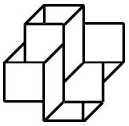


Laboratório Nacional de Computação Científica

Programa de Pós Graduação em Modelagem Computacional

Cadeias de Markov Quânticas

Por

Raqueline Azevedo Medeiros Santos

PETRÓPOLIS, RJ - BRASIL

ABRIL DE 2010

CADEIAS DE MARKOV QUÂNTICAS

Raqueline Azevedo Medeiros Santos

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM MODELAGEM COMPUTACIONAL

Aprovada por:

Prof. Renato Portugal, D.Sc.

(Presidente)

Prof. Marcelo Dutra Fragoso, Ph.D.

Prof. Celina Miraglia Herrera de Figueiredo, D.Sc.

PETRÓPOLIS, RJ - BRASIL
ABRIL DE 2010

Santos, Raqueline Azevedo Medeiros

S237c Cadeias de Markov Quânticas / Raqueline Azevedo Medeiros Santos. Petropólis, RJ. : Laboratório Nacional de Computação Científica, 2010.

xiv, 79 p. : il.; 29 cm

Orientador: Renato Portugal

Dissertação (Mestrado) – Laboratório Nacional de Computação Científica, 2010.

1.Computadores Quânticos. 2. Cadeias de Markov. 3. Caminhos aleatórios. 4. Tempo de alcance. 5. Caminhos quânticos. I. Portugal, Renato. II. LNCC/MCT. III. Título.

CDD 004.1

"Vários caminhos podem levar ao mesmo lugar. Difícil é saber o tempo para alcançá-lo."

Agradecimentos

A Deus. Aos meus pais, Irani e Guilherme, e a minha irmã, Regina, que, apesar da distância, sempre me apoiaram. Obrigada por sua confiança, carinho e incentivo. A todos da minha família, que sempre torceram por mim. A minha tia Zefinha, pelas dicas e ajuda na correção do texto.

Ao Prof. Renato Portugal, por sua orientação, paciência, atenção, respeito, confiança e ajuda essencial para o desenvolvimento deste trabalho.

Aos colegas do curso, que me ajudaram e me acompanharam durante essa caminhada, em especial a Milla, por sua amizade. Ao grupo de Computação Quântica por proveitosas discussões durante os seminários.

Ao LNCC, seus professores e funcionários. A CAPES, pelo apoio financeiro.

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

CADEIAS DE MARKOV QUÂNTICAS

Raqueline Azevedo Medeiros Santos

Abril , 2010

Orientador: Renato Portugal, D.Sc.

Em Ciência da Computação, os caminhos aleatórios são utilizados em algoritmos randômicos, especialmente em algoritmos de busca, quando desejamos encontrar um estado marcado numa cadeia de Markov. Nesse tipo de algoritmo é interessante estudar o Tempo de Alcance, que está associado a sua complexidade computacional. Nesse contexto, descrevemos a teoria clássica de cadeias de Markov e caminhos aleatórios, assim como o seu análogo quântico. Dessa forma, definimos o Tempo de Alcance sob o escopo das cadeias de Markov quânticas. Além disso, expressões analíticas calculadas para o Tempo de Alcance quântico e para a probabilidade de encontrarmos um elemento marcado num grafo completo são apresentadas como os novos resultados dessa dissertação.

Abstract of Dissertation presented to LNCC/MCT as a partial fulfillment of the requirements for the degree of Master of Sciences (M.Sc.)

QUANTUM MARKOV CHAINS

Raqueline Azevedo Medeiros Santos

April, 2010

Advisor: Renato Portugal, D.Sc.

In Computer Science, random walks are used in randomized algorithms, specially in search algorithms, where we desire to find a marked state in a Markov chain. In this type of algorithm, it is interesting to study the Hitting Time, which is associated to its computational complexity. In this context, we describe the classical theory of Markov chains and random walks, as well as their quantum analogue. In this way, we define the Hitting Time under the scope of quantum Markov chains. Moreover, analytical expressions calculated for the quantum Hitting Time and for the probability of finding a marked element on the complete graph are presented as the new results of this dissertation.

Sumário

Lista de Figuras

Figura

Lista de Tabelas

Tabela

Lista de Símbolos

- $\Pr(\cdot)$: 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
- P: matriz de transição de probabilidade de uma cadeia de Markov
- $(\cdot)^*$: transposto
- mdc: máximo divisor comum
- $G = (V, E)$: grafo descrito pelo conjunto de vértices V e pelo conjunto de arestas E ($|V| = n$ e $|E| = a$)
- $d(i)$: grau de saída do vértice i de um grafo
- $H_{i,j}$: tempo de alcance clássico - tempo esperado de sair do vértice i e chegar ao vértice j pela primeira vez
- $O(\cdot)$: 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 - $\mathbf{1}^T = (11 \cdots 1)$
- $\mathbb{R}$: conjunto dos números reais
- $\mathbb{C}$: conjunto dos números complexos
- $\Gamma(i)$: 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'_M: matriz obtida de P zerando as linhas e colunas indexadas pelos elementos de M
- P': matriz obtida de P, fazendo $p'_{xy} = \delta_{xy}$ para cada $x \in M$
- $H_M(\rho)$: tempo de alcance clássico para o conjunto M, partindo de uma distribuição de probabilidade ρ
- h_M: tempo de alcance clássico para o conjunto M, partindo da distribuição uniforme
- $\lambda(A)$: 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 $A\big|\psi_j\big\rangle$
- $\Pi_{\mathcal{K}}$: projeção ortogonal em $\mathcal{K}$
- $ref_{\mathcal{K}}$: 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
- $T_n(\cos\alpha)$: polinômio de Chebyshev do primeiro tipo - $T_n(\cos\alpha) = \cos(n\alpha)$
- $U_n(\cos\alpha)$: polinômio de Chebyshev do segundo tipo - $U_n(\cos\alpha) = \dfrac{\sin((n+1)\alpha)}{\sin\alpha}$
- $j_0(\cdot)$: primeira função de Bessel esférica - $j_0(x) = \dfrac{\sin x}{x}$

Introdução

Imagine que você agora é um viajante a fim de conhecer as belezas das cidades brasileiras. Longe de ser um viajante qualquer, você possui uma maneira peculiar de escolher o seu próximo destino. Em sua posse existe uma moeda especial que se adequa a cada cidade, contendo suas cidades vizinhas. Dessa forma, ao jogar a moeda, você obterá uma das cidades vizinhas com igual probabilidade. O resultado da moeda será, portanto, seu próximo destino. É verdade que talvez você seja um viajante um pouco sem rumo, que está a mercê da sorte. Mas, considere isso como parte da aventura.

O matemático russo Andrey A. Markov (1856-1922) estudou sistemas de objetos que mudam de um estado para outro, de acordo com probabilidades específicas. Quando um estado inicial pode nos levar para estados subsequentes e, por sua vez, esses estados podem nos levar a outros estados adicionais, o resultado será uma cadeia de Markov se a probabilidade de mover-se para um próximo estado depender somente do estado atual. A teoria de cadeias de Markov oferece um método poderoso para analisar o comportamento probabilístico numa ampla variedade de sistemas (Peterson, 1998). Então, podemos modelar sua viagem através de uma cadeia de Markov ou, também, através de um caminho aleatório num grafo.

Os caminhos aleatórios, como ferramenta algorítmica, podem ser aplicados numa grande variedade de problemas. Como afirma Kempe (2003b), eles provêem um paradigma geral para explorar um conjunto exponencialmente grande de estruturas combinatórias, através da utilização de simples transições locais. A relevância dos caminhos aleatórios e cadeias de Markov pode ser vista, principalmente, quando falamos do problema de busca, que é um problema relevante em

Ciência da Computação. O algoritmo de Schöning (Schöning, 1999) que provê a base para a melhor solução atual para o problema do 3-SAT é um exemplo disso.

Apesar do seu espírito aventureiro, você está muito ansioso, não aguenta mais o frio da cidade de Petrópolis e não vê a hora de conhecer as belas praias da cidade de Natal. Para diminuir um pouco essa ansiedade, podemos calcular uma estimativa do tempo que você levará para chegar lá. Essa medida é conhecida como Tempo de Alcance, que, nesse caso, trata-se do tempo esperado de sair de Petrópolis e chegar a Natal pela primeira vez.

Devido a natureza probabilística do caminho, o Tempo de Alcance é geralmente maior que o tempo para percorrer o menor caminho entre o ponto de partida e o destino. Geralmente, o Tempo de Alcance é de interesse quando usamos um caminho aleatório para buscar um estado marcado numa cadeia de Markov. Consequentemente, ele está intrinsicamente relacionado com a eficiência desses algoritmos de busca.

Esta dissertação encontra-se dividida em duas partes. Na primeira parte, a Parte Clássica, iniciamos mostrando, no Capítulo 1, a teoria das cadeias de Markov. Em seguida, definimos o que são os caminhos aleatórios em grafos, sua relação com as cadeias de Markov e quais as medidas utilizadas em sua análise quantitativa. No Capítulo 2, tratamos do Tempo de Alcance em caminhos aleatórios, mostrando exemplos para diferentes grafos. Além disso, estendemos sua definição para um conjunto de elementos e analisamos sua complexidade computacional.

Agora, você pode deixar o mundo clássico para se transformar num viajante quântico. No mundo quântico, é permitido coisas que não são possíveis no mundo clássico, como, por exemplo, estar em mais de um lugar ao mesmo tempo. Mas, pode ir tirando o cavalinho da chuva que o mundo quântico não é tão liberal quanto você pensa. Nos encontramos sob a rígida regência das leis da Mecânica Quântica.

Dessa forma, imagine-se partindo de todas as cidades ao mesmo tempo. Dizemos que você se encontra numa superposição de estados, onde cada estado identifica a possibilidade de estar numa cidade diferente. Se você se sentiu pouco à

vontade com a idéia de estar em superposição, podemos utilizar um ponto de vista alternativo: a interpretação dos muitos mundos. Nessa segunda visão o universo é dividido em vários universos: em cada universo você se encontrará numa cidade diferente. Mas, segundo Singh (2004), não importa se adotamos a interpretação da superposição ou dos muitos mundos, a teoria quântica é uma filosofia desconcertante.

Com relação a sua moeda, ela não terá mais utilidade. Ao invés dela, você passará a viajar através de um operador unitário. Não se preocupe que ele não é tão misterioso quanto parece: ao aplicar esse operador no seu estado atual, ele poderá levá-lo para outro estado ou para uma superposição de outros estados.

Depois de passar um tempo viajando você já está se sentindo um pouco cansado, talvez até meio enjoado com toda essa história de superposição. Então, você decide parar. Mas, você se depara com a seguinte indagação: será que vou ficar em superposição para sempre? Bom, a resposta é nem sempre. As vezes, chega a hora em que precisamos interferir no nosso sistema. Isso pode ser feito através de uma medida, que irá acabar com a superposição, permitindo-nos voltar para uma única cidade novamente. A cada estado dessa superposição está associado um valor, que chamamos de amplitude. Ao realizar uma medida, iremos colapsar para um dos estados possíveis com probabilidade igual ao valor dessa amplitude ao quadrado. É verdade que essas amplitudes podem ser modificadas pelo nosso operador unitário. Entretanto, existe uma regra que devemos obedecer: a soma dos quadrados das amplitudes de todos os estados em superposição deve ser sempre igual a 1.

Os caminhos quânticos são os análogos quânticos dos caminhos aleatórios clássicos. Essa denominação surgiu pela primeira vez na literatura em (Aharonov et al., 1993). De acordo com Kempe (2003b), a idéia é que o computador quântico pode implementar um caminho quântico eficientemente e pode utilizá-lo para resolver certas tarefas computacionais. Assim, é possível que ao usar as propriedades dos caminhos quânticos possamos encontrar algoritmos quânticos mais eficientes.

Ambainis (2004) conseguiu, através de um passeio quântico num grafo de

Johnson, resolver o problema da distinção de elementos, obtendo um algoritmo quântico mais eficiente do que o algoritmo clássico. A partir dele, foram surgindo outros algoritmos baseados em caminhos quânticos. Como exemplo, temos o algoritmo para verificação do produto de matrizes (Buhrman e Spalek, 2006) e o algoritmo para teste de comutatividade em grupos (Magniez e Nayak, 2007).

A definição do Tempo de Alcance, no caso quântico, é mais complicada devido a superposição de estados. Na literatura surgiram diferentes noções para o Tempo de Alcance quântico (Kempe, 2003a; Krovi e Brun, 2006; Kempf e Portugal, 2009; Szegedy, 2004a). Em contrapartida, é visível a importância do seu estudo pois, ao conseguirmos mostrar que ele é menor que o Tempo de Alcance clássico, então será possível encontrar algoritmos quânticos mais eficientes para problemas que não podem ser resolvidos eficientemente num computador clássico.

A segunda parte desta dissertação é dedicada à Parte Quântica, que se baseia principalmente no trabalho de Szegedy (2004a). Definimos o análogo quântico das cadeias de Markov, no Capítulo 3. Essas cadeias de Markov quânticas são obtidas a partir da quantização de um caminho bipartido, que, por sua vez, pode ser obtido a partir da duplicação de uma cadeia de Markov.

No Capítulo 4, apresentamos uma definição de Tempo de Alcance quântico que é uma extensão natural da definição clássica. Além disso, apresentamos os resultados obtidos para essa nova definição associada às cadeias de Markov quânticas e estabelecemos sua relação com o Tempo de Alcance clássico.

A seguir, no Capítulo 5, descrevemos o algoritmo para detectar elementos marcados num grafo, aplicando-o ao problema da distinção de elementos. Mostramos que o algoritmo obtido possuirá a mesma complexidade que o algoritmo desenvolvido por Ambainis (2004) e, também, explicamos qual a vantagem de utilizá-lo.

A nossa contribuição original para este trabalho pode ser vista no Capítulo 6, onde apresentamos expressões analíticas para o Tempo de Alcance quântico e para a probabilidade de encontrar um elemento marcado num conjunto de vértices mar-

cados num grafo completo. Essas grandezas desempenham um papel importante pois interferem diretamente na análise de complexidade de algoritmos de busca nesse grafo. Esses novos resultados obtidos para o grafo completo estão descritos em (Santos e Portugal, 2010).

Parte I

Parte Clássica

Capítulo 1

Cadeias de Markov e Caminhos Aleatórios

1.1 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, e não de como ele chegou ao estado presente. 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. Entretanto, o que segue nessa seção é apenas um resumo dessa teoria, mostrando apenas algumas definições úteis e propriedades importantes que serão utilizadas no decorrer dessa dissertação.

Uma cadeia de Markov é um sistema que se move através de um conjunto contável 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 $j \in \Omega$:

$$\Pr(X_{t+1} = j | X_0 = i_0, X_1 = i_1, ..., X_t = i) = \Pr(X_{t+1} = j | X_t = i) = P_{ij}, \quad (1.1)$$

onde $i_0, i_1, ..., i \in \Omega$.

Como se trata de um processo estocástico, segue que,

$$\sum_{j \in \Omega} P_{ij} = 1 \quad \forall i \in \Omega. \tag{1.2}$$

P é denominada matriz de transição de probabilidade.

Seja $\pi(t)$ a distribuição de probabilidade num instante t, ou seja, $\pi(t)_i = \Pr(X_t = i)$. Temos que,

$$\pi(t+1)^* = \pi(t)^* P \Rightarrow \pi(t)^* = \pi(0)^* P^t. \tag{1.3}$$

1.1.1 Distribuição estacionária

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

$$\pi^* = \pi^* P. \tag{1.4}$$

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

1.1.2 Irredutibilidade

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

$$\exists n : P_{ij}^n > 0 \quad \forall i, j, \tag{1.5}$$

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.

1.1.3 Periodicidade

O período de um estado i é dado por

$$r(i) = mdc\{n \geq 1 : P_{ii}^n > 0\} \tag{1.6}$$

(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 $r(i)$.

1.1.4 Reversibilidade

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

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

$$\pi_i P_{ij} = \pi_j \overline{P}_{ji} \quad \forall i, j \in \Omega. \tag{1.7}$$

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

1.1.5 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. Entretanto, essa única distribuição estacionária é independente da

condição inicial λ. Esse fato será importante para diferenciar os caminhos aleatórios dos caminhos quânticos (Venegas-Andraca, 2008).

1.2 Caminhos Aleatórios

Não existe muita diferença entre a teoria de caminhos aleatórios em grafos e a teoria de cadeias de Markov. Cadeias de Markov podem ser vistas como caminhos aleatórios em grafos direcionados com pesos nas arestas; cadeias de Markov simétricas podem ser vistas como caminhos aleatórios em grafos regulares e não-direcionados; e, cadeias de Markov reversíveis podem ser vistas como caminhos aleatórios em grafos não-direcionados (Lovász, 1993).

Um caminho aleatório num grafo é uma cadeia de Markov cujo conjunto de estados é o conjunto de vértices do grafo. Considere um grafo $G = (V, E)$, o caminhante parte de um vértice i e se move para um vizinho j de i. Do vértice j, ele se moverá para um de seus vizinhos e, assim, sucessivamente. A transição de um dado vértice para um vértice adjacente é definida de acordo com alguma distribuição de probabilidade. É usual definir:

$$P_{ij} = \begin{cases} \dfrac{1}{d(i)}, & \text{se a aresta } (i,j) \in E \\ 0, & \text{caso contrário} \end{cases} \tag{1.8}$$

onde $d(i)$ é o grau de saída do vértice i, ou seja, o número de arestas que saem de i.

1.2.1 Medidas

Ao estudar caminhos aleatórios, algumas questões básicas surgem, tais como: O caminho aleatório retorna para o seu ponto de partida? Quanto teremos que caminhar antes de retornar ao ponto de partida? Quanto teremos que caminhar antes de vermos um dado vértice ou antes de passarmos por todos os vértices?

Para responder alguma dessas questões veremos, a seguir, algumas medidas que possuem um papel bastante importante na análise quantitativa dos caminhos

aleatórios:

- Tempo de Alcance (*Hitting time* ou *Access time*) ($H_{i,j}$) - Tempo esperado de chegar pela primeira vez ao vértice j, começando do vértice i.

- *Commute time* ($k_{i,j}$) - Tempo esperado para que o caminhante começando em i vá até j e retorne a i: $k_{i,j} = H_{i,j} + H_{j,i}$.

- *Cover time* - Tempo esperado para que o caminhante passe por todos os vértices.

- *Mixing rate* - Medida de quão rápido o caminho aleatório converge para sua distribuição estacionária.

- *Mixing time* (τ_ϵ) - Dada uma cadeia de Markov ergódica que induz uma distribuição de probabilidade $\lambda_u(t)$ no instante t. O *mixing time* é definido como o primeiro instante de tempo t tal que $\lambda_u(t)$ está a uma distância ϵ de π para todo $t \geq T$, independente do estado inicial, ou seja,

$$\tau_\epsilon = \max_u \min_t \{t | t \geq T \Rightarrow ||\lambda_u(t) - \pi|| < \epsilon\}. \tag{1.9}$$

É perceptível os diferentes caminhos que podemos tomar ao estudar os caminhos aleatórios. E, dessa forma, podemos encontrar sua atuação em diferentes áreas como Ciência da Computação, Física, Economia e Biologia. Em (Aldous e Fill, 1994) e (Lovász, 1993) temos uma ampla descrição sobre os caminhos aleatórios em grafos e cadeias de Markov, assim como, algumas das medidas citadas anteriormente.

Capítulo 2

Tempo de Alcance

O Tempo de Alcance é importante em muitas aplicações algorítmicas que utilizam caminhos aleatórios, como o k-SAT e o problema de conectividade em grafos. Podemos ainda destacar que a solução mais eficiente para o problema 3-SAT é baseado no Tempo de Alcance de um caminho aleatório (Kempe, 2003a).

O Tempo de Alcance, segundo Motwani e Raghavan (1995), é expresso da seguinte maneira:

$$H_{i,j} = \sum_{t>0} t p_{ij}(t), \tag{2.1}$$

onde

$$p_{ij}(t) = \Pr(X_1 \neq j, X_2 \neq j, ..., X_{t-1} \neq j, X_t = j | X_0 = i). \tag{2.2}$$

É importante notar que o Tempo de Alcance não é simétrico, ou seja, $H_{i,j} \neq H_{j,i}$.

Isso pode ser facilmente notado no grafo da Figura 2.1 a seguir, que é conhecido na literatura como "grafo pirulito". Ele é composto por uma clique[1] com n vértices e associado a um dos vértices dessa clique, segue uma reta de tamanho n.

É possível mostrar que $H_{v,u} = O(n^2)$ e $H_{u,v} = O(n^3)$. Mas, primeiro vamos calcular o Tempo de Alcance numa reta com n vértices.

[1] Uma clique num grafo é um subgrafo que é um grafo completo.

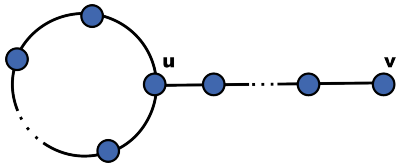


Figura 2.1: Grafo pirulito: composto por uma clique com n vértices e associado ao vértice u segue uma reta de tamanho n.

2.1 Tempo de Alcance na reta finita

Considere o grafo da Figura 2.2, a seguir. Queremos encontrar $H_{1,n}$. Para isso, vamos tentar encontrar uma relação para $H_{i,i+1}$, ou seja, vamos determinar o Tempo de Alcance entre dois vértices adjacentes.

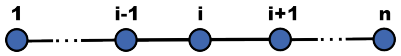


Figura 2.2: Reta finita com n vértices.

Começando de um vértice $1 < i < n$, vemos que temos igual probabilidade de ir ao vértice $i+1$ e $i-1$. Se o caminhante move para $i+1$, o tempo de alcançar o vértice $i+1$ é 1. Mas, se o caminhante escolhe mover-se para $i-1$, ele primeiro terá que voltar ao vértice i antes de atingir o vértice $i+1$.

Assim, podemos construir a seguinte expressão:

$$H_{i,i+1} = \frac{1}{2}.1 + \frac{1}{2}(1 + H_{i-1,i} + H_{i,i+1}) \tag{2.3}$$

que nos leva a

$$\begin{aligned} H_{i,i+1} &= 2 + H_{i-1,i} \\ &= 2 + 2 + H_{i-2,i-1} \\ &\vdots \\ &= 2(i-1) + H_{1,2}. \end{aligned} \tag{2.4}$$

Como $H_{1,2} = 1$, segue que $H_{i,i+1} = 2i - 1$. Assim, o Tempo de Alcance $H_{1,n}$

será dado por:

$$H_{1,n} = \sum_{i=1}^{n-1} 2i - 1 = (n-1)^2. \tag{2.5}$$

Com esse resultado do Tempo de Alcance na reta, claramente percebemos para o caso do grafo pirulito que $H_{v,u} = O(n^2)$. Agora, para mostrar que $H_{u,v} = O(n^3)$, temos que encontrar o Tempo de Alcance num grafo completo.

2.2 Tempo de Alcance no grafo completo

É perceptível que o Tempo de Alcance no grafo completo é o mesmo para todos os vértices do grafo, já que todos os vértices estão conectados a todos. Então $H_{i,j} = H_{GC}$ para todo i, j, com $i \neq j$. Podemos ver um exemplo de grafo completo na Figura 2.3.

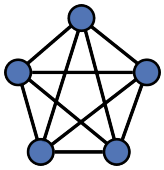


Figura 2.3: Grafo completo com $n = 5$.

Seguindo o mesmo raciocínio utilizado anteriormente para a reta, o Tempo de Alcance no grafo completo será dado por:

$$H_{GC} = \frac{1}{n-1}.1 + (n-2).\frac{1}{n-1}(1 + H_{GC}). \tag{2.6}$$

E, portanto,

$$H_{GC} = n - 1. \tag{2.7}$$

Outra maneira de calcular o Tempo de Alcance é utilizar a fórmula descrita em (2.1). Para isso, é preciso conhecer quem é $p_{ij}(t)$. Mas, nesse caso, é fácil perceber que a probabilidade de sair de um vértice e chegar pela primeira vez a outro vértice do grafo no instante t é dada por $\left(\frac{n-2}{n-1}\right)^t \frac{1}{n-1}$.

Substituindo em (2.1), obteremos o mesmo resultado:

$$H_{GC} = \sum_{t=1}^{\infty} t \left(\frac{n-2}{n-1}\right)^t \frac{1}{n-1} = n-1. \tag{2.8}$$

Agora, podemos voltar ao nosso problema. Então, considere a Figura 2.4, a seguir. Desejamos saber quem é $H_{1,n+1}$.

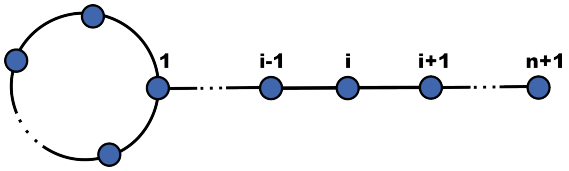


Figura 2.4: Grafo pirulito.

Para isso, vamos encontrar primeiro quem é $H_{i,i+1}$. Podemos perceber que $H_{i,i+1}$ possui a mesma relação obtida pela Equação (2.4) para o caso do Tempo de Alcance na reta. A diferença, nesse caso, é o $H_{1,2}$, pois, na reta, só existe uma possibilidade: sair do vértice 1 e ir para o vértice 2. Já no grafo pirulito, temos que contar com a possibilidade do caminhante entrar na clique. Dessa forma,

$$\begin{aligned} H_{1,2} &= \frac{1}{n}.1 + (n-1)\frac{1}{n}(1 + H_{GC} + H_{1,2}) \\ &= \frac{1}{n}.1 + (n-1)\frac{1}{n}(1 + (n-1) + H_{1,2}) \\ &= 1 + (n-1)n \\ &= O(n^2). \end{aligned} \tag{2.9}$$

Substituindo (2.9) em (2.4), obtemos $H_{i,i+1} = O(n^2)$. E, portanto,

$$H_{1,n+1} = \sum_{i=1}^{n} H_{i,i+1} = \sum_{i=1}^{n} O(n^2) = nO(n^2) = O(n^3). \tag{2.10}$$

Outro exemplo importante a ser visto é o Tempo de Alcance no ciclo, descrito a seguir.

2.3 Tempo de Alcance no ciclo

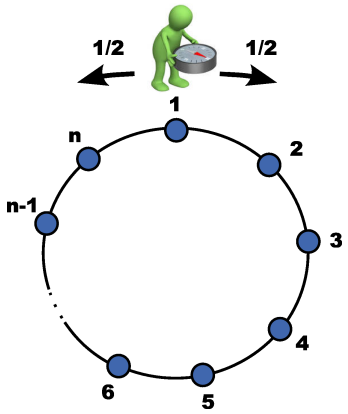


Figura 2.5: Ciclo com n vértices. A probabilidade do caminhante se mover para um dos dois vértices adjacentes é $\frac{1}{2}$.

Para encontrarmos o Tempo de Alcance no ciclo, vamos definir o Tempo de Alcance em termos de distância, já que é visível a existência de uma simetria nesse caso, ou seja, $H_{1,n} = H_{1,2}$, por exemplo. Então, considere H_j, o Tempo de Alcance entre dois vértices com distância j. Assim, $H_{1,2} = H_1$. Além disso, sabemos que $H_j = H_{n-j}$. A Figura 2.5 nos ajudará a ilustrar esse exemplo. Consequentemente, nossa equação para o Tempo de Alcance, será dada por:

$$\begin{aligned} H_j &= \frac{1}{2}(1 + H_{j-1}) + \frac{1}{2}(1 + H_{j+1}) \\ &= 1 + \frac{1}{2}H_{j-1} + \frac{1}{2}H_{j+1}. \end{aligned} \tag{2.11}$$

Fazendo $\Delta_j = H_j - H_{j+1}$, temos

$$\begin{aligned} \Delta_j &= 1 + \frac{1}{2}\Delta_{j-1} + \frac{1}{2}\Delta_j \\ &= 2 + \Delta_{j-1} \\ &= 2j + \Delta_0 = 2j + H_0 - H_1 = 2j - H_1. \end{aligned} \tag{2.12}$$

Lembrando que $H_0 = H_n = 0$. Substituindo o valor de Δ_j na equação

anterior, obteremos

$$\begin{aligned} H_{j+1} &= H_j + H_1 - 2j \\ H_j &= H_{j-1} + H_1 - 2(j-1). \end{aligned} \tag{2.13}$$

Fazendo $j = n$, pode-se verificar que $H_1 = H_{n-1} = n - 1$. Assim,

$$H_j = H_{j-1} + (n-1) - 2(j-1). \tag{2.14}$$

Resolvendo essa equação recursiva, encontramos que

$$H_j = j(n-j). \tag{2.15}$$

2.4 Tempo de Alcance num grafo genérico

Nessa seção, vamos encontrar o Tempo de Alcance entre dois vértices de um grafo $G = (V, E)$, $|V| = n$ e $|E| = a$, como é descrito em Lovász (1993). Essa equação estará relacionada com os autovalores da matriz de transição de probabilidade.

Podemos perceber que 1 é o maior autovalor da matriz de transição de probabilidade P com π seu correspondente autovetor à esquerda e, $\mathbf{1}$ seu autovetor à direita. Pois, é verdade que, $P^*\pi = \pi$ expressa o fato de π ser a distribuição estacionária e, $P\mathbf{1} = \mathbf{1}$ nos diz que P é uma matriz estocástica.

Infelizmente, P não é simétrica, a não ser que G seja regular. Mas, sabemos que $P = DA$, onde A é a matriz de adjacências de G e D é uma matriz diagonal onde $D_{ii} = \frac{1}{d(i)}$. Então, considere a matriz simétrica $N = D^{1/2}AD^{1/2} = D^{-1/2}PD^{1/2}$. Quando P é simétrica, $N = P$. Portanto, podemos obter a decomposição espectral para N:

$$N = \sum_{k=1}^{n} \lambda_k v_k v_k^*, \tag{2.16}$$

onde $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ são os autovalores de N e $v_1, \cdots, v_n$ seus correspondentes autovetores normalizados.

Uma simples substituição nos mostra que $w_i = \sqrt{d(i)}$ é autovetor de N com autovalor 1. Logo, segue do Teorema de Perron-Frobenius (ver (Meyer, 2000), cap. 9) que $\lambda_1 = 1 > \lambda_2 \geq \cdots \geq \lambda_n \geq -1$ (se G não for bipartido então, $\lambda_n > -1$). Assim, normalizando w, obtemos $v_1 = (1/\sqrt{2a})w$, ou seja, $v_{1i} = \sqrt{d(i)/2a} = \sqrt{\pi_i}$. E, dessa forma, teremos

$$P^t = D^{1/2}N^tD^{-1/2} = \sum_{k=1}^{n} \lambda_k^t D^{1/2} v_k v_k^* D^{-1/2} = Q + \sum_{k=2}^{n} \lambda_k^t D^{1/2} v_k v_k^* D^{-1/2}, \quad (2.17)$$

onde $Q_{ij} = \pi_j$.

O próximo passo será encontrar uma descrição matricial para o Tempo de Alcance.

Considere $H \in \mathbb{R}^{n\times n}$, a matriz cujos elementos H_{ij} representam o Tempo de Alcance do vértice i para o vértice j. Considere, também, $\Gamma(i)$ a vizinhança do vértice i. Para $i \neq j$, temos a seguinte equação

$$H_{i,j} = 1 + \frac{1}{d(i)} \sum_{v\in\Gamma(i)} H_{v,j}, \quad (2.18)$$

indicando que saindo do vértice i temos uma certa probabilidade, $1/d(i)$, de seguir para um de seus vizinhos e, a partir desse vizinho v, seguir para o vértice j. Essa equação nada mais é do que uma generalização para o método que utilizamos anteriormente a fim de encontrar os Tempos de Alcance na reta, no ciclo e no grafo completo. Expressando-a em notação matricial, chegamos a

$$F = J + PH - H, \quad (2.19)$$

onde $J_{ij} = 1\ \forall i, j$.

Poderíamos pensar que a matriz F seria a matriz onde todos os seus elementos são nulos. Entretanto, temos que considerar o caso em que $i = j$ e, portanto, F será uma matriz diagonal. A fim de obtê-la, aplicaremos F na distribuição

estacionária π:

$$F^*\pi = J\pi + H^*(P - I)^*\pi = J\pi = \mathbf{1}, \tag{2.20}$$

o que nos dá, $F_{ii} = \dfrac{1}{\pi_i} = \dfrac{2a}{d(i)}$, ou seja, $F = 2aD$.

Portanto, chegamos finalmente a nossa equação matricial para H, dada por,

$$(I - P)H = J - 2aD. \tag{2.21}$$

Nosso objetivo é resolvê-la a fim de encontrarmos H. Entretanto, a matriz $(I - P)$ não é invertível. Além disso, para toda matriz X satisfazendo à Equação (2.21), $X + \mathbf{1}b^*$ também satisfaz, para qualquer vetor b (pois, $\mathbf{1}$ é autovetor de P com autovalor 1).

Assim, uma simples substituição nos mostra que $(I - P + Q)^{-1}(J - 2aD)$ é solução para a Equação (2.21). Onde a matriz Q também pode ser expressa como $\mathbf{1}\pi^*$.

Da Equação (2.17), segue que

$$I - P + Q = I - \sum_{k=2}^{n} \lambda_k D^{1/2} v_k v_k^* D^{-1/2}. \tag{2.22}$$

E, consequentemente,

$$(I - P + Q)^{-1} = \sum_{k=2}^{n} \frac{1}{1 - \lambda_k} D^{1/2} v_k v_k^* D^{-1/2}. \tag{2.23}$$

Multiplicando por $(J - 2aD)$, encontraremos que

Teorema 2.1 (Lovász (1993))**.**

$$H_{ij} = 2a \sum_{k=2}^{n} \frac{1}{1 - \lambda_k} \left(\frac{v_{kj}^2}{d(j)} - \frac{v_{ki} v_{kj}}{\sqrt{d(i)d(j)}} \right), \tag{2.24}$$

onde v_{ki} é a i-ésima componente do autovetor de N associado ao autovalor λ_k.

A partir desse teorema, outros resultados importantes são facilmente demonstrados, como a média do Tempo de Alcance com relação à distribuição estacionária:

$$\begin{aligned}\sum_{j=1}^{n}\pi_j H_{ij} &= \sum_{j=1}^{n}\pi_j 2a\sum_{k=2}^{n}\frac{1}{1-\lambda_k}\left(\frac{v_{kj}^2}{d(j)}-\frac{v_{ki}v_{kj}}{\sqrt{d(i)d(j)}}\right)\\ &= \sum_{j=1}^{n}\sum_{k=2}^{n}\frac{1}{1-\lambda_k}\left(v_{kj}^2-v_{ki}v_{kj}\sqrt{\frac{d(j)}{d(i)}}\right)\\ &= \sum_{k=2}^{n}\frac{1}{1-\lambda_k}\left(\sum_{j=1}^{n}v_{kj}^2-\frac{v_{ki}}{\sqrt{d(i)}}\sum_{j=1}^{n}v_{kj}\sqrt{d(j)}\right).\end{aligned} \tag{2.25}$$

Lembrando que, $\|v_k\| = 1$ e, v_k é ortogonal a v_1, onde $v_{1i} = \sqrt{\pi_i} = \sqrt{\frac{d(i)}{2a}}$. Segue que,

$$\sum_{j=1}^{n}\pi_j H_{ij} = \sum_{k=2}^{n}\frac{1}{1-\lambda_k}(1-0) = \sum_{k=2}^{n}\frac{1}{1-\lambda_k}. \tag{2.26}$$

Da mesma forma, podemos obter:

$$\sum_{i=1}^{n}\pi_i H_{ij} = \frac{2a}{d(j)}\sum_{k=2}^{n}\frac{1}{1-\lambda_k}v_{kj}^2. \tag{2.27}$$

2.5 Tempo de Alcance para um subconjunto M

Depois de termos feito toda a análise do Tempo de Alcance para um determinado vértice num grafo, vamos pensar no caso em que estamos procurando mais de um vértice, ou seja, queremos saber o tempo esperado para alcançar um desses vértices.

Dada uma cadeia de Markov ergódica com matriz de transição de probabilidade P num espaço de estados X, com $|X| = n$ e um subconjunto de elementos marcados $M \subseteq X$, $|M| = m$. Segundo Szegedy (2004a), o tempo estimado para que a cadeia, saindo de uma distribuição de probabilidade ρ, encontre um elemento de M, é dado por:

$$H_M(\rho) = \rho_M^*(I - P_M)^{-1}\mathbf{1}, \tag{2.28}$$

onde P_M é a matriz obtida de P, removendo as linhas e colunas indexadas por M e ρ_M é o vetor obtido de ρ, retirando as entradas indexadas por M.

Como podemos visualizar essa cadeia de Markov como um caminho aleatório num grafo, nosso objetivo será mostrar o resultado descrito pela Equação (2.28) através da Equação (2.21), que descreve uma equação matricial para o Tempo de Alcance. Para isso, considere $[P'_M]_{n\times n}$, a matriz obtida de P, zerando as linhas e colunas indexadas pelos elementos de M. Podemos considerar, sem perda de generalidade, que $M = \{k, k+1, ..., n\}$, com $k > 0$.

Adicionando $(P - P'_M)H$ em (2.21), temos:

$$\begin{aligned} (I-P)H + (P-P'_M)H &= J - 2aD + (P-P'_M)H \\ (I-P'_M)H &= J - 2aD + (P-P'_M)H. \end{aligned} \tag{2.29}$$

Como estamos interessados em descobrir o tempo esperado de encontrar um elemento de M, podemos considerar $p_{ij} = 0$ e $H_{ij} = 0\ \forall i \in M$. Pois, lembrando que o Tempo de Alcance é o tempo esperado de chegar ao destino desejado pela primeira vez, de acordo com a Equação (2.18), o Tempo de Alcance para o conjunto M não dependerá nem da probabilidade, nem do Tempo de Alcance de sair de um elemento desse conjunto para outro qualquer.

Dessa forma, as matrizes da Equação (2.29) são da seguinte forma:

$$P = \left[\begin{array}{ccc|ccc} p_{11} & \cdots & p_{1(k-1)} & p_{1k} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ p_{(k-1)1} & \cdots & p_{(k-1)(k-1)} & p_{(k-1)k} & \cdots & p_{(k-1)n} \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]; \tag{2.30}$$

$$P'_M = \left[\begin{array}{ccc|ccc} p_{11} & \cdots & p_{1(k-1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ p_{(k-1)1} & \cdots & p_{(k-1)(k-1)} & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right] = \left[\begin{array}{c|c} P_M & 0 \\ \hline 0 & 0 \end{array}\right]; \tag{2.31}$$

$$P - P'_M = \left[\begin{array}{ccc|ccc} 0 & \cdots & 0 & p_{1k} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & p_{(k-1)k} & \cdots & p_{(k-1)n} \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]; \tag{2.32}$$

$$H = \left[\begin{array}{ccc|ccc} 0 & \cdots & H_{1(k-1)} & H_{1k} & \cdots & H_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ H_{(k-1)1} & \cdots & 0 & H_{(k-1)k} & \cdots & H_{(k-1)n} \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right] = \left[\begin{array}{c|c} H' & H'' \\ \hline 0 & 0 \end{array}\right]; \tag{2.33}$$

$$(P - P'_M)H = \left[\begin{array}{ccc|ccc} 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]; \tag{2.34}$$

$$J - 2aD = \left[\begin{array}{ccc|ccc} 1-\frac{1}{\pi_1} & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1-\frac{1}{\pi_{k-1}} & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & 1-\frac{1}{\pi_k} & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1-\frac{1}{\pi_n} \end{array}\right]. \tag{2.35}$$

Para encontrarmos H, a partir da Equação (2.29), precisamos calcular $(I - P'_M)^{-1}$:

$$I - P'_M = \left[\begin{array}{ccc|ccc} 1-p_{11} & \cdots & -p_{1(k-1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -p_{(k-1)1} & \cdots & 1-p_{(k-1)(k-1)} & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{array}\right] = \left[\begin{array}{c|c} I - P_M & 0 \\ \hline 0 & I \end{array}\right]. \tag{2.36}$$

Consequentemente,

$$(I - P'_M)^{-1} = \left[\begin{array}{c|c} (I - P_M)^{-1} & 0 \\ \hline 0 & I \end{array}\right]. \tag{2.37}$$

De acordo com o que foi dito inicialmente, estamos tratando de uma cadeia ergódica e, portanto, segundo Szegedy (2004a), $(I - P_M)$ possui inversa. Dessa forma, segue da Equação (2.29) que:

$$H = (I - P'_M)^{-1}(J - 2aD). \tag{2.38}$$

Substituindo (2.37) e (2.35), obtemos

$$H = \left[\begin{array}{c|c} (I - P_M)^{-1} & 0 \\ \hline 0 & I \end{array}\right] \cdot \left[\begin{array}{ccc|ccc} 1 - \frac{1}{\pi_1} & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 - \frac{1}{\pi_{k-1}} & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & 1 - \frac{1}{\pi_k} & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 - \frac{1}{\pi_n} \end{array}\right]. \tag{2.39}$$

Mas estamos interessado em saber quem é H'' (ver Equação (2.33)), que nos dá o Tempo de Alcance para M. Vamos chamar as colunas de H'' de H_i, $i \in M$. Ou seja,

$$H = \left[\begin{array}{c|ccc} & H_{1k} & \cdots & H_{1n} \\ H' & \vdots & \ddots & \vdots \\ & H_{(k-1)k} & \cdots & H_{(k-1)n} \\ \hline 0 & \multicolumn{3}{c}{0} \end{array}\right] = \left[\begin{array}{c|cccc} & | & | & \cdots & | \\ H' & H_k & H_{k+1} & \cdots & H_n \\ & | & | & \cdots & | \\ \hline 0 & \multicolumn{4}{c}{0} \end{array}\right]. \tag{2.40}$$

Das Equações (2.39) e (2.40), claramente vemos que,

$$H_k = H_{k+1} = \cdots = H_n = (I - P_M)^{-1}\mathbf{1}, \tag{2.41}$$

ou seja,

$$H_M = (I - P_M)^{-1}\mathbf{1}, \tag{2.42}$$

onde $[H_M]_{(n-m)\times 1}$ nos dá todos os Tempos de Alcance de um vértice $i \in V \backslash M$ para o conjunto M.

Por sua vez, ainda falta considerar a distribuição de probabilidade inicial. Podemos expressar o Tempo de Alcance para M, partindo de uma distribuição de probabilidade ρ, como:

$$H_M(\rho) = \sum_{x \in X} \rho_x H_{x,M}. \tag{2.43}$$

Assim, considerando a Equação (2.43), a partir da Equação (2.42) chegamos a Equação (2.28): $H_M(\rho) = \rho_M^*(I - P_M)^{-1}\mathbf{1}$.

Outra maneira de obtermos essa equação pode ser encontrada em (Itakura, 2008). O Tempo de Alcance é definido como uma média (esperança). Logo, para uma variável aleatória T, que assume somente valores inteiros não-negativos, podemos expressar a Equação (2.1) como

$$H_M = \sum_{t=0}^{\infty} \Pr(T > t). \tag{2.44}$$

Essa definição para a esperança pode ser encontrada em (James, 2006). No nosso caso, $\Pr(T > t)$ é a probabilidade de não termos alcançado um elemento marcado depois de t passos. Essa também é a probabilidade de ainda estarmos num estado pertencente a $X - M$. Como estamos falando de Tempo de Alcance, queremos parar assim que encontrarmos um elemento marcado. Então, consideraremos a sequinte matriz:

$$P' = \begin{pmatrix} P_M & P'' \\ 0 & I \end{pmatrix}, \tag{2.45}$$

onde $(P_M \;\; P'')$ são as linhas de P correspondentes a $X - M$ e, $(0 \;\; I)$, as linhas correspondentes aos estados em M. Supondo que partimos de uma distribuição de probabilidade ρ, nosso estado após t passos é dado por $\rho^* P'^t$. Assim,

$$\Pr(T > t) = \rho^* P'^t \mathbf{1}_{X-M} = \rho_M^* P_M^t \mathbf{1}, \tag{2.46}$$

onde $\mathbf{1}_{X-M}$ é o vetor que contém 1 nas primeiras $|X - M|$ entradas e 0 no restante.

Consequentemente,

$$\begin{aligned} H_M(\rho) &= \sum_{t=0}^{\infty} \rho_M^* P_M^t \mathbf{1} \\ &= \rho_M^* \left(\sum_{t=0}^{\infty} P_M^t \right) \mathbf{1} \\ &= \rho_M^* (I - P_M)^{-1} \mathbf{1}. \end{aligned} \tag{2.47}$$

2.5.1 Tempo de Alcance para um subconjunto no ciclo

Como exemplo, vamos calcular o Tempo de Alcance para um conjunto M num ciclo com n vértices. Nesse caso, a matriz de transição de probabilidade é dada por:

$$P = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & \cdots & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & \cdots & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & \cdots & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & 0 & \cdots & \frac{1}{2} & 0 \end{bmatrix}. \tag{2.48}$$

Dado que desejamos encontrar o Tempo de Alcance para o vértice n, ou seja, $M = \{n\}$, a matriz $I - P_M$, será uma matriz em banda, como vemos, a seguir.

$$I - P_M = \begin{bmatrix} 1 & -\frac{1}{2} & 0 & \cdots & 0 & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & \cdots & 0 & 0 \\ 0 & -\frac{1}{2} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & \cdots & -\frac{1}{2} & 1 \end{bmatrix}. \tag{2.49}$$

Por sua vez, podemos obter a inversa dessa matriz, seguindo algumas regras, onde os elementos de cada uma de suas colunas são múltiplos do último elemento de cada coluna (o mesmo também é válido para os elementos das linhas). Além disso, trata-se de uma matriz simétrica.

Assim, é fácil verificar que $(I - P_M)^{-1}$ será dada por,

$$(I - P_M)^{-1} = \frac{1}{n}. \begin{bmatrix} 2(n-1) & 2(n-2) & 2(n-3) & \cdots & 4 & 2 \\ 2(n-2) & 4(n-2) & 4(n-3) & \cdots & 8 & 4 \\ 2(n-3) & 4(n-3) & 6(n-3) & \cdots & 12 & 6 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 4 & 8 & 12 & \cdots & 4(n-2) & 2(n-2) \\ 2 & 4 & 6 & \cdots & 2(n-2) & 2(n-1) \end{bmatrix}. \tag{2.50}$$

Agora, para calcular o Tempo de Alcance, basta multiplicarmos essa matriz pelo vetor **1**. Logo, para cada linha teremos,

$$\begin{aligned} H_{iM} &= \frac{1}{n}\left(\sum_{j=1}^{n-i}(2i)j + \sum_{j=1}^{i-1}2(j)(n-i)\right) \\ &= \frac{1}{n}\left(2i\sum_{j=1}^{n-i}j + 2(n-i)\sum_{j=1}^{i-1}j\right) \\ &= \frac{1}{n}\left(i\left((n-i+1)^2 - (n-i+1)\right) + (n-i)(i^2-i)\right) \\ &= i(n-i). \end{aligned} \tag{2.51}$$

O que nos dá o mesmo resultado que obtivemos anteriormente, descrito na Equação (2.15).

Como exemplo, veja o caso para $n = 5$:

$$(I - P_M)^{-1} = \frac{1}{5}. \begin{bmatrix} 8 & 6 & 4 & 2 \\ 6 & 12 & 8 & 4 \\ 4 & 8 & 12 & 6 \\ 2 & 4 & 6 & 8 \end{bmatrix}. \tag{2.52}$$

De forma que,

$$(I - P_M)^{-1}\mathbf{1} = \frac{1}{5}.\begin{bmatrix} 8 & 6 & 4 & 2 \\ 6 & 12 & 8 & 4 \\ 4 & 8 & 12 & 6 \\ 2 & 4 & 6 & 8 \end{bmatrix}.\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \\ 6 \\ 4 \end{bmatrix} = \begin{bmatrix} 1(5-1) \\ 2(5-2) \\ 3(5-3) \\ 4(5-4) \end{bmatrix}. \quad (2.53)$$

Portanto, temos os Tempos de Alcance para o vértice 5: $H_{15} = H_{45} = 4$ e $H_{25} = H_{35} = 6$.

Poderíamos pensar agora o que aconteceria, nesse caso, se $m > 1$, com $M = \{k, k+1, ..., n\}$.

Analisando a matriz P para o caso $n = 5$ e $m = 2$, por exemplo,

$$P = \left[\begin{array}{ccc|cc} 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \hline 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 \end{array}\right], \quad (2.54)$$

podemos perceber que ao eliminarmos as linhas e colunas dos elementos referentes ao conjunto M, vemos que a matriz P_M será igual a matriz obtida para o caso quando $n = 4$ e $m = 1$.

Logo, podemos concluir que a matriz P_M, para o caso geral, é igual a uma matriz $P'_{M'}$, onde $n' = n - m + 1$ e $|M'| = 1$. Assim, da Equação (2.51), obtemos que o Tempo de Alcance num ciclo com n vértices para um subconjunto M será dado por,

$$H_{iM} = i(n - m + 1 - i), \qquad i = 1...n - m. \quad (2.55)$$

Se supormos que estamos partindo da distribuição estacionária π, segue que,

$$H_M(\pi) = \pi^*_M(I - P_M)^{-1}\mathbf{1} = \sum_{i=1}^{n-m} \pi_i i(n - m + 1 - i). \quad (2.56)$$

Mas, segundo Motwani e Raghavan (1995), a distribuição estacionária de um grafo conectado e não-direcionado, é dada por

$$\pi_i = \frac{d(i)}{2a} \qquad \forall i \in V. \tag{2.57}$$

Logo, para o caso do ciclo, que é um grafo regular,

$$\pi_i = \frac{1}{n} \qquad \forall i \in V. \tag{2.58}$$

Substituindo (2.58) em (2.56), temos

$$H_M(\pi) = \frac{1}{n} \sum_{i=1}^{n-m} i(n - m + 1 - i). \tag{2.59}$$

Fazendo $n = 6$ e $m = 2$, por exemplo, obtemos:

$$H_M(\pi) = \frac{1}{6}(4 + 6 + 6 + 4) = \frac{10}{3}. \tag{2.60}$$

2.5.2 Conexão com o autovalor

Nesta seção, vamos expressar a equação do Tempo de Alcance para um subconjunto em função dos autovalores da matriz P_M.

Considere que a matriz P é simétrica, ou seja, $P = P^*$. Em particular, isso implica que sua distribuição estacionária é uniforme. Podemos expressar P_M na sua forma espectral:

$$P_M = \sum_{k=1}^{n-m} \lambda'_k v'_k v'^*_k, \tag{2.61}$$

onde v'_k é autovetor normalizado de P_M associado ao autovalor λ'_k.

Considere u (vetor de tamanho n), a distribuição uniforme em X, ou seja, $u = \frac{1}{n}\mathbf{1}$ e u_M (vetor de tamanho $n-m$), o vetor obtido de u removendo os elementos indexados por M. Defina,

$$\hat{u} = \sqrt{n} u_M = \frac{1}{\sqrt{n}}\mathbf{1} = \sum_{k=1}^{n-m} \nu_k v'_k, \tag{2.62}$$

onde ν_k $(1 \leq k \leq n-m)$ são os coeficientes de $\hat{u}$ expressos na base de autovetores de P_M.

Assim,

$$\begin{aligned} H_M(u) = \frac{1}{n}\sum_{x\in X} H_{x,M} &= u_M^*(I-P_M)^{-1}\mathbf{1} \\ &= \frac{1}{n}\mathbf{1}^*(I-P_M)^{-1}\mathbf{1} \\ &= \hat{u}^*(I-P_M)^{-1}\hat{u}. \end{aligned} \tag{2.63}$$

Mas,

$$(I-P_M) = \sum_{k=1}^{n-m}(1-\lambda'_k)v'_k v'^*_k. \tag{2.64}$$

E, como $\lambda'_k \neq 1 \quad \forall k$,

$$(I-P_M)^{-1} = \sum_{k=1}^{n-m}\frac{1}{1-\lambda'_k}v'_k v'^*_k. \tag{2.65}$$

Substituindo (2.65) em (2.63), teremos

$$h_M \stackrel{\text{def}}{=} H_M(u) = \frac{1}{n}\sum_{x\in X} H_{x,M} = \hat{u}^*(I-P_M)^{-1}\hat{u} = \sum_{k=1}^{n-m}|\nu_k|^2\frac{1}{1-\lambda'_k}. \tag{2.66}$$

Lema 2.1 (Szegedy (2004a))**.**

$$h_M = O\left(\frac{1}{1-\lambda(P_M)}\right), \tag{2.67}$$

onde $\lambda(P_M)$ é o maior autovalor de P_M, em módulo, e o autovetor principal é o seu autovetor associado.

Demonstração.

$$\sum_{k=1}^{n-m}|\nu_k|^2\frac{1}{1-\lambda'_k} \leq \frac{1}{1-\lambda(P_M)}\sum_{k=1}^{n-m}|\nu_k|^2 \leq \frac{1}{1-\lambda(P_M)}. \tag{2.68}$$

Pois,

$$||\hat{u}|| = \sum_{k=1}^{n-m} |\nu_k|^2 = \frac{n-m}{n} \leq 1. \tag{2.69}$$

Logo, $h_M = O\left(\frac{1}{1-\lambda(P_M)}\right)$.

□

Esse resultado é importante e será utilizado, posteriormente, para compararmos com o Tempo de Alcance quântico, visualizando seu ganho com relação ao clássico.

2.5.2.1 Exemplo

Vamos analisar o caso do grafo completo. A matriz P_M de um grafo completo é da forma:

$$P_M = \begin{bmatrix} 0 & \frac{1}{n-1} & \frac{1}{n-1} & \cdots & \frac{1}{n-1} & \frac{1}{n-1} \\ \frac{1}{n-1} & 0 & \frac{1}{n-1} & \cdots & \frac{1}{n-1} & \frac{1}{n-1} \\ \frac{1}{n-1} & \frac{1}{n-1} & 0 & \cdots & \frac{1}{n-1} & \frac{1}{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{1}{n-1} & \frac{1}{n-1} & \frac{1}{n-1} & \cdots & 0 & \frac{1}{n-1} \\ \frac{1}{n-1} & \frac{1}{n-1} & \frac{1}{n-1} & \cdots & \frac{1}{n-1} & 0 \end{bmatrix}. \tag{2.70}$$

Podemos, então, escrever P_M na sua forma espectral:

$$P_M = \frac{n-m-1}{n-1} v'_{n-m} v'^{*}_{n-m} - \frac{1}{n-1} \sum_{k=1}^{n-m-1} v'_k v'^{*}_k, \tag{2.71}$$

onde

$$v'_{n-m} = \frac{1}{\sqrt{n-m}}\mathbf{1} \text{ e } v'_k = \frac{1}{\sqrt{k+k^2}} \left(\sum_{i=1}^{k} e_i - k e_{k+1} \right), \tag{2.72}$$

sendo e_i o vetor que possui 1 na coordenada i e 0 nas outras.

Dessa forma, temos que

$$\begin{aligned} H_M &= (I - P_M)^{-1}\mathbf{1} \\ &= \left(\left(1 - \frac{n-m-1}{n-1}\right)^{-1} v'_{n-m}v'^{*}_{n-m} + \left(1 + \frac{1}{n-1}\right)^{-1} \sum_{k=1}^{n-m-1} v'_k v'^{*}_k\right)\mathbf{1} \\ &= \frac{n-1}{m} v'_{n-m}v'^{*}_{n-m}\mathbf{1} + \frac{n-1}{n} \sum_{k=1}^{n-m-1} v'_k v'^{*}_k \mathbf{1}. \end{aligned} \tag{2.73}$$

Como, $v'^{*}_{n-m}\mathbf{1} = \dfrac{n-m}{\sqrt{n-m}}$ e $v'^{*}_k\mathbf{1} = 0\ \forall k$, segue que,

$$H_M = \frac{(n-1)}{m}\frac{(n-m)}{\sqrt{n-m}} v'_{n-m} = \frac{n-1}{m}\mathbf{1}. \tag{2.74}$$

Assim, o Tempo de Alcance, partindo da distribuição estacionária $\pi = \dfrac{1}{n}\mathbf{1}$, será dado por

$$H_M(\pi) = \pi^*(I - P_M)^{-1}\mathbf{1} = \pi^*\frac{n-1}{m}\mathbf{1} = \frac{(n-m)}{n}\frac{(n-1)}{m}. \tag{2.75}$$

Como,

$$\frac{(n-m)}{n} \leq 1 \Rightarrow \frac{(n-m)}{n}\frac{(n-1)}{m} \leq \frac{(n-1)}{m}, \tag{2.76}$$

então, $H_M(\pi)$ é $O\left(\dfrac{n}{m}\right) = O\left(\dfrac{1}{1-\lambda(P_M)}\right)$, como vimos no Lema 2.1.

Parte II

Parte Quântica

Capítulo 3

Cadeias de Markov Quânticas

Considere uma cadeia de Markov com matriz de transição de probabilidade P e conjunto de estados X. Como vimos, uma cadeia de Markov pode ser vista como um caminho aleatório num grafo $G = (V, E)$, fazendo $V = X$.

Vamos pensar como seria uma caminhada nas arestas de um grafo: a aresta (x, u), $x, u \in X$, representa o estado do caminho estando em x, dado que o estado anterior é u. Logo, um passo nesse caminho nas arestas nos levará de (x, u) para (y, x) com probabilidade p_{xy}:

$$(x, u) \stackrel{p_{xy}}{\rightarrow} (y, x). \tag{3.1}$$

Na maioria dos artigos a maneira usual de definir caminhos quânticos discretos (ou seja, o processo de quantização dos caminhos aleatórios) introduz um espaço moeda em adição ao espaço de estados (ou de vértices do grafo). Em (Kempe, 2003b; Venegas-Andraca, 2008; Ambainis, 2003), podemos encontrar uma descrição completa sobre caminhos quânticos.

O operador evolução para um passo do caminho é dado pelo produto de dois operadores unitários. O primeiro é o operador moeda (C) que atua somente no espaço moeda e pode ser ou não dependente do estado atual em que se encontra o caminhante (se o grafo for regular, por exemplo, esse operador pode ser independente, já que os vértices do grafo possuem o mesmo grau). O segundo é o operador de deslocamento (S) que é controlado pelo estado da moeda e leva um vértice para

um de seus vizinhos, ou seja, podemos definir

$$S\big|r\big\rangle\big|x\big\rangle \rightarrow \big|r\big\rangle\big|x_r\big\rangle, \tag{3.2}$$

onde x_r é o r-ésimo vizinho de x.

Como vemos em Santha (2008), podemos definir o espaço moeda como X. Nesse caso, o nosso espaço, $\big\{\big|x,y\big\rangle : x,y \in X\big\}$, coincide com as arestas do grafo. Então, um passo no caminho, para o estado inicial $\big|x,u\big\rangle$, será dado por:

$$SC\big|x,u\big\rangle \rightarrow S\big|x,y\big\rangle \rightarrow \big|y,x\big\rangle, \tag{3.3}$$

onde o operador moeda, assim definido, é controlado pelo primeiro registrador: ele muda o segundo registrador para um dos vizinhos do primeiro.

Vamos definir outro operador C' que atua como C, sendo controlado pelo segundo registrador e atuando no primeiro:

$$C'\big|x,y\big\rangle \rightarrow \big|z,y\big\rangle. \tag{3.4}$$

C' leva o estado $\big|x,y\big\rangle$ em $\big|z,y\big\rangle$ alterando o primeiro registrador para o valor z que é um vizinho de y.

Então, podemos ver que $SCSC = C'C$. Pois,

$$SCSC\big|x,u\big\rangle \rightarrow SCS\big|x,y\big\rangle \rightarrow SC\big|y,x\big\rangle \rightarrow S\big|y,z\big\rangle \rightarrow \big|z,y\big\rangle, \tag{3.5}$$

$$C'C\big|x,u\big\rangle \rightarrow C'\big|x,y\big\rangle \rightarrow \big|z,y\big\rangle. \tag{3.6}$$

Logo, podemos nos livrar do operador de deslocamento e dois passos no caminho serão alcançados pela aplicação sucessiva do operador moeda, alternando os registradores alvo e de controle.

Essa noção diferente de um caminho, evoluindo através de dois operadores que alternadamente transformam o segundo registrador num dos vizinhos do primeiro e; depois levam o primeiro registrador num dos vizinhos do segundo;

é descrita por Santha (2008), como uma motivação para o trabalho do Szegedy (2004a,b). Pois, nesse trabalho são definidos dois operadores unitários que fazem o papel de C e C' e que, como veremos, serão dados por reflexões em dois espaços diferentes. Para isso, ele utiliza a idéia de um caminho bipartido, como descreveremos a seguir. Vale ainda ressaltar que a noção de caminho quântico desenvolvida por Szegedy foi inspirada pela idéia de caminhos quânticos descrita por (Ambainis, 2004).

3.1 Caminhos Bipartidos

Num caminho bipartido (P, Q) temos dois conjuntos de estados: X e Y. P e Q são matrizes que descrevem as probabilidades de X para Y e Y para X, respectivamente.

Como P e Q são estocásticas, temos:

$$\sum_{y \in Y} p_{xy} = 1 \quad \forall x \in X, \tag{3.7}$$

$$\sum_{x \in X} q_{yx} = 1 \quad \forall y \in Y. \tag{3.8}$$

Vejamos, a seguir um exemplo de um caminho bipartido. Sejam $X = \{x_1, x_2\}$ e $Y = \{y_1, y_2, y_3\}$ com,

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{bmatrix} \text{ e } Q = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3.9}$$

Então, podemos representar esse exemplo através do grafo bipartido, vide Figura 3.1. Dessa forma, o caminhante pode sair da aresta (x_1, y_1) para a aresta (y_2, x_1) com probabilidade $p_{x_1 y_2} = \frac{1}{2}$.

É interessante notar que toda cadeia de Markov pode ser convertida num caminho bipartido através de uma simples operação de "duplicação". Ou seja,

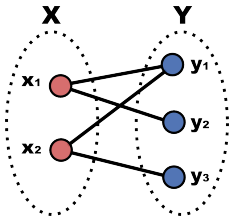
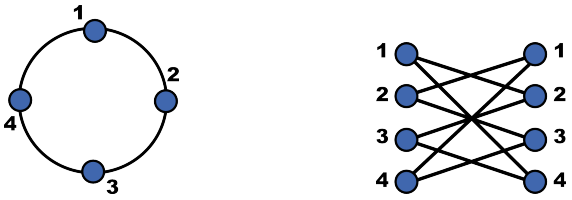


Figura 3.1: Grafo bipartido cujo conjunto de vértices é dado por $V = X \cup Y = \{x_1, x_2, y_1, y_2, y_3\}$ e cujas arestas são determinadas pelas matrizes P e Q, vide (3.9).

fazemos $Y = X$ e $Q = P$. Como exemplo, considere $X = \{1, 2, 3, 4\}$ com,

$$P = \begin{bmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{bmatrix}. \tag{3.10}$$

A Figura 3.2(a) representa o grafo associado ao caminho aleatório (cadeia de Markov, X) e o grafo bipartido da Figura 3.2(b) representa o grafo associado ao caminho bipartido (P, Q), em que $P = Q$ e $X = Y$, associado a essa cadeia de Markov. Vemos que $(x, y) \in E \Leftrightarrow (x, y) \in E'$.



(a) G = (V,E) (b) G' = (V',E')

Figura 3.2: Grafos associados à cadeia de Markov com conjunto de estados $X = \{1, 2, 3, 4\}$ e matriz de transição de probabilidade definida em (3.10).

3.2 Quantização de um Caminho Bipartido

Para definirmos um caminho quântico num grafo bipartido, vamos associar ao grafo o espaço de Hilbert $\mathcal{H}^{|X|\times|Y|} = \mathcal{H}^{|X|} \otimes \mathcal{H}^{|Y|}$. $\{|x\rangle : x \in X\}$ e $\{|y\rangle : y \in Y\}$ são as bases computacionais de $\mathcal{H}^{|X|}$ e $\mathcal{H}^{|Y|}$, respectivamente. Dessa forma, vamos quantizar o caminho bipartido (P, Q), definindo dois operadores unitários em

$\mathcal{H}^{|X|\times|Y|}$, cuja base computacional é $\{|x\rangle|y\rangle : x \in X, y \in Y\}$.

Seja $|\psi\rangle \in \mathcal{H}$, $\Pi_\psi = |\psi\rangle\langle\psi|$ é uma projeção ortogonal em $|\psi\rangle$. E,

$$ref_\psi = 2\Pi_\psi - I = 2|\psi\rangle\langle\psi| - I \tag{3.11}$$

é uma reflexão em relação a $|\psi\rangle$, pois

$$\left(2|\psi\rangle\langle\psi| - I\right)|\psi\rangle = |\psi\rangle, \tag{3.12}$$

$$\left(2|\psi\rangle\langle\psi| - I\right)|\psi\rangle^\perp = -|\psi\rangle^\perp. \tag{3.13}$$

Assim, seja $\mathcal{K}$ um subespaço de $\mathcal{H}$ gerado por um conjunto de estados ortogonais $\{|\psi_i\rangle\}$. Então,

$$\Pi_\mathcal{K} = \sum_i \Pi_{\psi_i} = \sum_i |\psi_i\rangle\langle\psi_i| \tag{3.14}$$

é uma projeção ortogonal em $\mathcal{K}$. E, $ref_\mathcal{K} = 2\Pi_\mathcal{K} - I$ é uma reflexão em relação a $\mathcal{K}$.

Defina $\mathcal{A} = span\left(\{|\phi_x\rangle : x \in X\}\right)$ e $\mathcal{B} = span\left(\{|\psi_y\rangle : y \in Y\}\right)$, onde

$$|\phi_x\rangle = |x\rangle \otimes \left(\sum_{y\in Y} \sqrt{p_{xy}}|y\rangle\right) = \sum_{y\in Y} \sqrt{p_{xy}}|x\rangle|y\rangle, \tag{3.15}$$

$$|\psi_y\rangle = \left(\sum_{x\in X} \sqrt{q_{yx}}|x\rangle\right) \otimes |y\rangle = \sum_{x\in X} \sqrt{q_{yx}}|x\rangle|y\rangle. \tag{3.16}$$

Por construção, vemos que $\{|\phi_x\rangle : x \in X\}$ e $\{|\psi_y\rangle : y \in Y\}$ são bases ortonormais de $\mathcal{A}$ e $\mathcal{B}$, respectivamente.

Definição 3.1 (Szegedy (2004a))**.** *A operação unitária $W = ref_\mathcal{B} ref_\mathcal{A}$, definida em $\mathcal{H}^{|X|\times|Y|}$, é chamada de quantização do caminho bipartido (P, Q).*

Onde,

$$ref_\mathcal{A} = 2\Pi_\mathcal{A} - I = 2\sum_{x\in X} |\phi_x\rangle\langle\phi_x| - I, \tag{3.17}$$

$$ref_\mathcal{B} = 2\Pi_\mathcal{B} - I = 2\sum_{y\in Y} |\psi_y\rangle\langle\psi_y| - I. \tag{3.18}$$

$\mathcal{A}$ e $\mathcal{B}$ também são conhecidos como os espaços gerados pelas colunas dos operadores $A : \mathcal{H}^{|X|} \to \mathcal{H}^{|X|\times|Y|}$ e $B : \mathcal{H}^{|Y|} \to \mathcal{H}^{|X|\times|Y|}$, respectivamente. Onde:

$$A = \sum_{x\in X} \big|\phi_x\big\rangle\big\langle x\big| \tag{3.19}$$

é a matriz cujas colunas são formadas pelos vetores $\big|\phi_x\big\rangle$. E,

$$B = \sum_{y\in Y} \big|\psi_y\big\rangle\big\langle y\big| \tag{3.20}$$

é a matriz cujas colunas são formadas pelos vetores $\big|\psi_y\big\rangle$.

Logo, segue que,

$$AA^* = \sum_{i,j\in X} \big|\phi_i\big\rangle\big\langle i\big|j\big\rangle\big\langle\phi_j\big| = \sum_{x\in X} \big|\phi_x\big\rangle\big\langle\phi_x\big| = \sum_{x\in X} \Pi_{\phi_x} = \Pi_{\mathcal{A}}, \tag{3.21}$$

$$BB^* = \sum_{i,j\in Y} \big|\psi_i\big\rangle\big\langle i\big|j\big\rangle\big\langle\psi_j\big| = \sum_{y\in Y} \big|\psi_y\big\rangle\big\langle\psi_y\big| = \sum_{y\in Y} \Pi_{\psi_y} = \Pi_{\mathcal{B}}. \tag{3.22}$$

Então, podemos reescrever

$$ref_{\mathcal{A}} = 2\Pi_{\mathcal{A}} - I = 2AA^* - I, \tag{3.23}$$

$$ref_{\mathcal{B}} = 2\Pi_{\mathcal{B}} - I = 2BB^* - I. \tag{3.24}$$

Para entendermos melhor como funciona esse tipo de passeio, ou seja, como se dá a evolução do sistema pelo operador W; vamos exemplificar, utilizando o grafo apresentado na Figura 3.3.

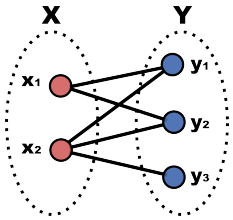


Figura 3.3: Grafo bipartido cujo conjunto de vértices é dado por $V = X \cup Y$ onde, $X = \{x_1, x_2\}$ e $Y = \{y_1, y_2, y_3\}$.

Com as seguintes matrizes de transição de probabilidade

$$P = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{bmatrix} \text{ e } Q = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{3} & \frac{2}{3} \\ 0 & 1 \end{bmatrix}, \tag{3.25}$$

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

$$\left\{|x_1\rangle|y_1\rangle, |x_1\rangle|y_2\rangle, |x_1\rangle|y_3\rangle, |x_2\rangle|y_1\rangle, |x_2\rangle|y_2\rangle, |x_2\rangle|y_3\rangle\right\}. \tag{3.26}$$

Os estados $|\phi_{x_i}\rangle$ são descritos como:

$$|\phi_{x_1}\rangle = \sqrt{\frac{1}{2}}|x_1\rangle|y_1\rangle + \sqrt{\frac{1}{2}}|x_1\rangle|y_2\rangle, \tag{3.27}$$

$$|\phi_{x_2}\rangle = \sqrt{\frac{1}{4}}|x_2\rangle|y_1\rangle + \sqrt{\frac{1}{4}}|x_2\rangle|y_2\rangle + \sqrt{\frac{1}{2}}|x_2\rangle|y_3\rangle. \tag{3.28}$$

E os estados $|\psi_{y_i}\rangle$:

$$|\psi_{y_1}\rangle = \sqrt{\frac{1}{2}}|x_1\rangle|y_1\rangle + \sqrt{\frac{1}{2}}|x_2\rangle|y_1\rangle, \tag{3.29}$$

$$|\psi_{y_2}\rangle = \sqrt{\frac{1}{3}}|x_1\rangle|y_2\rangle + \sqrt{\frac{2}{3}}|x_2\rangle|y_2\rangle, \tag{3.30}$$

$$|\psi_{y_3}\rangle = |x_2\rangle|y_3\rangle. \tag{3.31}$$

A partir disso, é possível escrever as matrizes A e B, que possuem como

elementos de suas colunas, os estados $\big|\phi_{x_i}\big\rangle$ e $\big|\psi_{y_i}\big\rangle$, respectivamente.

$$A = \begin{bmatrix} \sqrt{\frac{1}{2}} & 0 \\ \sqrt{\frac{1}{2}} & 0 \\ 0 & 0 \\ 0 & \sqrt{\frac{1}{4}} \\ 0 & \sqrt{\frac{1}{4}} \\ 0 & \sqrt{\frac{1}{2}} \end{bmatrix} \text{ e } B = \begin{bmatrix} \sqrt{\frac{1}{2}} & 0 & 0 \\ 0 & \sqrt{\frac{1}{3}} & 0 \\ 0 & 0 & 0 \\ \sqrt{\frac{1}{2}} & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{3.32}$$

Com essas duas matrizes em mãos, é fácil encontrar o operador W, que é dado por: $W = (2BB^* - I)(2AA^* - I)$,

$$W = \begin{bmatrix} 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{\sqrt{2}}{2} \\ -\frac{1}{3} & 0 & 0 & \frac{\sqrt{2}}{3} & -\frac{\sqrt{2}}{3} & \frac{2}{3} \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{2\sqrt{2}}{3} & 0 & 0 & \frac{1}{6} & -\frac{1}{6} & \frac{\sqrt{2}}{6} \\ 0 & 0 & 0 & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & 0 \end{bmatrix}. \tag{3.33}$$

Aplicando o operador W ao estado $\big|x_1\big\rangle\big|y_1\big\rangle$, vemos que

$$W\big|x_1\big\rangle\big|y_1\big\rangle = W \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -\frac{1}{3} \\ 0 \\ 0 \\ \frac{2\sqrt{2}}{3} \\ 0 \end{bmatrix} = -\frac{1}{3}\big|x_1\big\rangle\big|y_2\big\rangle + \frac{2\sqrt{2}}{3}\big|x_2\big\rangle\big|y_2\big\rangle. \tag{3.34}$$

Então, partindo de $\big|x_1\big\rangle\big|y_1\big\rangle$ (podemos interpretar esse estado como a posição do caminhante, estando no vértice x_1, tendo saído do vértice y_1), após a aplicação do operador de evolução, o caminhante terá probabilidade $\frac{1}{9}$ de estar no vértice x_1,

vindo de y_2 e probabilidade $\frac{8}{9}$ de estar no vértice x_2, vindo de y_2.

3.2.1 Análise espectral de W

A fim de calcular o espectro de W, vamos utilizar a decomposição em valores singulares da seguinte matriz: $D(A,B) = A^*B$, que é chamada de matriz discriminante.

$$D(A,B) = A^*B = \sum_{\substack{x\in X\\ y\in Y}} \big|x\big\rangle \big\langle\phi_x\big|\psi_y\big\rangle \big\langle y\big|. \tag{3.35}$$

Mas,

$$\begin{aligned}\big\langle\phi_x\big|\psi_y\big\rangle &= \left(\sum_{i\in Y}\sqrt{p_{xi}}\big\langle x\big|\big\langle i\big|\right)\left(\sum_{j\in X}\sqrt{q_{yj}}\big|j\big\rangle\big|y\big\rangle\right)\\ &= \sum_{i\in Y, j\in X}\sqrt{p_{xi}q_{yj}}\,\big\langle x\big|j\big\rangle\big\langle i\big|y\big\rangle\\ &= \sqrt{p_{xy}q_{yx}}.\end{aligned} \tag{3.36}$$

Substituindo em (3.35),

$$D(A,B) = \sum_{\substack{x\in X\\ y\in Y}} \sqrt{p_{xy}q_{yx}}\big|x\big\rangle\big\langle y\big|, \tag{3.37}$$

ou seja, $D(A,B)$ é a matriz cujos elementos são dados por $D(A,B)_{ij} = \sqrt{p_{ij}q_{ji}}$.

Seja $\big|v\big\rangle \in \mathcal{H}^{|Y|}$, podemos interpretar

$$AD(A,B)\big|v\big\rangle = AA^*B\big|v\big\rangle = \Pi_{\mathcal{A}}B\big|v\big\rangle \tag{3.38}$$

como uma projeção ortogonal de $\mathcal{B}$ em $\mathcal{A}$.

Da mesma forma, se $\big|w\big\rangle \in \mathcal{H}^{|X|}$, então

$$BD(A,B)^*\big|w\big\rangle = BB^*A\big|w\big\rangle = \Pi_{\mathcal{B}}A\big|w\big\rangle \tag{3.39}$$

é uma projeção ortogonal de $\mathcal{A}$ em $\mathcal{B}$.

Agora, considere λ o valor singular de $D(A,B)$ com $\big|v\big\rangle$ e $\big|w\big\rangle$ seus vetores

singulares associados (normalizados). Então, as seguintes identidades são satisfeitas:

$$D(A,B)\big|v\big\rangle = \lambda\big|w\big\rangle \Rightarrow A^*B\big|v\big\rangle = \lambda\big|w\big\rangle, \tag{3.40}$$

$$D(A,B)^*\big|w\big\rangle = \lambda\big|v\big\rangle \Rightarrow B^*A\big|w\big\rangle = \lambda\big|v\big\rangle. \tag{3.41}$$

Dessa forma, temos

$$AA^*B\big|v\big\rangle = \lambda A\big|w\big\rangle \Rightarrow \Pi_{\mathcal{A}}B\big|v\big\rangle = \lambda A\big|w\big\rangle, \tag{3.42}$$

$$BB^*A\big|w\big\rangle = \lambda B\big|v\big\rangle \Rightarrow \Pi_{\mathcal{B}}A\big|w\big\rangle = \lambda B\big|v\big\rangle. \tag{3.43}$$

Podemos notar que,

$$\big|\big|B\big|v\big\rangle\big|\big| = \big|\big|\big|v\big\rangle\big|\big| = 1 \text{ e } \big|\big|A\big|w\big\rangle\big|\big| = \big|\big|\big|w\big\rangle\big|\big| = 1 \tag{3.44}$$

pois,

$$\big|\big|A\big|w\big\rangle\big|\big| = \sqrt{\big\langle w\big|A^*A\big|w\big\rangle} = \sqrt{\big\langle w\big|w\big\rangle} = \big|\big|\big|w\big\rangle\big|\big| = 1, \tag{3.45}$$

$$\big|\big|B\big|v\big\rangle\big|\big| = \sqrt{\big\langle v\big|B^*B\big|v\big\rangle} = \sqrt{\big\langle v\big|v\big\rangle} = \big|\big|\big|v\big\rangle\big|\big| = 1. \tag{3.46}$$

Portanto, das Equações (3.42), (3.43), (3.44) e, como as projeções não aumentam o tamanho do vetor, todos os valores singulares de $D(A,B)$ são no máximo 1. Além disso, os valores singulares são positivos por definição. Logo, podemos escrever λ, valor singular de $D(A,B)$, como

$$\lambda = \cos\theta, \quad 0 \leq \theta \leq \pi/2, \tag{3.47}$$

onde θ é o ângulo entre os subespaços $\mathcal{A}$ e $\mathcal{B}$ $\big($pois, $\big\langle w\big|A^*B\big|v\big\rangle = \cos\theta\big)$.

Agora, estamos prontos para encontrar o espectro de W.

Teorema 3.1 (Szegedy (2004a))**.** *Sejam* $\cos\theta_1, \ldots, \cos\theta_l$ *os valores singulares de* $D(A,B)$ *em* $(0,1)$ *e seus vetores singulares associados* $\big|v_k\big\rangle$ *e* $\big|w_k\big\rangle (1 \leq k \leq l)$*:*

(1) Em $\langle \mathcal{A}, \mathcal{B} \rangle$ os autovalores de W que têm parte imaginária não nula 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 $\mathcal{A} \cap \mathcal{B}$, W atua como I. $\mathcal{A} \cap \mathcal{B}$ coincide com o conjunto de vetores singulares de $D(A, B)$ com valor singular 1;

(3) Em $\mathcal{A} \cap \mathcal{B}^\perp$ e $\mathcal{A}^\perp \cap \mathcal{B}$, W atua como $-I$. $\mathcal{A} \cap \mathcal{B}^\perp$ coincide com o conjunto de vetores singulares à esquerda de $D(A, B)$ e $\mathcal{A}^\perp \cap \mathcal{B}$ coincide com o conjunto de vetores singulares à direita de $D(A, B)$ com valor singular 0;

(4) Em $\langle \mathcal{A}, \mathcal{B} \rangle^\perp = \mathcal{A}^\perp \cap \mathcal{B}^\perp$, W atua como I.

Demonstração. Sabemos que $W = ref_{\mathcal{B}} ref_{\mathcal{A}} = (2\Pi_{\mathcal{B}} - 1)(2\Pi_{\mathcal{A}} - 1)$. Para cada par de vetores singulares $\big|v\big\rangle$ e $\big|w\big\rangle$ com valor singular λ:

$$\Pi_{\mathcal{A}} B\big|v\big\rangle = \lambda A\big|w\big\rangle \text{ e } \Pi_{\mathcal{B}} A\big|w\big\rangle = \lambda B\big|v\big\rangle, \tag{3.48}$$

ou seja, $\big\langle B\big|v\big\rangle, A\big|w\big\rangle\big\rangle$ é invariante sob a ação de W. Pois, seja $\big|u\big\rangle \in \big\langle B\big|v\big\rangle, A\big|w\big\rangle\big\rangle$, $W\big|u\big\rangle \in \big\langle B\big|v\big\rangle, A\big|w\big\rangle\big\rangle$.

Vamos, agora, tentar achar os autovalores de W a partir dos valores singulares de $D(A, B)$:

- $\lambda = \cos\theta = 1 \Rightarrow \theta = 0$

$$\Pi_{\mathcal{A}} B\big|v\big\rangle = A\big|w\big\rangle \text{ e } \Pi_{\mathcal{B}} A\big|w\big\rangle = B\big|v\big\rangle. \tag{3.49}$$

$\Rightarrow B\big|v\big\rangle$ e $A\big|w\big\rangle \in \mathcal{A} \cap \mathcal{B}$. Isso ocorre porque o ângulo entre $\mathcal{A}$ e $\mathcal{B}$ é 0. Consequentemente, em $\mathcal{A} \cap \mathcal{B}$, W atua como a identidade. E, portanto, $\mathcal{A} \cap \mathcal{B}$ são autovetores de W com autovalor 1.

- $\lambda = \cos\theta = 0 \Rightarrow \theta = \pi/2$

$$\Pi_{\mathcal{A}} B\big|v\big\rangle = 0 \text{ e } \Pi_{\mathcal{B}} A\big|w\big\rangle = 0. \tag{3.50}$$

Para que isso ocorra teremos: $B\big|v\big\rangle \in \mathcal{A}^{\perp} \cap \mathcal{B}$ e $A\big|w\big\rangle \in \mathcal{A} \cap \mathcal{B}^{\perp}$. Nesses conjuntos, W atua como $-I$, ou seja, todo vetor em $\mathcal{A}^{\perp} \cap \mathcal{B}$ e em $\mathcal{A} \cap \mathcal{B}^{\perp}$ é autovetor de W com autovalor -1.

- $\lambda = \cos\theta \in (0, 1)$

$$\Pi_{\mathcal{A}} B\big|v\big\rangle = \cos\theta A\big|w\big\rangle \text{ e } \Pi_{\mathcal{B}} A\big|w\big\rangle = \cos\theta B\big|v\big\rangle. \tag{3.51}$$

Esse é o caso em que $\big\langle B\big|v\big\rangle, A\big|w\big\rangle\big\rangle$ tem dimensão 2. Então, vamos tentar encontrar β tal que $\big|u\big\rangle = A\big|w\big\rangle + \beta B\big|v\big\rangle$ seja autovetor de W, ou seja, $W\big|u\big\rangle = e^{i\alpha}\big|u\big\rangle$ (já que W é unitário, seus autovalores são da forma $e^{i\alpha}$).

$$\begin{aligned}
W\big|u\big\rangle &= (2\Pi_{\mathcal{B}} - 1)(2\Pi_{\mathcal{A}} - 1)\left(A\big|w\big\rangle + \beta B\big|v\big\rangle\right) \\
&= (2\Pi_{\mathcal{B}} - 1)\left(A\big|w\big\rangle + 2\beta\Pi_{\mathcal{A}} B\big|v\big\rangle - \beta B\big|v\big\rangle\right) \\
&= (2\Pi_{\mathcal{B}} - 1)\left(A\big|w\big\rangle + 2\beta\cos\theta A\big|w\big\rangle - \beta B\big|v\big\rangle\right) \\
&= (2\Pi_{\mathcal{B}} - 1)\left((1 + 2\beta\cos\theta)A\big|w\big\rangle - \beta B\big|v\big\rangle\right) \\
&= 2(1 + 2\beta\cos\theta)\Pi_{\mathcal{B}} A\big|w\big\rangle - (1 + 2\beta\cos\theta)A\big|w\big\rangle - \beta B\big|v\big\rangle \\
&= (2 + 4\beta\cos\theta)\cos\theta B\big|v\big\rangle - (1 + 2\beta\cos\theta)A\big|w\big\rangle - \beta B\big|v\big\rangle \\
&= (-1 - 2\beta\cos\theta)A\big|w\big\rangle + (2\cos\theta + 4\beta\cos^2\theta - \beta)B\big|v\big\rangle.
\end{aligned} \tag{3.52}$$

Assim, resolvendo o seguinte sistema de equações:

$$\begin{cases} e^{i\alpha} = -1 - 2\beta\cos\theta \\ \beta e^{i\alpha} = 2\cos\theta + 4\beta\cos^2\theta - \beta \end{cases} \tag{3.53}$$

encontramos que: $\beta = -e^{\pm i\theta}$ e $\alpha = \pm 2\theta$. Portanto, $\big|u\big\rangle = A\big|w\big\rangle - e^{\pm i\theta} B\big|v\big\rangle$ com $\lambda = e^{\pm 2i\theta}$.

É importante ressaltar que no caso em que $\langle B|v\rangle, A|w\rangle\rangle$ tem dimensão 2, a aplicação de W a um dos elementos desse espaço realiza duas reflexões em dois eixos diferentes, o que equivale a realizar uma rotação cujo ângulo é o dobro do ângulo entre esses eixos. Então, teremos que, nesse espaço bidimensional, W aplicará uma rotação de 2θ.

Os vetores singulares de $D(A, B)$ descrevem o comportamento de W em $\langle \mathcal{A}, \mathcal{B}\rangle$. Em $\langle \mathcal{A}, \mathcal{B}\rangle^{\perp} = \mathcal{A}^{\perp} \cap \mathcal{B}^{\perp}$ é fácil ver que W atuará como I. Seja $|u\rangle$ um vetor nesse conjunto,

$$(2\Pi_{\mathcal{B}} - 1)(2\Pi_{\mathcal{A}} - 1)|u\rangle = (2\Pi_{\mathcal{B}} - 1)\left(-|u\rangle\right) = -\left(-|u\rangle\right) = |u\rangle. \tag{3.54}$$

□

3.2.2 Evolução do Sistema

Seja $|z\rangle \in \langle \mathcal{A}, \mathcal{B}\rangle$ unitário. Nosso objetivo, nessa seção, é estudar uma média associada a evolução do sistema: $|z\rangle$, $W|z\rangle$, $W^2|z\rangle$, ..., $W^T|z\rangle$, como vemos em Szegedy (2004a). Este estudo será importante pois estará associado a definição do Tempo de Alcance no caso quântico.

Assim, defina,

$$\mathcal{F}(z, T) = \frac{1}{T+1} \sum_{t=0}^{T} \langle z|W^t|z\rangle . \tag{3.55}$$

$|z\rangle$ mora no subespaço $\langle A|w\rangle, B|v\rangle\rangle$, que é invariante sob W, com $\cos\theta$ seu valor singular associado. Mas, se fizermos $|z\rangle = \sum_k \nu_k |z_k\rangle$ tal que $\left|\left||z_k\rangle\right|\right| = 1$ e $|z_k\rangle \in \langle A|w_k\rangle, B|v_k\rangle\rangle$ bidimensional com $\cos\theta_k$ o valor singular associado, então,

$$\begin{aligned} \mathcal{F}(z, T) &= \frac{1}{T+1} \sum_{t=0}^{T} \langle z|W^t|z\rangle \\ &= \frac{1}{T+1} \sum_{t=0}^{T} \sum_{k} \nu_k^2 \langle z_k|W^t|z_k\rangle . \end{aligned} \tag{3.56}$$

Nesse caso, temos que $\langle z_k|W^t|z_k\rangle = \cos(2t\theta_k)$, pois como já vimos, nesse espaço bidimensional, W realiza uma rotação cujo ângulo é o dobro do ângulo

entre os eixos de suas reflexões. Utilizando desse fato e considerando a seguinte identidade,

$$\sum_{t=0}^{T}\cos(t\beta)=\frac{\cos(T\beta)-\cos((T+1)\beta)+1-\cos\beta}{2(1-\cos\beta)}, \tag{3.57}$$

temos que

$$\begin{aligned}\mathcal{F}(z,T)&=\frac{1}{T+1}\sum_{t=0}^{T}\sum_{k}\nu_k^2\cos(2t\theta_k)\\&=\sum_{k}\nu_k^2\frac{\cos(2T\theta_k)-\cos(2(T+1)\theta_k)+1-\cos(2\theta_k)}{2(T+1)(1-\cos 2\theta_k)}.\end{aligned} \tag{3.58}$$

Vamos, então, obter um limite superior para $\mathcal{F}(z,T)$. Naturalmente, podemos ver que

$$\mathcal{F}(z,T)=\frac{1}{T+1}\sum_{t=0}^{T}\left\langle z\middle|W^t\middle|z\right\rangle\leq\frac{1}{T+1}\sum_{t=0}^{T}\left\langle z\middle|z\right\rangle\leq\sum_{k}\nu_k^2 \tag{3.59}$$

já que W é um operador unitário composto por duas reflexões.

Além disso, utilizando as inequações $|\cos\alpha-\cos\beta|\leq|\alpha-\beta|$ e $1-\cos\alpha\geq\alpha^2/8\Rightarrow\alpha\leq 8(1-\cos\alpha)/\alpha$, temos

$$\begin{aligned}\mathcal{F}(z,T)&=\sum_{k}\nu_k^2\frac{\cos(2T\theta_k)-\cos(2(T+1)\theta_k)+1-\cos(2\theta_k)}{2(T+1)(1-\cos(2\theta_k))}\\&\leq\sum_{k}\nu_k^2\frac{|2T\theta_k-2(T+1)\theta_k|+|0-2\theta_k|}{2(T+1)(1-\cos(2\theta_k))}\\&\leq\sum_{k}\nu_k^2\frac{4\theta_k}{2(T+1)(1-\cos(2\theta_k))}\\&\leq\sum_{k}\nu_k^2\frac{2\left(\frac{8(1-\cos(2\theta_k))}{2\theta_k}\right)}{2(T+1)(1-\cos(2\theta_k))}\\&\leq\sum_{k}\nu_k^2\frac{4}{(T+1)\theta_k}.\end{aligned} \tag{3.60}$$

Portanto, de (3.59) e (3.60),

$$\mathcal{F}(z,T) \leq \sum_k \nu_k^2 \min\left\{1, \frac{4}{(T+1)\theta_k}\right\}. \tag{3.61}$$

Lema 3.1 (Szegedy (2004a)). *Seja* $E = \sum_k \nu_k^2/\theta_k$, $T \geq 100E$. *Temos que* $\mathcal{F}(z,T) \leq 0.5$.

Demonstração. Definindo $K = \{k|1/\theta_k > 10E\}$ temos que

$$E = \sum_{k\in K} \frac{\nu_k^2}{\theta_k} + \sum_{k\notin K} \frac{\nu_k^2}{\theta_k} > \sum_{k\in K} \nu_k^2 10E + \sum_{k\notin K} \frac{\nu_k^2}{\theta_k} \geq 10E \sum_{k\in K} \nu_k^2. \tag{3.62}$$

Logo,

$$\sum_{k\in K} \nu_k^2 \leq 0.1. \tag{3.63}$$

De (3.61), segue que:

$$\mathcal{F}(z,T) \leq \sum_{k\in K} \nu_k^2 + \sum_{k\notin K} \nu_k^2 \frac{4}{(T+1)\theta_k} \leq 0.1 + \frac{4.10E}{100E} \leq 0.5. \tag{3.64}$$

□

Esse Lema 3.1 terá um papel importante quando formos encontrar um limite superior para o Tempo de Alcance quântico, que será definido no capítulo a seguir.

Capítulo 4

Tempo de Alcance Quântico

Na literatura podemos encontrar várias contibuições a respeito do Tempo de Alcance em caminhos quânticos. As referências (Kempe, 2003a) e (Krovi e Brun, 2006) definem maneiras diferentes para calcular o Tempo de Alcance, que variam entre, deixar o caminho evoluir até que a probabilidade de atingir um elemento marcado ultrapasse um determinado valor; ou fazer uma medida 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, 2004a) define o Tempo de Alcance sob o escopo da quantização de um caminho bipartido. Além disso, ele é descrito para um subconjunto de elementos marcados $M \subseteq X$, como veremos, a seguir.

4.1 Definição

Assumiremos daqui em diante que $X = Y$, $P = P^*$ e $P = Q$. Vamos alterar o nosso caminho, utilizando a matriz P', já definida na seção 2.5, dada por:

$$P' = \begin{pmatrix} P_M & P'' \\ 0 & I \end{pmatrix}. \tag{4.1}$$

Essa matriz estocástisca faz com que ao encontrar um elemento marcado, o caminhante permaneça nesse estado. Ou seja, a evolução do sistema, partindo de uma distribuição de probabilidade, nos levará a algum elemento marcado (nesse caso, todos os caminhos não levam a Roma e, sim, a M). Como vemos na descrição da matriz P', teremos $p'_{xy} = \delta_{xy}$ para cada elemento $x \in M$.

Podemos perceber que o Tempo de Alcance clássico, partindo da distribuição estacionária π, ou seja, $\sum_x \pi_x H_{x,M}$, coincide com o primeiro t em que a norma em L_1 de $\pi^* P'^t - \pi^*$ se torna suficientemente grande. Pois, somente a partir de um determinado instante t, o caminhante terá alcançado um dos elementos marcados.

Chamaremos W_P, a quantização de P e $W_{P'}$, a quantização de P'. A intenção de Szegedy (2004a) é definir o Tempo de Alcance de W_P como o menor t tal que a norma em L_2 de $W_{P'}^t \big|\phi_0\big\rangle - \big|\phi_0\big\rangle$ seja suficientemente grande. Onde,

$$\big|\phi_0\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y \in X} \sqrt{p_{xy}} \big|x\big\rangle \big|y\big\rangle \tag{4.2}$$

é o estado inicial. É válido lembrar que a matriz P é simétrica e, consequentemente, a distribuição estacionária será uniforme.

O estado inicial é invariante sob a ação de W_P, pois

$$\big|\phi_0\big\rangle = \frac{1}{\sqrt{n}} \sum_{x,y \in X} \sqrt{p_{xy}} \big|x\big\rangle \big|y\big\rangle = \sum_{x \in X} \frac{1}{\sqrt{n}} \sum_{y \in X} \sqrt{p_{xy}} \big|x\big\rangle \big|y\big\rangle = \sum_{x \in X} \frac{1}{\sqrt{n}} \big|\phi_x\big\rangle \in \mathcal{A}. \tag{4.3}$$

Mas, $p_{xy} = p_{yx}$, logo

$$\big|\phi_0\big\rangle = \sum_{y \in X} \frac{1}{\sqrt{n}} \sum_{x \in X} \sqrt{p_{yx}} \big|x\big\rangle \big|y\big\rangle = \sum_{y \in X} \frac{1}{\sqrt{n}} \big|\psi_y\big\rangle \in \mathcal{B}. \tag{4.4}$$

Ou seja, $\big|\phi_0\big\rangle \in \mathcal{A} \cap \mathcal{B}$ e, pelo Teorema 3.1, $\big|\phi_0\big\rangle$ é autovetor de W_P com autovalor 1.

Entretanto, $\big|\phi_0\big\rangle$ não permanecerá invariante sob a ação de $W_{P'}$. A cada passo, ele será modificado até que se torne um estado bem diferente. Isso ocorre porque $W_{P'}$ se comportará de maneira diferente nos estados $\big|x\big\rangle\big|y\big\rangle$ em que ou $\big|x\big\rangle$

ou $\big|y\big\rangle$ é um elemento em M.

Definição 4.1 (Szegedy (2004a)). *O Tempo de Alcance de W_P para um conjunto de elementos marcados M é o número de passos, $H_{P,M} = T$, tal que*

$$F(T) \geq 1 - \frac{m}{n}, \tag{4.5}$$

onde

$$F(T) = \frac{1}{T+1} \sum_{t=0}^{T} \Big|\Big|W_{P'}^{t}\big|\phi_0\big\rangle - \big|\phi_0\big\rangle\Big|\Big|^2. \tag{4.6}$$

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

Se considerarmos o espectro de $W_{P'}$ podemos encontrar uma expressão para a Equação (4.6). Seguindo o Teorema 3.1, do capítulo anterior, vamos chamar

$$\big|\alpha_j^{\pm}\big\rangle = \frac{A\big|w_j\big\rangle - \mathrm{e}^{\pm\, i\theta_j} B\big|v_j\big\rangle}{\sqrt{2}\sin\theta_j} \tag{4.7}$$

os autovetores normalizados de $W_{P'}$ com autovalores $e^{\pm 2i\theta_j}$, $0 < \theta_j \leq \frac{\pi}{2}$, que nos totaliza no máximo $2n$ autovetores de $W_{P'}$. Pois, os autovetores $\big|\alpha_j^{\pm}\big\rangle$ dependem dos vetores singulares da matriz discriminante, que é uma matriz quadrada de dimensão n. Os autovetores restantes pertencem ao autoespaço de autovalor 1, vamos chamá-los de $\big|\alpha_j\big\rangle$. Consequentemente, o número de autovetores dependerá da multiplicidade do valor singular 1 da matriz discriminante.

Podemos expressar nossa condição inicial na base de autovetores do operador de evolução:

$$\big|\phi_0\big\rangle = \sum_{j=1}^{n-k} \left(c_j^{+}\big|\alpha_j^{+}\big\rangle + c_j^{-}\big|\alpha_j^{-}\big\rangle\right) + \sum_{j=n-k+1}^{n^2-n+k} c_j\big|\alpha_j\big\rangle, \tag{4.8}$$

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

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

$$c_j^{\pm} = \langle \alpha_j^{\pm} | \phi_0 \rangle \tag{4.9}$$

e obedecem a seguinte condição

$$\sum_{j=1}^{n-k} \left(\left| c_j^{+} \right|^2 + \left| c_j^{-} \right|^2 \right) + \sum_{j=n-k+1}^{n^2-n+k} \left| c_j \right|^2 = 1. \tag{4.10}$$

Dessa forma, somente os valores singulares de D diferentes de 1 serão utilizados para calcular o Tempo de Alcance, pois ao aplicarmos o operador de evolução na condição inicial, obtemos

$$W_{P'}^t | \phi_0 \rangle = \sum_{j=1}^{n-k} \left(c_j^{+} \mathrm{e}^{2i\theta_j t} | \alpha_j^{+} \rangle + c_j^{-} \mathrm{e}^{-2i\theta_j t} | \alpha_j^{-} \rangle \right) + \sum_{j=n-k+1}^{n^2-n+k} c_j | \alpha_j \rangle \tag{4.11}$$

e ao fazermos a diferença $W_{P'}^t | \phi_0 \rangle - | \phi_0 \rangle$, vemos que os termos no autoespaço de autovalor 1 irão desaparecer. Assim, a partir das Equações (4.11) e (4.8), temos que

$$\left\| W_{P'}^t | \phi_0 \rangle - | \phi_0 \rangle \right\|^2 = 4 \sum_{j=1}^{n-k} \left| c_j \right|^2 \big(1 - T_{2t}(\cos\theta_j) \big), \tag{4.12}$$

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

Usando as Equações (4.12) e (4.6), obtemos

$$F(T) = \frac{2}{T+1} \sum_{j=1}^{n-k} \left| c_j \right|^2 \big(2\,T + 1 - U_{2T}(\cos\theta_j) \big), \tag{4.13}$$

onde U_n é o n-ésimo polinômio de Chebyshev do segundo tipo. Portanto, o Tempo de Alcance quântico é dado por

$$H_{P,M} = \left\lceil F^{-1} \left(1 - \frac{m}{n} \right) \right\rceil. \tag{4.14}$$

4.2 Resultados

Nesta seção, veremos alguns resultados obtidos a partir da definição do Tempo de Alcance quântico. Como consequência, obteremos a relação entre os Tempos de Alcance clássico e quântico, mostrando o ganho que existe ao utilizarmos essa nova definição.

Lema 4.1 (Szegedy (2004a))**.** *O Tempo de Alcance de W_P com respeito a M é, no máximo,*

$$\frac{100}{1-\frac{m}{n}} \sum_{k=1}^{n-m} \nu_k^2 \sqrt{\frac{1}{1-\lambda'_k}}, \tag{4.15}$$

onde $\left|v'_1\right\rangle, \ldots, \left|v'_{n-m}\right\rangle$ são os autovetores normalizados de P_M com, $\lambda'_1, \ldots, \lambda'_{n-m}$ 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, $\left|\hat{u}\right\rangle = \sum_{k=1}^{n-m} \nu_k \left|v'_k\right\rangle$.

Demonstração. Sabemos que $D_{ij} = \sqrt{p_{ij}q_{ji}}$. Nesse caso, temos $P = Q$ e $p_{ij} = p_{ji}$. Logo,

$$P' = \begin{pmatrix} P_M & P'' \\ 0 & I \end{pmatrix} \Rightarrow D = \begin{pmatrix} P_M & 0 \\ 0 & I \end{pmatrix}. \tag{4.16}$$

Para $1 \leq k \leq n-m$, considere $\left|v_k\right\rangle$ o vetor obtido de $\left|v'_k\right\rangle$, aumentando com zeros as coordenadas indexadas por M. É fácil ver que $\left|v_k\right\rangle$ $(1 \leq k \leq n-m)$ e $\left|x\right\rangle$ $(x \in M)$ são autovetores de D. Nesse caso, como D é simétrica, o módulo dos seus autovalores são os seus valores singulares.

Defina,

$$\left|\phi_k\right\rangle = \sum_{x,y \in X} \left\langle x|v_k\right\rangle \sqrt{p_{xy}} \left|x\right\rangle \left|y\right\rangle = \sum_{x \in X} \left\langle x|v_k\right\rangle \left|\phi_x\right\rangle = A\left|v_k\right\rangle, \tag{4.17}$$

$$\left|\psi_k\right\rangle = \sum_{x,y \in X} \left\langle y|v_k\right\rangle \sqrt{p_{yx}} \left|x\right\rangle \left|y\right\rangle = \sum_{y \in X} \left\langle y|v_k\right\rangle \left|\psi_y\right\rangle = B\left|v_k\right\rangle. \tag{4.18}$$

Como consequência do Teorema 3.1, temos que o subespaço $\left\langle \left|\phi_k\right\rangle, \left|\psi_k\right\rangle \right\rangle$ é

invariante sob $W_{P'}$. Vamos escrever $\big|\phi_0\big\rangle = \big|\phi_{01}\big\rangle + \big|\phi_{02}\big\rangle$ onde,

$$\big|\phi_{01}\big\rangle = \frac{1}{\sqrt{n}} \sum_{\substack{x\in X\setminus M \\ y\in X}} \sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle, \tag{4.19}$$

$$\big|\phi_{02}\big\rangle = \frac{1}{\sqrt{n}} \sum_{\substack{x\in M \\ y\in X}} \sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle. \tag{4.20}$$

Note que,

(1) $\big\langle\phi_{01}\big|\phi_{02}\big\rangle = 0$

(2) $\big\langle\phi_{02}\big|\phi_{02}\big\rangle = \dfrac{m}{n} = \epsilon$ pois,

$$\big|\phi_{02}\big\rangle = \sum_{x\in M} \frac{1}{\sqrt{n}} \sum_{y\in X} \sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle = \sum_{x\in M} \frac{1}{\sqrt{n}}\big|\phi_x\big\rangle; \tag{4.21}$$

(3) $\big|\phi_{01}\big\rangle = \sum_{k=1}^{n-m} \nu_k\big|\phi_k\big\rangle$ pois,

$$\frac{1}{\sqrt{n}}\mathbf{1} = \sum_{k=1}^{n-m} \nu_k\big|v'_k\big\rangle \Rightarrow \frac{1}{\sqrt{n}} = \sum_{k=1}^{n-m} \nu_k \big\langle x\big|v'_k\big\rangle \quad \forall x \in X\setminus M, \tag{4.22}$$

substituindo em $\big|\phi_{01}\big\rangle$, obtemos:

$$\begin{aligned} \big|\phi_{01}\big\rangle &= \sum_{\substack{x\in X\setminus M \\ y\in X}} \left(\sum_{k=1}^{n-m} \nu_k \big\langle x\big|v'_k\big\rangle\right) \sqrt{p_{xy}}\big|x\big\rangle\big|y\big\rangle \\ &= \sum_{k=1}^{n-m} \nu_k \sum_{x\in X\setminus M} \big\langle x\big|v'_k\big\rangle \big|\phi_x\big\rangle \\ &= \sum_{k=1}^{n-m} \nu_k \sum_{x\in X} \big\langle x\big|v_k\big\rangle \big|\phi_x\big\rangle = \sum_{k=1}^{n-m} \nu_k\big|\phi_k\big\rangle; \end{aligned} \tag{4.23}$$

(4) $\big\langle\phi_{01}\big|\phi_{01}\big\rangle = 1 - \epsilon = \sum_{k=1}^{n-m} \nu_k^2$.

Agora, vamos considerar:

$$T \geq \frac{100}{1-\frac{m}{n}} \sum_{k=1}^{n-m} \nu_k^2 \sqrt{\frac{1}{1-\lambda'_k}} = \frac{100}{1-\epsilon} \sum_{k=1}^{n-m} \nu_k^2 \sqrt{\frac{1}{1-\cos\theta_k}}. \tag{4.24}$$

Mas, $1 - \cos\alpha \geq \alpha^2/8$. Então,

$$\begin{aligned} T &\geq \frac{100}{1-\epsilon}\sum_{k=1}^{n-m}\nu_k^2\sqrt{\frac{1}{\theta_k^2/8}} \\ &\geq \frac{100}{1-\epsilon}\sum_{k=1}^{n-m}\nu_k^2\frac{\sqrt{8}}{\theta_k} \\ &\geq 100\sum_{k=1}^{n-m}\frac{\nu_k^2}{1-\epsilon}\theta_k^{-1}. \end{aligned} \tag{4.25}$$

Segundo a definição de $\big|\phi_{01}\big\rangle$, obtida pelo item (3), podemos aplicar o Lema 3.1 para $\big|z\big\rangle = \frac{1}{\sqrt{1-\epsilon}}\big|\phi_{01}\big\rangle$. Dessa forma, obtemos que $\mathcal{F}(z,T) \leq 0.5$.

Mas,

$$\begin{aligned} \mathcal{F}(z,T) &= \frac{1}{T+1}\sum_{t=0}^{T}\big\langle z\big|W_{P'}^t\big|z\big\rangle \\ &= \frac{1}{T+1}\sum_{t=0}^{T}\frac{1}{1-\epsilon}\big\langle\phi_{01}\big|W_{P'}^t\big|\phi_{01}\big\rangle \\ &= \frac{1}{1-\epsilon}\mathcal{F}(\phi_{01},T). \end{aligned} \tag{4.26}$$

Logo,

$$\frac{1}{1-\epsilon}\mathcal{F}(\phi_{01},T) \leq 0.5 \Rightarrow \mathcal{F}(\phi_{01},T) \leq 0.5(1-\epsilon). \tag{4.27}$$

Como,

$$\mathcal{F}(\phi_{02},T) = \frac{1}{T+1}\sum_{t=0}^{T}\big\langle\phi_{02}\big|W_{P'}^t\big|\phi_{02}\big\rangle \leq \frac{1}{T+1}\sum_{t=0}^{T}\big\langle\phi_{02}\big|\phi_{02}\big\rangle \leq \epsilon. \tag{4.28}$$

Então, temos

$$\begin{aligned} \mathcal{F}(\phi_0,T) &= \mathcal{F}(\phi_{01},T) + \mathcal{F}(\phi_{02},T) \\ &\leq (1-\epsilon)0.5 + \epsilon = 0.5 + 0.5\epsilon. \end{aligned} \tag{4.29}$$

Precisamos estimar,

$$
\begin{aligned}
F(T) = \frac{1}{T+1}\sum_{t=0}^{T}\left|\left|W_{P'}^{t}\left|\phi_0\right\rangle - \left|\phi_0\right\rangle\right|\right|^2 &= \frac{1}{T+1}\sum_{t=0}^{T}\left(2 - 2\left\langle\phi_0\right|W_{P'}^{t}\left|\phi_0\right\rangle\right) \\
&= 2 - 2\mathcal{F}(\phi_0, T) \\
&\geq 2 - 2(0.5 + 0.5\epsilon) \\
&\geq 1 - \epsilon.
\end{aligned}
\tag{4.30}
$$

□

Corolário 4.1 (Szegedy (2004a))**.** *Para toda cadeia de Markov ergódica X, tal que $P = P^*$ e $M \subseteq X$, $m \leq \frac{n}{2}$, o Tempo de Alcance de W_P com respeito a M é $O\left(\sqrt{\frac{1}{1-\lambda(P_M)}}\right)$.*

Demonstração. Como

$$
\sum_{k=1}^{n-m}\nu_k^2 \leq 1, \tag{4.31}
$$

temos que

$$
\begin{aligned}
\sum_{k=1}^{n-m}\nu_k^2\sqrt{\frac{1}{1-\lambda_k'}} &\leq \sqrt{\sum_{k=1}^{n-m}\nu_k^2\frac{1}{1-\lambda_k'}} \\
&\leq \sqrt{\frac{1}{1-\lambda(P_M)}\sum_{k=1}^{n-m}\nu_k^2} \\
&\leq \sqrt{\frac{1}{1-\lambda(P_M)}}.
\end{aligned}
\tag{4.32}
$$

□

Consequentemente, o Tempo de Alcance quântico tem ganho quadrático em relação ao clássico, pois, como vimos no Lema 2.1 do Capítulo 2, o Tempo de Alcance clássico é $O\left(\frac{1}{1-\lambda(P_M)}\right)$.

Lema 4.2 (Szegedy (2004b))**.** *Dado que a diferença entre os dois maiores autovalores de P seja maior que δ e $\frac{m}{n} \geq \epsilon$ então $\lambda(P_M) \leq 1 - \epsilon\delta/2$.*

Demonstração. (Szegedy, 2004b) □

Esse resultado é importante pois relaciona o espectro da matriz P_M com o da matriz P. E, portanto, podemos expressar o Tempo de Alcance em termos de ϵ e δ.

Capítulo 5

Algoritmo de Detecção

A condição $\frac{1}{T+1}\sum_{t=0}^{T}\left|\left|W_{P'}^{t}\left|\phi_0\right\rangle - \left|\phi_0\right\rangle\right|\right|^2 \geq 1 - \frac{m}{n}$ não implica que ao medirmos $W_{P'}^{t}\left|\phi_0\right\rangle$ tenhamos um elemento marcado com probabilidade constante. Entretanto, muitas vezes precisamos apenas resolver o problema de detectar se o conjunto de elementos marcados é vazio ou não (Szegedy, 2004a).

É importante notar que em computação quântica, detectar e encontrar um elemento marcado são problemas substancialmente diferentes, ao contrário do que acontece na computação clássica (Magniez et al., 2009) .

Então, considere o Algoritmo 1, a seguir, que recebe W (que pode ser tanto W_P quanto $W_{P'}$ mas, não sabemos qual dos dois), escolhe aleatoriamente $1 \leq t \leq T$ e cria o estado

$$\frac{1}{2}\left|0\right\rangle\left(\left|\phi_0\right\rangle + W^t\left|\phi_0\right\rangle\right) + \frac{1}{2}\left|1\right\rangle\left(\left|\phi_0\right\rangle - W^t\left|\phi_0\right\rangle\right), \tag{5.1}$$

onde o primeiro registrador é um registrador de controle adicional.

Então, o algoritmo começa do estado inicial

$$\left|\psi_0\right\rangle = \left|0\right\rangle \otimes \left|\phi_0\right\rangle. \tag{5.2}$$

Na linha 2, ele aplica H (porta Hadamard[1]) no registrador de controle, transfor-

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

Algoritmo 1: Detecta Marcado (Szegedy, 2004b)

```
1  Coloque os registradores no estado inicial: |0⟩ ⊗ |φ_0⟩
2  Aplique H no registrador de controle
3  repita
4  |  se o registrador de controle for |1⟩ então
5  |  |  Aplique W;
6  até t vezes
7  Aplique H^{-1} no registrador de controle
8  Meça o estado final: |b⟩|i⟩|j⟩
9  se b = 1 ou i ∈ M então
10 |  retorna "elemento marcado detectado";
11 senão
12 |  retorna "conjunto de elementos marcados é vazio";
```

mando $\big|\psi_0\big\rangle$ em

$$\big|\psi_1\big\rangle = (H \otimes I)\big|\psi_0\big\rangle = \frac{1}{\sqrt{2}}\big|0\big\rangle\big|\phi_0\big\rangle + \frac{1}{\sqrt{2}}\big|1\big\rangle\big|\phi_0\big\rangle. \tag{5.3}$$

Depois, seguimos para a linha 3, onde aplicamos o operador W, t vezes, no estado que contém o registrador de controle igual a $\big|1\big\rangle$ (isso equivale a aplicar o operador W-controlado):

$$\big|\psi_2\big\rangle = C\left(W^t\right)\big|\psi_1\big\rangle = \frac{1}{\sqrt{2}}\big|0\big\rangle\big|\phi_0\big\rangle + \frac{1}{\sqrt{2}}\big|1\big\rangle W^t\big|\phi_0\big\rangle. \tag{5.4}$$

Em seguida, na linha 7, aplicamos $H^{-1} = H$ no registrador de controle:

$$\begin{aligned}\big|\psi_3\big\rangle = (H \otimes I)\big|\psi_2\big\rangle &= \frac{1}{2}\left(\big|0\big\rangle + \big|1\big\rangle\right)\big|\phi_0\big\rangle + \frac{1}{2}\left(\big|0\big\rangle - \big|1\big\rangle\right)W^t\big|\phi_0\big\rangle \\ &= \frac{1}{2}\big|0\big\rangle\left(\big|\phi_0\big\rangle + W^t\big|\phi_0\big\rangle\right) + \frac{1}{2}\big|1\big\rangle\left(\big|\phi_0\big\rangle - W^t\big|\phi_0\big\rangle\right).\end{aligned} \tag{5.5}$$

Na linha 8, fazemos a medida usando os projetores da base computacional, obtendo

$$\big|\psi_4\big\rangle = \big|b\big\rangle\big|i\big\rangle\big|j\big\rangle. \tag{5.6}$$

E, finalmente, após realizada a medida, poderemos concluir se o conjunto de elementos marcados é ou não vazio.

5.1 Análise do Algoritmo

Vamos analisar os dois casos: quando M é vazio, implicando que $W = W_P$ e quando M não é vazio, $W = W_{P'}$.

Então, se $W = W_P$, o registrador de controle é $\big|0\big\rangle$ com probabilidade 1, pois $\big|\phi_0\big\rangle$ é autovetor de W_P com autovalor 1 e, como consequência, o estado $\big|\psi_3\big\rangle$ se reduz a

$$\big|\psi_3\big\rangle = \big|0\big\rangle \left(\big|\phi_0\big\rangle + W^t\big|\phi_0\big\rangle\right). \tag{5.7}$$

Mas, se $W = W_{P'}$, o registrador de controle é $\big|1\big\rangle$ com probabilidade

$$\frac{1}{4(T+1)} \sum_{t=0}^{T} \left|\left|W^t\big|\phi_0\big\rangle - \big|\phi_0\big\rangle\right|\right|^2 \geq \frac{1}{4}\left(1 - \frac{m}{n}\right). \tag{5.8}$$

Ou seja, a probabilidade é da ordem do Tempo de Alcance quântico. Considerando que $m \leq \frac{n}{2}$, por exemplo, a probabilidade de M não ser vazio é, pelo menos, $\frac{1}{8}$.

5.2 Exemplo

Como exemplo, vamos descrever como podemos aplicar o algoritmo de Szegedy para resolver o problema da distinção de elementos (*Element Distinctness*).

5.2.1 O problema da distinção de elementos

Dado um conjunto de elementos, $\{x_1, \ldots, x_N\}$, queremos saber se todos 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) mostra como resolver esse problema através de um passeio quântico num grafo de Johnson[2] com complexidade $O\left(N^{\frac{2}{3}}\right)$, atingindo o limite inferior, mostrado por Shi (2002), para algoritmos quânticos.

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

5.2.2 Aplicando o algoritmo de Szegedy

Para utilizarmos o método de Szegedy também iremos utilizar um grafo de Johnson. 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 $r-1$. Na Figura (5.1), vemos um exemplo de um grafo de Johnson, $J_{4,2,1}$.

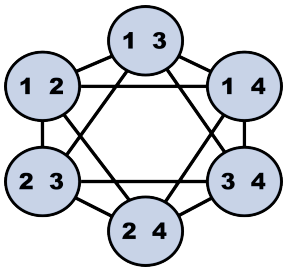


Figura 5.1: Grafo de Johnson, $J_{4,2,1}$. Os vértices são subconjuntos de tamanho 2 do seguinte conjunto $\{1,2,3,4\}$. Dois vértices estão conectados se a intersecção entre eles possui 1 elemento apenas.

Um vértice do grafo é marcado se ele contém um par de elementos iguais. Nosso espaço de estados X terá tamanho

$$n = \binom{N}{r}, \tag{5.9}$$

e as componentes de sua matriz de transição de probabilidade são dados por

$$p_{ij} = \begin{cases} \dfrac{1}{r(N-r)}, & \text{se } \left|i \cap j\right| = r-1; \\ 0, & \text{caso contrário.} \end{cases} \tag{5.10}$$

Ou seja,

$$P = \frac{J_{N,r,r-1}}{r(N-r)}. \tag{5.11}$$

Segundo Itakura (2008) os dois maiores autovalores de $J_{N,r,r-1}$ são: $\lambda_1 = r(N-r)$ e $\lambda_2 = r(N-r) - N$. Consequentemente, a diferença entre os dois

maiores autovalores de P é

$$\delta = 1 - \frac{\lambda_2}{r(N-r)} = \frac{N}{r(N-r)} > \frac{1}{r}. \tag{5.12}$$

Precisamos estabelecer um limite inferior pra $\frac{m}{n}$. Para isso, temos que considerar o caso em que temos apenas um par de elementos iguais. Assim,

$$\frac{m}{n} \geq \frac{\binom{N}{r-2}}{\binom{N}{r}} = \frac{r(r-1)}{(N-r-2)(N-r-1)} \geq \frac{r^2}{2N^2}. \tag{5.13}$$

Agora, podemos utilizar o Lema 4.2, que relaciona o espectro de P_M com o espectro de P. A partir das Equações (5.12) e (5.13), temos

$$\lambda(P_M) \leq 1 - \frac{\epsilon\delta}{2} = 1 - \frac{r}{4N^2}. \tag{5.14}$$

Substituindo esse valor no Tempo de Alcance quântico, obtemos

$$H_{P,M} = O\left(\sqrt{\frac{1}{1-\lambda(P_M)}}\right) = O\left(\frac{N}{\sqrt{r}}\right), \tag{5.15}$$

que é exatamente o resultado obtido por Ambainis (2004). Ao fazermos $r = N^{\frac{2}{3}}$, teremos $H_{P,M} = O\left(N^{\frac{2}{3}}\right)$. A vantagem de utilizarmos o algoritmo de Szegedy deve-se ao fato de não precisarmos de algoritmos diferentes quando temos mais de uma solução, ou seja, quando temos mais de um par de elementos iguais no nosso conjunto; ao contrário do que acontece no algoritmo de Ambainis.

Capítulo 6

Tempo de Alcance no Grafo Completo

Após termos visto todo o desenvolvimento desta teoria de cadeias de Markov quânticas que, nada mais é do que a quantização do caminho bipartido obtido de uma cadeia de Markov; vamos aplicá-la ao grafo completo para, assim, completarmos nosso entendimento. Os resultados deste capítulo encontram-se descritos em (Santos e Portugal, 2010).

Vamos considerar que os vértices do grafo são numerados de 1 a n e que os últimos m vértices são marcados. Relembrando a decomposição espectral de P_M do grafo completo, apresentada na seção 2.5.2:

$$P_M = \frac{n-m-1}{n-1}\big|v'_{n-m}\big\rangle\big\langle v'_{n-m}\big| - \frac{1}{n-1}\sum_{k=1}^{n-m-1}\big|v'_k\big\rangle\big\langle v'_k\big|, \tag{6.1}$$

onde

$$\big|v'_{n-m}\big\rangle = \frac{1}{\sqrt{n-m}}\sum_{j=1}^{n-m}\big|j\big\rangle \text{ e } \big|v'_k\big\rangle = \frac{1}{\sqrt{k+k^2}}\left(\sum_{j=1}^{k}\big|j\big\rangle - k\big|k+1\big\rangle\right). \tag{6.2}$$

6.1 Valores e vetores singulares da matriz discriminante

Os elementos da matriz estocástica P', que é obtida a partir da matriz estocástica P para o grafo completo, são dados por:

$$p'_{xy} = \begin{cases} \dfrac{1-\delta_{xy}}{n-1}, & 1 \le x \le n-m; \\ \delta_{xy}, & n-m < x \le n. \end{cases} \tag{6.3}$$

Sabemos que os elementos da matriz discriminante $D_{xy} = \sqrt{p_{xy}q_{yx}}$. Então, a matriz discriminante associada a matriz P', nesse caso, é uma matriz simétrica descrita como:

$$D = \begin{pmatrix} P_M & 0 \\ 0 & I \end{pmatrix}. \tag{6.4}$$

Dessa forma, seus valores singulares equivalem aos autovalores de P_M e de I em módulo. Considere $\big|v_k\big\rangle$ o vetor obtido de $\big|v'_k\big\rangle$ aumentando com zeros as coordenadas indexadas por M. A Tabela 6.1 mostra os valores e vetores singulares para a matriz D.

Valor singular	Vetor singular à direita	Vetor singular à esquerda	Intervalo
$\cos\theta_1 = \frac{1}{n-1}$	$\big\|v_k\big\rangle$	$\big\|w_k\big\rangle = -\big\|v_k\big\rangle$	$1 \leq k \leq n-m-1$
$\cos\theta_2 = \frac{n-m-1}{n-1}$	$\big\|v_{n-m}\big\rangle$	$\big\|w_{n-m}\big\rangle = \big\|v_{n-m}\big\rangle$	$k = n-m$
$\cos\theta_3 = 1$	$\big\|v_k\big\rangle = \big\|k\big\rangle$	$\big\|w_k\big\rangle = \big\|k\big\rangle$	$n-m+1 \leq k \leq n$

Tabela 6.1: Valores e vetores singulares da matriz discriminante D, associada a matriz estocástica P', para um grafo completo com n vértices e m vértices marcados.

6.2 Autovalores e autovetores de $W_{P'}$

Utilizando o Teorema 3.1, podemos obter uma boa parte dos autovalores e autovetores de $W_{P'}$ a partir dos valores e vetores singulares da matriz discriminante. Entretanto, não conhecemos uma expressão para todos os autovetores de autovalor 1. Mas, como vimos na seção 4.1, esse autoespaço não será utilizado no cálculo do Tempo de Alcance quântico. O espectro de $W_{P'}$ é apresentado na Tabela 6.2, a seguir.

Autovalor	Autovetor	Intervalo
$e^{\pm 2i\theta_1}$	$\big\|\alpha_k^{\pm}\big\rangle = \dfrac{A\big\|w_k\big\rangle - e^{\pm i\theta_1}B\big\|v_k\big\rangle}{\sqrt{2}\sin\theta_1}$	$1 \leq k \leq n-m-1$
$e^{\pm 2i\theta_2}$	$\big\|\alpha_{n-m}^{\pm}\big\rangle = \dfrac{A\big\|w_{n-m}\big\rangle - e^{\pm i\theta_2}B\big\|v_{n-m}\big\rangle}{\sqrt{2}\sin\theta_2}$	$k = n-m$
1	$\big\|\alpha_k\big\rangle$	$1 \leq k \leq n^2-2n-2m$

Tabela 6.2: Autovalores e autovetores do operador de evolução $W_{P'}$ para o grafo completo.

Consequentemente, temos que

$$\begin{aligned} W_{P'} &= e^{2i\theta_1}\sum_{k=1}^{n-m-1}\big|\alpha_k^+\big\rangle\big\langle\alpha_k^+\big| + e^{-2i\theta_1}\sum_{k=1}^{n-m-1}\big|\alpha_k^-\big\rangle\big\langle\alpha_k^-\big| + e^{2i\theta_2}\big|\alpha_{n-m}^+\big\rangle\big\langle\alpha_{n-m}^+\big| + \\ &\quad e^{-2i\theta_2}\big|\alpha_{n-m}^-\big\rangle\big\langle\alpha_{n-m}^-\big| + \sum_{k=1}^{n^2-2(n-m)}\big|\alpha_k\big\rangle\big\langle\alpha_k\big|. \end{aligned} \tag{6.5}$$

6.3 Tempo de Alcance

Para calcularmos o Tempo de Alcance quântico, vamos utilizar a Equação (4.13) para $F(T)$, descrita no capítulo 4. Para o grafo completo, temos

$$\begin{aligned} F(T) =& \frac{2}{T+1}\left(\left(2T+1-U_{2T}\left(\frac{1}{n-1}\right)\right)\sum_{j=1}^{n-m-1}\big|c_j\big|^2 + \right. \\ & \left.\big|c_{n-m}\big|^2\left(2T+1-U_{2T}\left(\frac{n-m-1}{n-1}\right)\right)\right). \end{aligned} \tag{6.6}$$

Precisamos calcular $\big|c_j\big| = \big|c_j^{\pm}\big| = \big|\,\langle\alpha_j^{\pm}|\phi_0\rangle\,\big|$. A condição inicial, nesse caso, se reduz para:

$$\big|\phi_0\big\rangle = \frac{1}{\sqrt{n(n-1)}}\sum_{x,y=1}^{n}(1-\delta_{xy})\big|x\big\rangle\big|y\big\rangle. \tag{6.7}$$

Lembrando que

$$\big|\phi_x\big\rangle = \sum_{y=1}^{n} \sqrt{p'_{xy}}\big|x\big\rangle\big|y\big\rangle \text{ e } \big|\psi_y\big\rangle = \sum_{x=1}^{n} \sqrt{p'_{yx}}\big|x\big\rangle\big|y\big\rangle, \tag{6.8}$$

a partir de (6.3), podemos notar que

$$\big\langle\phi_j\big|\phi_0\big\rangle = \big\langle\psi_j\big|\phi_0\big\rangle = \begin{cases} 1, & 1 \leq j \leq n-m; \\ 0, & n-m < j \leq n. \end{cases} \tag{6.9}$$

Dessa forma, temos que

$$\begin{aligned}
\big\langle\alpha_k^{\pm}\big|\phi_0\big\rangle &= \frac{1}{\sqrt{2}\sin\theta_1}\left(\big\langle v_k\big|\left(-A^* - e^{\mp i\theta_1}B^*\right)\big|\phi_0\big\rangle\right) \\
&= -\frac{1}{\sqrt{2}\sin\theta_1}\left(\sum_{x=1}^{n}\big\langle v_k\big|x\big\rangle\big\langle\phi_x\big|\phi_0\big\rangle + e^{\mp i\theta_1}\sum_{y=1}^{n}\big\langle v_k\big|y\big\rangle\big\langle\psi_y\big|\phi_0\big\rangle\right) \\
&= -\frac{1}{\sqrt{2n}\sin\theta_1}\left(\sum_{x=1}^{n-m}\big\langle v_k\big|x\big\rangle + e^{\mp i\theta_1}\sum_{y=1}^{n-m}\big\langle v_k\big|y\big\rangle\right) \\
&= -\frac{(1+e^{\mp i\theta_1})}{\sqrt{2n}\sin\theta_1}\sum_{x=1}^{n-m}\big\langle v_k\big|x\big\rangle \\
&= -\frac{(1+e^{\mp i\theta_1})}{\sqrt{2n}\sin\theta_1\sqrt{k+k^2}}\sum_{x=1}^{n-m}\left(\sum_{j=1}^{k}\big\langle j\big|x\big\rangle - k\big\langle k+1\big|x\big\rangle\right) \\
&= -\frac{(1+e^{\mp i\theta_1})}{\sqrt{2n}\sin\theta_1\sqrt{k+k^2}}(k-k) = 0,
\end{aligned} \tag{6.10}$$

$$\begin{aligned}
\big\langle\alpha_{n-m}^{\pm}\big|\phi_0\big\rangle &= \frac{1}{\sqrt{2}\sin\theta_2}\left(\big\langle v_{n-m}\big|\left(A^* - e^{\mp i\theta_2}B^*\right)\big|\phi_0\big\rangle\right) \\
&= \frac{1}{\sqrt{2}\sin\theta_2}\left(\sum_{x=1}^{n}\big\langle v_{n-m}\big|x\big\rangle\big\langle\phi_x\big|\phi_0\big\rangle + e^{\mp i\theta_2}\sum_{y=1}^{n}\big\langle v_{n-m}\big|y\big\rangle\big\langle\psi_y\big|\phi_0\big\rangle\right) \\
&= \frac{1}{\sqrt{2}\sin\theta_2\sqrt{n-m}}\left(\sum_{x=1}^{n-m}\big\langle\phi_x\big|\phi_0\big\rangle - e^{\mp i\theta_2}\sum_{y=1}^{n-m}\big\langle\psi_y\big|\phi_0\big\rangle\right) \\
&= \frac{1}{\sqrt{2}\sin\theta_2\sqrt{n-m}\sqrt{n}}\left((n-m) - e^{\mp i\theta_2}(n-m)\right) \\
&= \frac{\sqrt{n-m}}{\sqrt{2n}\sin\theta_2}(1 - e^{\mp i\theta_2}).
\end{aligned} \tag{6.11}$$

E, portanto,

$$c_j^{\pm} = \begin{cases} 0, & 1 \leq j \leq n-m-1; \\ \frac{\sqrt{n-m}\left(1-\mathrm{e}^{\mp i\theta_2}\right)}{\sqrt{2n}\,\sin\theta_2}, & j = n-m. \end{cases} \tag{6.12}$$

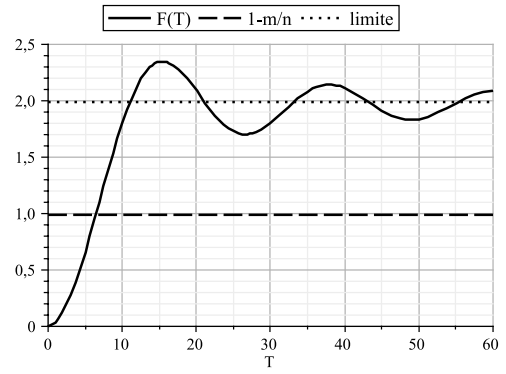
Substituindo (6.12) em (6.6), obtemos

$$F(T) = \frac{2\,(n-1)\,(n-m)\left(2\,T+1-U_{2T}\left(\frac{n-m-1}{n-1}\right)\right)}{n\,(2\,n-m-2)\,(T+1)}. \tag{6.13}$$

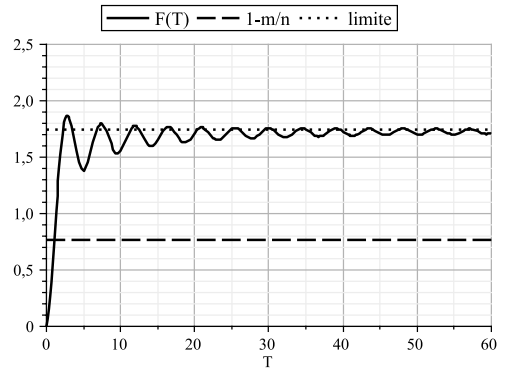
Nos gráficos da Figura 6.1, podemos analisar o comportamento da função $F(T)$. Ela cresce rapidamente passando da linha tracejada, que marca o valor $1-\frac{m}{n}$, e depois oscila em torno de seu valor limite, que é dado por

$$\lim_{T\to\infty} F(T) = \frac{4(n-1)(n-m)}{n(2n-m-2)} \tag{6.14}$$

e está representado pela linha pontilhada. O Tempo de Alcance é justamente o instante em que $F(T)$ intercepta a reta $1-\frac{m}{n}$.



(a) $n = 100$ e $m = 1$. Nesse caso, $H_{P,M} \approx 6.45$.



(b) $n = 100$ e $m = 23$. Nesse caso, $H_{P,M} \approx 1.05$.

Figura 6.1: Gráficos da função $F(T)$ (linha sólida), $1-\frac{m}{n}$ (linha tracejada) e $\frac{4(n-1)(n-m)}{n(2n-m-2)}$ (linha pontilhada) para um grafo completo. O Tempo de Alcance é o tempo T em que $F(T) = 1-\frac{m}{n}$.

Como o Tempo de Alcance é dado por $F^{-1}\left(1-\frac{m}{n}\right)$, ao fazermos a expansão

em séries para essa equação com $n \gg m$, obtemos

$$H_{P,M} = \frac{j_0^{-1}\left(\frac{1}{2}\right)}{2}\sqrt{\frac{n}{2\,m}} - \frac{\sqrt{1-\frac{1}{4}\,j_0^{-1}\left(\frac{1}{2}\right)^2}}{1+2\sqrt{1-\frac{1}{4}\,j_0^{-1}\left(\frac{1}{2}\right)^2}} + O\left(\frac{1}{\sqrt{n}}\right), \tag{6.15}$$

onde j_0 é a primeira função de Bessel esférica (Abramowitz e Stegun, 1972). O valor de $j_0^{-1}\left(\frac{1}{2}\right)$ é aproximadamente 1.9. Então, considerando apenas o primeiro termo da Equação (6.15), temos

$$H_{P,M} \approx 0.67\sqrt{\frac{n}{m}}. \tag{6.16}$$

6.4 Evolução do caminho

Apesar do cálculo do Tempo de Alcance quântico não necessitar do autoespaço de autovalor 1, se quisermos calcular a probabilidade de sucesso num instante t, ou seja, se evoluirmos o sistema até t e quisermos saber qual a probabilidade de obtermos um elemento marcado, precisamos considerar esse autoespaço e encontrar $W_{P'}^t\big|\phi_0\big\rangle$ explicitamente.

No caso do grafo completo, os autovetores $\big|\alpha_{n-m}^{\pm}\big\rangle$ e alguns autovetores associados ao autovalor 1 são ortogonais a condição inicial. Assim, da Equação (6.5), temos

$$W_{P'}^t\big|\phi_0\big\rangle = e^{2i\theta_2 t}c_{n-m}^{+}\big|\alpha_{n-m}^{+}\big\rangle + e^{-2i\theta_2 t}c_{n-m}^{-}\big|\alpha_{n-m}^{-}\big\rangle + \sum_{k=1}^{n^2-2(n-m)} c_k\big|\alpha_k\big\rangle. \tag{6.17}$$

Substituindo $\big|\alpha_{n-m}^{\pm}\big\rangle$, descritos na Tabela 6.2, e $c_{n-m}^{\pm}$, obtidos na Equação (6.12), obtemos

$$\begin{aligned} W_{P'}^t\big|\phi_0\big\rangle \;=\; & \frac{1}{\sqrt{n(n-1)}}\left(\frac{2(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2}\sum_{x,y=1}^{n-m}\left(1-\delta_{xy}\right)\big|x\big\rangle\big|y\big\rangle + \right. \\ & \left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2} - U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}\big|x\big\rangle\big|y\big\rangle \; + \\ & \left.\left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2} + U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=n-m+1}^{n}\sum_{y=1}^{n-m}\big|x\big\rangle\big|y\big\rangle\right) \; + \end{aligned}$$

$$\sum_{k=1}^{n^2-2(n-m)} c_k\big|\alpha_k\big\rangle. \tag{6.18}$$

Da expressão acima, a parte associada ao autovalor 1 pode ser determinada pelo método de tentativa e erro, diretamente a partir da estrutura da matriz $W_{P'}$:

$$\begin{aligned}\sum_{k=1}^{n^2-2(n-m)} c_k\big|\alpha_k\big\rangle \;=\; & \frac{1}{\sqrt{n(n-1)}}\left(\frac{-m}{2n-m-2}\sum_{x,y=1}^{n-m}(1-\delta_{xy})\big|x\big\rangle\big|y\big\rangle+\right.\\ & \frac{n-m-1}{2n-m-2}\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}\left(\big|x\big\rangle\big|y\big\rangle+\big|y\big\rangle\big|x\big\rangle\right)+\\ & \left.\sum_{x,y=n-m+1}^{n}(1-\delta_{xy})\big|x\big\rangle\big|y\big\rangle\right).\end{aligned} \tag{6.19}$$

Com isso, conseguimos obter uma expressão explícita para a evolução do sistema:

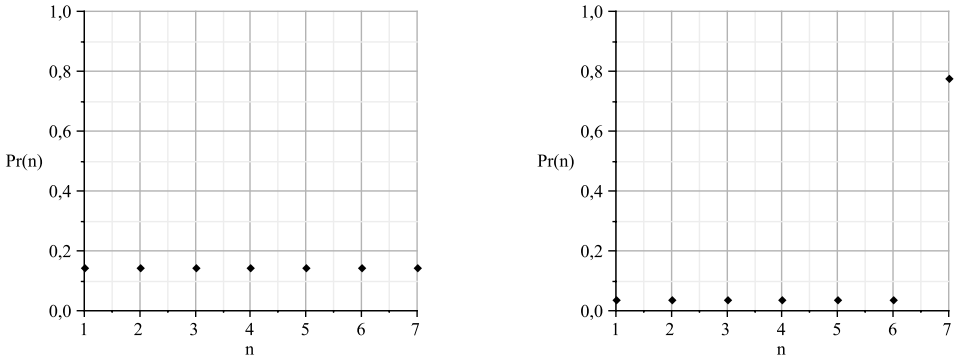
$$\begin{aligned}W_{P'}^{t}\big|\phi_0\big\rangle = & \frac{1}{\sqrt{n(n-1)}}\left(\frac{2(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)-m}{2\,n-m-2}\sum_{x,y=1}^{n-m}\big(1-\delta_{xy}\big)\big|x\big\rangle\big|y\big\rangle+\right.\\ & \left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)+n-m-1}{2\,n-m-2}-U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}\big|x\big\rangle\big|y\big\rangle\;+\\ & \left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)+n-m-1}{2\,n-m-2}+U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=n-m+1}^{n}\sum_{y=1}^{n-m}\big|x\big\rangle\big|y\big\rangle\Bigg)\;+\\ & \left.\sum_{x,y=n-m+1}^{n}(1-\delta_{xy})\big|x\big\rangle\big|y\big\rangle\right).\end{aligned} \tag{6.20}$$

6.5 Probabilidade de encontrar um elemento marcado

Segundo Nielsen e Chuang (2005), os sistemas quânticos evoluem de acordo com transformações unitárias. Para sistemas que não interagem com outros sistemas, isso está correto, mas devem existir momentos em que os experimentadores e seus equipamentos deverão observar o sistema para verificar o que está acontecendo dentro dele, uma intervenção que acaba com o isolamento do sistema, e que não é necessariamente descrita por uma transformação unitária.

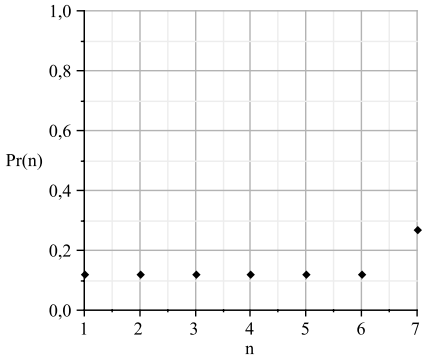
Ao fazermos $W_{P'}^{t}\big|\phi_0\big\rangle$, evoluindo o sistema até um instante t, podemos determinar qual é a distribuição de probabilidade dos vértices do grafo. Dessa forma, a

Figura 6.2 apresenta os gráficos dessa distribuição de probabilidade para diferentes instantes de tempo, considerando um elemento marcado num grafo completo com $n = 7$ vértices.

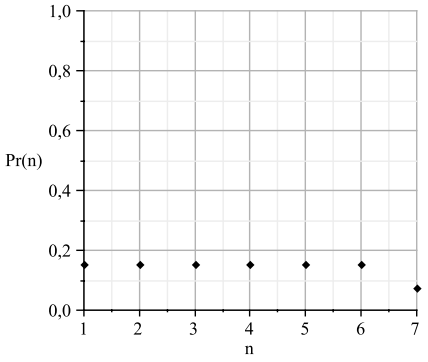


(a) $t = 0$

(b) $t = 1$



(c) $t = 2$



(d) $t = 3$

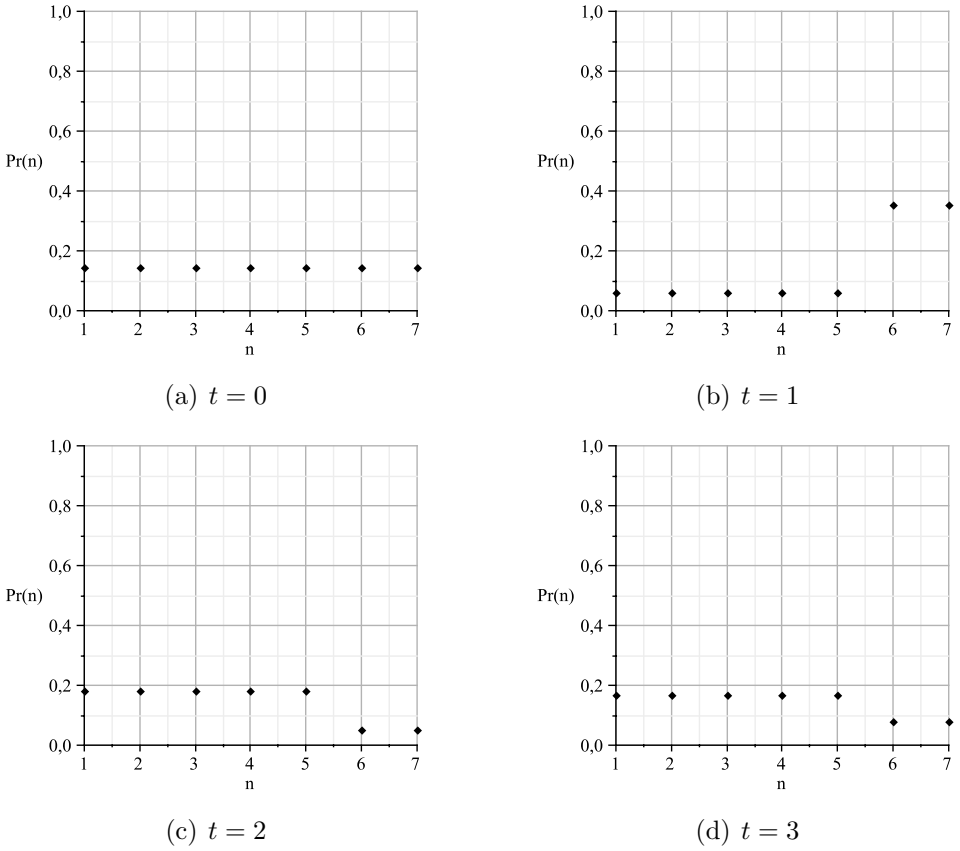
Figura 6.2: Gráficos da distribuição de probabilidade dos vértices de um grafo completo com $n = 7$ vértices e $m = 1$ vértices marcados, obtida a partir da evolução do sistema num instante t, $W_{P'}^{t}\big|\phi_0\big\rangle$.

A Figura 6.2(a) mostra o estado inicial $\big|\phi_0\big\rangle$, onde podemos perceber que sua distribuição de probabilidade equivale à distribuição estacionária ou uniforme.

É importante notar a diferença de probabilidade entre o vértice marcado e os outros vértices: nem sempre o elemento marcado tem a maior probabilidade, diferentemente da evolução clássica onde a probabilidade do elemento marcado tende sempre a aumentar. Mas, isso acontece porque em computação quântica temos uma evolução unitária e, portanto, reversível.

Como afirma Aharonov et al. (2000), o fato das matrizes unitárias preservarem a norma dos vetores implica que a distância entre dois vetores descrevendo

o sistema em instantes de tempo subsequentes não converge para zero. O mesmo comportamento pode ser visto também na Figura 6.3, a seguir, que considera dois elementos marcados.



(a) $t = 0$ (b) $t = 1$

(c) $t = 2$ (d) $t = 3$

Figura 6.3: Gráficos da distribuição de probabilidade dos vértices de um grafo completo com $n = 7$ vértices e $m = 2$ vértices marcados, obtida a partir da evolução do sistema num instante t, $W^t_{P'}\big|\phi_0\big\rangle$.

Nosso objetivo é determinar uma expressão para a probabilidade de encontrarmos um elemento marcado. Para isso, precisamos realizar uma medida no nosso estado atual, $\big|\psi(t)\big\rangle = W^t_{P'}\big|\phi_0\big\rangle$. Vamos utilizar os projetores da base do nosso espaço de Hilbert. De acordo com o postulado da medida[1] , a probabilidade de obtermos um elemento marcado, ou seja, obtermos $x \in M$ é dada por $p_M(t) = \big\langle\psi(t)\big|\mathcal{P}_M\big|\psi(t)\big\rangle$, onde

$$\mathcal{P}_M = \sum_{x=n-m+1}^{n} \big|x\big\rangle\big\langle x\big| \otimes I_n \tag{6.21}$$

[1] ver (Nielsen e Chuang, 2005), capítulo 2.

é um projetor no espaço gerado pelos elementos marcados.

Portanto, usando a Equação (6.20), obtemos

$$p_M(t) = \frac{m(m-1)}{n(n-1)} + \frac{m(n-m)}{n(n-1)} \left(\frac{n-1}{2\,n-m-2} T_{2t}\left(\frac{n-m-1}{n-1} \right) + U_{2t-1}\left(\frac{n-m-1}{n-1} \right) + \frac{n-m-1}{2n-m-2} \right)^2 . \tag{6.22}$$

O gráfico de $p_M(t)$ é apresentado na Figura 6.4, a seguir.

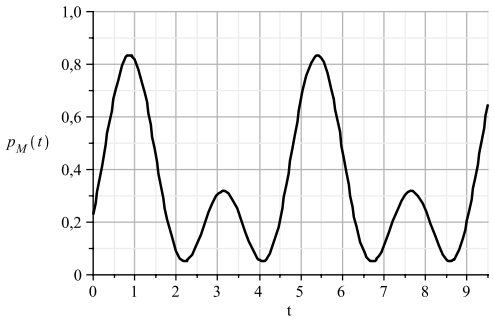


Figura 6.4: Gráfico da probabilidade de encontrar um elemento marcado em função do tempo, para um grafo completo com $n = 100$ e $m = 23$. O valor de $t = 0$ é $\frac{m}{n}$ e o período dessa função é $\frac{\pi}{\theta_2}$.

Dessa forma, podemos encontrar o máximo de $p_M(t)$. E, o primeiro ponto de máximo ocorre em

$$t_{\max} = \frac{\arctan\left(\frac{\sqrt{2n-m-2}}{\sqrt{m}} \right)}{2 \arccos\left(\frac{n-m-1}{n-1} \right)}, \tag{6.23}$$

cuja expansão assintótica é

$$t_{\max} = \frac{\pi}{4}\sqrt{\frac{n}{2\,m}} - \frac{1}{4} + O\left(\frac{1}{\sqrt{n}} \right), \tag{6.24}$$

para $n \gg m$. Substituindo esse resultado na expressão da probabilidade, p_M, obtemos

$$p_M(t_{\max}) = \frac{1}{2} + \sqrt{\frac{m}{2\,n}} + O\left(\frac{1}{n} \right). \tag{6.25}$$

Portanto, nesse contexto, para qualquer valor de n e m, a probabilidade de

encontrar um elemento marcado é maior que $\frac{1}{2}$, se a medida for feita no tempo $t_{\max}$. O instante $t_{\max}$ é menor que o Tempo de Alcance descrito pela Equação (6.16), já que $\frac{\pi}{4\sqrt{2}} \approx 0.56$. Assim, o valor da probabilidade de sucesso de um algoritmo que utiliza o Tempo de Alcance como tempo de parada será menor do que se tomássemos a probabilidade em $t_{\max}$. Avaliando p_M em $H_{P,M}$ e fazendo a expansão assintótica para $n \gg m$, temos

$$p_M(H_{P,M}) = \frac{1}{8}\, j_0^{-1} \left(\frac{1}{2}\right)^2 + O\left(\frac{1}{\sqrt{n}}\right). \tag{6.26}$$

O primeiro termo é aproximadamente 0.45 e é independente de n e m. Isso mostra que o Tempo de Alcance também é um bom parâmetro para ser utilizado como ponto de parada para algoritmos de busca num grafo completo.

Como vimos, $H_{P,M}$, descrito pela Equação (6.16), e t_{max}, vide Equação (6.24), são $O\left(\sqrt{\frac{n}{m}}\right)$. Consequentemente, tanto o problema de detectar quanto o de encontrar um elemento marcado num conjunto de vértices marcados num grafo completo possuem a mesma complexidade computacional.

Considerações Finais

Na Parte Clássica, vimos as definições para cadeias de Markov e caminhos aleatórios. Depois, discutimos sobre o Tempo de Alcance clássico. Em destaque, mostramos que a complexidade do Tempo de Alcance para um conjunto de elementos está relacionada com a norma espectral da matriz P_M.

Na Parte Quântica, apresentamos as idéias de Szegedy para definir as cadeias de Markov quânticas, assim como, o Tempo de Alcance quântico. E um dos principais resultados discutidos foi o ganho quadrático do Tempo de Alcance quântico com relação ao clássico. Esse resultado é importante pois permite o desenvolvimento de algoritmos quânticos mais eficientes; fato que pode ser comprovado em trabalhos posteriores ao do Szegedy.

Magniez et al. (2007) faz uma junção das técnicas desenvolvidas em (Ambainis, 2003) e (Szegedy, 2004a), para desenvolver um algoritmo que encontra um elemento marcado numa cadeia de Markov. Esse algoritmo também combina os algoritmos de busca (Grover, 1996) e de estimação de fase (Cleve et al., 1998). Nesse caso, a cadeia de Markov precisa ser ergódica e reversível, restringindo menos o espaço de atuação do algoritmo em relação ao de Szegedy, que utiliza cadeias ergódicas e simétricas.

Já Magniez et al. (2009) estende o resultado do Tempo de Alcance quântico de Szegedy (2004a) para cadeias de Markov ergórdicas e reversíveis. Através da definição de um novo Tempo de Alcance, tanto clássico quanto quântico, que considera um fator de erro; ele consegue mostrar um limite inferior e superior para essa nova definição. Além disso, ele melhora a probabilidade de encontrar um elemento marcado usando o método de Tulsi (2008).

Destacamos, também, os resultados novos obtidos para o grafo completo. Com isso, pudemos obter um melhor entendimento do método de Szegedy, verificando os resultados obtidos com o que foi visto na teoria. Apresentamos expressões tanto para o Tempo de Alcance quântico quanto para a probabilidade de encontrarmos um elemento marcado nesse grafo.

Ainda no caso do grafo completo, o tempo em que o caminhante atinge a maior probabilidade nos elementos marcados é menor que o Tempo de Alcance quântico. Em contrapartida, o valor da probabilidade no instante determinado pelo Tempo de Alcance quântico é constante, viabilizando-o também como um bom parâmetro para ser utilizado como ponto de parada em algoritmos de busca nesse grafo. Mostramos, também, que os problemas de busca e detecção no grafo completo possuem a mesma complexidade computacional.

Ao considerarmos outros grafos, podemos afirmar que descobrir o espectro da matriz P_M muitas vezes não é uma tarefa fácil. Apesar de Szegedy apresentar um teorema espectral para o operador de evolução, descrevendo um método para calcular os autovetores que estão associados aos autovalores diferentes de 1; caso queiramos obter uma expressão explícita para a evolução do caminho, será necessário calcular o autoespaço associado ao autovalor 1. Por isso, o cálculo da probabilidade de encontrar um elemento marcado é mais elaborado do que o cálculo do Tempo de Alcance quântico. Em trabalhos futuros, podemos analisar o comportamento das cadeias de Markov quânticas em outros grafos, como a malha e o hipercubo. Além disso, outro problema que ainda se encontra em aberto na literatura refere-se a encontrar um limite inferior para o Tempo de Alcance quântico.

Apesar de muitas vezes a vida no mundo quântico parecer mais complicada que no mundo clássico, no mundo quântico parece que nossos problemas são resolvidos de forma mais eficiente.

Referências Bibliográficas

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. Disponível em: `arXiv:quant-ph/0012090`.

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

D. Aldous e J. Fill. **Reversible Markov Chains and Random Walks on Graphs**. Monography in preparation, 1994. Disponível em: `http://www.stat.berkeley.edu/~aldous/RWG/book.html`.

A. Ambainis. Quantum walks and their algorithmic applications. **International Journal of Quantum Information**, 1(4):507–518, 2003. Disponível em: `arXiv:quant-ph/0403120`.

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

H. Buhrman e R. Spalek. Quantum verification of matrix products. In: **Proceedings of the 17th ACM-SIAM Symposium on Discrete Algorithms**, páginas 880–889, 2006.

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

R. Cleve, A. Ekert, C. Macchiavello, e M. Mosca. Quantum algorithms revisited. In: **Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences**, páginas 339–354, 1998.

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.

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

B. R. James. **Probabilidade: um curso em nível intermediário**. IMPA, 2006.

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

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

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

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

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

L. Lovász. Random walks on graphs: a survey. **Combinatorics, Paul Erdös is Eighty**, 2:1–46, 1993.

F. Magniez e A. Nayak. Quantum complexity of testing group commutativity. **Algorithmica**, 48(3):221–232, 2007.

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. Disponível em: `arXiv:quant-ph/0808.0084`.

F. Magniez, A. Nayak, J. Roland, e M. Santha. Search via quantum walk. In: **Proceedings of the 39th ACM Symposium on Theory of Computing**, páginas 575–584, 2007.

C. D. Meyer. **Matrix Analysis and Applied Linear Algebra**. SIAM, 2000.

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

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

I. Peterson. **The Jungles of Randomness: a Mathematical Safari**. Wiley, 1998.

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

M. Santha. Quantum walk based search algorithms. In: **Proceedings of the 5th Theory and Applications of Models of Computation (TAMC08)**, páginas 31–46, 2008. Disponível em: `arXiv:quant-ph/0808.0059`.

R. A. M. Santos e R. Portugal. Quantum hitting time on the complete graph. Artigo aceito para publicação no International Journal of Quantum Information. Disponível em: `arXiv:quant-ph/0912.1217`, 2010.

U. Schöning. A probabilistic algorithm for k-sat and constraint satisfaction problems. In: **Proceedings of the 40th Annual Symposium on Foundations of Computer Science**, páginas 17–19, 1999.

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

S. Singh. **O livro dos códigos.** Record, 4ª edição, 2004.

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

M. Szegedy. Spectra of quantized walks and a $\sqrt{\delta\epsilon}$-rule, 2004b. Disponível em: `arXiv:quant-ph/0401053`.

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.