'}^t$ é o operador de evolução depois de t passos, usando a matriz estocástica modificada.

Podemos identificar $1 - \frac{m}{n}$ como o valor da distância[1] entre a distribuição de probabilidades uniforme e a distribuição de probabilidades uniforme somente nos elementos marcados.

2.2 Expressão para $F(T)$ em termos do espectro de $U_{P'}$

Se considerarmos o espectro de $U_{P'}$ podemos encontrar uma expressão para a Eq. (2.4). Seguindo o Teorema 1.3.1, do capítulo anterior, sejam

$$\big|\alpha_j^{\pm}\big\rangle = \frac{A\big|w_j\big\rangle - \mathrm{e}^{\pm\, i\theta_j} B\big|v_j\big\rangle}{\sqrt{2}\sin\theta_j} \tag{2.5}$$

os autovetores normalizados de $U_{P'}$ com autovalores $e^{\pm 2i\theta_j}$, $0 < \theta_j \leq \frac{\pi}{2}$. Temos então no máximo $2n$ autovetores de $U_{P'}$ pois, os autovetores $\big|\alpha_j^{\pm}\big\rangle$ dependem dos vetores singulares da matriz discriminante C com valores singulares diferentes de 1, e C é uma matriz quadrada de dimensão n. Os autovetores restantes pertencem ao autoespaço de autovalor 1, vamos chamá-los de $\big|\alpha_j\big\rangle$. Podemos expressar nossa

[1] Veja (Nielsen e Chuang, 2005), cap. 9, para o cálculo da distância, tanto clássico quanto quântico, entre distribuições de probabilidades.

condição inicial na base de autovetores do operador de evolução:

$$\big|\psi(0)\big\rangle = \sum_{j=1}^{n-k} \left(c_j^+ \big|\alpha_j^+\big\rangle + c_j^- \big|\alpha_j^-\big\rangle\right) + \sum_{j=n-k+1}^{n^2-n+k} c_j \big|\alpha_j\big\rangle, \tag{2.6}$$

onde k é a multiplicidade do valor singular 1 da matriz discriminante. Os coeficientes $c_j^{\pm}$ são descritos por

$$c_j^{\pm} = \big\langle \alpha_j^{\pm} \big| \psi(0) \big\rangle \tag{2.7}$$

e obedecem a seguinte condição

$$\sum_{j=1}^{n-k} \left(\big|c_j^+\big|^2 + \big|c_j^-\big|^2 \right) + \sum_{j=n-k+1}^{n^2-n+k} \big|c_j\big|^2 = 1. \tag{2.8}$$

Dessa forma, somente os valores singulares de C diferentes de 1 serão utilizados para calcular o tempo de alcance quântico, pois ao aplicarmos o operador de evolução na condição inicial, obtemos

$$U_{P'}^t \big|\psi(0)\big\rangle = \sum_{j=1}^{n-k} \left(c_j^+ \mathrm{e}^{2i\theta_j t} \big|\alpha_j^+\big\rangle + c_j^- \mathrm{e}^{-2i\theta_j t} \big|\alpha_j^-\big\rangle\right) + \sum_{j=n-k+1}^{n^2-n+k} c_j \big|\alpha_j\big\rangle \tag{2.9}$$

e ao fazermos a diferença $U_{P'}^t \big|\psi(0)\big\rangle - \big|\psi(0)\big\rangle$, vemos que os termos no autoespaço de autovalor 1 irão desaparecer. Assim, a partir das Equações (2.9) e (2.6), temos que

$$\Big\| U_{P'}^t \big|\psi(0)\big\rangle - \big|\psi(0)\big\rangle \Big\|^2 = 4 \sum_{j=1}^{n-k} \big|c_j\big|^2 \big(1 - T_{2t}(\cos\theta_j)\big), \tag{2.10}$$

onde $\big|c_j\big| = \big|c_j^+\big| = \big|c_j^-\big|$ e T_n é o n-ésimo polinômio de Chebyshev do primeiro tipo (Abramowitz e Stegun, 1972).

Usando as Equações (2.10) e (2.4), obtemos

$$F(T) = \frac{2}{T+1} \sum_{j=1}^{n-k} \big|c_j\big|^2 \big(2\,T + 1 - U_{2T}(\cos\theta_j)\big), \tag{2.11}$$

onde U_n é o n-ésimo polinômio de Chebyshev do segundo tipo. O tempo de alcance

quântico é dado por

$$H_{P,M} = \left\lceil F^{-1}\left(1 - \frac{m}{n}\right)\right\rceil. \tag{2.12}$$

2.3 Limiar para o tempo de alcance quântico

Szegedy (2004) mostrou um limite superior para o tempo de alcance quântico, como veremos no Teorema 2.3.1, a seguir. Como consequência, obteremos a relação entre os tempos de alcance clássico e quântico, mostrando o ganho que existe ao utilizarmos essa nova definição.

Teorema 2.3.1 (Szegedy (2004)) Para toda cadeia de Markov ergódica e simétrica P, o tempo de alcance quântico de U_P com respeito a M é, no máximo,

$$\frac{100}{1 - \frac{m}{n}} \sum_{k=1}^{n-m} \nu_k^2 \sqrt{\frac{1}{1 - \lambda'_k}}, \tag{2.13}$$

onde $\left|v'_1\right\rangle, \ldots, \left|v'_{n-m}\right\rangle$ são os autovetores normalizados de P_M, os $\lambda'_1, \ldots, \lambda'_{n-m}$ seus autovalores associados, e ν_k são os coeficientes de $\left|\hat{u}\right\rangle = \frac{1}{\sqrt{n}}\mathbf{1}$ escritos na base de autovetores de P_M, ou seja, $\left|\hat{u}\right\rangle = \sum_{k=1}^{n-m} \nu_k \left|v'_k\right\rangle$. P_M é a matriz obtida de P removendo as linhas e colunas indexadas pelos elementos marcados.

Corolário 2.3.1 (Szegedy (2004)) Para toda cadeia de Markov ergódica e simétrica P e dado que $M \subseteq X$ com $m \leq \frac{n}{2}$, o tempo de alcance quântico de U_P com respeito a M é $O\left(\sqrt{\frac{1}{1-\lambda(P_M)}}\right)$, onde $\lambda(P_M)$ é o maior autovalor de P_M.

Consequentemente, o tempo de alcance quântico tem ganho quadrático em relação ao clássico, pois, como podemos ver detalhadamente em (Santos, 2010), o tempo de alcance clássico é $O\left(\frac{1}{1-\lambda(P_M)}\right)$.

Capítulo 3

Passeio quântico de Szegedy no ciclo

Para descrever o comportamento de um passeio quântico num grafo é importante encontrar a decomposição espectral do operador de evolução. Dessa forma, teremos conhecimento do que ocorre no sistema em cada instante de tempo. Entretanto, encontrar a decomposição desse operador muitas vezes não é um tarefa fácil. Santos e Portugal (2010a) analisaram o passeio quântico de Szegedy no grafo completo e mostraram que ele possui ganho quadrático na busca por vértices marcados. A seguir, descreveremos a primeira contribuição dessa tese, mostrando o que acontece no passeio quântico de Szegedy no ciclo, calculando o tempo de alcance quântico e a probabilidade de encontrar um vértice marcado nesse grafo.

Vamos considerar que os vértices do grafo são numerados de 1 a n e que os últimos m vértices são marcados. A matriz P_M é obtida a partir da matriz estocástica P (ou P') removendo as linhas e colunas correspondentes aos elementos marcados. Por exemplo, para os ciclos da Figura 3.1, temos as seguintes matrizes

(a) P (b) P'

Figura 3.1: *Ciclo com 5 vértices. O grafo* (a) *não possui vértice marcado e está associado a matriz* P*. O grafo* (b) *possui um vértice marcado,* $M = \{5\}$*, e está associado a matriz* P'*.*

associadas,

$$P = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 \end{bmatrix} \text{ e } P' = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.1}$$

A matriz P_M, para $m = 1$, é obtida removendo a última linha e a última coluna,

$$P_M = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & 0 \end{bmatrix}. \tag{3.2}$$

Podemos observar que P_M é um caso especial das matrizes de Toeplitz (Trench, 1985), e sua decomposição espectral é descrita a seguir.

$$P_M = \sum_{j=1}^{n-m} \cos\left(\frac{j\pi}{n-m+1}\right) \left|v'_j\right\rangle\left\langle v'_j\right|, \tag{3.3}$$

onde

$$\left|v'_j\right\rangle = \sqrt{\frac{2}{n-m+1}} \sum_{k=1}^{n-m} \sin\left(\frac{jk\pi}{n-m+1}\right) \left|k\right\rangle. \tag{3.4}$$

3.1 Valores e vetores singulares da matriz discriminante

Através do Teorema 1.3.1, podemos obter boa parte dos autovalores e autovetores de $U_{P'}$ a partir da descomposição singular da matriz discriminante $C = A^\dagger B$. Sabemos que as componentes $C_{xy} = \sqrt{p_{xy}p_{yx}}$. Então, a matriz discriminante associada a matriz P', nesse caso, é uma matriz simétrica descrita como:

$$C = \begin{bmatrix} P_M & 0 \\ 0 & I_m \end{bmatrix}. \tag{3.5}$$

Dessa forma, os valores singulares de C são os módulos dos autovalores de P_M e I_m. Considere $\left|v_j\right\rangle$, o vetor $\left|v'_j\right\rangle$ acrescido de m zeros, compatível com a dimensão de C. Os vetores singulares à direita $\left|v_j\right\rangle$ são os autovetores de P_M. Se o autovalor de P_M for negativo, o vetor singular à esquerda será o negativo do autovetor de P_M.

Em resumo, $\left|v_j\right\rangle$ e $\operatorname{sgn}\left(\cos\left(\frac{j\pi}{n-m+1}\right)\right)\left|v_j\right\rangle$, $1 \leq j \leq n-m$ são os vetores singulares à direita e à esquerda,[1] respectivamente, com valores singulares $\cos\theta_j = \left|\cos\left(\frac{j\pi}{n-m+1}\right)\right|$. Finalmente, a submatriz I_m adiciona a lista o valor singular 1 com multiplicidade m e vetores singulares $\left|j\right\rangle$ associados, onde $n-m+1 \leq j \leq n$. Veja a Tabela 3.1.

Valor singular	Vetor singular à direita	Vetor singular à esquerda
$\cos\theta_j = \left\|\cos\left(\frac{j\pi}{n-m+1}\right)\right\|$ $(1 \leq j \leq n-m)$	$\left\|v_j\right\rangle$	$\left\|w_j\right\rangle = \operatorname{sgn}\left(\cos\left(\frac{j\pi}{n-m+1}\right)\right)\left\|v_j\right\rangle$
1 $(n-m+1 \leq j \leq n)$	$\left\|v_j\right\rangle = \left\|j\right\rangle$	$\left\|w_j\right\rangle = \left\|j\right\rangle$

Tabela 3.1: *Valores e vetores singulares da matriz discriminante C, associada a matriz estocástica P', para um ciclo com n vértices e m vértices marcados.*

3.2 Espectro do operador de evolução

Os autovalores e autovetores de $U_{P'}$ que podem ser obtidos dos valores e vetores singulares de C são descritos na Tabela 3.2. Ficam faltando $n^2 - 2n + m$ autovetores, todos associados ao autovalor 1. Felizmente, para calcular o tempo de alcance quântico, o autoespaço de autovalor 1 não será necessário.

[1] $\operatorname{sgn}(x)$ é a função sinal.

Autovalor	Autovetor	Intervalo
$\mathrm{e}^{\pm 2i\theta_j}$	$\big\lvert\alpha_j^{\pm}\big\rangle = \frac{\left(sgn\left(\cos\left(\frac{j\pi}{n-m+1}\right)\right)A - \mathrm{e}^{\pm i\theta_j}B\right)\big\lvert v_j\big\rangle}{\sqrt{2}\sin\theta_j}$	$1 \leq j \leq n-m$
1	$\big\lvert\alpha_j\big\rangle = A\big\lvert j\big\rangle$	$1 \leq j \leq m$
1	$\big\lvert\alpha_j\big\rangle$	$m+1 \leq j \leq n^2 - 2(n-m)$

Tabela 3.2: *Autovalores e autovetores do operador de evolução $U_{P'}$. Os vetores $\big\lvert v_j\big\rangle$ são dados pela Eq.* (3.4)*. No autoespaço de autovalor 1, temos $n^2 - 2n + m$ autovetores sem expressão.*

Consequentemente, temos que

$$U_{P'} = \sum_{j=1}^{n-m} e^{2i\theta_j}\big\lvert\alpha_j^+\big\rangle\big\langle\alpha_j^+\big\rvert + \sum_{j=1}^{n-m} e^{-2i\theta_j}\big\lvert\alpha_j^-\big\rangle\big\langle\alpha_j^-\big\rvert + \sum_{j=1}^{n^2-2(n-m)} \big\lvert\alpha_j\big\rangle\big\langle\alpha_j\big\rvert. \tag{3.6}$$

3.3 Tempo de alcance quântico

A condição inicial do passeio quântico é dada por

$$\big\lvert\psi(0)\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y=1}^{n} \sqrt{p_{xy}}\big\lvert x, y\big\rangle. \tag{3.7}$$

Seja $c_j^{\pm} = \big\langle\alpha_j^{\pm}\big\rvert\psi(0)\big\rangle$ e $\big\lvert c_j\big\rvert = \big\lvert c_j^+\big\rvert = \big\lvert c_j^-\big\rvert$, pois $\big\lvert\alpha_j^+\big\rangle$ e $\big\lvert\alpha_j^-\big\rangle$ são complexos conjugados. Usando os autovetores da Tabela 3.2 e a expressão para $\big\lvert\psi(0)\big\rangle$, obtemos

$$|c_j|^2 = \frac{1-(-1)^j}{n(n-m+1)\left(1-\cos\left(\frac{j\pi}{n-m+1}\right)\right)}, \quad 1 \leq j \leq n-m. \tag{3.8}$$

Vamos utilizar a Eq. (2.11) para $F(T)$. Para o ciclo, temos

$$F(T) = \frac{2}{T+1} \sum_{j=1}^{n-m} |c_j|^2 (2T + 1 - U_{2T}(\cos\theta_j)). \tag{3.9}$$

Substituindo a expressão para $|c_j|^2$ e $\cos\theta_j$, temos

$$F(T) = \frac{2}{n(n-m+1)(T+1)} \sum_{j=1}^{n-m} \frac{(1-(-1)^j)\left(2T+1-U_{2T}\left(\left|\cos\left(\frac{j\pi}{n-m+1}\right)\right|\right)\right)}{\left(1-\cos\left(\frac{j\pi}{n-m+1}\right)\right)}. \tag{3.10}$$

A Figura 3.2 mostra o comportamento da função $F(T)$. $F(T)$ cresce rapidamente através da linha pontilhada $1-\frac{m}{n}$, e depois oscila em torno do seu valor limite. Esse é um comportamento recorrente que também pode ser visto para o caso do grafo completo, como vemos em (Santos e Portugal, 2010a).

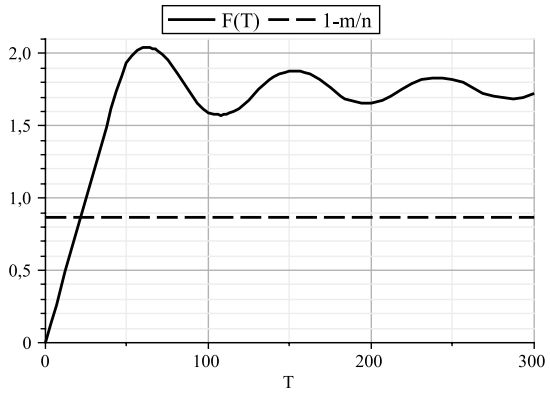


Figura 3.2: *Função $F(T)$ (linha sólida) e $1-\frac{m}{n}$ (linha tracejada) para $n=100$ e $m=13$. O tempo de alcance quântico pode ser visto no gráfico como o instante T tal que $F(T)=1-\frac{m}{n}$, que é aproximadamente* 21.75 *nesse caso.*

Com o objetivo de calcular o tempo de alcance quântico, vamos dividir $F(T)$ em dois termos:

$$\begin{aligned} F(T) &= \frac{2(2T+1)}{n(n-m+1)(T+1)} \sum_{j=1}^{n-m} \frac{(1-(-1)^j)}{1-\cos\left(\frac{j\pi}{n-m+1}\right)} - \\ &\quad \frac{2}{n(n-m+1)(T+1)} \sum_{j=1}^{n-m} \frac{(1-(-1)^j)\sin\left(\frac{(2T+1)j\pi}{n-m+1}\right)}{\left(1-\cos\left(\frac{j\pi}{n-m+1}\right)\right)\sin\left(\frac{j\pi}{n-m+1}\right)}. \end{aligned} \tag{3.11}$$

É fácil mostrar que o primeiro termo é equivalente a

$$\frac{2(2T+1)}{n(n-m+1)(T+1)} \left\lfloor \frac{(n-m+1)^2}{2} \right\rfloor. \tag{3.12}$$

O segundo termo não é tão simples quanto o primeiro. Vamos considerar a seguinte

função auxiliar

$$f(t) = \sum_{j=1}^{k-1} \frac{(1-(-1)^j)\sin\left(\frac{j\pi t}{k}\right)}{\left(1-\cos\left(\frac{j\pi}{k}\right)\right)\sin\left(\frac{j\pi}{k}\right)}. \tag{3.13}$$

Claramente, $f(t)$ é uma soma de senos que assume valor 0 quando $t = 0$ ou $t = k$. Além disso, o comportamento de $f(t)$ assemelha-se a função $\sin\left(\frac{\pi t}{k}\right)$. Dessa forma, podemos encontrar a e b tais que $f(t) \approx at(k-t) + b\sin\left(\frac{\pi t}{k}\right)$. Usando as seguintes equivalências

$$f\left(\frac{k}{2}\right) \approx \left(\frac{k}{2}\right)^3 + \frac{k}{4}\left(1-(-1)^{\left\lfloor\frac{k}{2}\right\rfloor}\right), \tag{3.14}$$

$$f'(0) \approx \left\lfloor\frac{k^2}{2}\right\rfloor, \tag{3.15}$$

nós obtemos

$$a = \frac{2\pi(1-(-1))^{\left\lfloor\frac{k}{2}\right\rfloor} - 8\left\lfloor\frac{k^2}{2}\right\rfloor + k^2\pi}{2k(\pi-4)}, \tag{3.16}$$

$$b = -\frac{k\left(2(1-(-1))^{1+\left\lfloor\frac{k}{2}\right\rfloor} - 2\left\lfloor\frac{k^2}{2}\right\rfloor + k^2\right)}{\pi-4}. \tag{3.17}$$

A Figura 3.3 mostra a função $f(t)$ e sua aproximação $at(k-t) + b\sin\left(\frac{\pi t}{k}\right)$, para $k = 10$. A diferença entre as duas funções vai ficando quase imperceptível, a medida que aumentamos o valor de k.

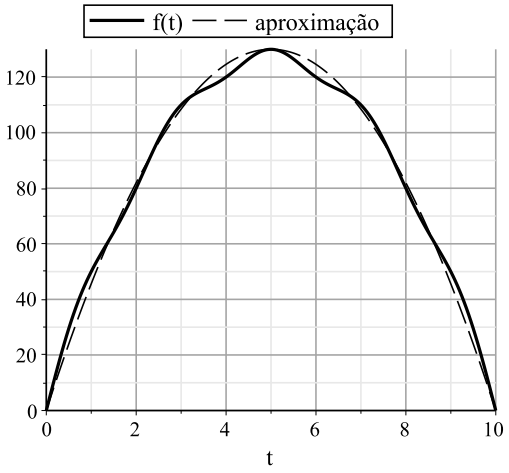


Figura 3.3: *Função $f(t)$ (linha sólida) e sua aproximação (linha tracejada). Nesse caso, $k = 10$ e podemos observar a diferença entre as duas funções. A medida que aumentarmos k, essa diferença será menos perceptível.*

Substituindo $t = 2T + 1$ e $k = n - m + 1$ em $f(t)$, nós podemos obter uma

aproximação para o segundo termo de $F(T)$. Dessa forma, a expansão assintótica para $F(T)$ é

$$F(T) = \frac{(2T+1)^2}{(T+1)n} + O\left(\frac{1}{n^2}\right). \tag{3.18}$$

Para $n \gg m$, o tempo de alcance quântico $H_{P,M}$ é obtido empregando o método de inversão de série na equação $F(T) = 1 - \frac{m}{n}$. Os primeiros termos são

$$H_{P,M} = \frac{n-m}{4} + O\left(\frac{1}{n}\right). \tag{3.19}$$

3.4 Probabilidade de encontrar um elemento marcado

Ao contrário do que acontece no cálculo do tempo de alcance quântico, para calcular a distribuição de probabilidades nos vértices do grafo em um instante t, precisaremos da decomposição espectral completa do operador de evolução. Entretanto, a partir da observação de simulações desse passeio quântico encontramos uma outra forma para solucionar esse problema. A partir da Eq. (1.16), podemos obter as componentes da matriz do operador de evolução, $U_{P'}$:

$$\big\langle c,d\big|U_{P'}\big|a,b\big\rangle = 4\sqrt{p'_{dc}p'_{ab}p'_{da}p'_{ad}} - 2\sqrt{p'_{dc}p'_{da}}\delta_{bd} - 2\sqrt{p'_{ab}p'_{ad}}\delta_{ac} + \delta_{ac}\delta_{bd}. \tag{3.20}$$

Considere qualquer $\big|\gamma\big\rangle \in \mathcal{H}^{n^2}$ trocando o sinal de alguns termos da condição inicial, ou seja,

$$\big\langle a,b\big|\gamma\big\rangle = \alpha_{a,b}\big\langle a,b\big|\psi(0)\big\rangle, \tag{3.21}$$

onde $\alpha_{a,b} \in \{-1,1\}$. Usando que

$$\big\langle a,b\big|\psi(0)\big\rangle = \sqrt{\frac{p_{ab}}{n}}, \tag{3.22}$$

obtemos

$$\big\langle c,d\big|U_{P'}\big|\gamma\big\rangle \;=\; \sum_{a,b=1}^{n}\big\langle c,d\big|U_{P'}\big|a,b\big\rangle\big\langle a,b\big|\gamma\big\rangle = \frac{1}{\sqrt{n}}\left(4\sum_{a=1}^{n-m}\sum_{b=1}^{n}\alpha_{a,b}p_{ab}\sqrt{p'_{dc}p'_{da}p_{ad}}-\right.$$

$$2\sum_{a=1}^{n}\alpha_{a,d}\sqrt{p_{ad}p'_{da}p'_{dc}} - 2\sum_{b=1}^{n}\alpha_{c,b}\sqrt{p_{cb}p'_{cb}p'_{cd}} + \alpha_{c,d}\sqrt{p_{cd}}\Bigg). \quad (3.23)$$

Defina $x \oplus y = x + y \mod n$. As componentes $\langle c, d|U_{P'}|\gamma\rangle$ obtidas da Eq. (3.23) são descritas a seguir.

- Se $c \in X\backslash M$ e $d \in X$:

$$\langle c, d|U_{P'}|\gamma\rangle = \frac{1}{\sqrt{n}}(|\alpha_{c,((c-1)\oplus 1+1)} + \alpha_{c,((c-1)\oplus(n-1)+1)}| - 1)\alpha_{c,d}\sqrt{p_{cd}}; \quad (3.24)$$

- Se $c \in M$ e $d \in X\backslash M$:

$$\langle c, d|U_{P'}|\gamma\rangle = \frac{1}{\sqrt{n}}(|\alpha_{c,((c-1)\oplus 1+1)} + \alpha_{c,((c-1)\oplus(n-1)+1)}| - 1)\alpha_{c,d}\sqrt{p_{cd}}; \quad (3.25)$$

- Se $c \in M$ e $d \in M$:

$$\langle c, d|U_{P'}|\gamma\rangle = \frac{1}{\sqrt{n}}\alpha_{c,d}\sqrt{p_{cd}}. \quad (3.26)$$

Observando as Eqs. (3.24), (3.25) e (3.26) e usando que $\alpha_{c,d}$ é 1 ou -1, podemos concluir que

$$\langle c, d|\psi(t)\rangle = \beta_{c,d}\langle c, d|\psi(0)\rangle, \quad (3.27)$$

onde $\beta_{c,d} \in \{-1, 1\}$.

A probabilidade de encontrar um elemento marcado é calculada através do projetor $\mathcal{P}_M$ no espaço vetorial gerado pelos elementos marcados, ou seja

$$\mathcal{P}_M = \sum_{x=n-m+1}^{n} |x\rangle\langle x| \otimes I_n. \quad (3.28)$$

A probabilidade é, então, dada por $p_M(t) = \langle\psi(t)|\mathcal{P}_M|\psi(t)\rangle$. A Eq. (3.27) implica que

$$\langle\psi(t)|\mathcal{P}_M|\psi(t)\rangle = \langle\psi(0)|\mathcal{P}_M|\psi(0)\rangle. \quad (3.29)$$

Assim,

$$p_M(t) = \frac{m}{n}. \tag{3.30}$$

Esse resultado é consequência do fato que $\left|\psi(t)\right\rangle$ difere da condição inicial apenas no sinal de suas componentes. Dessa forma, a distribuição de probabilidades se mantém a mesma durante a evolução do passeio quântico.

3.5 Conclusões

As contribuições desse capítulo são as expressões analíticas calculadas para o tempo de alcance quântico e para a probabilidade de encontrar um elemento num conjunto de vértices marcados para o passeio quântico de Szegedy no ciclo. Szegedy (2004) provou que para grafos conexos, não-direcionados e não-bipartidos, o tempo de alcance quântico é da ordem da raiz do tempo de alcance clássico. Em princípio, não poderíamos utilizar esse resultado para o ciclo, já que o ciclo par é um grafo bipartido. Entretanto, nós mostramos que não existe nenhuma diferença entre os tempos de alcance quântico para o caso par e ímpar. Ambos apresentam o mesmo resultado, e o tempo de alcance quântico tem ganho quadrático com relação ao clássico. O tempo de alcance clássico para o ciclo é $O(n^2)$.

Para o ciclo, a distribuição de probabilidades é uma pequena constante quando $n \gg m$. Esse resultado difere do resultado obtido para o grafo completo (Santos e Portugal, 2010a), onde o instante em que atingimos a probabilidade máxima e o tempo de alcance quântico são muito próximos e a probabilidade de sucesso é constante, ou seja, ela não depende de n ou m. O passeio quântico de Szegedy no ciclo pode ser usado para calcular o tempo de alcance quântico mas não é útil para ser usado como um algoritmo de busca, já que a probabilidade de obter um elemento marcado depende de n, o que aumenta a complexidade do algoritmo, tornando-o menos eficiente que o algoritmo clássico. No caso clássico, a busca no ciclo é $O(n)$ se percorremos todos os vértices do grafo sem usar um passeio aleatório, que é mais custoso, nesse caso.

As publicações referentes a esse capítulo são:

- (Santos e Portugal, 2010b) - Quantum hitting time on the cycle. In: Proceedings of III WECIQ - Workshop-School of Computation and Quantum Information, 2010;

- (Santos e Portugal) - Quantum hitting time and percolation in the cycle. Artigo em preparação a ser submetido para International Journal of Quantum Information.

Capítulo 4

Distribuição limite

De acordo com Portugal (2013), a evolução do estado quântico é determinada pelas potências dos autovalores do operador de evolução. Em sistemas finitos, tem-se um padrão *quasiperiódico* na evolução temporal, impedindo a convergência para uma determinada distribuição limite. Uma possível saída é definir uma nova distribuição chamada distribuição de probabilidades média, que evolui estocasticamente e converge para uma distribuição limite. Essa teoria foi descrita por Aharonov et al. (2000) para o passeio quântico com moeda. Além disso, para o caso clássico, quando uma cadeia de Markov converge para sua distribuição limite, essa distribuição é independente da condição inicial. No caso quântico, ocorre o contrário, a distribuição limite é dependente da condição inicial.

Dessa forma, de acordo com (Aharonov et al., 2000), temos a seguinte definição para a distribuição limite no caso quântico. Seja o estado do passeio quântico no instante t dado por

$$\big|\psi(t)\big\rangle = U^t\big|\psi(0)\big\rangle. \tag{4.1}$$

Suponha que $\{\big|\alpha_k\big\rangle\}$ é uma base ortonormal de autovetores de U com autovalores $e^{2\pi i\lambda_k}$ associados, então

$$U = \sum_k e^{2\pi i\lambda_k}\big|\alpha_k\big\rangle\big\langle\alpha_k\big|. \tag{4.2}$$

O estado inicial pode ser escrito na base de autovetores de U, como segue,

$$\big|\psi(0)\big\rangle = \sum_k c_k \big|\alpha_k\big\rangle, \tag{4.3}$$

onde $c_k = \big\langle \alpha_k \big| \psi(0) \big\rangle$.

A probabilidade de encontrar o caminhante no vértice $x \in X$ é dada por

$$p(x,t) = \sum_y |\big\langle x, y \big| \psi(t) \big\rangle|^2. \tag{4.4}$$

Então, a distribuição de probabilidades média é descrita como

$$\overline{p}(x,T) = \frac{1}{T} \sum_{t=0}^{T-1} p(x,t). \tag{4.5}$$

Defina

$$\pi(x) = \lim_{T\to\infty} \overline{p}(x,T). \tag{4.6}$$

Esse limite existe e pode ser explicitamente calculado desde que seja dada a distribuição inicial. A seguinte expressão é obtida para a distribuição limite:

$$\pi(x) = \sum_{y\in Y} \sum_{k,k'(\lambda_k=\lambda_{k'})} c_k c_{k'}^* \big\langle x, y \big| \alpha_k \big\rangle \big\langle \alpha_{k'} \big| x, y \big\rangle. \tag{4.7}$$

Se todos os autovalores forem diferentes (de multiplicidade 1), podemos reduzir a expressão para

$$\pi(x) = \sum_k |c_k|^2 \sum_{y\in Y} |\big\langle x, y \big| \alpha_k \big\rangle|^2. \tag{4.8}$$

Nosso objetivo é calcular a distribuição limite no passeio quântico de Szegedy.

4.1 Distribuição limite no passeio quântico de Szegedy

O operador de evolução do passeio quântico de Szegedy é descrito por

$$U_{P,Q} = \mathcal{R}_B \, \mathcal{R}_A = \left(2 \sum_{y\in Y} \big|\Psi_y\big\rangle\big\langle\Psi_y\big| - I \right) \left(2 \sum_{x\in X} \big|\Phi_x\big\rangle\big\langle\Phi_x\big| - I \right) \tag{4.9}$$

De acordo com o Teorema 1.3.1, sejam $\cos\theta_1, \cos\theta_2, ..., \cos\theta_l$ os valores singulares de $C = A^\dagger B$ ($C_{xy} = \sqrt{p_{xy}q_{yx}}$) que pertencem ao intervalo $[0, 1)$. E, sejam $\big|v_j\big\rangle$ e $\big|w_j\big\rangle$ $(1 \leq j \leq l)$ seus vetores singulares associados. Então,

$$\big|\alpha_j^\pm\big\rangle = \frac{A\big|w_j\big\rangle - e^{\pm i\theta_j} B\big|v_j\big\rangle}{\sqrt{2}\sin\theta_j} \tag{4.10}$$

são os autovetores normalizados de $U_{P,Q}$ com autovalor $e^{\pm 2i\theta_j}$, $1 \leq j \leq l$. Considere a seguinte condição inicial

$$\big|\psi(0)\big\rangle = \sum_{j=1}^{l} \left(c_j^+ \big|\alpha_j^+\big\rangle + c_j^- \big|\alpha_j^-\big\rangle\right), \tag{4.11}$$

onde $c_j^\pm = \big\langle \alpha_j^\pm \big| \psi(0) \big\rangle$. Note que essa condição inicial é ortogonal ao autoespaço de autovalor 1. Assim, a partir da Eq. (4.7) a distribuição limite é dada por

$$\pi(x) = \sum_{j,j'(\theta_j = \theta_{j'})} \left(c_j^+ c_{j'}^{*+} \sum_{y \in Y} \big\langle x, y \big| \alpha_j^+ \big\rangle \big\langle \alpha_{j'}^+ \big| x, y \big\rangle + c_j^- c_{j'}^{*-} \sum_{y \in Y} \big\langle x, y \big| \alpha_j^- \big\rangle \big\langle \alpha_{j'}^- \big| x, y \big\rangle \right) \tag{4.12}$$

com

$$\begin{aligned} \big\langle x, y \big| \alpha_j^\pm \big\rangle &= \big\langle x, y \big| \left(\frac{A\big|w_j\big\rangle - e^{\pm i\theta_j} B\big|v_j\big\rangle}{\sqrt{2}\sin\theta_j} \right) \\ &= \frac{1}{\sqrt{2}\sin\theta_j} \left(\sqrt{p_{xy}} \big\langle x \big| w_j \big\rangle - e^{\pm i\theta_j} \sqrt{q_{yx}} \big\langle y \big| v_j \big\rangle \right). \end{aligned} \tag{4.13}$$

4.1.1 Autovalores com multiplicidade 1

Considerando que todos os autovalores são diferentes, ou seja, cada autovalor tem multiplicidade 1, podemos reescrever a distribuição limite como

$$\pi(x) = \sum_{j=1}^{l} \left(|c_j^+|^2 \sum_{y \in Y} |\big\langle x, y \big| \alpha_j^+ \big\rangle|^2 + |c_j^-|^2 \sum_{y \in Y} |\big\langle x, y \big| \alpha_j^- \big\rangle|^2 \right), \tag{4.14}$$

com

$$\sum_{y\in Y}|\langle x,y|\alpha_j^{\pm}\rangle|^2=\frac{1}{2\sin^2\theta_j}\Bigg(|\langle x|w_j\rangle|^2+\sum_{y\in Y}\big(q_{yx}|\langle y|v_j\rangle|^2- \\ e^{\mp i\theta_j}\sqrt{p_{xy}q_{yx}}\langle x|w_j\rangle\langle v_j|y\rangle-e^{\pm i\theta_j}\sqrt{p_{xy}q_{yx}}\langle w_j|x\rangle\langle y|v_j\rangle\big)\Bigg)\,, \tag{4.15}$$

utilizando a Eq. (4.13).

Caso $|v_j\rangle$ e $|w_j\rangle$ forem reais, então teremos $|c_j|^2=|c_j^+|^2=|c_j^-|^2$ e

$$|\langle x,y|\alpha_j^{\pm}\rangle|^2=\frac{1}{2\sin^2\theta_j}\left(p_{xy}|\langle x|w_j\rangle|^2-2\cos\theta_j\sqrt{p_{xy}q_{yx}}\langle x|w_j\rangle\langle v_j|y\rangle+q_{yx}|\langle y|v_j\rangle|^2\right). \tag{4.16}$$

Nesse caso, utilizando as Eqs. (4.14), (4.15) e (4.16), obtemos uma nova expressão para $\pi(x)$, dada por,

$$\pi(x)=\sum_{j=1}^{l}\frac{|c_j|^2}{\sin^2\theta_j}\left(|\langle x|w_j\rangle|^2-2\cos\theta_j\langle x|w_j\rangle\sum_{y\in Y}\sqrt{p_{xy}q_{yx}}\langle v_j|y\rangle+\sum_{y\in Y}q_{yx}|\langle y|v_j\rangle|^2\right). \tag{4.17}$$

4.1.2 Limite na malha bidimensional

Considere uma malha bidimensional $N\times N$ com condições de contorno periódicas, como na Figura 4.1.

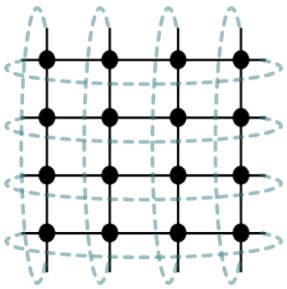


Figura 4.1: *Malha bidimensional* 4×4 *com condições de contorno periódicas.*

A matriz de probabilidade P tem sua decomposição espectral dada por:

$$P=\sum_{x,y=0}^{N-1}\lambda_{x,y}|v_{x,y}\rangle\langle v_{x,y}| \tag{4.18}$$

onde

$$\lambda_{x,y} = \frac{1}{2}\left(\cos\left(\frac{2\pi x}{N}\right) + \cos\left(\frac{2\pi y}{N}\right)\right), \tag{4.19}$$

$$\big|v_{x,y}\big\rangle = \frac{1}{N}\sum_{a,b=0}^{N-1} e^{\frac{2\pi i}{N}(ax+by)}\big|a,b\big\rangle. \tag{4.20}$$

Lembre que $X = Y$ e $P = Q$, nesse caso. Os vetores singulares da matriz discriminante C serão $\big|v_j\big\rangle = \big|v_{x,y}\big\rangle$ e $\big|w_j\big\rangle = \mathrm{sgn}(\lambda_{x,y})\big|v_{x,y}\big\rangle$.

Vamos considerar a condição inicial partindo da origem $(0,0)$. Desse forma,

$$\big|\psi(0)\big\rangle = \sum_{y=0}^{N-1}\sqrt{p_{0y}}\big|0,y\big\rangle. \tag{4.21}$$

Essa condição inicial não é ortogonal ao autoespaço de autovalor 1. Portanto, iremos obter um limite inferior para a distribuição limite, nesse caso. Como existem autovalores com multiplicidade diferente de 1, utilizaremos a Eq. (4.12), ou seja,

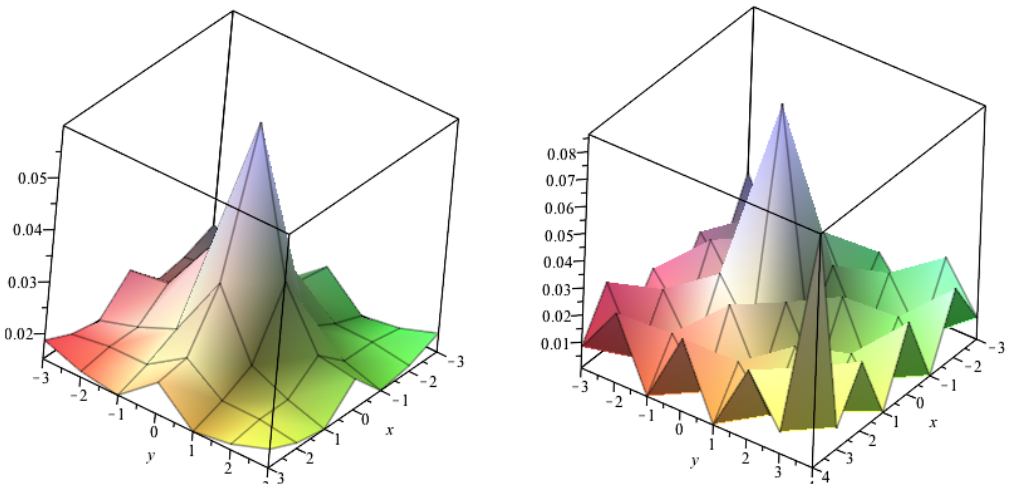
$$\pi(x) \geq \sum_{j,j'(\theta_j=\theta_{j'})}\left(c_j^+ c_{j'}^{*+}\sum_{y\in Y}\big\langle x,y\big|\alpha_j^+\big\rangle\big\langle\alpha_{j'}^+\big|x,y\big\rangle + c_j^- c_{j'}^{*-}\sum_{y\in Y}\big\langle x,y\big|\alpha_j^-\big\rangle\big\langle\alpha_{j'}^-\big|x,y\big\rangle\right) \tag{4.22}$$

com

$$\big\langle x,y\big|\alpha_j^\pm\big\rangle = \frac{\sqrt{p_{xy}}}{\sqrt{2}\sin\theta_j}\left(\big\langle x\big|w_j\big\rangle - e^{\pm i\theta_j}\big\langle y\big|v_j\big\rangle\right) \tag{4.23}$$

já que P é simétrica.

A Figura 4.2 apresenta o valor desse limite inferior para a distribuição limite nas malhas bidimensionais 7×7 e 8×8 calculadas numericamente. A soma total da distribuição em todos os pontos é aproximadamente 0.97 para o caso 7×7 e 0.96 para o caso 8×8, mostrando que esse limite está bem próximo do valor exato da distribuição. Além disso, podemos notar diferenças no comportamento entre os casos par e ímpar. O gráfico da malha 7×7 apresenta um pico máximo na origem $(0,0)$, que é um comportamento similar ao que acontece no passeio quântico com moeda, como podemos ver em (Marquezino, 2010). Já para o gráfico da malha 8×8, temos dois picos iguais em $(0,0)$ e $(4,4)$. Entretanto, como esses valores são limites inferiores, é possível que a parte que falta para completar o



(a) 7×7 (b) 8×8

Figura 4.2: *Limite inferior para a distribuição limite na malha bidimensional com condição inicial* $\big|\psi(0)\big\rangle$.

valor exato da distribuição limite contribua para o aumento do pico em $(0, 0)$, o que nos levaria a um comportamento similar aos demais casos; ou é possível que este seja um comportamento particular do caso par. É importante ressaltar que o mesmo comportamento, para os casos par e ímpar, é obtido quando calculamos para outros tamanhos de malhas.

4.1.3 O caso P'

Seja P' o passeio absorvente no conjunto de vértices marcados $M \subseteq X$. Considere que P é reversível. Faça $\cos\theta_j = |\lambda_j|$, onde λ_j é um autovalor de P_M com autovetor $\big|v_j\big\rangle$. Nesse caso, os vetores singulares $\big|w_j\big\rangle = \mathrm{sgn}(\lambda_j)\big|v_j\big\rangle$ e $\big|v_j\big\rangle$ são obtidos a partir dos autovetores de P_M. Note que $\big\langle y\big|v_j\big\rangle = \big\langle x\big|w_j\big\rangle = 0$ se $x, y \in M$, pois m zeros são acrescentados ao final desses estados para corresponder com a dimensão de C. Dessa forma, se considerarmos que todos os autovalores são diferentes, a partir da Eq. (4.17), obtemos,

- se $x \in M$, então

$$\pi(x) = \sum_{j=1}^{l} \frac{|c_j|^2}{\sin^2\theta_j} \sum_{y \notin M} p_{yx} |\big\langle y\big|v_j\big\rangle|^2; \tag{4.24}$$

- se $x \notin M$, então

$$\pi(x) = \sum_{j=1}^{l} \frac{|c_j|^2}{\sin^2\theta_j} \left(|\langle x|w_j\rangle|^2 - 2\cos\theta_j \langle x|w_j\rangle \sum_{y\notin M} \sqrt{p_{xy}p_{yx}} \langle v_j|y\rangle + \sum_{y\notin M} p_{yx} |\langle y|v_j\rangle|^2 \right). \tag{4.25}$$

Para o passeio quântico com vértices marcados, geralmente utilizamos a seguinte condição inicial

$$\big|\psi(0)\big\rangle = \sum_{x,y} \sqrt{\pi_x p_{xy}} \big|x,y\big\rangle = \sum_{x\in X} \sqrt{\pi_x} \big|\Phi_x\big\rangle = \sum_{y\in X} \sqrt{\pi_y} \big|\Psi_y\big\rangle, \tag{4.26}$$

onde π é a distribuição estacionária de P e $\pi_x = \frac{d_i}{2a}$ (d_i é o grau do vértice i e a é o número de arestas do grafo P). No caso em que P é simétrico, $\pi_x = \frac{1}{\sqrt{n}}$. Então, podemos obter um limite inferior para $\pi(x)$, já que a condição inicial não é ortogonal ao autoespaço de autovalor 1 que não é conhecido totalmente. O valor de c_j para esse caso é calculado, a seguir.

Lembrando que $\big|\alpha_j^{\pm}\big\rangle = \frac{A\big|w_j\big\rangle - e^{\pm i\theta_j} B\big|v_j\big\rangle}{\sqrt{2}\sin\theta_j}$, $1 \le j \le n-m$, $j \notin M$, temos

$$c_j^{\pm} = \big\langle \alpha_j^{\pm} \big| \psi(0)\big\rangle = \frac{1}{\sqrt{2}\sin\theta_j} \left(\big\langle w_j\big|A^{\dagger}\big|\psi(0)\big\rangle - e^{\mp i\theta_j} \big\langle v_j\big|B^{\dagger}\big|\psi(0)\big\rangle \right). \tag{4.27}$$

Calculando os valores de $\big\langle w_j\big|A^{\dagger}\big|\psi(0)\big\rangle$ e $\big\langle v_j\big|B^{\dagger}\big|\psi(0)\big\rangle$, temos:

$$\big\langle w_j\big|A^{\dagger}\big|\psi(0)\big\rangle = \sum_{x\notin M} \big\langle w_j\big|x\big\rangle \sqrt{\pi_x}, \tag{4.28}$$

$$\big\langle v_j\big|B^{\dagger}\big|\psi(0)\big\rangle = \sum_{y\notin M} \big\langle v_j\big|y\big\rangle \sqrt{\pi_y}. \tag{4.29}$$

Substituindo na Eq. (4.27), obtemos

$$c_j^{\pm} = \frac{1}{\sqrt{2}\sin\theta_j} \sum_{x\notin M} \sqrt{\pi_x} \left(\big\langle w_j\big|x\big\rangle - e^{\mp i\theta_j} \big\langle v_j\big|x\big\rangle \right). \tag{4.30}$$

4.1.4 Limite no grafo completo

Considerando o passeio quântico com m elementos marcados num grafo completo com n vértices, temos que a matriz P_M é dada por

$$P_M = \frac{n-m-1}{n-1}\big|v_{n-m}\big\rangle\big\langle v_{n-m}\big| - \frac{1}{n-1}\sum_{k=1}^{n-m-1}\big|v_k\big\rangle\big\langle v_k\big|, \tag{4.31}$$

onde

$$\big|v_k\big\rangle = \frac{1}{\sqrt{k+k^2}}\left(\sum_{j=1}^{k}\big|j\big\rangle - k\big|k+1\big\rangle\right), \tag{4.32}$$

$$\big|v_{n-m}\big\rangle = \frac{1}{\sqrt{n-m}}\sum_{j=1}^{n-m}\big|j\big\rangle. \tag{4.33}$$

Os valores singulares e seus respectivos vetores singulares à direita e à esquerda são

- $1 \leq k \leq n-m-1$, $\cos\theta_k = |\lambda_k| = \frac{1}{n-1}$, $\big|v_k\big\rangle$, $\big|w_k\big\rangle = -\big|v_k\big\rangle$;
- $k = n-m$, $\cos\theta_k = |\lambda_k| = \frac{n-m-1}{n-1}$, $\big|v_k\big\rangle$, $\big|w_k\big\rangle = \big|v_k\big\rangle$.

Considere a condição inicial dada pela Eq. (4.26). Nesse caso, temos

$$\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}}\sum_{x,y}\sqrt{p_{xy}}\big|x,y\big\rangle = \frac{1}{\sqrt{n}}\sum_{x\in X}\big|\Phi_x\big\rangle = \frac{1}{\sqrt{n}}\sum_{y\in X}\big|\Psi_y\big\rangle. \tag{4.34}$$

Vamos obter um limite inferior para a distribuição limite. Nesse caso, vemos que temos um autovalor com multiplicidade maior que 1. Mas, veremos a seguir que essa parte não influenciará no cálculo e, portanto, poderemos obter uma expressão analítica para esse limite utilizando as Eqs. (4.24) e (4.25).

A partir da Eq. (4.30), para $1 \leq k \leq n-m-1$, temos

$$\begin{aligned} c_k^{\pm} &= \frac{1}{\sqrt{2n}\sin\theta_k}\sum_{x\notin M}\left(-\big\langle v_k\big|x\big\rangle - e^{\mp i\theta_k}\big\langle v_k\big|x\big\rangle\right) \\ &= \frac{(-1-e^{\mp i\theta_k})}{\sqrt{2n}\sin\theta_k}\left(\sum_{x=1}^{k}\frac{1}{\sqrt{k+k^2}} - \frac{k}{\sqrt{k+k^2}}\right) = 0. \end{aligned} \tag{4.35}$$

Para $k = n - m$, temos

$$\begin{aligned} c^{\pm}_{n-m} &= \frac{1}{\sqrt{2n}\sin\theta_{n-m}} \sum_{x\notin M} \left(\langle v_{n-m}|x\rangle - e^{\mp i\theta_{n-m}}\langle v_{n-m}|x\rangle\right) \\ &= \frac{\sqrt{n-m}(1-e^{\mp i\theta_{n-m}})}{\sqrt{2n}\sin\theta_{n-m}}. \end{aligned} \tag{4.36}$$

Consequentemente,

$$|c_{n-m}|^2 = \frac{n-m}{2n\sin^2\theta_{n-m}}(2-2\cos\theta_{n-m}) = \frac{(n-m)(1-\cos\theta_{n-m})}{n\sin^2\theta_{n-m}}. \tag{4.37}$$

4.1.4.1 Expressão para $\pi(x)$

No caso em que $x \in M$, a partir da Eq. (4.24), temos

$$\begin{aligned} \pi(x) &\geq \frac{|c_{n-m}|^2}{\sin^2\theta_{n-m}} \sum_{y\notin M} p_{yx}|\langle y|v_{n-m}\rangle|^2 \\ &= \frac{|c_{n-m}|^2(n-1)}{m(2n-m-2)}. \end{aligned} \tag{4.38}$$

Substituindo o valor de $|c_{n-m}|^2$, obtemos

$$\pi(x) \geq \frac{(n-1)^2(n-m)}{nm(2n-m-2)^2}. \tag{4.39}$$

No caso em que $x \notin M$, da Eq. (4.25), temos

$$\begin{aligned} \pi(x) \geq \frac{|c_{n-m}|^2}{\sin^2\theta_{n-m}} \Bigg(& |\langle x|w_{n-m}\rangle|^2 + \sum_{y\notin M} p_{yx}|\langle y|v_{n-m}\rangle|^2 - \\ & -2\cos\theta_{n-m}\langle x|w_{n-m}\rangle \sum_{y\notin M} \sqrt{p_{xy}p_{yx}}\langle v_{n-m}|y\rangle \Bigg) \\ = |c_{n-m}|^2 & \frac{(3n-2m-3)}{(n-m)(2n-m-2)}. \end{aligned} \tag{4.40}$$

Substituindo o valor de $|c_{n-m}|^2$, obtemos

$$\pi(x) \geq \frac{(n-1)(3n-2m-3)}{n(2n-m-2)^2}. \tag{4.41}$$

Na Figura 4.3 podemos ver a soma das probabilidades em todos os vértices, ou seja,

$$\sum_{x\in M}\pi(x)+\sum_{x\in X\setminus M}\pi(x), \tag{4.42}$$

para diferentes valores de n e m, utilizando os valores de $\pi(x)$ dados pelas Eqs. (4.39) e (4.41). Podemos notar que essa soma é bem próxima de 1 quando m é menor. Isso se deve ao fato que o aumento de m, aumenta o subespaço de autovalor 1 que não está sendo levado em consideração no cálculo desse limite inferior para a distribuição limite.

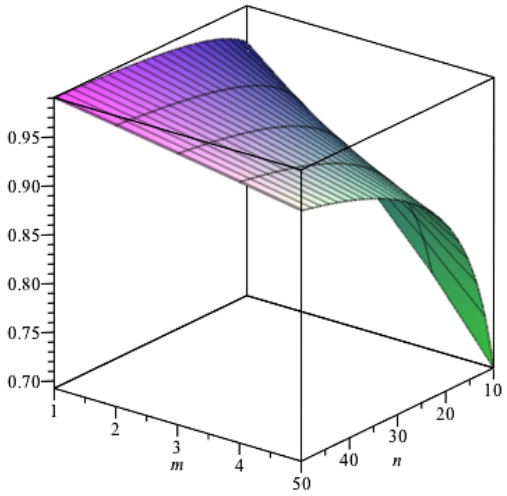


Figura 4.3: *Soma das probabilidades em todos os vértices, para* $n = 10\ldots50$ *e* $m = 1\ldots5$.

4.1.5 Limite no ciclo

Já calculamos a expressão para $\big|\psi(t)\big\rangle = U_{P'}^{t}\big|\psi(0)\big\rangle$ para o ciclo, no capítulo anterior. Vimos que $\big\langle x,y\big|\psi(t)\big\rangle = \beta_{xy}\big\langle x,y\big|\psi(0)\big\rangle$, onde $\beta_{x,y}\in\{-1,1\}$. Então, $p(x,t)=\frac{1}{n}\ \forall x\in X$ e, dessa forma, $\pi(x)=\frac{1}{n}\ \forall x\in X$. É interessante notar que, nesse caso, a distribuição limite no passeio quântico no ciclo é igual a clássica.

4.2 Conclusões

Como pudemos acompanhar nesse capítulo, calcular a distribuição limite num passeio quântico depende da condição inicial e do espectro do operador de evolução. Para o passeio quântico de Szegedy, em princípio, não temos conhecimento total do seu autoespaço de autovalor 1. Se a condição inicial não possuir interseção com esse autoespaço, então podemos obter uma expressão exata para a distribuição limite. Caso contrário, obteremos um limite inferior. Entretanto, vimos através dos exemplos apresentados que esse limite inferior está bem próximo do valor exato para as condições iniciais consideradas. Na malha bidimensional, sem elementos marcados e condição inicial na origem, pudemos observar um comportamento similar ao do passeio quântico com moeda onde temos um pico na origem, para o caso ímpar. Em contraste, o caso par apresenta dois picos. No grafo completo, com elementos marcados, vimos que ao aumentar o número de elementos marcados obteremos um limite inferior para a distribuição limite mais distante do seu valor exato, pois quando aumentamos o número de elementos marcados também estamos aumentando o autoespaço de autovalor 1. No caso do ciclo, temos uma distribuição limite uniforme, como já era esperado pelos resultados analíticos do Capítulo 3.

Capítulo 5

Tempo de alcance quântico descoerente

Quando falamos que um sistema quântico possui uma evolução unitária estamos considerando que ele está completamente isolado do resto do universo. Entretanto, isso não acontece no mundo real. Nesse caso, temos que considerar sistemas quânticos abertos em que há interação com o ambiente e, consequentemente, possível destruição da informação quântica do sistema. Esse processo responsável por reduzir a coerência quântica é chamado de *descoerência*. Trata-se de um efeito colateral inevitável em qualquer implementação de um computador quântico, fazendo as características clássicas do sistema físico emergirem e as vantagens da computação quântica serem perdidas (Bacon, 2001; Kendon, 2007).

A descoerência é geralmente modelada como uma evolução não-unitária do passeio quântico, em que podemos adicionar uma operação extra, não-unitária (um operador de medição, por exemplo), ou podemos, também, substituir a moeda e/ou o operador de deslocamento por operadores não-unitários. Saber o quão rápido o passeio quântico torna-se clássico com o aumento da descoerência, ou o quanto o passeio quântico é sensível a pequenas descoerências são algumas das questões analisadas nessa área.

Brun et al. (2003) mostraram como o passeio quântico com moeda passa a se comportar como um passeio aleatório clássico devido a descoerência na moeda e a utilização de moedas de dimensões maiores. Kendon e Tregenna (2003) estudaram as consequências computacionas da descoerência na moeda. Alagic e Russell (2005)

analisaram o efeito da realização de medições independentes para o passeio quântico de tempo contínuo no hipercubo. Kendon (2007) apresenta uma revisão sobre a descoerência em passeios quânticos.

A descoerência inspirada em percolação foi analisada em vários trabalhos (Romanelli et al., 2005; Oliveira et al., 2006; Xu e Liu, 2008; Leung et al., 2010; Lovett et al., 2011) usando os modelos de passeios quânticos contínuo e discreto com moeda. Por exemplo, Romanelli et al. (2005) trabalharam com o passeio quântico unidimensional e consideraram a possibilidade de que, em um dado instante de tempo, uma ou mais ligações entre os vértices estivessem interrompidas. Essa técnica foi posteriormente generalizada para o caso bidimensional por Oliveira et al. (2006). Recentemente, Kollar et al. (2012) analisaram o comportamento assintótico do passeio quântico com moeda afetado por um modelo de descoerência similar ao que veremos nesse capítulo.

No passeio quântico de Szegedy, Chiang (2010) analisa a sensibilidade desse passeio quântico a perturbação. Esse trabalho supõe a existência de uma matriz simétrica de erro E que é introduzida por causa da limitação da representação numérica do sistema, de forma que a nova matriz de probabilidade é expressa por $Q = P + E$. Ele mostra que nesse passeio perturbado, onde a magnitude do erro é $||E||$, o ganho quadrático para o tempo de alcance quântico será anulado quando $||E|| \geq \Omega(\delta(1 - \delta m/n))$; δ é a diferença entre os dois maiores autovalores de P, m é o número de vértices marcados e n é o número de vértices do grafo.

Neste capítulo, propomos analisar como o passeio quântico de Szegedy se comporta ao ser afetado por um modelo de descoerência inspirado em percolação. O tempo de alcance quântico descoerente será definido e obteremos uma generalização do resultado de Szegedy para o tempo de alcance quântico. Simulações desse modelo de descoerência também serão apresentadas para diferentes grafos.

5.1 Modelo

5.1.1 O que é percolação?

Em 1975, Broadbent e Hammersley introduziram o modelo de percolação através da formulação de um modelo estocástico simples para a situação de uma pedra porosa imersa em água. Em duas dimensões esse modelo é descrito da seguinte forma. Considere o grafo $\mathbb{Z}^2$, cujos vértices são o conjunto $\mathbb{Z}^2$ e as arestas ligam pares de pontos com distância euclidiana 1. Considere $p \in [0, 1]$. Fazendo cada aresta do grafo ser independentemente *aberta* com probabilidade p e *fechada* com probabilidade $1 - p$, nosso subgrafo aleatório será definido possuindo o mesmo conjunto de vértices de $\mathbb{Z}^2$ mas tendo apenas as arestas declaradas como abertas. As arestas representam as passagens internas da pedra e iremos modelá-la como uma subseção finita de $\mathbb{Z}^2$, como vemos na Figura 5.1. Quando a pedra é imersa na

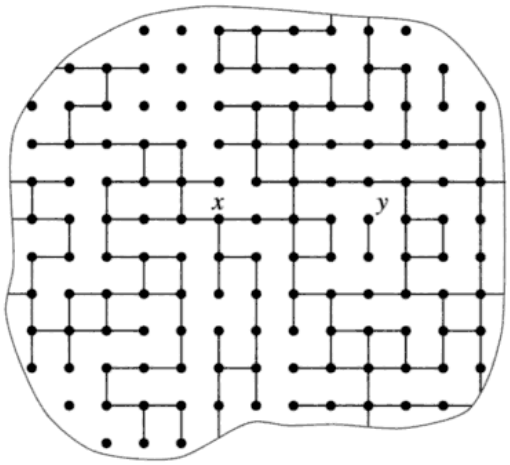


Figura 5.1: *Esboço em duas dimensões da estrutura de uma pedra porosa. Quando imersa na água, o vértice x será molhado pela invasão da água, enquanto que o vértice y permanecerá seco (Grimmett, 1999).*

água, o vértice x dentro da pedra é molhado se, e somente se, existe um caminho de x para algum vértice na borda da pedra, usando somente as arestas abertas. Uma das preocupações da teoria de percolação trata-se da existência de tais caminhos e de como a estrutura desse subgrafo aleatório depende do valor numérico de p. O modelo de percolação, anteriormente descrito, é chamado percolação de elos

(*bond percolation*). Um outro modelo em que os vértices, ao invés das arestas, são declarados abertos ou fechados aleatoriamente, é denominado percolação de sítios (*site percolation*). A teoria de percolação tem sido amplamente estudada, como podemos ver em (Grimmett, 1999; Stauffer e Aharony, 1994).

5.1.2 Descoerência inspirada em percolação

Vamos, agora, introduzir o modelo de descoerência inspirado em percolação, que pode ser explicado da seguinte maneira. Suponha que o caminhante está em um vértice do grafo. Antes de se mover para algum vértice vizinho, cada aresta do grafo pode ser removida e cada não-aresta pode ser inserida com probabilidade p. Com probabilidade $1 - p$, cada aresta e não-aresta permanece inalterada. Depois dessa mudança na topologia do grafo, o caminhante se move seguindo a dinâmica do modelo. O grafo original é reiniciado e o processo repete-se no próximo passo. A Figura 5.2 ilustra esse processo. Dessa forma, trata-se de um processo de percolação dinâmica de elos.

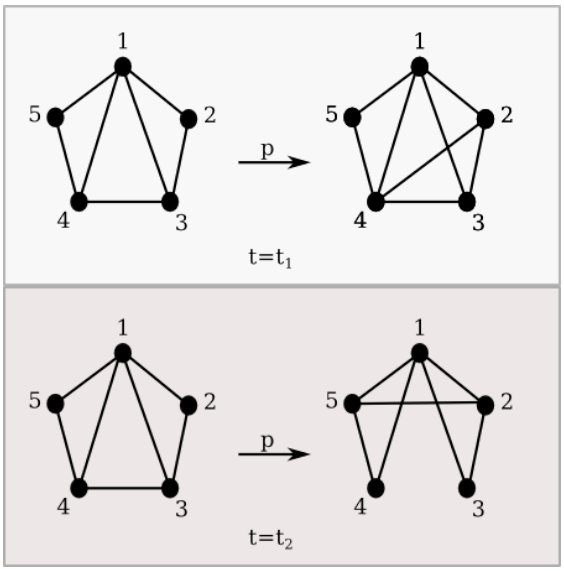


Figura 5.2: *Exemplo da dinâmica da descoerência. O grafo original encontra-se a esquerda. Em* $t = 0$*, a aresta* $(2, 4)$ *foi inserida no grafo, após realizado o processo de descoerência. Em* $t = 1$*, o grafo é reiniciado e aplicamos novamente a remoção ou inserção de arestas dependendo da probabilidade* p*. Nesse passo, a aresta* $(3, 4)$ *foi removida e a aresta* $(2, 5)$ *inserida.*

A probabilidade de ocorrência de uma matriz P_i é determinada da seguinte

forma. Se $0 < p < 1$, então $Pr(P_i) = (1-p)^{a_c - a_d} p^{a_d}$, onde $a_c = \frac{n(n-1)}{2}$ é o número de arestas do grafo completo com n vértices e a_d é o número de arestas removidas mais o número de arestas inseridas para obter P_i a partir de P. Se $p = 0$, $Pr(P_i = P) = 1$, e $Pr(P_i \neq P) = 0$. Se $p = 1$, temos $Pr(P_i = \bar{P}) = 1$, e $Pr(P_i \neq \bar{P}) = 0$, onde $\bar{P}$ é o complemento de P. A evolução sob descoerência máxima ocorre quando $p = 1/2$, pois a cada passo estaremos selecionando um grafo completamente aleatório.

Outro modelo de descoerência pode ser analisado nesse ponto. Se for permitida apenas a remoção de arestas (inserção de arestas não é permitida), a_c deve ser substituído pelo número de arestas do grafo original e a_d será o número de arestas removidas.

A dinâmica com a descoerência apresenta um novo comportamento porque, a cada passo, o grafo pode estar mudando. Esse processo muda a matriz de probabilidade, o que leva a modificações no operador de evolução. Dessa forma, ao invés de termos uma evolução usual do passeio quântico como $\big|\psi(t)\big\rangle = U_P^t \big|\psi(0)\big\rangle$, teremos

$$\big|\psi(t)\big\rangle = U_{P_t} U_{P_{t-1}} \dots U_{P_1} \big|\psi(0)\big\rangle =: U_{\vec{P}_t} \big|\psi(0)\big\rangle, \tag{5.1}$$

onde $\vec{P}_t = (P_1, \dots, P_{t-1}, P_t)$ e $U_{\vec{P}_t} = U_{P_t} U_{P_{t-1}} \dots U_{P_1}$. As matrizes P_i's não são necessariamente iguais e são independentes entre si. Elas são obtidas a partir de P e, para cada P_i, temos uma matriz P_i' associada dependendo da cardinalidade de M.

Nesse contexto, será útil definir um operador que representará o comportamento médio dos operadores afetados pela descoerência. Seja

$$\bar{U}_{dec} := \sum_P Pr(P) U_P, \tag{5.2}$$

o operador obtido fazendo uma média sobre todos os possíveis operadores de evolução afetados pela descoerência. O resultado a seguir mostra que a média sobre todas as possíveis sequências $\vec{P}$, de tamanho T, e de acordo com sua distribuição

de probabilidades, é igual a $\bar{U}_{dec}^{T}$.

Lema 5.1.1 Para $t \leq T$ temos

$$\sum_{\vec{P}_T} Pr(\vec{P}_T) U_{\vec{P}_t} = \bar{U}_{dec}^{t}. \tag{5.3}$$

Prova Como $Pr(\vec{P}_T) = \prod_{i=1}^{T} Pr(P_i)$, temos que

$$\begin{aligned}
&\sum_{\vec{P}_T} Pr(\vec{P}_T) U_{P_t} U_{P_{t-1}} \dots U_{P_1} = \sum_{\vec{P}_T} \prod_{i=1}^{T} Pr(P_i) U_{P_t} U_{P_{t-1}} \dots U_{P_1} \\
&= \sum_{P_T} \sum_{P_{T-1}} \dots \sum_{P_2} \left(\prod_{i=2}^{T} Pr(P_i) \right) U_{P_t} U_{P_{t-1}} \dots U_{P_2} \left(\sum_{P_1} Pr(P_1) U_{P_1} \right) \\
&= \sum_{P_T} \sum_{P_{T-1}} \dots \sum_{P_{t+1}} Pr(P_T) Pr(P_{T-1}) \dots Pr(P_{t+1}) \bar{U}_{dec}^{t} \\
&= \bar{U}_{dec}^{t}
\end{aligned}$$

∎

Para definir o tempo de alcance quântico para a evolução descoerente, temos que fazer uma média sobre todas as possíveis sequências $\vec{P}$. Defina,

$$F_{dec}(T) := \sum_{\vec{P}_T} Pr(\vec{P}_T) \left(\frac{1}{T+1} \sum_{t=0}^{T} \left\| U_{\vec{P}_t} \big|\psi(0)\big\rangle - \big|\psi(0)\big\rangle \right\|^2 \right). \tag{5.4}$$

Lema 5.1.2

$$F_{dec}(T) = 2 - \frac{2}{T+1} \sum_{t=0}^{T} \big\langle \psi(0) \big| \bar{U}_{dec}^{t} \big| \psi(0) \big\rangle. \tag{5.5}$$

Prova Expandindo a Eq. (5.4) e usando que a condição inicial e os operadores de evolução são reais, obtemos

$$\begin{aligned}
F_{dec}(T) &= \sum_{\vec{P}_T} Pr(\vec{P}_T) \left(\frac{1}{T+1} \sum_{t=0}^{T} \left(2 - 2 \big\langle \psi(0) \big| U_{\vec{P}_t} \big| \psi(0) \big\rangle \right) \right) \\
&= \frac{1}{T+1} \sum_{t=0}^{T} \left(2 - 2 \big\langle \psi(0) \big| \left(\sum_{\vec{P}_T} Pr(\vec{P}_T) U_{\vec{P}_t} \right) \big| \psi(0) \big\rangle \right).
\end{aligned} \tag{5.6}$$

Usando o Lema 5.1.1, nós obtemos a Eq. (5.5). ∎

Agora, podemos definir naturalmente o tempo de alcance quântico descoerente (*decoherent quantum hitting time*), usando a expressão de F_{dec} obtida no Lema 5.1.2.

Definição 5.1.1 O tempo de alcance quântico descoerente $H_{P,M}^{dec}$ de um passeio quântico com operador de evolução U_P dado pela Eq. (1.16) e condição inicial $\big|\psi(0)\big\rangle$ descrita pela Eq. (2.2) é definido como o menor número de passos T tal que

$$F_{dec}(T) \geq 1 - \frac{m}{n}. \tag{5.7}$$

Note que quando $p = 0$, nós temos a definição original, veja Definição 2.1, já que $\bar{U}_{dec} = U_{P'}$.

5.2 Limiar para o tempo de alcance quântico descoerente

É importante mencionar que estamos considerando cadeias de Markov ergódicas com matrizes de probabilidade simétricas. Dessa forma, o resultado a seguir generaliza o resultado de Szegedy (2004), Teorema 2.3.1, introduzindo um termo de descoerência.

Teorema 5.2.1 O tempo de alcance quântico descoerente $H_{P,M}^{dec}$ de um passeio quântico com operador de evolução U_P, dado pela Eq. (1.16), condição inicial $\big|\psi(0)\big\rangle$, e $p \leq \frac{1}{400 a_c E}$, onde

$$E = \frac{1}{1 - \frac{m}{n}} \sum_{k=1}^{n-m} \frac{\nu_k^2}{\arccos(\lambda'_k)}, \tag{5.8}$$

é no máximo

$$\frac{8}{1 - \frac{m}{n}} \sum_{k=1}^{n-m} \frac{\nu_k^2}{\sqrt{1 - \lambda'_k}} + \frac{1434\, a_c\, p}{\left(1 - \frac{m}{n}\right)^2} \left(\sum_{k=1}^{n-m} \frac{\nu_k^2}{\sqrt{1 - \lambda'_k}} \right)^2. \tag{5.9}$$

Prova Usando a expressão (5.9) e substituindo λ'_k por $\cos\theta_k$, defina

$$T(p) = 8\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\sqrt{1-\cos\theta_k}} + 1434a_cp\left(\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\sqrt{1-\cos\theta_k}}\right)^2, \quad (5.10)$$

onde $\epsilon = \frac{m}{n}$. A partir de agora, vamos omitir a dependência de p para o tempo T. Usando que $1-\cos\alpha \geq 2\alpha^2/5$ ($\alpha \in (0, \pi/2]$), obtemos que

$$T \leq 13\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\theta_k} + 3585a_cp\left(\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\theta_k}\right)^2. \quad (5.11)$$

Da relação $1-\cos\alpha \leq \alpha^2$, obtemos

$$T \geq 8\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\theta_k} + 1434a_cp\left(\sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\theta_k}\right)^2. \quad (5.12)$$

E usando que $E = \sum_{k=1}^{n-m}\frac{\nu_k^2}{(1-\epsilon)\theta_k}$, temos

$$8E + 1434a_cpE^2 \leq T \leq 13E + 3585a_cpE^2. \quad (5.13)$$

A condição inicial pode ser escrita como $\big|\psi(0)\big\rangle = \big|\psi_{M^\perp}\big\rangle + \big|\psi_M\big\rangle$, onde

$$\big|\psi_{M^\perp}\big\rangle = \frac{1}{\sqrt{n}}\sum_{\substack{x\in X\setminus M\\ y\in X}}\sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle, \quad (5.14)$$

$$\big|\psi_M\big\rangle = \frac{1}{\sqrt{n}}\sum_{\substack{x\in M\\ y\in X}}\sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle. \quad (5.15)$$

Note que $\|\big|\psi_{M^\perp}\big\rangle\|^2 = 1-\epsilon$, $\|\big|\psi_M\big\rangle\|^2 = \epsilon$ e $\big\langle\psi_M\big|\psi_{M^\perp}\big\rangle = 0$. Além disso, podemos escrever $\big|\psi_{M^\perp}\big\rangle$ como

$$\big|\psi_{M^\perp}\big\rangle = \sum_{k=1}^{n-m}\nu_k A\big|v_k\big\rangle. \quad (5.16)$$

Lembre que em decorrência do Teorema 1.3.1, que apresenta a decomposição espectral do operador de evolução, o subespaço gerado pelos vetores $A\big|w_k\big\rangle$ e $B\big|v_k\big\rangle$ é invariante sob a ação de $U_{P'}$. Além disso, $\big\langle w_k\big|A^\dagger B\big|v_k\big\rangle = \cos\theta_k$, ou seja o ângulo

entre esses dois vetores é θ_k. Mais ainda, a aplicação do operador de evolução realiza duas reflexões em dois eixos diferentes, o que equivale a realizar uma rotação cujo ângulo é o dobro do ângulo entre esses eixos.

Nós queremos mostrar que $F_{dec}(T)$ é maior ou igual a $1-\frac{m}{n}$ quando T está no intervalo (5.13). Usando a Eq. (5.6) e $\big|\psi(0)\big\rangle = \big|\psi_{M^\perp}\big\rangle + \big|\psi_M\big\rangle$, podemos reescrever $F_{dec}(T)$ como

$$F_{dec}(T) = 2 - 2(G_M + G_{M,M^\perp} + G_{M^\perp}), \tag{5.17}$$

onde

$$G_M = \frac{1}{T+1}\sum_{\vec{P}_T} Pr(\vec{P}_T) \sum_{t=0}^{T} \big\langle \psi_M \big| U_{\vec{P}_t} \big| \psi_M \big\rangle, \tag{5.18}$$

$$G_{M,M^\perp} = \frac{1}{T+1}\sum_{\vec{P}_T} Pr(\vec{P}_T) \sum_{t=0}^{T} \left(\big\langle \psi_{M^\perp} \big| U_{\vec{P}_t} \big| \psi_M \big\rangle + \big\langle \psi_M \big| U_{\vec{P}_t} \big| \psi_{M^\perp} \big\rangle \right) \tag{5.19}$$

$$G_{M^\perp} = \frac{1}{T+1}\sum_{\vec{P}_T} Pr(\vec{P}_T) \sum_{t=0}^{T} \big\langle \psi_{M^\perp} \big| U_{\vec{P}_t} \big| \psi_{M^\perp} \big\rangle. \tag{5.20}$$

Vamos estabelecer cotas para G_M, $G_{M,M^\perp}$ e $G_{M^\perp}$:

$$G_M \leq \frac{1}{T+1}\sum_{\vec{P}_T} Pr(\vec{P}_T) \sum_{t=0}^{T} \big\langle \psi_M \big| \psi_M \big\rangle = \epsilon, \tag{5.21}$$

pois $U_{\vec{P}_t}$ é unitário. A Expressão (5.19) pode ser expandida em dois termos

$$\begin{aligned} G_{M,M^\perp} = {} & \frac{1}{T+1} Pr\left(\vec{P}_T = (P', \ldots, P')\right) \sum_{t=0}^{T} \left(\big\langle \psi_{M^\perp} \big| U_{P'}^t \big| \psi_M \big\rangle + \big\langle \psi_M \big| U_{P'}^t \big| \psi_{M^\perp} \big\rangle \right) \\ & + \frac{1}{T+1} \sum_{\vec{P}_T \neq (P', \ldots, P')} Pr(\vec{P}_T) \sum_{t=0}^{T} \left(\big\langle \psi_{M^\perp} \big| U_{\vec{P}_t} \big| \psi_M \big\rangle + \big\langle \psi_M \big| U_{\vec{P}_t} \big| \psi_{M^\perp} \big\rangle \right). \end{aligned} \tag{5.22}$$

O primeiro termo da Eq. (5.22) é zero porque $\big|\psi_{M^\perp}\big\rangle$ se encontra no espaço gerado por $A\big|w_k\big\rangle$ e $B\big|v_k\big\rangle$, que é invariante sob a ação de $U_{P'}$ e, dessa forma, $\big\langle \psi_{M^\perp} \big| U_{P'}^t \big| \psi_M \big\rangle + \big\langle \psi_M \big| U_{P'}^t \big| \psi_{M^\perp} \big\rangle = 0$. Cada vez que aplicamos o operador de evolução a $\big|\psi_{M^\perp}\big\rangle$ realizamos uma rotação cujo ângulo é o dobro do ângulo entre os eixos

de reflexão. Quando fazemos $\langle\psi_{M^\perp}|U^t_{P'}$, estamos aplicando as duas reflexões em ordem diferente, ou seja, $\mathcal{R}_\mathcal{A}\mathcal{R}_\mathcal{B}$, ao invés de, $\mathcal{R}_\mathcal{B}\mathcal{R}_\mathcal{A}$ e, assim, realizamos uma rotação no sentido contrário, o que implica que $\langle\psi_{M^\perp}|U^t_{P'}|\psi_M\rangle = -\langle\psi_M|U^t_{P'}|\psi_{M^\perp}\rangle$. A Figura 5.3 é apenas uma ilustração exemplificando o que acontece nesse caso.

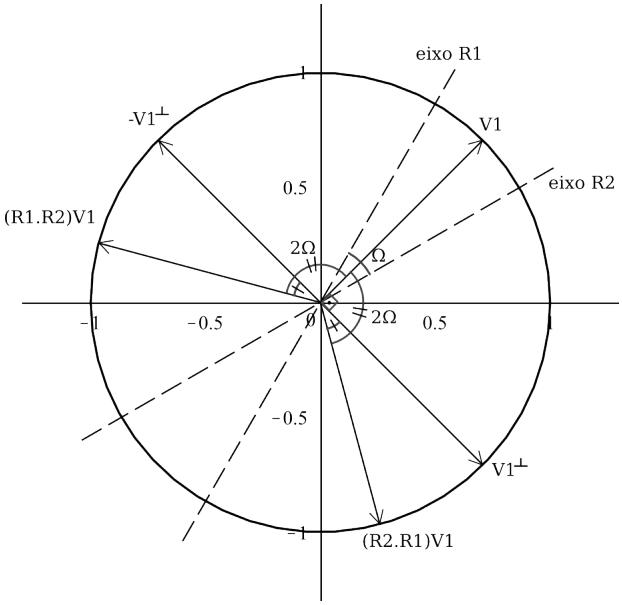


Figura 5.3: *Ilustração da aplicação de duas reflexões $R1$ e $R2$ no vetor $V1$. O ângulo entre os eixos de rotação é Ω. A aplicação das duas reflexões em $V1$ faz uma rotação de 2Ω. Podemos observar que o ângulo entre $V1^\perp$ e $(R2.R1)V1$ é o mesmo ângulo formado entre $-V1^\perp$ e $(R1.R2)V1$.*

Para o segundo termo de $G_{M,M^\perp}$, tomando $\epsilon \leq 1/2$, temos

$$\begin{aligned}\langle\psi_{M^\perp}|U_{\vec{P}_t}|\psi_M\rangle + \langle\psi_M|U_{\vec{P}_t}|\psi_{M^\perp}\rangle &\leq 2\max\left\{\langle\psi_M|\psi_M\rangle, \langle\psi_{M^\perp}|\psi_{M^\perp}\rangle\right\} \\ &= 2\max\{\epsilon, 1-\epsilon\} \\ &= 2(1-\epsilon).\end{aligned} \tag{5.23}$$

Assim, usando que $(1-p)^{a_cT} = 1 - a_cpT + \frac{a_cTp^2}{2}(a_cT-1) + O(p^3)$, temos

$$G_{M,M^\perp} \leq 2(1-\epsilon)(1-(1-p)^{a_cT}) \leq 2(1-\epsilon)a_cpT. \tag{5.24}$$

Finalmente, vamos estabelecer um limite para $G_{M^\perp}$,

$$\begin{aligned} G_{M^\perp} &= \frac{1}{T+1} Pr(\vec{P}_T = (P', \ldots, P')) \sum_{t=0}^{T} \left\langle \psi_{M^\perp} \middle| U_{P'}^t \middle| \psi_{M^\perp} \right\rangle + \qquad (5.25) \\ &\quad \frac{1}{T+1} \sum_{\vec{P}_T \neq (P', \ldots, P')} Pr(\vec{P}_T) \sum_{t=0}^{T} \left\langle \psi_{M^\perp} \middle| U_{\vec{P}_t} \middle| \psi_{M^\perp} \right\rangle \\ &\leq \frac{(1-\epsilon)(1-p)^{a_c T}}{T+1} \sum_{k=1}^{n-m} \frac{\nu_k^2}{1-\epsilon} \sum_{t=0}^{T} \cos(2t\theta_k) + \qquad (5.26) \\ &\quad (1-\epsilon)(1-(1-p)^{a_c T}). \end{aligned}$$

Da Eq. (13) do artigo de Szegedy (2004), sabemos que

$$\frac{1}{T+1} \sum_{k=1}^{n-m} \frac{\nu_k^2}{1-\epsilon} \sum_{t=0}^{T} \cos(2t\theta_k) \leq \frac{1}{T+1} \sum_{k=1}^{n-m} \frac{4\nu_k^2}{(1-\epsilon)\theta_k}. \qquad (5.27)$$

Usando novamente a expansão em série de Taylor para $(1-p)^{a_c T}$ e que $\frac{4E}{T} \leq \frac{1}{2}$, obtido através da expressão (5.13), temos

$$\begin{aligned} G_{M^\perp} &\leq (1-\epsilon) \left((1-p)^{a_c T} \frac{4E}{T} + (1-(1-p)^{a_c T} \right) \\ &\leq (1-\epsilon) \left((1 - a_c p T) \frac{4E}{T} + a_c p T \right). \end{aligned} \qquad (5.28)$$

A partir das Eqs. (5.21), (5.24), e (5.28), obtemos

$$G_M + G_{M,M^\perp} + G_{M^\perp} \leq \epsilon + (1-\epsilon) \left(\frac{4E}{T} - 4a_c p E + 3 a_c p T \right). \qquad (5.29)$$

Usando que T pertence ao intervalo (5.13),

$$\frac{4E}{T} - 4a_c p E + 3 a_c p T \leq \frac{1}{2(1 + 179.25 a_c p E)} + 35 a_c p E + 10755 a_c^2 p^2 E^2 \leq \frac{1}{2}, \qquad (5.30)$$

se escolhermos $p \leq \frac{1}{400 a_c E}$. Então, temos

$$G_M + G_{M,M^\perp} + G_{M^\perp} \leq \frac{\epsilon + 1}{2}, \qquad (5.31)$$

e, portanto,

$$F_{dec}(T) \geq 2 - 2\left(\frac{\epsilon+1}{2}\right) = 1 - \epsilon. \tag{5.32}$$

∎

Corolário 5.2.1 O tempo de alcance quântico descoerente $H^{dec}_{P,M}$ de U_P com respeito a qualquer $M \subseteq X$ com $m \leq n/2$ e $0 \leq p \leq \frac{1}{400a_cE}$, onde

$$E = \frac{1}{1-\frac{m}{n}} \sum_{k=1}^{n-m} \frac{\nu_k^2}{\arccos(\lambda'_k)},$$

é da ordem $O\left(\frac{1}{\sqrt{1-\lambda(P_M)}}\right)$, onde $\lambda(P_M)$ é o maior autovalor de P_M.

Prova Usando que $1 - \cos\alpha \geq 2\alpha^2/5$, obtemos

$$E \geq \frac{1}{2} \sum_{k=1}^{n-m} \frac{\nu_k^2}{1-\epsilon} \sqrt{\frac{1}{1-\cos\theta_k}} \tag{5.33}$$

e

$$p \leq \frac{1}{200a_c \sum_{k=1}^{n-m} \frac{\nu_k^2}{1-\epsilon}\sqrt{\frac{1}{1-\lambda'_k}}}. \tag{5.34}$$

Substituindo a Eq. (5.34) pela expressão de $H^{dec}_{P,M}$ dada por (5.9) e como

$$\sum_k^{n-m} \nu_k^2 \sqrt{\frac{1}{1-\lambda'_k}} \leq \sqrt{\sum_k^{n-m} \frac{\nu_k^2}{1-\lambda'_k}} \leq \sqrt{\frac{1}{1-\lambda(P_M)}}, \tag{5.35}$$

concluímos que $H^{dec}_{P,M}$ é $O\left(\frac{1}{\sqrt{1-\lambda(P_M)}}\right)$. ∎

A expressão (5.9) do Teorema 5.2.1 mostra que o tempo de alcance quântico descoerente apresenta um termo adicional que é proporcional ao quadrado do termo usual. Se p for pequeno o suficiente, a contribuição do novo termo para o tempo de alcance cresce como uma função linear em termos de p. O Corolário 5.2.1 descreve um intervalo de p tal que o ganho quadrático ainda é válido.

5.3 O problema de detecção

É importante notar que em computação quântica, detectar e encontrar um elemento marcado são problemas substancialmente diferentes, ao contrário do que acontece geralmente na computação clássica (Magniez et al., 2009). Szegedy (2004) desenvolveu um algoritmo de detecção para cadeias de Markov ergódicas e simétricas que tem complexidade de tempo da ordem do tempo de alcance quântico.

Para identificar o porquê de as vezes precisarmos apenas detectar se o conjunto de elementos marcados é vazio ou não, considere o problema da distinção de elementos (*element distinctness*). Dado um conjunto de elementos, $\{x_1, \ldots, x_N\}$, queremos saber se todos os elementos são, ou não distintos, ou seja, queremos saber se existem i,j com $i \neq j$ tal que $x_i = x_j$. O melhor algoritmo clássico tem complexidade $O(N \log N)$ e é resolvido fazendo a ordenação dos elementos. Dessa forma, se existirem dois elementos iguais, eles estarão em posições adjacentes. Ambainis (2004) desenvolveu um algoritmo quântico para resolver esse problema, utilizando um passeio quântico num grafo de Johnson,[1] com complexidade $O\left(N^{\frac{2}{3}}\right)$, atingindo o limite inferior, mostrado por Shi (2002). O algoritmo de detecção de Szegedy também pode ser utilizado para resolver esse problema utilizando o grafo de Johnson e apresentando a mesma complexidade, $O\left(N^{\frac{2}{3}}\right)$ (Itakura, 2008).

Então, seja $J_{N,r,r-1}$ o grafo de Johnson cujos vértices são subconjuntos de tamanho r de um conjunto com N elementos e cujas arestas conectam vértices cujo tamanho de sua intersecção é $r-1$. Um vértice do grafo é marcado se ele contém um par de elementos iguais. Na Figura (5.4), vemos um exemplo de um grafo de Johnson, $J_{4,2,1}$. Então, nesse caso, saber se o conjunto de elementos marcados é vazio ou não determina se todos os elementos do dado conjunto são todos distintos ou não, resolvendo o problema da distinção de elementos.

[1] Grafo cujos vértices são subconjuntos de um conjunto fixo e cujas arestas conectam vértices que diferem num determinado número de elementos.

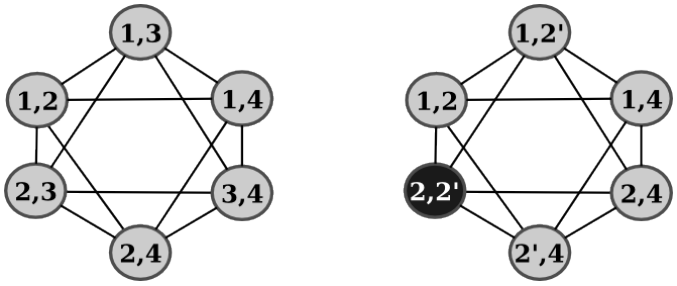


Figura 5.4: *Grafos de Johnson, $J_{4,2,1}$. No grafo da esquerda, os vértices são subconjuntos de tamanho 2 do seguinte conjunto $\{1,2,3,4\}$. No grafo da direita, os vértices são subconjuntos de tamanho 2 do seguinte conjunto $\{1,2,2,4\}$ e o vértice $(2,2')$ é marcado, utilizamos $2'$ para distinguir no grafo os dois elementos que são iguais. Dois vértices estão conectados se a intersecção entre eles possui 1 elemento apenas.*

5.3.1 Descoerência no algoritmo de detecção de Szegedy

Seja $\mathcal{M} \subseteq 2^X$ um conjunto de subconjuntos não-vazios de M. O problema de detecção determina se o conjunto de elementos marcado é vazio ou pertence a $\mathcal{M}$.

Teorema 5.3.1 Suponha que T é um limite superior para

$$16 \sum_{k=1}^{n-|M|} \frac{\nu_k^2}{\sqrt{1-\lambda_k'}} + 5736 a_c p \left(\sum_{k=1}^{n-|M|} \frac{\nu_k^2}{\sqrt{1-\lambda_k'}} \right)^2 , \tag{5.36}$$

onde M corre sobre todos os elementos de $\mathcal{M}$ (λ_k' e ν_k dependem de M) e p obedece a mesma inequação do Teorema 5.2.1. Neste caso, o problema de detecção pode ser resolvido em tempo T com *bounded two-sided error*.

Selecionando $0 \leq t \leq T$ aleatoriamente, o Algoritmo 1 cria o estado

$$\frac{1}{2}|0\rangle \left(|\psi(0)\rangle + U_t U_{t-1} \dots U_1 |\psi(0)\rangle \right) + \frac{1}{2}|1\rangle \left(|\psi(0)\rangle - U_t U_{t-1} \dots U_1 |\psi(0)\rangle \right) , \tag{5.37}$$

onde $U_1, \dots, U_t$ são os operadores unitários obtidos pela dinâmica da descoerência e o primeiro registrador é um registrador de controle adicional, de um qubit. Depois ele faz uma medição na base computacional e, a partir do resultado obtido no registrador de controle, ele identifica se $M = \emptyset$ ou $M \in \mathcal{M}$.

Algoritmo 1: *Detecta se marcado*

Entrada: $U_1, \ldots, U_t$
Saída: 0 ($M = \emptyset$) ou 1 ($M \in \mathcal{M}$)

```
1  início
2      prepare o estado: |0⟩|ψ(0)⟩;
3      aplique H no registrador de controle;
4      aplique C(U_1), ..., C(U_t), onde C(U) é o U-controlado;
5      aplique H no registrador de controle;
6      meça na base computacional;
7      se o registrador de controle for 1 então
8          retorna 1
9      senão
10         retorna 0
```

Em mais detalhes, o algoritmo começa no estado inicial

$$\big|\psi_1\big\rangle = \big|0\big\rangle \otimes \big|\psi(0)\big\rangle. \tag{5.38}$$

Na Linha 3, aplicamos H (porta Hadamard[2]) no registrador de controle, transformando $\big|\psi_1\big\rangle$ em

$$\big|\psi_2\big\rangle = (H \otimes I)\big|\psi_1\big\rangle = \frac{1}{\sqrt{2}}\big|0\big\rangle\big|\psi(0)\big\rangle + \frac{1}{\sqrt{2}}\big|1\big\rangle\big|\psi(0)\big\rangle. \tag{5.39}$$

Depois, seguimos para a Linha 4, aplicando os operadores $U_1, \ldots, U_t$ no estado que contém o registrador de controle igual a $\big|1\big\rangle$ (equivalente a aplicar o operador U_i-controlado):

$$\big|\psi_3\big\rangle = C(U_t)\ldots C(U_1)\big|\psi_2\big\rangle = \frac{1}{\sqrt{2}}\big|0\big\rangle\big|\psi(0)\big\rangle + \frac{1}{\sqrt{2}}\big|1\big\rangle U_t \ldots U_1\big|\psi(0)\big\rangle. \tag{5.40}$$

Em seguida, na Linha 5, aplicamos H no registrador de controle:

$$\begin{aligned}\big|\psi_4\big\rangle = (H \otimes I)\big|\psi_3\big\rangle &= \frac{1}{2}\left(\big|0\big\rangle + \big|1\big\rangle\right)\big|\psi(0)\big\rangle + \frac{1}{2}\left(\big|0\big\rangle - \big|1\big\rangle\right) U_t \ldots U_1\big|\psi(0)\big\rangle \\ &= \frac{1}{2}\big|0\big\rangle\left(\big|\psi(0)\big\rangle + U_t \ldots U_1\big|\psi(0)\big\rangle\right) + \frac{1}{2}\big|1\big\rangle\left(\big|\psi(0)\big\rangle - U_1 \ldots U_t\big|\psi(0)\big\rangle\right).\end{aligned} \tag{5.41}$$

[2] Operador unitário descrito por $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Fazendo a medição na base computacional do estado $\big|\psi_4\big\rangle$, as probabilidades de obter o registrador de controle no estado 0 ou 1 são

$$P^{(0)} = \frac{1}{4}\Big|\Big|\big|\psi(0)\big\rangle + U_tU_{t-1}\ldots U_1\big|\psi(0)\big\rangle\Big|\Big|^2, \tag{5.42}$$

$$P^{(1)} = \frac{1}{4}\Big|\Big|\big|\psi(0)\big\rangle - U_tU_{t-1}\ldots U_1\big|\psi(0)\big\rangle\Big|\Big|^2. \tag{5.43}$$

Vamos analisar o que acontece após realizada a medição (Linha 6). Note que, quando usamos o Algoritmo 1, não sabemos qual dos dois operadores, U_P ou $U_{P'}$, estão sendo usados. Então, se $M = \emptyset$, o registrador de controle estará no estado $\big|0\big\rangle$ com probabilidade de pelo menos $(1-p)^{a_cT}$, que é a probabilidade de termos $U = U_P$. Pois, como sabemos $U_P\big|\psi(0)\big\rangle = \big|\psi(0)\big\rangle$ e, nesse caso, teremos $\big|\psi(0)\big\rangle - U_tU_{t-1}\ldots U_1\big|\psi(0)\big\rangle = 0$ o que torna a probabilidade de obter o registrador de controle no estado $\big|1\big\rangle$ igual a zero.

Caso $M \in \mathcal{M}$, o registrador de controle estará no estado $\big|1\big\rangle$ com probabilidade de pelo menos

$$\frac{1}{4(T+1)}\sum_{\vec{P}_T} Pr(\vec{P}_T)\sum_{t=0}^{T}\Big|\Big|\big|\psi(0)\big\rangle - U_{\vec{P}_t}\big|\psi(0)\big\rangle\Big|\Big|^2 \geq \frac{1}{4}\left(1-\frac{m}{n}\right). \tag{5.44}$$

A Eq. (5.44) é obtida da Eq. (5.43) fazendo duas médias: uma no tempo, porque o algoritmo seleciona um tempo t aleatoriamente, e outra média sobre as possíveis sequências $\vec{P}_T$, já que o algoritmo pode ser afetado pela descoerência. Portanto, usando que $\frac{m}{n} \leq \frac{1}{2}$, nós obteremos 1 no registrador de controle com probabilidade de pelo menos $\frac{1}{8}$, o que significa que temos pelo menos um elemento marcado.

Esse resultado pode ser melhorado se considerarmos o modelo de descoerência que permite apenas a remoção de arestas do grafo (inserções não são permitidas). Podemos resolver o problema de detecção com tempo T com *bounded one-sided error*, pois a condição inicial será invariante sob a ação de qualquer U_{P_i} quando M é vazio, como podemos ver pelo Lema 5.3.1. Nesse caso, $\big|\psi(0)\big\rangle - U_tU_{t-1}\ldots U_1\big|\psi(0)\big\rangle = 0$ e a probabilidade de obter $\big|0\big\rangle$ no registrador de controle quando não há nenhum vértice marcado será 1.

Lema 5.3.1 Seja P um grafo obtido através da remoção de arestas do grafo Q, simétrico. Seja $\big|\psi(0)\big\rangle$ a condição inicial associada ao grafo Q, ou seja,

$$\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y\in X} \sqrt{q_{xy}}\big|x,y\big\rangle. \tag{5.45}$$

Então,

$$U_P\big|\psi(0)\big\rangle = \big|\psi(0)\big\rangle. \tag{5.46}$$

Prova A partir da definição do operador de evolução, vide Eq. (1.16), podemos obter as componentes da sua matriz:

$$\big\langle a,b\big|U_P\big|c,d\big\rangle = 4\sqrt{p_{ad}p_{da}p_{ab}p_{dc}} - 2\delta_{ac}\sqrt{p_{ab}p_{cd}} - 2\delta_{bd}\sqrt{p_{ba}p_{dc}} + \delta_{ac}\delta_{bd}. \tag{5.47}$$

As componentes da condição inicial são

$$\big\langle a,b\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y\in X} \sqrt{q_{xy}}\big\langle a,b\big|x,y\big\rangle = \sqrt{\frac{q_{ab}}{n}}. \tag{5.48}$$

Queremos mostrar que $\big\langle a,b\big|U_P\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}}\sqrt{q_{ab}}$. Usando as Eqs. (5.47) e (5.48), temos

$$\begin{aligned}
\big\langle a,b\big|U_P\big|\psi(0)\big\rangle &= \sum_{c,d\in X} \big\langle a,b\big|U_P\big|c,d\big\rangle\big\langle c,d\big|\psi(0)\big\rangle \\
&= \frac{1}{\sqrt{n}}\left(4\sqrt{p_{ab}}\sum_{d\in X}\sqrt{p_{ad}p_{da}}\sum_{c\in X}\sqrt{p_{dc}q_{dc}} - \right. \\
&\left. - 2\sqrt{p_{ab}}\sum_{d\in X}\sqrt{p_{ad}q_{ad}} - 2\sqrt{p_{ba}}\sum_{c\in X}\sqrt{p_{bc}q_{bc}} + \sqrt{q_{ab}}\right).
\end{aligned} \tag{5.49}$$

Até agora usamos apenas o fato que Q é simétrico. Considere $\deg_P(x)$, o grau do vértice x no grafo P. Lembrando que,

$$p_{xy} = \begin{cases} \dfrac{1}{\deg_P(x)}, & \text{se } (x,y) \text{ é uma aresta do grafo;} \\ 0, & \text{caso contrário;} \end{cases} \tag{5.50}$$

e como P é obtido de Q através da remoção de arestas, note que,

$$\sum_{y\in X}\sqrt{p_{xy}q_{xy}} = \min\{\deg_P(x),\deg_Q(x)\}\sqrt{\frac{1}{\deg_P(x)\deg_Q(x)}} = \sqrt{\frac{\deg_P(x)}{\deg_Q(x)}}. \quad (5.51)$$

O grafo Q é simétrico e, portanto, todos os vértices tem o mesmo grau. Denotaremos, $\deg_Q(x) = \deg_Q \forall x \in X$. Dessa forma,

$$\begin{aligned}\big\langle a,b\big|U_P\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}}\Bigg(4\sqrt{p_{ab}}\sum_{d\in X}\sqrt{p_{ad}p_{da}}\sqrt{\frac{\deg_P(d)}{\deg_Q}} - \\ - 2\sqrt{p_{ab}}\sqrt{\frac{\deg_P(a)}{\deg_Q}} - 2\sqrt{p_{ba}}\sqrt{\frac{\deg_P(b)}{\deg_Q}} + \sqrt{q_{ab}}\Bigg).\end{aligned} \quad (5.52)$$

Com mais alguma manipulação algébrica podemos checar que

$$\big\langle a,b\big|U_P\big|\psi(0)\big\rangle = \sqrt{\frac{q_{ab}}{n}}. \quad (5.53)$$

∎

5.4 Simulações

Considerando o modelo de descoerência apresentado anteriormente, simulações computacionais foram feitas para a evolução do passeio quântico, sob a ação da descoerência, no ciclo, grafo completo, hipercubo e malha bidimensional com condições de contorno periódicas. É importante mencionar que não implementamos o operador $\bar{U}_{dec}$ porque ele necessita de um custo computacional exponencial que está relacionado ao número de possíveis configuração do grafo, $O(2^{a_c})$. Então, a cada passo de tempo nós obtemos uma matriz estocástica P_i que depende da probabilidade de descoerência p. O operador de evolução, $U_{P_i'}$, é criado a cada passo e, o tempo de alcance quântico é calculado numericamente seguindo a Definição 2.1. Nesse caso, $\big|\psi(t)\big\rangle$ é descrito por

$$\big|\psi(t)\big\rangle = U_{P_t}\ldots U_{P_1}\big|\psi(0)\big\rangle = U_{\vec{P}_t}\big|\psi(0)\big\rangle, \quad (5.54)$$

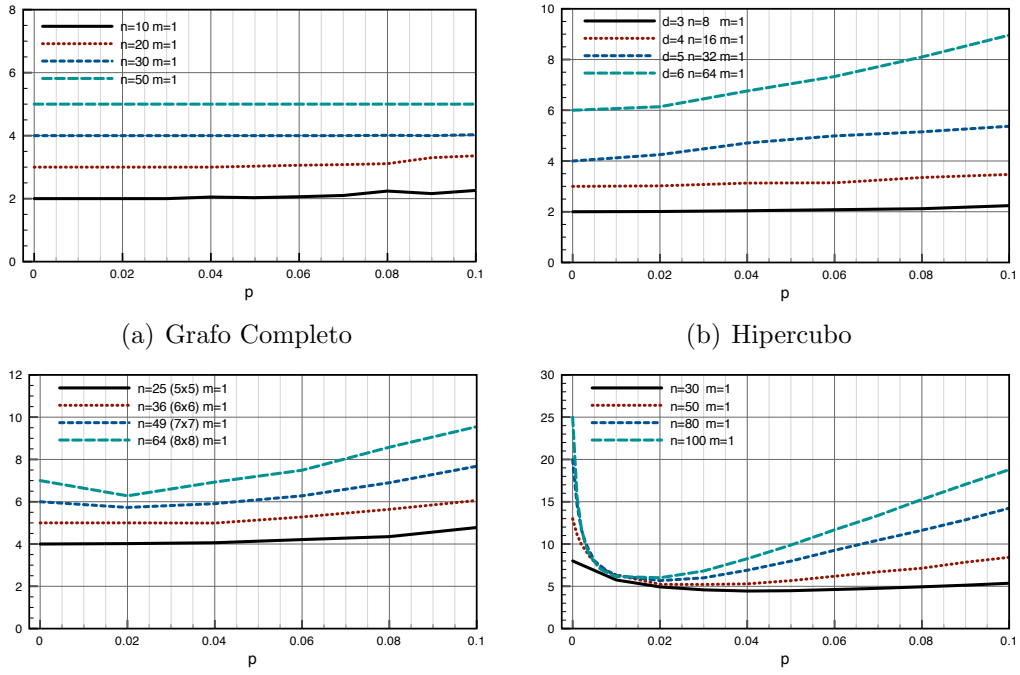
e a expressão para $F(T)$ é dada por

$$F(T) = \frac{1}{T+1} \sum_{t=0}^{T} \left\| U_{\vec{P}_t} |\psi(0)\rangle - |\psi(0)\rangle \right\|^2. \tag{5.55}$$

Seja $H_{\vec{P}_t,M} = F^{-1}(1 - m/n)$, fazemos uma média de 100 aplicações da dinâmica do modelo de descoerência na evolução do passeio quântico, ou seja, dado que a aplicação j gera uma sequência $\vec{P}_t^{\,j}$, fazemos

$$HT_{avg} = \frac{1}{100} \sum_{j=1}^{100} H_{\vec{P}_t^{\,j},M}. \tag{5.56}$$

A Figura 5.5 apresenta as médias do tempo de alcance quântico, HT_{avg}, para o grafo completo, hipercubo, malha bidimensional e ciclo, variando os valores de n e p.



(a) Grafo Completo

(b) Hipercubo

(c) Malha bidimensional

(d) Ciclo

Figura 5.5: *Média dos tempos de alcance quântico, HT_{avg}, para o grafo completo, hipercubo, malha bidimensional e ciclo, variando os valores de n. A probabilidade de descoerência $p \in [0, 0.1]$.*

Para o grafo completo, o tempo de alcance quântico permanece praticamente o mesmo para o intervalo de p selecionado. Já para o hipercubo, o intervalo de

p em que o tempo de alcance permanece o mesmo é menor que no grafo completo. O caso do ciclo é diferente dos demais. Podemos observar que o tempo de alcance quântico diminuiu assim que admitimos uma pequena probabilidade de descoerência afetando o sistema. Por exemplo, quando $n = 100$, o menor valor é atingido quando $p = 0.02$. Nesse caso, $HT_{avg} \simeq 6.01$, enquanto que, para $p = 0$, $HT_{avg} = H_{P,M} = 25$. O tempo de alcance quântico voltará a crescer quando p aumentar. Para o caso da malha bidimensional podemos observar que o tempo de alcance quântico começa a decrescer um pouco quando aumentamos o valor de n. É possível que para valores de n maiores possamos observar um comportamento similar ao do ciclo.

É importante mencionar que os gráficos da Figura 5.5 apresentarão comportamento similar se fizermos $m > 1$. Além disso, para $p > 0.1$, o comportamento do tempo de alcance quântico será o mesmo para todos os casos. Já que ele crescerá e irá para o infinito quando $p = 1$. Como exemplo, podemos ver na Figura 5.6 o que acontece para o ciclo num intervalo maior de p.

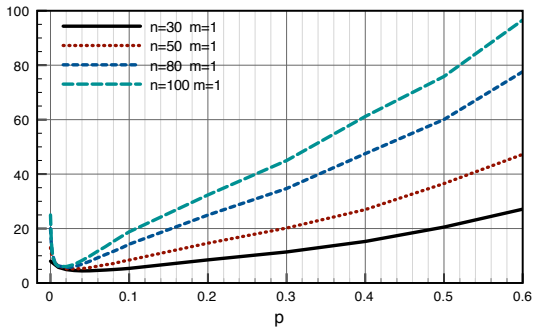


Figura 5.6: *Média dos tempos de alcance quântico, HT_{avg}, para o ciclo.*

O caso em que $p = 1$ pode ser estudado analiticamente e expressa o tempo de alcance no complemento do grafo original, $\bar{P}$, como podemos ver na Proposição 5.4.1. A condição inicial associada ao grafo original é invariante sob a ação do operador de evolução, nesse caso. Isso ocorre porque a condição inicial é uma superposição sobre todas as arestas do grafo original e essas arestas não existem em seu complemento.

Proposição 5.4.1 $U_{\bar{P}'}\big|\psi(0)\big\rangle = \big|\psi(0)\big\rangle$, onde $\bar{P}$ é o complemento de P e

$$\big|\psi(0)\big\rangle = \frac{1}{\sqrt{n}}\sum_{x\in X}\big|\Phi_x\big\rangle = \frac{1}{\sqrt{n}}\sum_{y\in X}\big|\Psi_y\big\rangle = \frac{1}{\sqrt{n}}\sum_{x,y\in X}\sqrt{p_{xy}}\big|x,y\big\rangle. \tag{5.57}$$

Prova Seja

$$U_{\bar{P}'} = \left(2\sum_{y\in X}\big|\bar{\Psi}_y\big\rangle\big\langle\bar{\Psi}_y\big| - I\right)\left(2\sum_{x\in X}\big|\bar{\Phi}_x\big\rangle\big\langle\bar{\Phi}_x\big| - I\right). \tag{5.58}$$

Note que, se $\bar{p}'_{xy} \neq 0 \Rightarrow p_{xy} = 0$ e se $\bar{p}'_{xy} = 0 \Rightarrow p_{xy} \neq 0$, ou seja, $\bar{p}'_{xy}.p_{xy} = 0$. Assim, é fácil verificar que $\big\langle\Phi_x\big|\bar{\Phi}_{x'}\big\rangle = 0$ e $\big\langle\Psi_y\big|\bar{\Psi}_{y'}\big\rangle = 0$. Logo, a partir, de (5.57) e (5.58), vemos que, $U_{\bar{P}'}\big|\psi(0)\big\rangle = \big|\psi(0)\big\rangle$. ∎

5.4.1 Distribuição de probabilidade no ciclo

Como vimos no Capítulo 3, a probabilidade de encontrar um vértice marcado após realizada a medição é dada por

$$p_M(t) = \big\langle\psi(t)\big|\mathcal{P}_M\big|\psi(t)\big\rangle, \tag{5.59}$$

onde

$$\mathcal{P}_M = \sum_{x=n-m+1}^{n}\big|x\big\rangle\big\langle x\big| \otimes I_n. \tag{5.60}$$

De acordo com a Seção 3.4, na evolução do passeio quântico no ciclo, a distribuição de probabilidades nos vértices do grafo permanece invariante, $p_M(t) = \frac{m}{n}$. Ao permitir a ação da descoerência no sistema podemos ver na Figura 5.7 que a probabilidade aumenta nos primeiros instantes de tempo. Esse gráfico mostra o caso do ciclo para $n = 100$ and $m = 1$. A probabilidade p_M alcança o seu valor máximo para $t = 12$ e $p = 0.1$. Nesse caso, $p_M(12) \simeq 0.063$.

O tempo de alcance quântico está associado a uma quantidade que pode ser interpretada como uma média sobre as distâncias entre duas distribuições de probabilidades, a distribuição do estado do passeio quântico no tempo t e a distribuição do estado inicial. Dessa forma, a Figura 5.7 explica o comportamento da

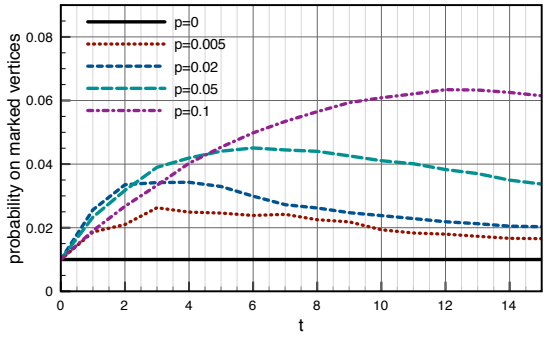


Figura 5.7: *Probabilidade nos elementos marcados, $p_M(t)$, para o ciclo com $n = 100$ e $m = 1$.*

Figura 5.5(d), em que o valor do tempo de alcance quântico diminui porque existe um aumento na probabilidade nos vértices marcados durante o início da evolução do passeio. Esse efeito é causado devido o modelo de descoerência permitir a inserção de arestas no grafo. É claro que depende do grafo também, pois como pudemos observar, esse comportamento não é visto para o hipercubo, por exemplo. Provavelmente, há relação com a conectividade do grafo.

Considerando o caso da Figura 5.7, para p maior que 0.1, o valor de p_M começa a decrescer novamente. Todas as curvas para os valores de p subsequentes estarão abaixo da curva para $p = 0.1$. Para $p = 1$, temos a mesma distribuição de probabilidade que em $p = 0$, que é $p_M(t) = \frac{m}{n}$, embora os dois casos apresentem diferentes valores para o tempo de alcance quântico. Quando $p = 1$, o tempo de alcance quântico vai para o infinito porque $\big|\psi(0)\big\rangle$ é um autovetor do operador de evolução, como explicado anteriormente. Para $p = 0$, embora os estados $\big|\psi(t)\big\rangle$ e $\big|\psi(0)\big\rangle$ tenham a mesma distribuição de probabilidade, eles são estados diferentes. Assim, é possível calcular o tempo de alcance quântico, como mostramos no Capítulo 3.

5.5 Conclusões

Nós propomos um modelo de descoerência inspirado em percolação no passeio quântico de Szegedy. Esse modelo é caracterizado pela possibilidade de remover ou inserir arestas a cada passo de tempo com probabilidade p. A matriz de proba-

bilidade associada ao grafo e o operador de evolução são passíveis de mudanças a cada passo de tempo. Definimos o tempo de alcance quântico descoerente usando um novo operador, que é obtido fazendo uma média sobre todos os possíveis operadores de evolução afetados pela descoerência. Note que quando a probabilidade de percolação p é zero, o operador de evolução é igual ao da definição original do Szegedy e o tempo de alcance quântico descoerente é igual ao tempo de alcance quântico original (Szegedy, 2004).

Provamos que, para p suficientemente pequeno, o tempo de alcance quântico descoerente apresenta um termo adicional que depende linearmente de p, preservando o ganho quadrático do tempo de alcance quântico com relação ao clássico. Além disso, o problema de detecção pode ser resolvido em tempo da ordem do tempo de alcance quântico descoerente com *bounded two-sided error*, e com *bounded one-sided error* se o modelo de descoerência não permitir a inserção de arestas.

Simulações do modelo de descoerência foram realizadas para o ciclo, grafo completo, hipercubo e malha bidimensional. Essas simulações são úteis para entender como o modelo de descoerência afeta o passeio quântico em determinados grafos e explica alguns efeitos que não aparecem no estudo analítico. O comportamento no ciclo é bem diferente dos demais grafos analisados. É possível que o modelo de descoerência beneficie a busca nesse grafo, já que a inserção de arestas contribuem com o aumento da probabilidade nos vértices marcados.

As publicações referentes a esse capítulo são:

- (Santos e Portugal, 2012a) - Decoherence in Szegedy's quantum walk. In: Proceedings of the XXXIV Congresso Nacional de Matemática Aplicada e Computacional, 2012;

- (Santos e Portugal, 2012b) - Simulations of quantum Markov chains on percolation graphs. In: Proceedings of IV WECIQ - Workshop-School of Computation and Quantum Information, 2012;

- (Santos et al., 2014) - Decoherence in quantum Markov chains. Quantum

Information Processing, 2014;

- (Santos e Portugal) - Quantum hitting time and percolation in the cycle. Artigo em preparação a ser submetido para International Journal of Quantum Information.

Capítulo 6

Avaliação de fórmulas booleanas

O primeiro algoritmo quântico a resolver o problema de avaliar uma fórmula booleana foi o algoritmo de Grover (1996), que pode ser formulado para computar o OU-lógico de N bits $x_1, \ldots, x_N$. Para isso, basta procurar pelo bit 1 nos bits de entrada. O algoritmo de Grover pode ser generalizado para calcular expressões mais gerais que utilizam o E-lógico e o OU-lógico (Buhrman et al., 1998; Hoyer et al., 2003). O algoritmo para avaliar fórmulas contendo operadores NÃO-E-lógico (NAND), baseado num passeio quântico de tempo contínuo, e utilizando o modelo de consulta quântica (*quantum query model*), foi desenvolvido por Farhi et al. (2008). A versão de tempo discreto foi proposta independentemente por Ambainis et al. (2007) e Childs et al. (2007b). Esses algoritmos foram depois generalizados por vários autores. Uma revisão pode ser encontrada em (Ambainis, 2010).

Estamos interessados no algoritmo quântico de Childs et al. (2007b) para o caso da árvore binária NÃO-E cheia. Esse algoritmo é baseado num passeio quântico numa árvore aumentada e utiliza o algoritmo quântico de estimação de fase (Mosca e Ekert, 1998) para distinguir o caso em que a fórmula é verdadeira e o caso em que a fórmula é falsa. Para N variáveis, ele avalia uma fórmula NÃO-E usando $O(\sqrt{N})$ consultas e requer $T = 320\lfloor\sqrt{N}\rfloor$ passos do passeio quântico. O algoritmo clássico requer tempo $O(N^{0.754})$ (Snir, 1985; Saks e Wigderson, 1986).

Através de simulações computacionais do algoritmo de Childs et al. (2007b), pretendemos analisar o seu comportamento executando apenas o passeio quântico

na árvore aumentada, sem aplicar o algoritmo de estimação de fase. Também vamos observar como certos tipos de consultas com falha afetam o comportamento do algoritmo. Um tipo de consulta com falha similar, aplicada ao algoritmo de Grover (1996), foi estudada por (Regev e Schiff, 2008) e (Ambainis et al., 2013). Eles mostraram que se a chamada ao oráculo tiver uma certa probabilidade de falhar, então o ganho do algoritmo quântico desaparece e ele se torna semelhante a uma busca exaustiva clássica.

6.1 Modelo

Considere uma fórmula booleana com N variáveis $x_1, x_2, \ldots, x_N$, onde cada variável aparece apenas uma vez na fórmula. Vamos representar o E (AND) por $\wedge$ e o NÃO-E (NAND) por $\overline{\wedge}$. Pelas regras da lógica booleana podemos substituir os operadores {NÃO, E, OU} por $\{\overline{\wedge}\}$. O operador $\overline{\wedge}$ é descrito, como segue. $y_1 \,\overline{\wedge}\, y_2 \,\overline{\wedge} \cdots \overline{\wedge}\, y_k$ retorna 1 se $y_1 \wedge y_2 \wedge \cdots \wedge y_k = 0$ (ou seja, $y_i = 0$ para algum $i \in \{1, \ldots, k\}$); e retorna 0, caso contrário. Além disso, uma fórmula booleana pode ser representada por uma árvore, onde as variáveis estão nas folhas e os operadores lógicos são nós internos da árvore. Classicamente, o resultado da avaliação da fórmula pode ser obtida na raiz da árvore. Na Figura 6.1 vemos a representação em árvore da fórmula $\sigma(x_1, x_2, x_3, x_4) = (x_1 \overline{\wedge} x_2) \overline{\wedge} (x_3 \overline{\wedge} x_4)$. Vamos considerar o caso

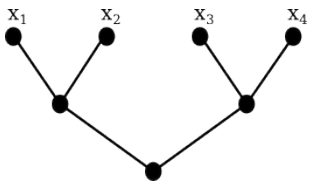


Figura 6.1: *Árvore representando a fórmula booleana:* $\sigma(x_1, x_2, x_3, x_4) = (x_1 \overline{\wedge} x_2) \overline{\wedge} (x_3 \overline{\wedge} x_4)$. *Nas folhas da árvore, temos as variáveis. Os nós internos representam o resultado ao aplicar o operador* $\overline{\wedge}$ *nos seus filhos.*

mais simples em que temos uma fórmula NÃO-E balanceada que é representada por uma árvore binária cheia.

Além disso, utilizaremos o modelo de consulta quântico (*quantum query model*) em que os valores das variáveis podem ser acessados através de consultas, O,

a uma caixa preta, também chamada de oráculo. Para o caso discreto, definimos a ação do operador O nos estados da base $\big|i, c\big\rangle$ onde $i \in \{0, 1, \ldots, N\}$. O operador unitário O_x (onde $x = (x_1, \ldots, x_N)$) transforma o estado $\big|0, c\big\rangle$ em $\big|0, c\big\rangle$ e o estado $\big|i, c\big\rangle$ em $(-1)^{x_i}\big|i, c\big\rangle$, para $i \in \{1, 2, \ldots, N\}$. O objetivo é resolver o dado problema fazendo o menor número de consultas possíveis.

6.2 Ideia dos algoritmos

Os algoritmos quânticos que iremos mencionar, a seguir, para avaliar uma expressão booleana, realizam um passeio quântico numa árvore aumentada. A ideia utilizada é que o valor da fórmula afeta o espectro do operador de evolução ou do hamiltoniano em questão, de forma que é possível utilizar o algoritmo quântico de estimação de fase para distinguir entre os dois casos, em que a fórmula é verdadeira, $\sigma(x) = 1$, ou falsa, $\sigma(x) = 0$.

6.2.1 Tempo contínuo

O algoritmo de Farhi et al. (2008) utiliza um passeio quântico contínuo numa árvore aumentada por uma reta infinita conectada a raiz pelo vértice 0 e para cada folha que contém uma variável $x_i = 1$, adicionamos um novo vértice e uma aresta conectando-os. Podemos ver um exemplo dessa árvore aumentada na Figura 6.2 O estado inicial do passeio quântico é

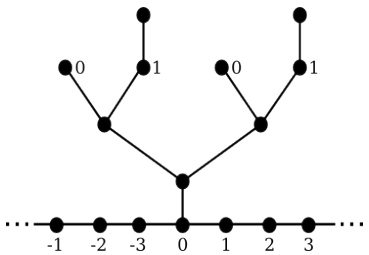


Figura 6.2: *Árvore aumentada por uma reta infinita e arestas extras nas folhas.*

$$\big|\psi(0)\big\rangle = \sum_{i \leq 0} \alpha_i \big|i\big\rangle, \tag{6.1}$$

que possui amplitudes diferentes de zero para os vértices da reta à esquerda de 0. Com tempo $O(\sqrt{N})$ obteremos um estado $\left|\psi'\right\rangle$. Se $\left|\psi'\right\rangle$ consistir de termos localizados à esquerda de 0, então $\sigma(x) = 0$ e, se $\left|\psi'\right\rangle$ consistir de termos localizados à direita de 0, então $\sigma(x) = 1$.

Mais tarde, esse algoritmo foi modificado por Childs et al. (2007b) considerando uma reta finita de tamanho $2L$, onde $L = O(\sqrt{N})$. Veja a Figura 6.3, como exemplo. A condição inicial nesse caso é

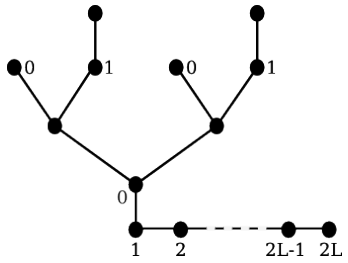


Figura 6.3: *Árvore aumentada por uma reta finita e arestas extras nas folhas.*

$$\left|\psi(0)\right\rangle = \frac{1}{\sqrt{L+1}} \sum_{k=0}^{L} (-1)^k \left|2k\right\rangle, \tag{6.2}$$

e é aplicado o algoritmo de estimação de fase para distinguir qual é o valor da fórmula booleana.

6.2.2 Tempo discreto

Ambainis et al. (2007) fazem uma decomposição do hamiltoniano utilizado no passeio contínuo e obtêm operadores unitários equivalentes para o caso discreto. As arestas extras nas folhas não são consideradas e temos um passeio quântico numa árvore aumentada por uma reta finita de tamanho $2L$.

Já no algoritmo de Childs et al. (2007a), sua versão mais simples apresenta uma árvore aumentada por apenas dois vértices, chamados r' e r'', que estão conectados a raiz da árvore. Um exemplo dessa árvore aumentada com profundidade $d = 2$ é mostrado na Figura 6.4. Como este algoritmo é do nosso interesse, vamos descrevê-lo com mais detalhes.

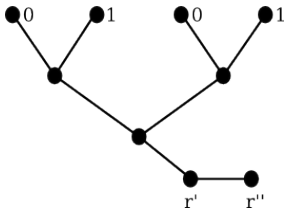


Figura 6.4: *Árvore aumentada pelos vértices r' e r'' conectados a raiz.*

O espaço do passeio quântico é gerado pelos estados $\big|v, c\big\rangle$, onde v é um vértice do grafo e $c \in \{\text{down}, \text{left}, \text{right}\}$ pertence ao espaço da moeda. A evolução do passeio quântico consiste na aplicação de dois operadores: primeiro o operador moeda C, atuando no espaço da moeda, seguido pelo operador de deslocamento S. O operador de evolução é, então, $U = SC$.

Como cada vértice do grafo pode ter diferentes graus, devemos restringir o espaço da moeda para cada tipo de vértice. Dessa forma, a aplicação da moeda dependerá do vértice a ser aplicado:

$$C = \sum_v \big|v\big\rangle\big\langle v\big| \otimes C_v, \tag{6.3}$$

onde:

- se $v = r''$, então $C_v = I$;
- se $v = r'$, $C_v = 2\big|\psi_1\big\rangle\big\langle\psi_1\big| - I$ com $\big|\psi_1\big\rangle = \frac{1}{\sqrt[4]{N}}\big|\text{right}\big\rangle + \sqrt{1 - \frac{1}{\sqrt{N}}}\big|\text{left}\big\rangle$;
- se v é um nó interno da árvore, então $C_v = 2\big|\psi_2\big\rangle\big\langle\psi_2\big| - I$ com $\big|\psi_2\big\rangle = \frac{1}{\sqrt{3}}\left(\big|\text{left}\big\rangle + \big|\text{right}\big\rangle + \big|\text{down}\big\rangle\right)$, que é uma superposição uniforme no espaço da moeda;
- se v é uma folha, então $C_v = (-1)^{x_i} I$, onde x_i é a variável na folha v.

O operador de deslocamento S atua da seguinte forma: se $c = \text{down}$, então caminhe para o pai do vértice v e defina c como left ou right dependendo de qual filho é v. E, se $c \in \{\text{left,right}\}$, então caminhe para o filho correspondente e defina c para down.

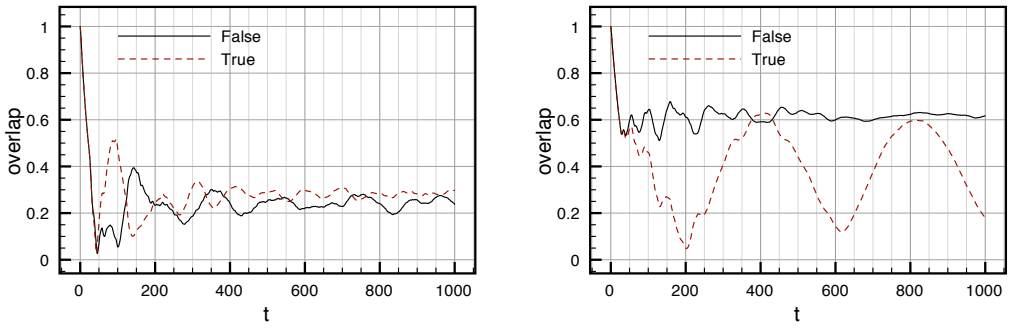
A ideia do algoritmo é a seguinte: se $\sigma(x) = 0$, então devemos ter um autoestado que está perto da condição inicial; e quando $\sigma(x) = 1$, esse estado não existe. Formalmente, quando $\sigma(x) = 0$, existe $\big|\psi\big\rangle$ tal que $\Big|\Big|\big|\psi\big\rangle - \big|\psi(0)\big\rangle\Big|\Big| \leq \epsilon$ e $U\big|\psi\big\rangle = i\big|\psi\big\rangle$. Quando $\sigma(x) = 1$, então, para qualquer autoestado $\big|\psi\big\rangle$ $\big(\text{com } U\big|\psi\big\rangle = \lambda\big|\psi\big\rangle\big)$, ou $\big|\psi\big\rangle \perp \big|\psi(0)\big\rangle$ ou $Re\lambda = \alpha/\sqrt{N}$ para alguma constante $\alpha > 0$. Para distinguir os dois casos, o algoritmo quântico de estimação de fase (Mosca e Ekert, 1998) é aplicado com a condição inicial $\big|\psi(0)\big\rangle = \big|r''\big\rangle\big|\text{left}\big\rangle$. O algoritmo utiliza $T = 320\lfloor\sqrt{N}\rfloor$ passos do passeio quântico e $O(\sqrt{N})$ consultas ao oráculo.

6.3 Simulações do algoritmo de Childs et al. (2007a)

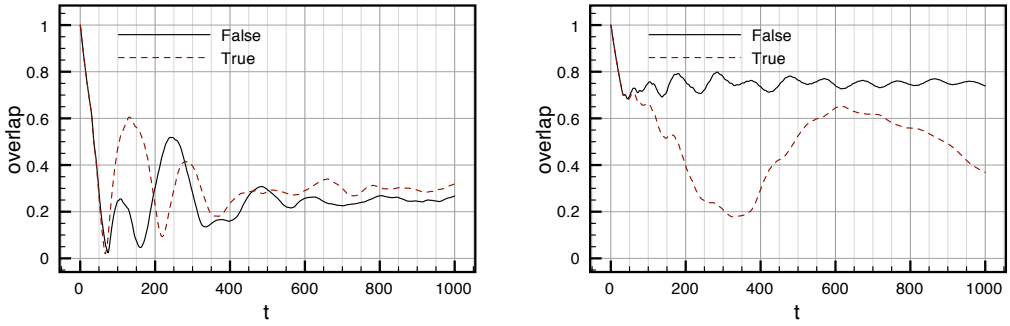
De acordo com o algoritmo, é importante observar o produto interno (*overlap*) entre o estado no instante t e o estado inicial durante a evolução do passeio quântico. O valor desse produto interno é zero a cada passo ímpar. Esses pontos serão ignorados nos gráficos, a seguir, onde mostraremos o valor absoluto desse produto interno em passos pares da evolução, $|\big\langle\psi(t)\big|\psi(0)\big\rangle|$.

A Figura 6.5 mostra a média do produto interno sobre 100 casos gerados aleatoriamente quando $\sigma(x) = 0$ e outros 100 casos em que $\sigma(x) = 1$. Observamos que a diferença máxima entre as curvas para o caso falso e verdadeiro acontece bem antes que $320\lfloor\sqrt{N}\rfloor$ (lembrando que, $N = 2^d$). Dessa forma, temos uma forte indicação de que é possível reduzir o número de passos do algoritmo e eliminar a etapa de estimação de fase.

É interessante notar a diferença no comportamento entre as profundidades ímpar e par. Para o caso par, o produto interno para o caso $\sigma(x) = 0$ torna-se mais perto de 1 à medida que a profundidade aumenta. Esse comportamento pode ser visualizado na Figura 6.6 que mostra a média sobre os 1000 passos da média do produto interno para diferentes profundidades. Para o caso ímpar, ainda não está muito claro o que acontece: parece que o comportamento limite converge para o mesmo valor ou cresce vagarosamente quando a profundidade aumenta.



(a) $d = 11$ (b) $d = 12$



(c) $d = 13$ (d) $d = 14$

Figura 6.5: *Média de* $|\langle\psi(t)|\psi(0)\rangle|$ *sobre 100 casos em que* $\sigma(x) = 0$ *(linha contínua) e 100 casos em que* $\sigma(x) = 1$ *(linha tracejada).*

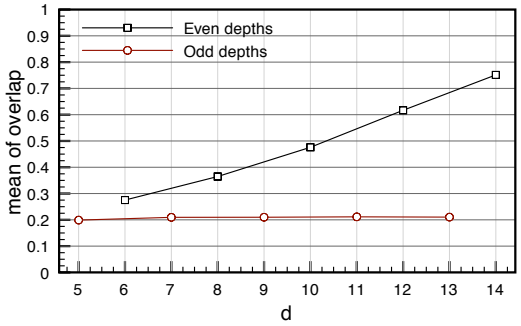


Figura 6.6: *Média do produto interno sobre 1000 passos para diferentes profundidades quando* $\sigma(x) = 0$.

6.3.1 Oráculo com falha

Agora, analisaremos o comportamento do algoritmo considerando o modelo com oráculo defeituoso ou com falha (*faulty oracle*). Nesse modelo, cada consulta ao oráculo pode retornar uma resposta incorreta. Se no modelo padrão (sem falha) o oráculo retorna o valor de uma variável x_i, então vamos denotar a saída do oráculo defeituoso como x_{F_i}. Note que x_i e $x_{F_i} \in \{0, 1\}$. Vamos definir nosso oráculo

defeituoso da seguinte maneira:

- $x_{F_i} = 1 - x_i$ com probabilidade p;
- $x_{F_i} = x_i$ com probabilidade $1 - p$.

Analisaremos o caso em que apenas uma variável apresenta oráculo defeituoso, ou seja, apenas uma das N variáveis pode ter seu valor invertido. Consequentemente, teremos dois casos diferentes: quando a fórmula é sensível ou não a inversão da variável, ou seja, num caso a inversão da variável não altera o valor da fórmula e noutro caso, inverter o valor da variável alterará o valor da fórmula. Devemos também analisar os dois casos em que a fórmula é verdadeira e falsa.

Nas simulações, as variáveis são geradas aleatoriamente com distribuição uniforme. Calculamos uma média sobre 100 rodadas, onde cada rodada evolui o passeio quântico por 1000 passos. Diferentes valores de probabilidades também são considerados.

6.3.1.1 Não sensível à inversão da variável

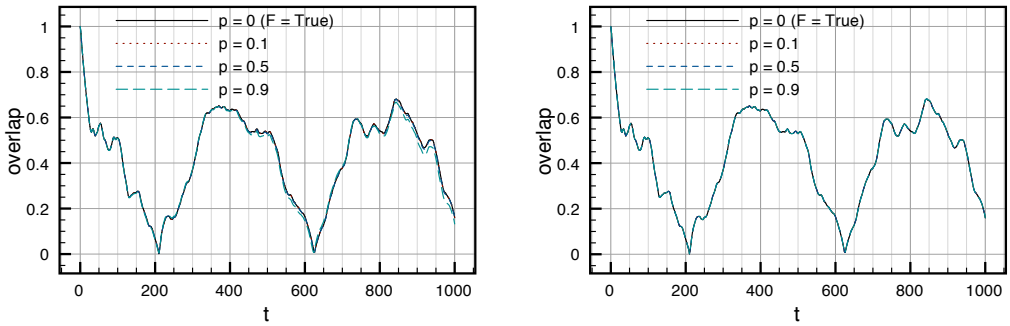
Considere o caso em que a variável, quando invertida, não altera o valor da fórmula. Então, vamos escolher uma variável $x_i = 0$ tal que

$$\sigma(x_1, \ldots, x_i, \ldots, x_N) = \sigma(x_1, \ldots, \bar{x_i}, \ldots, x_N),$$

onde $\bar{x} = \text{NÃO}\, x$. Além disso, vamos escolher outra variável $x_j = 1$ na fórmula satisfazendo a mesma condição de x_i.

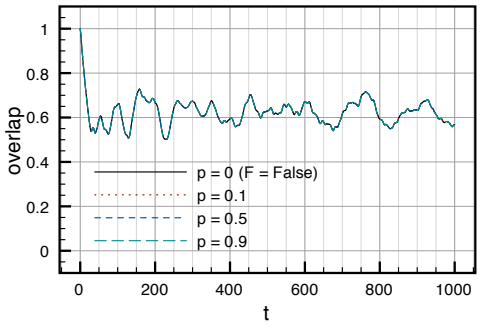
Os gráficos para profundidade $d = 12$ são apresentados na Figura 6.7. Como podemos ver, as curvas sobrepõe umas as outras e o algoritmo, nesse caso, não será afetado quando apenas uma variável é invertida (de acordo com uma probabilidade p) para as condições mencionadas.

O mesmo comportamento é visto para profundidades maiores. Além disso, independente do valor da probabilidade e do valor da variável que pode ser invertida, à medida que a profundidade aumenta, o algoritmo é menos afetado pelo

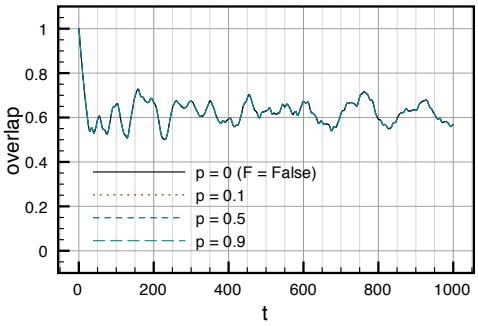


(a) $\sigma(x) = 1$ and $x_i = 0$

(b) $\sigma(x) = 1$ and $x_j = 1$



(c) $\sigma(x) = 0$ and $x_i = 0$



(d) $\sigma(x) = 0$ and $x_j = 1$

Figura 6.7: *Gráficos de* $|\langle\psi(t)|\psi(0)\rangle|$ *para 1000 passos com profundidade* $d = 12$.

oráculo defeituoso, ou seja, as curvas com probabilidades diferente de zero ficam cada vez mais próximas da curva com $p = 0$. É claro que se evoluirmos o passeio por mais tempo que o necessário para o algoritmo, a diferença entre essas curvas começa a aumentar.

6.3.1.2 Sensível à inversão da variável

Outro caso de interesse é quando a mudança no valor da variável altera o valor da fórmula. Considere que x_i é essa variável, então, se $\sigma(x_1, \ldots, x_i, \ldots, x_N) = 0$, temos $\sigma(x_1, \ldots, \bar{x_i}, \ldots, x_N) = 1$. As Figuras 6.8 e 6.9 apresentam esse modelo para árvores com profundidades $d = 13$ e $d = 14$, respectivamente.

Podemos observar que quando a probabilidade é pequena, por exemplo $p = 0.01$, a evolução é próxima da curva original. Um comportamento interessante é observado quando $p = 0.5$: ao invés de apresentar um comportamento intermediário entre os casos $p = 0$ e $p = 1$, a curva se aproxima de zero quando o número de passos aumenta.

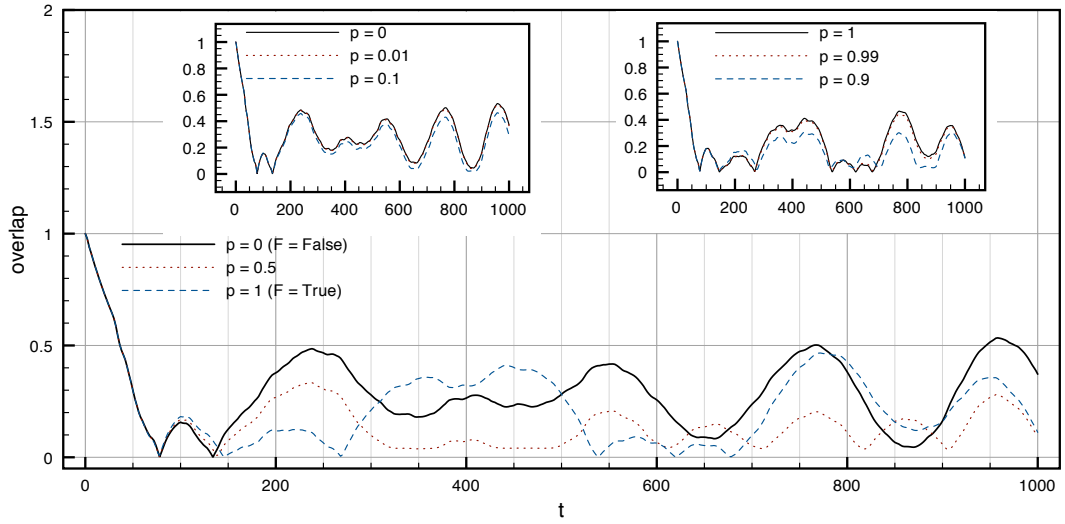


Figura 6.8: *Produto interno com a condição inicial,* $|\langle\psi(t)|\psi(0)\rangle|$*, para 1000 passos com profundidade* $d = 13$ *e* $\sigma(x) = 0$.

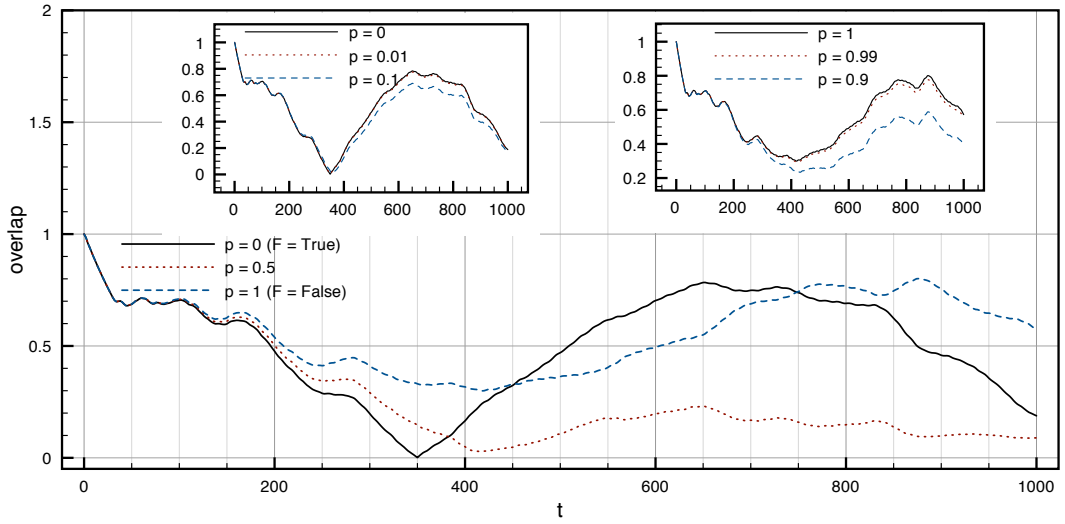


Figura 6.9: *Produto interno com a condição inicial,* $|\langle\psi(t)|\psi(0)\rangle|$*, para 1000 passos com profundidade* $d = 14$ *e* $\sigma(x) = 0$.

6.4 Conclusões

Simulações do algoritmo quântico de Childs et al. (2007a) para avaliação de fórmulas booleanas foram realizadas e alguns fatos importantes surgiram através da observação dos experimentos. Podemos mencionar a diferença entre o comportamento para profundidades par e ímpar. É interessante ver o que acontece se aumentarmos ainda mais a profundidade para o caso ímpar e comprovar de fato se ele se comporta como o caso par ou não, pois é possível que seu comportamento

seja mais lento que o caso par ou que ele convirja para algum valor independente da profundidade da árvore. As simulações indicam a possibilidade de eliminar a etapa de estimação de fase, já que podemos observar um comportamento médio distinto entre os casos em que a fórmula é verdadeira ou falsa fazendo apenas a evolução do passeio quântico. É interessante realizar um estudo analítico desse algoritmo para definir exatamente o ponto de parada do passeio quântico. Dessa forma, estaremos reduzindo a constante no valor do tempo de execução do algoritmo.

Para o modelo com oráculo defeituoso, analisamos o caso em que apenas uma variável da fórmula pode ser invertida com uma determinada probabilidade. No caso em que a fórmula não é sensível a essa variável, o comportamento do algoritmo é como esperado, identificamos quase nenhuma mudança em relação ao caso original. Para o caso em que a fórmula é sensível a variável, o algoritmo parece se comportar bem se a probabilidade for pequena. Mais experimentos podem ainda ser realizados nessa direção. É importante analisar o impacto considerando que mais de uma variável é afetada pelo oráculo defeituoso e analiticamente mostrar qual o valor de p para o qual esse algoritmo passa a se comportar como o clássico.

Mais ainda, seria interessante analisar o que acontece quando outras estruturas são utilizadas, ao invés de uma árvore. Isso pode nos levar ao desenvolvimento de novos algoritmos.

A publicação referente a esse capítulo é:

- (Santos e Rivosh, 2013) - A closer look at discrete-time quantum walk NAND formulae evaluation algorithm. In: Proceedings of the Workshop on Quantum and Classical Complexity, 2013;

Considerações Finais

Como pudemos perceber, a computação quântica tem tido um forte desenvolvimento nas últimas décadas. Com relação ao desenvolvimento de algoritmos quânticos, as cadeias de Markov quânticas ou passeios quânticos têm desempenhado um papel fundamental. Nosso trabalho contribui para o desenvolvimento dessa área, onde trazemos resultados que analisam o passeio quântico em grafos particulares e resultados mais gerais, que envolvem o impacto da descoerência sobre os algoritmos que são baseados nesses passeios quânticos.

O passeio quântico de Szegedy no ciclo com vértices marcados apresenta um comportamento que apenas altera os sinais das amplitudes da condição inicial, dada pela superposição uniforme sobre todas as arestas do grafo. A função $F(T)$ apresenta um comportamento similar ao do grafo completo. Obtivemos uma expressão analítica para o tempo de alcance quântico e vimos que não há diferença no cálculo para o caso em que o número de vértices é par ou ímpar. Em ambos casos, o tempo de alcance quântico também apresenta ganho quadrático com relação ao clássico.

Outro item importante no estudo de passeios quânticos é a distribuição limite. Sabemos que essa distribuição é diferente no caso quântico, já que ela depende da condição inicial. No caso clássico, por exemplo, para cadeias ergódicas e reversíveis a distribuição limite é única e independente da condição inicial. Em princípio, para o passeio quântico de Szegedy, não sabemos completamente quem é o autoespaço de autovalor 1. Dessa forma, se a condição inicial tem interseção com esse autoespaço podemos obter um limite inferior para a distribuição limite. Por sua vez, vimos para alguns casos particulares que esse limite está bem próximo do valor exato e

que, portanto, o autoespaço de autovalor 1 contribui com uma pequena porção no valor total da distribuição. É possível encontrar o valor exato dessa distribuição se utilizarmos uma condição inicial que não tem interseção com o autoespaço de autovalor 1, ou se descrevermos completamente esse subespaço. Como trabalho futuro, é interessante calcular o tempo de mistura (*mixing time*) nesse passeio.

A partir de um modelo de descoerência inspirado em percolação, em que permitimos a remoção e inserção de arestas no grafo, definimos o tempo de alcance quântico descoerente e estendemos o resultado de Szegedy adicionando um termo de descoerência. Mostramos que para uma probabilidade de descoerência suficientemente pequena o ganho quadrático com relação ao tempo de alcance clássico continua válido. O algoritmo de detecção apresenta um melhor resultado quando utilizamos o modelo com apenas remoção de arestas. Simulações desse modelo de descoerência foram realizadas para alguns grafos particulares. Podemos ressaltar que o impacto da descoerência no ciclo é bem distinto dos demais, onde vemos a diminuição do tempo de alcance para probabilidades de descoerência pequenas. Isso ocorre devido o modelo de descoerência permitir inserção de arestas entre vértices que estão distantes permitindo, assim, atingir os vértices marcados mais rapidamente.

Simulamos o algoritmo para avaliar fórmulas booleanas para o caso da árvore binária cheia onde temos uma expressão composta apenas por operadores NÃO-E. Consideramos o modelo com oráculo defeituoso afetando apenas uma variável. Nesse caso, vimos que o impacto causado por esse modelo é dependente da fórmula booleana. Pois, a fórmula pode ser ou não sensível a alteração no valor da variável. Como proposta de trabalhos futuros, é interessante analisar o que acontece quando mais de uma variável apresenta oráculo defeituoso e ver analiticamente qual o valor da probabilidade para o qual o algoritmo passa a se comportar como clássico. Além disso, também podemos estudar analiticamente o algoritmo e reduzir a constante do tempo de evolução do passeio quântico e eliminar a etapa de estimação de fase, como foi indicado pelas simulações. Esse algoritmo utiliza um passeio quântico

para resolver um problema que não é um problema de busca. Dessa forma, seria interessante utilizar de sua formatação e analisar o que acontece quando substituímos a estrutura da árvore por outros grafos. Isso pode levar ao desenvolvimento de novos algoritmos.

Referências Bibliográficas

G. Abal, R. Donangelo, M. Forets, e R. Portugal. Spatial quantum search in a triangular network, 2011. arXiv:quant-ph/1009.1422.

G. Abal, R. Donangelo, F. L. Marquezino, e R. Portugal. Spatial search on a honeycomb network. **Mathematical Structures in Computer Science**, 20: 999–1009, 2010.

M. Abramowitz e I. A. Stegun. **Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables**. Dover Publications, 1972.

D. Aharonov, A. Ambainis, J. Kempe, e U. Vazirani. Quantum walks on graphs. In: **Proceedings of the 33rd ACM Symposium on Theory of computing**, páginas 50–59, 2000. arXiv:quant-ph/0012090.

Y. Aharonov, L. Davidovich, e N. Zagury. Quantum random walks. **Physical Review A**, 48(2):1687–1690, 1993.

G. Alagic e A. Russell. Decoherence in quantum walks on the hypercube. **Physical Review A**, 2005.

A. Ambainis. Quantum walk algorithm for element distinctness. In: **Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science**, 2004.

A. Ambainis. Quantum algorithms for formula evaluation. arxiv:quant-ph/1006.3651, 2010.

A. Ambainis, A. Backurs, N. Nahimov, R. Ozols, e A. Rivosh. Search by quantum walks on two-dimensional grids without amplitude amplification. arXiv:quant-ph/1112.3337, 2011.

A. Ambainis, A. Backurs, N. Nahimov, e A. Rivosh. Grover's algorithm with errors. In: **Proceedings of MEMICS 2012, Lecture Noter in Computer Science**, volume 7721, páginas 180–189, 2013.

A. Ambainis, A. Childs, B. Reichardt, R. Spalek, e S. Zhang. Any and-or formula of size n can be evaluated in time $n^{1/2+o(1)}$ on a quantum computer. In: **Proceedings of FOCS**, páginas 363–372, 2007.

A. Ambainis, J. Kempe, e A. Rivosh. Coins make quantum walks faster. In: **Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms**, páginas 1099–1108, 2005.

D. M. Bacon. **Decoherence, Control, and Symmetry in Quantum Computers**. Tese de Doutorado, University of California at Berkeley, 2001.

T. A. Brun, H. A. Carteret, e A. Ambainis. Quantum to classical transition for random walks. **Physical Review Letters**, 91(130602), 2003.

H. Buhrman, R. Cleve, e A. Wigderson. Quantum vs. classical communication and computation. In: **Proceedings of the 30th ACM STOC**, páginas 63–68, 1998.

M. Chen. Mixing time of random walks on graphs. Dissertação de Mestrado, University of York, 2004. `http://keithbriggs.info/documents/Min_Chen_MSc.pdf`.

Chen-Fu Chiang. Sensitivity of quantum walks with perturbation. In: **Proceedings of the 10th Asian Conference on Quantum Information Science**, 2010.

A. Childs, E. Farhi, e S. Gutmann. An example of the difference between quantum and classical random walks. **Journal of Quantum Information Processing**, 1(35), 2002.

A. Childs, B. Reichardt, R. Spalek, e S. Zhang. Every nand formula on n variables can be evaluated in time $o(n^{1/2+\epsilon})$. version3, arXiv:quant-ph/0703015, 2007a.

A. Childs, B. Reichardt, R. Spalek, e S. Zhang. Every nand formula on n variables can be evaluated in time $o(n^{1/2+\epsilon})$. version1, arXiv:quant-ph/0703015, 2007b.

E. Farhi, J. Goldstone, e S. Gutmann. A quantum algorithm for the hamiltonian nand tree. **Theory of Computing**, 4:169–190, 2008.

E. Farhi e S. Gutmann. Quantum computation and decision trees. **Physical Review A**, 58:915–928, 1998.

Geoffrey Grimmett. **Percolation**. Springer, 1999.

L. K. Grover. A fast quantum mechanical algorithm for database search. In: **Proceedings of the 28th ACM Symposium on the Theory of Computing**, páginas 212–219, 1996.

B. Hein e G. Tanner. Quantum search algorithms on a regular lattice. **Physical Review A**, 82(1)(012326), 2010.

P. Hoyer, M. Mosca, e R. de Wolf. Quantum search on bounded-error inputs. In: **Proceedings of the 30th ICALP**, páginas 291–299, 2003.

Y. K. Itakura. Quantum algorithm for commutativity testing of a matrix set. Dissertação de Mestrado, University of Waterloo, 2008. arXiv:quant-ph/0509206v1.

J. Kempe. Discrete quantum walks hit exponentially faster. In: **Proc. 7th RANDOM**, páginas 354–369, 2003a. arXiv:quant-ph/0205083.

J. Kempe. Quantum random walks - an introductory overview. **Contemporary Physics**, 44(2):307–327, 2003b. arXiv:quant-ph/0303081.

A. Kempf e R. Portugal. Group velocity of discrete-time quantum walks. **Physical Review A**, 79(052317), 2009. arXiv:quant-ph/09014237.

V. Kendon. Decoherence in quantum walks - a review. **Mathematical Structures in Computer Science**, 17(6):1169–1220, 2007.

V. Kendon e B. Tregenna. Decoherence can be useful in quantum walks. **Physical Review A**, 67(042315), 2003.

B. Kollar, T. Kiss, J. Novotny, e I. Jex. Asymptotic dynamics of coined quantum walks on percolation graphs. **Physical Review Letters**, 108(230505), 2012.

H. Krovi e T. Brun. Hitting time for quantum walks on the hypercube. **Physical Review A**, 73(032341), 2006. arXiv:quant-ph/0510136.

H. Krovi, F. Magniez, M. Ozols, e J. Roland. Finding is as easy as detecting for quantum walks. In: **Proceedings of the 37th International Colloquium Conference on Automata, Languages and Programming**, páginas 540–551, 2010.

G. Leung, P. Knott, J. Bailey, e V. Kendon. Coined quantum walks on percolation graphs. **New Journal of Physics**, 12(123018), 2010.

D. A. Levin, Y. Peres, e E. L. Wilmer. **Markov Chains and Mixing Times**. American Mathematical Society, 2008. `http://www.uoregon.edu/~dlevin/MARKOV/`.

C. Liu e N. Petulante. On limiting distributions of quantum markov chains. **International Journal of Mathematics and Mathematical Sciences**, 2011 (740816), 2011.

C. Lomont. The hidden subgroup problem: review and open problems. arXiv:quant-ph/0411037, 2004.

N. B. Lovett, M. Everitt, R. M Heath, e V. Kendon. The quantum walk search algorithm: factors affecting efficiency. arXiv:quant-ph/1110.4366v2, 2011.

F. Magniez, A. Nayak, P. C. Richter, e M. Santha. On the hitting times of quantum versus random walks. In: **Proceedings of the Nineteenth Annual ACM -SIAM Symposium on Discrete Algorithms**, páginas 86–95, 2009.

F. L. Marquezino. **Análise, simulações e aplicações algorítmicas de caminhadas quânticas**. Tese de Doutorado, Laboratório Nacional de Computação Científica, 2010.

F. L. Marquezino, R. Portugal, G. Abal, e R. Donangelo. Mixing times in quantum walks on the hypercube. **Physical Review A**, 77(4):042312, 2008.

C. Moore e A. Russell. Quantum walks on the hypercube. In: **Proceedings of the 6th RANDOM, Lecture Notes in Computer Science**, volume 238, páginas 164–178, 2002.

M. Mosca e A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. **Selected papers from NASA QCQC'90, Lecture Notes in Computer Science**, 1509:174–188, 1998.

R. Motwani e P. Raghavan. **Randomized Algorithms**. Cambridge University Press, 1995.

M. A. Nielsen e I. L. Chuang. **Quantum computation and quantum information**. Cambridge University Press, UK, 2000.

M. A. Nielsen e I. L. Chuang. **Computação Quântica e Informação Quântica**. Bookman, 2005.

A. C. Oliveira, R. Portugal, e R. Donangelo. Decoherence in two-dimensional quantum walks. **Physical Review A**, 74(012312), 2006.

R. Portugal. **Quantum walks and search algorithms**. Springer, New York, 2013.

O. Regev e L. Schiff. Impossibility of a quantum speed-up with a faulty oracle. In: **Proceedings of ICALP**, páginas 773–781, 2008.

S. I. Resnick. **Adventures in Stochastic Processes**. Brikhäuser Boston, 1992.

A. Romanelli, R. Siri, G. Abal, A. Auyuanet, e R. Donangelo. Decoherence in the quantum walk on the line. **Physica A**, 347(C):137–152, 2005.

M. Saks e A. Wigderson. Probabilistic boolean decision trees and the complexity of evaluating game trees. In: **Proceedings of the 27th IEEE FOCS**, páginas 29–38, 1986.

R. A. M. Santos. Cadeias de markov quânticas. Dissertação de Mestrado, Laboratório Nacional de Computação Científica, 2010.

R. A. M. Santos e R. Portugal. Quantum hitting time on the complete graph. **International Journal of Quantum Information**, 8(5):881–894, 2010a.

R. A. M. Santos e R. Portugal. Quantum hitting time on the cycle. In: **Proceedings of III WECIQ - Workshop-School of Computation and Quantum Information**, 2010b.

R. A. M. Santos e R. Portugal. Decoherence in szegedy's quantum walk. In: **Proceedings of the XXXIV Congresso Nacional de Matemática Aplicada e Computacional**, 2012a.

R. A. M. Santos e R. Portugal. Simulations of quantum markov chains on percolation graphs. In: **Proceedings of IV WECIQ - Workshop-School of Computation and Quantum Information**, 2012b.

R. A. M. Santos, R. Portugal, e M. D. Fragoso. Decoherence in quantum markov chains. **Quantum Information Processing**, 13(2):559–572, 2014.

R. A. M. Santos e A. Rivosh. A closer look at discrete-time quantum walk nand formulae evaluation algorithm. In: **Proceedings of the Workshop on Quantum and Classical Complexity**, 2013.

N. Shenvi, J. Kempe, e K. B. Whaley. A quantum random walk search algorithm. **Physical Review A**, 67(052307), 2003.

Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. In: **Proceedings of FOCS'02**, páginas 513–519, 2002.

P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In: **Proceedings of the 35th FOCS**, páginas 124–134, 1994.

M. Snir. Lower bounds on probabilistic linear decision trees. **Theoretical Computer Science**, 38:69–82, 1985.

D. Stauffer e A. Aharony. **Introduction to percolation theory**. CRC Press, 1994.

F. W. Strauch. Connecting the discrete and continuous time quantum walks. **Physical Review A**, 74(3):030301, 2006.

M. Szegedy. Quantum speed-up of markov chain based algorithms. In: **Proceedings of the 45th Symposium on Foundations of Computer Science**, páginas 32–41, 2004.

W. F. Trench. On the eigenvalue problem for toeplitz band matrices. **Linear Algebra and its Applications**, 64:199–214, 1985.

A. Tulsi. Faster quantum walk algorithm for the two dimensional spatial search. **Physical Review A**, 78(012310), 2008.

S. E. Venegas-Andraca. **Quantum walks for computer scientists**. Morgan & Claypool, 2008.

X. P. Xu e F. Liu. Continuous-time quantum walks on erdös-rényi networks. **Physics Letters A**, 372:6727–6732, 2008.

Apêndice A

Cadeias de Markov

As cadeias de Markov são processos estocásticos sem memória, ou seja, o comportamento futuro de uma cadeia de Markov depende somente do seu estado atual. Em (Chen, 2004; Levin et al., 2008; Resnick, 1992; Motwani e Raghavan, 1995), podemos encontrar uma vasta descrição sobre a teoria das cadeias de Markov. A seguir, vamos apresentar algumas definições úteis e propriedades importantes das cadeias de Markov.

Uma cadeia de Markov, $\{X_{t_i}\}$, de maneira informal, é um sistema que se move através de um conjunto finito de estados Ω da seguinte maneira: dado $x \in \Omega$, a próxima posição é escolhida de acordo com uma probabilidade. Dada uma sequência de variáveis aleatórias $(X_0, X_1, ...)$, para cada $j \in \Omega$:

$$\Pr(X_{t+1} = j | X_0 = i_0, X_1 = i_1, ..., X_t = i) = \Pr(X_{t+1} = j | X_t = i) = P_{ij}, \quad \text{(A.1)}$$

onde $i_0, i_1, ..., i \in \Omega$. Como se trata de um processo estocástico, segue que,

$$\sum_{j \in \Omega} P_{ij} = 1 \quad \forall i \in \Omega. \quad \text{(A.2)}$$

P é denominada matriz de probabilidade.

Seja $\pi(t)$ a distribuição de probabilidades num instante t, ou seja, $\pi_i(t) =$

$\Pr(X_t = i)$. Temos que,

$$\pi(t+1)^\dagger = \pi(t)^\dagger P \Rightarrow \pi(t)^\dagger = \pi(0)^\dagger P^t. \tag{A.3}$$

A.1 Distribuição estacionária

A distribuição π é chamada *distribuição de equilíbrio* (ou *distribuição estacionária/invariante*) se ela satisfaz:

$$\pi^\dagger = \pi^\dagger P. \tag{A.4}$$

Ou seja, a distribuição estacionária é invariante sob a ação da matriz de probabilidade.

É notável que nem todas as cadeias de Markov possuem uma distribuição estacionária. Somente quando a cadeia satisfaz algumas restrições, a distribuição estacionária existirá e será única (Motwani e Raghavan, 1995).

A.2 Irredutibilidade

Uma cadeia de Markov é *irredutível* se cada estado pode ser alcançado por qualquer outro, ou seja:

$$\exists n : P_{ij}^n > 0 \quad \forall i, j, \tag{A.5}$$

onde P_{ij}^n é a probabilidade da cadeia de Markov estar no estado j depois de n passos, dado que ela tenha começado do estado i.

A.3 Periodicidade

O período de um estado i é dado por

$$r(i) = mdc\{n \geq 1 : P_{ii}^n > 0\} \tag{A.6}$$

(Se $\{n \geq 1 : P_{ii}^n > 0\} = \emptyset$, então $r(i) = 1$). Dizemos que i é aperiódico se $r(i) = 1$ e i é periódico se $r(i) > 1$.

Essa definição nos mostra que se $P_{ii}^n > 0$ então n é um inteiro múltiplo de $r(i)$, e $r(i)$ é o maior inteiro com essa propriedade. Dessa forma, retornar ao estado i só é possível via caminhos cujos tamanhos são múltiplos de $r(i)$.

A.4 Reversibilidade

Suponha que $X_n : -\infty < n < \infty$ é uma cadeia de Markov irredutível e aperiódica com matriz de probabilidade P e sua única distribuição estacionária π. Suponha ainda que X_n admite uma distribuição de probabilidades estacionária π para cada $n \in (-\infty, \infty)$.

Defina a cadeia inversa Y como: $Y_n = X_{-n}, -\infty < n < \infty$. A matriz de probabilidade $\overline{P}$ da cadeia Y pode ser obtida pela equação:

$$\pi_i P_{ij} = \pi_j \overline{P}_{ji} \quad \forall i, j \in \Omega. \tag{A.7}$$

Então, X será *reversível* se as matrizes de probabilidade de X e Y forem iguais, ou seja, $P = \overline{P}$.

A.5 Ergodicidade

Uma cadeia de Markov é ergódica se ela for irredutível e aperiódica. Além disso, uma cadeia de Markov ergódica tem uma única distribuição estacionária π. Então, para qualquer condição inicial λ teremos $\lambda P^t \to \pi$ quando $t \to \infty$. Dessa forma, num instante de tempo suficientemente grande, uma cadeia de Markov ergódica perderá toda a memória de onde ela começou e alcançará a sua distribuição estacionária π. Além disso, essa única distribuição estacionária é independente da condição inicial λ.