Notas em Matemática Aplicada **ISSN 2175-3385**

Volume 47, 2010

Editores

Célia A. Zorzo Barcelos
Universidade Federal de Uberlândia - UFU
Uberlândia, MG, Brasil

Eliana X.L. de Andrade
Universidade Estadual Paulista - UNESP
São José do Rio Preto, SP, Brasil

Maurílio Boaventura
Universidade Estadual Paulista - UNESP
São José do Rio Preto, SP, Brasil

A Sociedade Brasileira de Matemática Aplicada e Computacional - SBMAC publica, desde as primeiras edições do evento, monografias dos cursos que são ministrados nos CNMAC.

A partir do XXVI CNMAC, para a comemoração dos 25 anos da SBMAC, foi criada a série **Notas em Matemática Aplicada** para publicar as monografias dos minicursos ministrados nos CNMAC.

O livro correspondente a cada minicurso deve ser preparado em **Latex (compatível com o Miktex versão 2.7), as figuras em eps** e deve ter entre **80 e 120 páginas**. O texto deve ser redigido de forma clara, acompanhado de uma excelente revisão bibliográfica e de **exercícios de verificação de aprendizagem** ao final de cada capítulo.

Além do livro, cada responsável por minicurso deve preparar transparências e outros materiais didáticos que julgar convenientes. Todo o material será colocado à disposiçao dos interessados no site da SBMAC.

É objetivo da série publicar textos dos encontros regionais e de outros eventos patrocinados pela SBMAC.

Sociedade Brasileira de Matemática Aplicada e Computacional

2010

Notas em Matemática Aplicada

Títulos publicados para o XXXIII CNMAC - 2010

45 Tópicos de Análise Funcional na Computação Científica
Carlos Antonio de Moura e Denise Burgarelli

46 Descrições microscópica, macroscópica e cinética do fluxo de tráfego veicular
Liliana Madalena Gramani

47 **Algoritmos Quânticos de Busca**
Renato Portugal

48 Modelagem Matemática em Turbulência Atmosférica
Haroldo Fraga de Campos Velho

49 Métodos sem derivadas para minimização irrestrita
Maria Aparecida Diniz-Ehrhardt, Véra Lucia da Rocha Lopes e Lucas Garcia Pedroso

50 Sistemas Dinâmicos fuzzy: modelagens alternativas para sistemas biológicos
Moiseis dos Santos Cecconello, João de Deus Mendes da Silva e Rodney Carlos Bassanezi

Veja outros títulos da série ao final deste livro.
Arquivos no formato pdf disponíveis em
http://www.sbmac.org.br/notas.php

ALGORITMOS QUÂNTICOS DE BUSCA

Renato Portugal
portugal@lncc.br

Coordenação de Ciência da Computação
Laboratório Nacional de Computação Científica
Ministério da Ciência e Tecnologia

Sociedade Brasileira de Matemática Aplicada e Computacional

São Carlos - SP, Brasil
2010

Coordenação Editorial: Elbert Einstein Nehrer Macau

Coordenação Editorial da Série: Eliana Xavier Linhares de Andrade

Editora: SBMAC

Impresso na Gráfica: Lamanna - São Carlos (SP)

Capa: Matheus Botossi Trindade

Patrocínio: SBMAC

Catalogação elaborada pela Biblioteca do IBILCE/UNESP
Bibiotecária: Maria Luiza Fernandes Jardim Froner

Portugal, Renato
Algoritmos Quânticos de Busca - São Carlos, SP :
SBMAC, 2010, 137 p., 20.5 cm - (Notas em Matemática Aplicada; v. 47)

ISSN 2175-3385

1. Computação Quântica 2. Passeios Quânticos 3. Cadeia de Markov Quântica 4. Tempo de Alcance Quântico IV. Título. V. Série

CDD - 51

Agradecimentos

Agradeço o apoio do Laboratório Nacional de Computação Científica—LNCC, da Sociedade Brasileira de Matemática Aplicada e Computacional—SBMAC, o suporte financeiro da CAPES e do CNPq e em especial, o apoio do edital CT-INFO/2007, sem o qual dificilmente este livro teria seria produzido. Agradeço aos amigos e ao grupo de computação quântica do LNCC pelas diversas discussões e trocas de idéias que me ajudaram a aprofundar na área. Por último, do fundo de minha alma, agradeço o suporte emocional de minha família, a paciência que ela tem comigo e a felicidade que ela me traz.

Conteúdo

Prefácio

No presente contexto da Computação Quântica, sabe-se que o computador quântico tem um enorme potencial para problemas de busca, seja em banco de dados, seja em situações mais gerais, tendo impacto em qualquer problema que requer busca exaustiva. O algoritmo de Grover, primeiro de uma série de algoritmos quânticos de busca, foi altamente inovador por introduzir a técnica de amplificação de amplitude essencial para uma grande variedade de algoritmos. Apresentamos o algoritmo de Grover sob uma visão moderna útil para comparação com outros algoritmos de busca.

Com exceção do algoritmo de Grover, os algoritmos de busca são baseados em passeios quânticos. Boa parte do material deste livro se dedica aos passeios quânticos. Apresentamos inicialmente o modelo padrão baseado em uma moeda junto com um operador de deslocamento. Escolhemos dois grafos para uma análise mais detalhada: a reta (malha unidimensional) e o hipercubo. Descrevemos um modelo alternativo, proposto por Mario Szegedy, que permitiu definir o tempo de alcance quântico de maneira natural. Apresentamos em detalhes esse modelo no grafo completo. Diversos exercícios foram propostos para um bom entendimento da teoria.

A área de algoritmos quânticos tem como base a Mecânica Quântica que, por sua vez, usa extensamente a Álgebra Linear. Para minimizar a quantidade de pré-requisitos, apresentamos os princípios da Mecânica Quântica em um capítulo inicial e resumimos as principais definições e fatos da Álgebra Linear relevantes ao contexto em um apêndice. As sugestões de leitura, ao final de cada capítulo, podem ajudar muito a criar uma base para a leitura deste livro.

Comentários, sugestões e correções podem ser enviadas ao autor pelo e-mail `portugal@lncc.br`.

Petrópolis, 19 de abril de 2010.

Renato Portugal

Capítulo 1

Mecânica Quântica

É impossível fazer um resumo da Mecânica Quântica em poucas páginas. Como o objetivo deste livro é descrever algoritmos quânticos, limitaremos aos princípios da Mecânica Quântica e a descrevê-los como "regras do jogo". Suponha que você jogue Damas há muitos anos e domine diversas estratégias, mas você não conhece Xadrez. Suponha agora que alguém lhe descreva as regras do Xadrez. Em pouco tempo, você estará jogando um novo jogo. Certamente não estará dominando diversas estratégias do Xadrez, porém terá condições de jogar. Este capítulo tem um objetivo similar. Os postulados de uma teoria são como as regras do jogo. Se desrespeitarmos as regras, estaremos fora do jogo.

Na melhor das hipóteses, podemos nos concentrar em quatro postulados. O primeiro descreve a arena onde o jogo se passa. O segundo descreve a dinâmica do processo. O terceiro descreve como devemos fazer a composição de vários sistemas. O quarto descreve o processo da medição física. Todos esses postulados são descritos em termos da Álgebra Linear. É fundamental ter um conhecimento sólido dos resultados básicos dessa área. Além disso, o postulado dos sistemas compostos usa o conceito de produto tensorial, que é uma forma de combinar dois espaços vetoriais para construir um espaço vetorial maior. Também é importante estar familiarizado com esse conceito.

1.1 Espaço de Estados

O *estado* de um sistema físico descreve suas características físicas em um determinado instante. Usualmente descrevemos uma parte das possíveis características, que o sistema pode ter, pois, do contrário, os problemas físicos ficariam muito complexos. Por exemplo, o estado de rotação de uma bola

de bilhar pode ser caracterizado por um vetor no espaço $\mathbb{R}^3$. Nesse exemplo, não levaremos em consideração a velocidade linear da bola de bilhar, sua cor ou qualquer outra característica, que não esteja diretamente relacionada a sua rotação. O estado de rotação é totalmente caracterizado pelo eixo, pelo sentido e pela intensidade. Com três números reais caracterizamos o estado de rotação. Basta dar as componentes de um vetor, cuja direção caracteriza o eixo de rotação, cujo sentido caracteriza para qual lado a bola de bilhar está girando e cujo comprimento caracteriza a velocidade de rotação. Na Física Clássica, a direção do eixo de rotação pode variar continuamente assim como a intensidade de rotação.

Será que um *elétron*, considerado uma partícula elementar, isto é, não constituído de outras partículas menores, gira como uma bola de bilhar? A melhor maneira de responder a isto é fazendo experiências concretas para verificar se o elétron, de fato, gira e se obedece às leis da Física Clássica. Como o elétron tem carga, sua rotação produziria campos magnéticos, que poderiam ser medidos. Experiências desse tipo foram feitas, no início da Mecânica Quântica, com feixes de átomos de prata, depois com feixes de átomos de hidrogênio e, hoje em dia, elas são feitas com partículas individuais, sejam elétrons, sejam fótons. Tais resultados são efetivamente diferentes do que é previsto pelas leis da Física Clássica.

No caso do elétron, podemos enviá-lo através de um campo magnético na direção vertical (direção z), conforme o esquema da Fig. 1.1. Os possíveis resultados estão mostrados na figura. Ou o elétron bate no anteparo no ponto A ou no ponto B. Jamais encontramos o elétron no ponto O, que indica ausência de rotação. Essa experiência mostra que o *spin* do elétron só admite dois valores: *spin para cima* e *spin para baixo*, ambos com a mesma intensidade de "rotação". Esse resultado é bem diferente do clássico, já que a direção do eixo de rotação é quantizada, admitindo somente dois valores. A intensidade de rotação também é quantizada.

A Mecânica Quântica descreve o spin do elétron como um vetor unitário no espaço de Hilbert $\mathbb{C}^2$. O "spin para cima" é descrito pelo vetor

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

e "spin para baixo" pelo vetor

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Isso parece um paradoxo, pois os vetores $|0\rangle$ e $|1\rangle$ são ortogonais. Por que associar vetores ortogonais a "spin para cima" e "spin para baixo"? No espaço $\mathbb{R}^3$, se somarmos "spin para cima" com "spin para baixo" obtemos

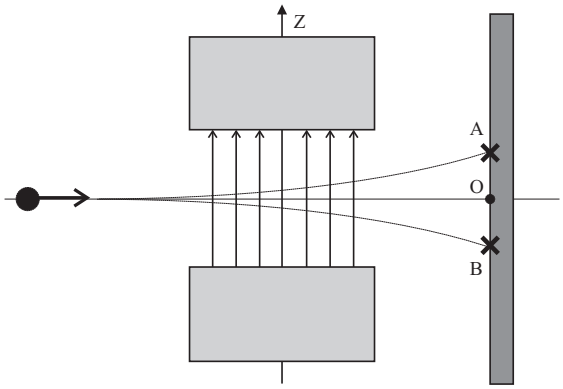

Figura 1.1: Desenho esquemático de um dispositivo experimental para medir o estado de rotação de um elétron. O elétron é enviado a uma velocidade fixa por um campo magnético na direção vertical. Ele bate em A ou B dependendo do sentido da rotação (*spin*). A distância dos pontos A e B ao ponto O depende da velocidade de rotação do elétron. Os resultados destas experiências são bem diferentes do que esperamos classicamente.

uma partícula parada sem rotação, pois a soma de dois vetores opostos de comprimentos iguais dá o vetor nulo, que descreve ausência de rotação. No mundo clássico, não é possível uma bola de bilhar girar tanto para um lado como para o outro ao mesmo tempo. Temos duas situações excludentes. Vale a *lógica do terceiro excluído*. A noção de "spin para cima" ou "spin para baixo" se refere ao $\mathbb{R}^3$, porém a Mecânica Quântica também descreve o comportamento do elétron antes da observação, isto é, antes de entrar no campo magnético, que visa a determinar seu estado de rotação.

Se o elétron não entrou no campo magnético e se ele está isolado do meio macroscópico ao redor, seu estado de spin é descrito por um combinação linear dos vetores $|0\rangle$ e $|1\rangle$, da seguinte forma

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle , \tag{1.1.1}$$

onde os coeficientes a_0 e a_1 são números complexos, que satisfazem ao vínculo

$$|a_0|^2 + |a_1|^2 = 1. \tag{1.1.2}$$

Como os vetores $|0\rangle$ e $|1\rangle$ são ortogonais, a soma não dá o vetor nulo. As possibilidades excludentes classicamente coexistem quanticamente. Essa coexistência é destruída quando tentamos observá-la usando o dispositivo da Fig. 1.1.

1.1.1 Postulado do Espaço de Estados

Um *sistema físico isolado* tem associado um espaço de Hilbert, chamado de *espaço de estados*. O estado do sistema é totalmente descrito por um vetor unitário, chamado de *vetor de estado*, nesse espaço de Hilbert.

Observações

1. O postulado do espaço de estados não nos diz qual é o espaço de Hilbert, que devemos usar para um dado sistema físico. Em geral, não é simples determinar a dimensão do espaço de Hilbert do sistema. No exemplo do spin do elétron, vimos que devemos usar o espaço de Hilbert de dimensão 2, porque só há duas possibilidades resultantes de um experimento para determinar o spin vertical do elétron. Sistemas físicos mais complexos admitem mais possibilidades, que podem ser um número infinito.

2. Um sistema está isolado se ele não influencia e não sofre influência da parte externa a ele. Em princípio, o sistema não precisa ser diminuto, porém é mais fácil isolar os sistemas pequenos com poucos átomos. Na prática, só conseguimos sistemas aproximadamente isolados, logo, o postulado do espaço de estados é uma idealização.

1.2 Evolução Unitária

O objetivo da Física não é simplesmente descrever o estado de um sistema físico em um determinado instante. O objetivo principal é determinar qual é o estado deste sistema no futuro. A teoria permite fazer previsões que podem ser confirmadas ou falseadas por experimentos físicos. Isso é equivalente a determinar quais são as leis dinâmicas a que o sistema obedece. Usualmente, tais leis são descritas por equações diferenciais. Elas governam a evolução temporal do sistema.

1.2.1 Postulado da Evolução

A evolução temporal de um sistema quântico fechado é descrita por uma transformação unitária. Se o estado do sistema quântico no instante t_1 é descrito pelo vetor $|\psi_1\rangle$, então o estado do sistema $|\psi_2\rangle$ no instante t_2 está relacionado a $|\psi_1\rangle$ por um operador unitário U, que depende apenas de t_1 e t_2 da seguinte forma

$$|\psi_2\rangle = U\,|\psi_1\rangle\,. \tag{1.2.3}$$

Observações

1. A ação de um operador unitário sobre um vetor preserva sua norma. Portanto se $|\psi\rangle$ é um vetor unitário, $U|\psi\rangle$ também o será.

2. Um *algoritmo quântico* consiste em uma prescrição de uma sequência de operadores unitários aplicados a uma condição inicial da forma

$$|\psi_n\rangle = U_n \cdots U_1 |\psi_1\rangle .$$

O estado $|\psi_n\rangle$ é medido retornando o resultado do algoritmo.

3. O postulado da evolução pode ser colocado sob a forma de uma equação diferencial, chamada *equação de Schrödinger*. Essa equação fornece um método para se obter o operador U uma vez dado o contexto físico em questão. O objetivo da Física é descrever a dinâmica de sistemas físicos, por isso, a equação de Schrödinger tem um papel fundamental. O objetivo da Ciência da Computação é analisar e implementar algoritmos, logo, o cientista da computação quer saber se é possível implementar de alguma forma um operador unitário previamente escolhido. A forma da Eq. (1.2.3) é conveniente para a área de algoritmos quânticos.

1.3 Sistemas Compostos

O espaço de estados de um *sistema composto* é o *produto tensorial* dos espaços de estados dos componentes. Se $|\psi_1\rangle, \cdots, |\psi_n\rangle$ descrevem os estados de n sistemas quânticos isoladamente, o estado do sistema composto é $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Um exemplo de sistema composto é a memória de um computador quântico de n *qubits*. Usualmente, a memória é dividida em conjunto de qubits, chamado de *registradores*. O espaço de estados da memória do computador é o produto tensorial dos espaços de estados dos registradores que, por sua vez, são obtidos pelo produto tensorial repetido do espaço de Hilbert $\mathbb{C}^2$ de cada *qubit*.

O espaço de estados da memória de um computador quântico de 2 qubits é $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. Portanto, qualquer vetor unitário de $\mathbb{C}^4$ representa o estado quântico de 2 qubits. Por exemplo, o vetor

$$|0,0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{1.3.4}$$

que pode ser escrito como $|0\rangle \otimes |0\rangle$, representa o estado de 2 elétrons ambos com spin para cima. Interpretação análoga se aplica a $|0,1\rangle$, $|1,0\rangle$ e $|1,1\rangle$. Considere agora o vetor unitário de $\mathbb{C}^4$ dado por

$$|\psi\rangle = \frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}}. \tag{1.3.5}$$

Qual é o estado de spin de cada elétron nesse caso? Para responder a essa pergunta, temos que fatorar $|\psi\rangle$ da seguinte forma:

$$\frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}} = \big(a\,|0\rangle + b\,|1\rangle\,\big) \otimes \big(c\,|0\rangle + d\,|1\rangle\,\big). \tag{1.3.6}$$

Podemos expandir o lado direito e igualar os coeficientes montando um sistema de equações para achar a, b, c e d. O estado do primeiro qubit será $a\,|0\rangle + b\,|1\rangle$ e do segundo $c\,|0\rangle + d\,|1\rangle$. Porém, há um problema: o sistema de equações não tem solução, ou seja, não existem coeficientes a, b, c e d, que satisfaçam à Eq. (1.3.6). Todo estado de um sistema composto que não pode ser fatorado é chamado de *emaranhado*. Esses estados são bem definidos quando olhamos o sistema composto como um todo, porém não podemos atribuir estados para as partes.

1.4 Processo de Medida

Em geral, medir um sistema quântico que se encontra no estado $|\psi\rangle$ visa a obter informações clássicas a respeito desse estado. Na prática, a medida é feita no laboratório usando instrumentos como lasers, magnetos, escalas e cronômetros. Na teoria, descrevemos o processo matematicamente de modo que haja correspondência com o que ocorre na prática. Medir um sistema físico que se encontra em um estado desconhecido, em geral, perturba esse estado de forma irreversível. Não tem como recuperar ou conhecer o estado antes da execução da medida. Se o estado não foi perturbado, então não foi possível obter qualquer informação sobre ele. Matematicamente, a perturbação é descrita por um *projetor*. Se esse projetor for sobre um espaço unidimensional, então diz-se que o estado quântico *projetor* e passa a ser descrito pelo vetor unitário pertencente ao espaço unidimensional. No caso geral, a projeção é sobre um espaço vetorial de dimensão maior que 1, e assim, diz-se que o colapso é parcial ou, no caso extremo, não há alteração no estado quântico do sistema.

1.4.1 Postulado da Medida

Uma *medida projetiva* é descrita por um operador hermitiano O, chamado de *observável*, no espaço de estados do sistema, que está sendo medido. O observável O tem uma *representação diagonal*

$$O = \sum_{\lambda} \lambda P_{\lambda}, \tag{1.4.7}$$

onde P_λ é o projetor no auto-espaço de O associado ao autovalor λ. Os possíveis resultados da medida correspondem aos autovalores λ do observável. Se o estado do sistema no momento da medida for $|\psi\rangle$, a probabilidade de se obter o resultado λ será

$$p_\lambda = \langle\psi| P_\lambda |\psi\rangle . \tag{1.4.8}$$

Se o resultado da medida for λ, o estado do sistema quântico imediatamente após a medida será

$$\frac{1}{\sqrt{p_\lambda}} P_\lambda |\psi\rangle . \tag{1.4.9}$$

Observações

1. Existe uma correspondência entre a disposição física do aparato de medida em um laboratório de Física e o observável O. Quando um físico experimental faz a medição de um sistema quântico, ele obtém números reais como resultado. Esses números correspondem aos autovalores λ do operador hermitiano O.

2. Os estados $|\psi\rangle$ e $e^{i\phi}|\psi\rangle$ têm a mesma *estatística de medida*, isto é, a mesma *distribuição de probabilidades* p_λ quando medidos pelo mesmo observável O. O termo $e^{i\phi}$ multiplicando um estado quântico é chamado de *fase global*.

1.4.2 Medida na Base Computacional

A *base computacional* do espaço $\mathbb{C}^2$ é o conjunto $\{ |0\rangle , |1\rangle \}$. No caso particular de um qubit, o observável da *medida na base computacional* é a matriz de Pauli Z, cuja decomposição espectral é

$$Z = (+1)P_{+1} + (-1)P_{-1}, \tag{1.4.10}$$

onde $P_{+1} = |0\rangle\langle 0|$ e $P_{-1} = |1\rangle\langle 1|$. Os possíveis resultados da medida são ± 1. Se o estado do qubit é dado pela Eq. (1.1.1), as probabilidades

associadas aos possíveis resultados são

$$p_{+1} = |a_0|^2, \tag{1.4.11}$$
$$p_{-1} = |a_1|^2 \tag{1.4.12}$$

e os estados associados logo após a medida serão $|0\rangle$ e $|1\rangle$, respectivamente. A rigor, cada um desses estados têm uma fase global que pode ser descartada. Note que

$$p_{+1} + p_{-1} = 1,$$

pois o estado $|\psi\rangle$ é unitário.

Antes de generalizar para n qubits, é interessante re-analisar o processo de medida de 1 qubit com outro observável dado por

$$O = \sum_{k=0}^{1} k \, |k\rangle \langle k| \, . \tag{1.4.13}$$

Como os autovalores de O são 0 e 1, toda a análise anterior se mantém se substituirmos $+1$ por 0 e -1 por 1. Com esse observável, existe uma correlação direta entre o resultado da medida e o estado final do qubit. Se o resultado for 0, o estado após a medida será $|0\rangle$. Se o resultado for 1, o estado após a medida será $|1\rangle$.

A *base computacional* de n qubits na notação decimal é o conjunto $\left\{ |0\rangle \, , \cdots , |2^n - 1\rangle \right\}$. A *medida na base computacional* é feita com o observável

$$O = \sum_{k=0}^{2^n-1} k \, P_k. \tag{1.4.14}$$

onde $P_k = |k\rangle \langle k|$. Um estado genérico de n qubits é dado por

$$|\psi\rangle = \sum_{k=0}^{2^n-1} a_k \, |k\rangle \, , \tag{1.4.15}$$

onde as amplitudes a_k satisfazem ao vínculo

$$\sum_k |a_k|^2 = 1. \tag{1.4.16}$$

A medida tem como resultado um valor inteiro k no intervalo $0 \leq k \leq 2^n - 1$ com a distribuição de probabilidades dada por

$$\begin{aligned} p_k &= \langle \psi | P_k | \psi \rangle \\ &= \left| \langle k | \psi \rangle \right|^2 \\ &= |a_k|^2. \end{aligned} \tag{1.4.17}$$

A Eq. (1.4.16) garante que a soma das probabilidades dê 1. O estado dos n qubits imediatamente após a medida é

$$\frac{P_k \left|\psi\right\rangle}{\sqrt{p_k}} \simeq \left|k\right\rangle . \tag{1.4.18}$$

O resultado da medida especifica em qual vetor da base computacional o estado $|\psi\rangle$ foi projetado. O resultado não fornece o valor do coeficiente a_k, isto é, de nenhuma das 2^n amplitudes a_k, que descrevem o estado $|\psi\rangle$. Suponha que queiramos encontrar o número k como resultado de um algoritmo. Esse resultado deverá estar codificado como um dos vetores da base computacional, gerador do espaço vetorial, a que o estado $|\psi\rangle$ pertence. Não é conveniente, em princípio, que o resultado em si esteja associado a uma das amplitudes. Se o resultado desejado for um número real não inteiro, então os k dígitos mais significativos deverão ser codificados como um vetor da base computacional. Após uma medida, temos chance de obter uma aproximação para k. Repetindo, as amplitudes do estado quântico em um algoritmo estão associadas às probabilidades de se obter um resultado e o número que especifica um *ket*, por exemplo o número k de $|k\rangle$, é um possível resultado do algoritmo.

A descrição do processo de medida usando o observável (1.4.14) é equivalente a medidas simultâneas ou em cascata dos qubits com o observável Z. Os possíveis resultados da medida com Z são ± 1. Medidas simultâneas ou em cascata de n qubits resultam numa sequência de n componentes ± 1. Por exemplo, para $n = 3$ qubits podemos ter $(-1, +1, +1)$. A relação de um resultado da medida desse tipo, como o que foi descrito anteriormente, é obtida substituindo-se cada resultado $+1$ por 0 e -1 por 1. Teremos, então, um número binário que pode ser convertido para base decimal fornecendo um dos valores k. No caso do exemplo com o resultado $(-1, +1, +1)$, obtemos 100, que corresponde ao número 4. O estado, logo após a medida, será dado pela aplicação do projetor

$$\begin{aligned} P_{-1,+1,+1} &= \left|1\right\rangle \left\langle 1\right| \otimes \left|0\right\rangle \left\langle 0\right| \otimes \left|0\right\rangle \left\langle 0\right| \\ &= \left|1,0,0\right\rangle \left\langle 1,0,0\right| \end{aligned} \tag{1.4.19}$$

no estado do sistema de 3 qubits seguido da *renormalização*. A renormalização, nesse caso, equivale a substituir o coeficiente por 1. O estado após a medida será $|1, 0, 0\rangle$. Portanto, numa medida usando a base computacional, seja com o observável (1.4.14), seja como operadores Z, podemos falar que o resultado foi $|1, 0, 0\rangle$, pois automaticamente sabemos que os autovalores de Z em questão são $(-1, +1, +1)$.

Uma medida simultânea com n observáveis Z não é equivalente a uma medida com o observável $Z \otimes \cdots \otimes Z$. A medida com esse último observável

retorna um único valor, que pode ser $+1$ ou -1, enquanto que com n observáveis Z, simultaneamente ou não, temos n valores ± 1. A medida em cascata é feita com os observáveis $Z \otimes I \otimes \cdots I$, $I \otimes Z \otimes \cdots I$, e assim por diante. Usualmente, empregamos uma notação mais compacta, Z_1, Z_2, sucessivamente, onde Z_1 quer dizer que o observável Z foi usado para o qubit 1 e o operador identidade para os qubits restantes.

1.4.3 Medida Parcial na Base Computacional

Suponha que o estado de 2 qubits é dado por

$$|\psi\rangle = \frac{3}{5\sqrt{2}}\,|0,0\rangle - \frac{3\,i}{5\sqrt{2}}\,|0,1\rangle + \frac{2\sqrt{2}}{5}\,|1,0\rangle - \frac{2\sqrt{2}\,i}{5}\,|1,1\rangle\,. \tag{1.4.20}$$

Pelo método descrito na seção anterior, concluímos que a probabilidade de obtermos o resultado $|0,0\rangle$ após uma medida do estado $|\psi\rangle$ na base computacional é $9/50$.

O termo *medida na base computacional* de n qubits subentende uma medida de todos os qubits. No entanto, existe a possibilidade de uma *medida parcial*, ou seja, medir uma parte dos qubits, cada um com o observável Z em cascata ou simultaneamente. O resultado, nesse caso, não é necessariamente um estado da base computacional. Por exemplo, medindo apenas o segundo qubit do estado $|\psi\rangle$ da Eq. (1.4.20) podemos obter o resultado 0 com probabilidade $1/2$ ou 1 também com probabilidade $1/2$. No primeiro caso, o estado logo após a medida será

$$\left(\frac{3}{5}\,|0\rangle + \frac{4}{5}\,|1\rangle\right) \otimes |0\rangle$$

e no segundo caso, o estado será

$$\left(\frac{3}{5}\,|0\rangle + \frac{4}{5}\,|1\rangle\right) \otimes |1\rangle\,.$$

Somente os qubits que sofreram a medição são projetados na base computacional.

Se tivermos um sistema composto dos subsistemas A e B, uma medida parcial do sistema B será feita com um observável da forma $I_A \otimes O_B$, onde I_A é o operador identidade do sistema A e O_B é um observável do sistema B. Fisicamente, isso quer dizer que o aparato de medida interagiu apenas com o subsistema B.

Se tivermos um registrador de m qubits junto com um registrador de n qubits, poderemos representar a base computacional na forma compacta

$\left\{ |i,j\rangle : 0 \leq i \leq 2^m - 1,\ 0 \leq j \leq 2^n - 1 \right\}$, onde tanto i como j estarão representados na base decimal. Um estado genérico será representado por

$$|\psi\rangle = \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^n-1} a_{ij} |i,j\rangle . \tag{1.4.21}$$

Suponha que meçamos todos os qubits do segundo registrador, a probabilidade de se obter o valor $0 \leq k \leq 2^n - 1$ é

$$\begin{aligned} p_k &= \langle\psi| (I \otimes P_k) |\psi\rangle \\ &= \sum_{i=0}^{2^m-1} |a_{ik}|^2 . \end{aligned} \tag{1.4.22}$$

O conjunto $\left\{p_1, \cdots, p_{2^n-1}\right\}$ é uma distribuição de probabilidades, que satisfaz a

$$\sum_{k=0}^{2^n-1} p_k = 1. \tag{1.4.23}$$

Se o resultado da medida for k, o estado logo após será

$$\frac{1}{\sqrt{p_k}} (I \otimes P_k) |\psi\rangle = \frac{1}{\sqrt{p_k}} \left(\sum_{i=0}^{2^m-1} a_{ik} |i\rangle \right) |k\rangle . \tag{1.4.24}$$

Exercício 1.1. *Como o resultado de uma medida do estado $|\psi\rangle$ com o observável O obedece a uma distribuição de probabilidades, podemos definir o valor esperado da medida como*

$$\langle O \rangle = \sum_{\lambda} p_\lambda \, \lambda,$$

e o desvio padrão como

$$\Delta O = \sqrt{\langle O^2 \rangle - \langle O \rangle^2}.$$

Mostre que $\langle O \rangle = \langle\psi| O |\psi\rangle$.

Exercício 1.2. *Suponha que o estado de um qubit seja $|1\rangle$.*

1. *Se uma medida é feita com o observável X, qual é o valor médio de X e qual é o desvio padrão?*
2. *Se uma medida é feita com o observável Z, qual é o valor médio de X e qual é o desvio padrão?*

Sugestões para Leitura

A quantidade de bons livros de Mecânica Quântica é muito grande. Para um contato inicial, sugerimos as Refs. [21, 52, 55]; para uma abordagem mais completa sugerimos a Ref. [15]; para quem está interessado apenas na aplicação da Mecânica Quântica na Computação Quântica, sugerimos as Refs. [49, 54, 44]; para uma abordagem mais conceitual, sugerimos as Refs. [51, 16].

Capítulo 2

Introdução ao Conceito de Passeio Quântico

Uma das técnicas mais promissoras para o desenvolvimento de algoritmos quânticos é a área de *passeios quânticos*. Essa técnica se diferencia das técnicas usadas em algoritmos algébricos, onde a transformada de Fourier é o ingrediente principal. Algoritmos baseados em passeios quânticos usam a técnica de *amplificação de amplitude* que foi introduzida no algoritmo de Grover. Porém, é possível ir além do algoritmo de Grover em termos de eficiência. O melhor algoritmo para resolver o problema de determinar se um conjunto tem todos elementos distintos ou não se baseia em passeios quânticos. Quando usamos o algoritmo de Grover para resolver esse problema, a solução é menos eficiente.

Antes de descrever a área de passeios quânticos, faremos uma breve revisão da área de *passeios aleatórios clássicos* com foco na velocidade de espalhamento da *distribuição de probabilidades*. Depois, vamos comparar a velocidade de espalhamento clássica com a quântica. Veremos que a probabilidade de encontrar a partícula longe da origem é maior no caso quântico. Esse fato é a principal arma que torna os algoritmos baseados em passeios quânticos mais rápidos do que os baseados em passeios aleatórios clássicos.

2.1 Passeio Aleatório Clássico

2.1.1 Passeio Aleatório na Reta

O exemplo mais simples de passeio aleatório clássico é o movimento de uma partícula sobre uma reta, cuja direção é determinada por uma moeda

não-viciada. Joga-se a moeda, se der coroa, a partícula dá um salto de uma unidade para direita, se der cara, dá um salto de uma unidade para a esquerda. Esse processo é repetido a cada unidade de tempo. Como esse processo é probabilístico, não podemos saber com certeza onde estará a partícula em um instante posterior, porém podemos calcular a probabilidade p dela estar em um determinado ponto n no instante de tempo inteiro t. Suponha que a partícula esteja na origem no instante $t = 0$, então $p(t = 0, n = 0) = 1$, como mostra a tabela da Fig. 2.1. No instante $t = 1$, a partícula pode estar em $n = -1$ com probabilidade $1/2$ e em $n = 1$ com probabilidade $1/2$. A probabilidade dela ocupar a posição $n = 0$ passa a ser zero. Seguindo esse raciocínio, podemos confirmar as probabilidades descritas na tabela da Fig. 2.1.

$t \backslash n$	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					$\frac{1}{2}$		$\frac{1}{2}$				
2				$\frac{1}{4}$		$\frac{1}{2}$		$\frac{1}{4}$			
3			$\frac{1}{8}$		$\frac{3}{8}$		$\frac{3}{8}$		$\frac{1}{8}$		
4		$\frac{1}{16}$		$\frac{1}{4}$		$\frac{3}{8}$		$\frac{1}{4}$		$\frac{1}{16}$	
5	$\frac{1}{32}$		$\frac{5}{32}$		$\frac{5}{16}$		$\frac{5}{16}$		$\frac{5}{32}$		$\frac{1}{32}$

Figura 2.1: Probabilidade da partícula estar na posição n no instante t, supondo que ela começa o passeio aleatório na origem. A probabilidade é zero nas células vazias.

Um termo genérico dessa tabela é dado por

$$p(t, n) = \frac{1}{2^t} \binom{t}{\frac{t+n}{2}}, \tag{2.1.1}$$

onde $\binom{a}{b} = \frac{a!}{(a-b)!b!}$. Essa equação é válida somente se $t + n$ for par e $n \leq t$. Se $t + n$ for ímpar ou $n > t$, a probabilidade é zero. Para t fixo, $p(t, n)$ é uma *distribuição binomial*. Para valores relativamente grandes de t fixos, a probabilidade em função de n tem uma curva característica. Na Fig. 2.2 mostramos três dessas curvas para $t = 72$, $t = 180$ e $t = 450$. A rigor, as curvas são envoltórias da distribuição de pontos, pois a probabilidade é zero para valores ímpares de n quando t é par. Outra maneira de interpretar as curvas da figura é com a soma $p(t, n) + p(t + 1, n)$, ou seja, temos duas distribuições superpostas.

Podemos ver na Fig. 2.2 que a altura do ponto central da curva diminui em função do tempo enquanto a largura aumenta. É natural perguntar

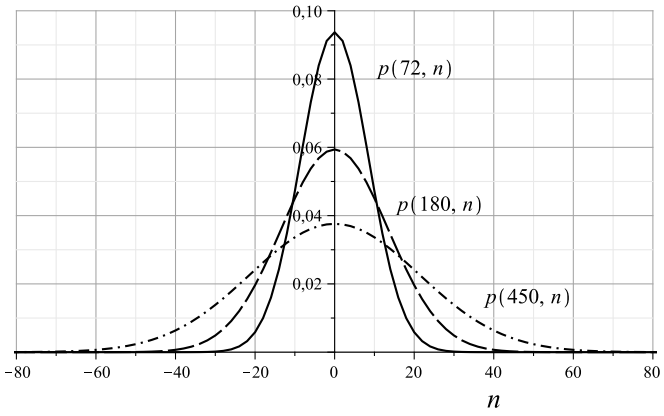

Figura 2.2: Distribuição de probabilidades do passeio aleatório clássico em uma malha unidimensional para $t = 72$, $t = 180$ e $t = 450$.

qual é a *velocidade de espalhamento* da distribuição de probabilidades. É importante determinar a que distância podemos encontrar a partícula da origem a medida que o tempo passa. A velocidade de espalhamento é uma grandeza estatística que captura essa ideia.

Uma forma de responder a essa pergunta é calculando o *desvio padrão* do espaço percorrido segundo a distribuição de probabilidades p, pois o desvio padrão é uma medida do espalhamento de uma distribuição de probabilidades. Como o valor médio de n é

$$\begin{aligned} \langle n \rangle &= \sum_{n=-\infty}^{\infty} n\, p(t,n) \\ &= 0, \end{aligned} \tag{2.1.2}$$

segue que o desvio padrão é

$$\begin{aligned} \sqrt{\langle n^2 \rangle - \langle n \rangle^2} &= \sqrt{\sum_{n=-\infty}^{\infty} n^2\, p(t,n)} \\ &= \sqrt{t}\,. \end{aligned} \tag{2.1.3}$$

Uma segunda forma de responder à pergunta é convertendo a distribuição binomial para uma expressão mais fácil de se lidar analiticamente. Substituindo a expressão binomial em termos do fatorial na Eq. (2.1.1) e

usando a aproximação de Stirling para valores grandes de t, a distribuição de probabilidades do passeio aleatório pode ser aproximada pela expressão

$$p\,(t,n) \approx \frac{2}{\sqrt{2\pi\,t}}\,\mathrm{e}^{-\frac{n^2}{2t}}. \tag{2.1.4}$$

Para t fixo e sem o fator 2 no numerador, essa função é chamada de *distribuição Gaussiana* ou *normal*. A largura da distribuição normal é definida como a metade da distância entre os pontos de inflexão. Igualando a derivada segunda $\partial^2 p/\partial n^2$ a zero, obtemos a largura $\sqrt{t}$. A velocidade esperada é a derivada temporal. Como estamos lidando com distribuições de probabilidades, o melhor que podemos fazer é usar grandezas médias.

Exercício 2.1. *O objetivo deste exercício é obter a Eq. (2.1.1). Primeiro mostre que, no instante t, o número total de possíveis caminhos da partícula é 2^t. No instante t a partícula se encontra na posição n. Suponha que a partícula deu a passos para direita e b passos para a esquerda. Encontre a e b em função de t e n. Agora concentre-se nos passos para a direita. De quantas maneiras a partícula pode dar a passos para a direita em t unidades de tempo? Ou, equivalentemente, temos t objetos, de quantas maneiras podemos selecionar a objetos? Mostre que a probabilidade da partícula estar na posição n é dada pela Eq. (2.1.1).*

Exercício 2.2. *O objetivo deste exercício é orientar o cálculo do somatório da Eq. (2.1.3). Renomeie o índice mudo do somatório para obter uma soma finita iniciando em $n = 0$ e correndo apenas para valores pares de n quando t for par e correndo apenas para valores ímpares de n quando t for ímpar. Use as identidades*

$$\sum_{n=0}^{t}\binom{t}{n} = 2^t, \quad \sum_{n=0}^{t} n\binom{t}{n} = t2^{t-1}, \quad \sum_{n=0}^{t} n^2\binom{t}{n} = t(t+1)2^{t-2}$$

e simplifique o resultado para mostrar que

$$\sum_{n=-\infty}^{\infty} n^2\,p(t,n) = t.$$

2.1.2 Cadeia de Markov Clássica Discreta

Uma *cadeia de Markov clássica* é um processo estocástico que assume valores em um conjunto discreto e obedece à seguinte propriedade: o próximo estado da cadeia depende apenas do estado atual, isto é, não é influenciado pelos estados passados. A cadeia de Markov pode ser vista como um grafo

direcionado onde os estados são representados pelos vértices e as arestas direcionadas indicam quais são os possíveis próximos estados. O próximo estado é decidido de forma aleatória. Note que o conjunto de estados é discreto, mas a evolução temporal pode ser discreta ou contínua. Portanto, o termo discreto ou contínuo do nome dessa área se refere apenas ao tempo.

Vamos começar descrevendo as *cadeias de Markov clássicas discretas*, ou seja, cadeias com a variável temporal discreta. A cada instante, a cadeia de Markov tem uma distribuição de probabilidades associada, que é o conjunto das probabilidades do caminhante estar nos estados ou vértices. Podemos descrever a distribuição de probabilidades com um vetor. Para isso, devemos escolher uma ordenação dos estados. Seja $\Gamma(X, E)$ um grafo com o conjunto de vértices $X = \{x_1, \cdots, x_n\}$ ($|X| = n$) e conjunto das arestas E. A distribuição de probabilidades é descrita por um vetor da forma

$$\begin{pmatrix} p_1(t) \\ \vdots \\ p_n(t) \end{pmatrix},$$

onde $p_1(t)$ é a probabilidade do caminhante estar no vértice x_1 no instante t. Analogamente para as outras componentes. Se o processo começa com o caminhante no primeiro vértice, temos que $p_1(0) = 1$ e $p_i(0) = 0$ para $i = 2, \cdots, n$. Em uma cadeia de Markov, não podemos descrever onde o caminhante estará precisamente no futuro, porém, podemos determinar sua distribuição de probabilidades uma vez conhecida a *matriz de transição* M, também denominada *matriz de probabilidades* ou *matriz estocástica*.

Se a distribuição de probabilidades for conhecida no instante t, poderemos obter a distribuição no instante $t + 1$ através da fórmula

$$p_i(t + 1) = \sum_{j=1}^{n} M_{i\,j}\, p_j(t). \tag{2.1.5}$$

Para garantir que $p_i(t + 1)$ seja uma distribuição de probabilidade, isto é, $p_i \geq 0, \forall i$ e $\sum_i p_i = 1$, a matriz M deve satisfazer às seguintes propriedades. As componentes de M devem ser números reais não-negativos e a soma das componentes de qualquer coluna de M deve ser igual a 1. Na forma vetorial temos

$$\vec{p}(t + 1) = M\, \vec{p}(t). \tag{2.1.6}$$

Como a matriz fica a esquerda, essa versão é chamada *matriz estocástica à esquerda*. Existe uma descrição correspondente que usa o vetor de probabilidades na forma transposta (vetor-linha) e a matriz fica a direita. Neste caso, a soma das componentes de cada linha deve dar 1.

A componente M_{ij} da matriz estocástica é a probabilidade do caminhante, que está no vértice x_i, ir para o vértice x_j. O caso mais simples é quando o grafo é não-direcionado e

$$M_{ij} = \frac{1}{d_i},$$

onde d_i é o *grau* ou *valência* do vértice x_i. Se não houver uma aresta de x_i para x_j, então $M_{ij} = 0$. Neste caso, o caminhante vai para um dos vértices adjacentes e a probabilidade de transição é a mesma para todos eles.

Vamos tomar o *grafo completo* com n vértices como exemplo. Todos os vértices estão ligados entre si por arestas não-direcionadas. Portanto, o grau de cada vértice é $1/(n-1)$. Os vértices não têm *laços*, portanto $M_{i\,i} = 0$, $\forall i$. A matriz estocástica é

$$M = \frac{1}{n-1}\begin{bmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{bmatrix}. \tag{2.1.7}$$

Se a condição inicial for um caminhante localizado no primeiro vértice, as distribuições de probabilidades nos primeiros instantes serão

$$\vec{p}(0) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \vec{p}(1) = \frac{1}{n-1}\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \quad \vec{p}(2) = \frac{1}{(n-1)^2}\begin{pmatrix} n-1 \\ n-2 \\ \vdots \\ n-2 \end{pmatrix}.$$

A distribuição de probabilidades em um instante qualquer é

$$\vec{p}(t) = \begin{pmatrix} f_n(t-1) \\ f_n(t) \\ \vdots \\ f_n(t) \end{pmatrix}, \tag{2.1.8}$$

onde a função $f_n(t)$ é

$$f_n(t) = \frac{1}{n}\left(1 - \frac{1}{(1-n)^t}\right). \tag{2.1.9}$$

Observe que, quando $t \to \infty$, a distribuição de probabilidades tende para a distribuição uniforme, que é a *distribuição limite* deste grafo.

Como motivação para a próxima seção, vamos fazer algumas observações sobre a estrutura dinâmica das cadeias de Markov discretas. A Eq. (2.1.6) é uma *equação recursiva* que pode ser resolvida e escrita como

$$\vec{p}(t) = M^t \, \vec{p}(0), \tag{2.1.10}$$

onde $\vec{p}(0)$ é a condição inicial. A matriz M governa um passo da evolução. As aplicações sucessivas geram a distribuição de probabilidades em qualquer instante. Esta descrição dinâmica é mais geral do que a descrição determinística. Em um processo determinístico, apenas uma possibilidade evolui com o tempo. Portanto, não temos um vetor de posições nem uma matriz de evolução. A posição é um escalar cuja dinâmica é descrita por uma função do tempo. No caso estocástico, temos que considerar todas as evoluções possíveis e descrevê-las em uma estrutura matricial. Porém, sabemos que apenas uma possibilidade de fato ocorre em uma situação concreta. A estrutura matricial da evolução estocástica será usada na próxima seção para descrever a evolução quântica. No entanto, a interpretação física do que acontece no nível físico concreto é nitidamente diferente do processo estocástico, pois, no caso quântico, não está correto afirmar que apenas uma das possibilidades ocorre. Do ponto de vista matemático, a mudança radical ocorre porque a matriz de evolução não é aplicada diretamente na distribuição de probabilidades e as componentes da matriz não precisam ser números reais positivos. No caso quântico, as componentes podem ser negativas ou complexas e a matriz de evolução é aplicada no vetor das *amplitudes de probabilidades*.

Exercício 2.3. *O objetivo desse exercício é obter a expressão (2.1.8). Por inspeção da matriz estocástica do grafo completo, mostre que* $p_2 = p_3 = \cdots = p_n$ *e* $p_1(t+1) = p_2(t)$. *Como a soma das componentes do vetor de probabilidades deve dar 1, mostre que* $p_2(t)$ *satisfaz à seguinte equação recursiva*

$$p_2(t) = \frac{1 - p_2(t-1)}{n-1}.$$

Usando a condição de parada $p_2(0) = 0$*, resolva a equação recursiva e mostre que* $p_2(t)$ *é dado por* $f_n(t)$*, como na Eq. (2.1.9).*

2.2 Passeio Aleatório Quântico Discreto

A construção dos modelos quânticos e suas equações usualmente é feita por um processo chamado de *quantização*. As variáveis momentum e energia são substituídas por operadores em um espaço de Hilbert, cuja dimensão depende dos graus de liberdade do sistema físico. Descrevemos o estado

do sistema quântico por um vetor no espaço de Hilbert e a evolução do sistema é governada por uma operação unitária se o sistema estiver totalmente isolado de interações com o mundo macroscópico ao redor. Se o sistema for composto por mais de uma componente, o espaço de Hilbert será o produto tensorial dos espaços de Hilbert das componentes. Como a evolução do sistema quântico é unitária, não há nenhum espaço para fenômenos randômicos. Portanto, em princípio, o nome *passeio aleatório quântico* é contraditório. Na literatura, o termo *passeio quântico* tem sido mais usado, porém sistemas quânticos, que não estão totalmente isolados do ambiente, podem ter *aleatoriedade*. Além disso, em algum momento vamos medir o sistema quântico para obter informações sobre ele. Neste momento, ocorre um processo que envolve uma distribuição de probabilidades.

O primeiro modelo de quantização de passeios aleatórios clássicos que vamos discutir é o *modelo a tempo discreto* ou simplesmente *modelo discreto*. A posição n do caminhante deve ser, no caso quântico, um vetor em um espaço de Hilbert $\mathcal{H}_P$ de dimensão infinita, cuja base computacional é $\left\{ |n\rangle : n \in \mathbb{Z} \right\}$. A evolução do passeio deve depender de uma "moeda" quântica. Se a moeda der "coroa" e o caminhante está descrito pelo vetor $|n\rangle$, ele deve passar a ser descrito por $|n+1\rangle$. Caso dê "cara", será descrito por $|n-1\rangle$. Como introduzir essa "moeda" no esquema? Podemos pensar em termos físicos. Suponha que um elétron seja o caminhante "aleatório" sobre uma malha unidimensional, o estado do elétron será descrito não só pela sua posição na malha, mas também pelo valor do seu spin, que poderá assumir dois valores: spin para cima ou spin para baixo. Assim, podemos condicionar a direção do movimento ao valor do spin. Se o elétron estiver na posição $|n\rangle$ e seu spin estiver para cima, ele deverá ir para $|n+1\rangle$ mantendo o mesmo valor de spin. Analogamente, quando seu spin estiver para baixo, ele deverá ir para $|n-1\rangle$. O espaço de Hilbert do sistema conjunto deve ser $\mathcal{H} = \mathcal{H}_M \otimes \mathcal{H}_P$, onde $\mathcal{H}_M$ é o espaço de Hilbert bidimensional associado a "moeda" cuja base computacional é $\left\{ |0\rangle , |1\rangle \right\}$. Podemos agora definir a "moeda" como qualquer matriz C de dimensão 2×2 unitária (C vem do termo *coin operator*), que atua em vetores no espaço de Hilbert $\mathcal{H}_M$.

O deslocamento de $|n\rangle$ para $|n+1\rangle$ ou para $|n-1\rangle$ deve ser descrito por um operador unitário, chamado operador de deslocamento S (S vem do termo *shift operator*). Ele deve operar da seguinte forma

$$S\,|0\rangle\,|n\rangle = |0\rangle\,|n+1\rangle\,, \tag{2.2.11}$$

$$S\,|1\rangle\,|n\rangle = |1\rangle\,|n-1\rangle\,. \tag{2.2.12}$$

Conhecendo-se a atuação de S na base computacional de $\mathcal{H}$, temos uma

descrição completa desse operador linear. Portanto, podemos deduzir que

$$S = |0\rangle\langle 0| \otimes \sum_{n=-\infty}^{\infty} |n+1\rangle\langle n| + |1\rangle\langle 1| \otimes \sum_{n=-\infty}^{\infty} |n-1\rangle\langle n| . \qquad (2.2.13)$$

Podemos re-obter Eqs. (2.2.11) e (2.2.12) aplicando S na base computacional.

No início do passeio quântico, devemos aplicar o operador moeda C no estado inicial, que é análogo ao papel de jogar a moeda no caso clássico. Isso produz uma rotação no estado da moeda. Se a moeda estiver descrita inicialmente por um dos estados da base computacional, o resultado poderá ser uma superposição de estados. Cada termo dessa superposição irá gerar um deslocamento em uma direção. Gostaríamos de escolher uma moeda não viciada de modo que gere um passeio simétrico em torno da origem. Vamos tomar o estado inicial com a partícula localizada na origem $|n = 0\rangle$ e o valor da moeda com spin para cima $|0\rangle$. Assim

$$|\psi(0)\rangle = |0\rangle|n = 0\rangle , \qquad (2.2.14)$$

onde $|\psi(0)\rangle$ denota o estado no instante inicial e $|\psi(t)\rangle$ denota o estado do passeio quântico no instante t.

A moeda mais usada para passeios quânticos unidimensionais é o operador de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} . \qquad (2.2.15)$$

Um passo consiste na aplicação de H no estado da moeda, ou seja, na aplicação de $H \otimes I$, onde I é o operador identidade do espaço de Hilbert $\mathcal{H}_P$ seguido da aplicação do operador de deslocamento S.

$$\begin{aligned} |0\rangle \otimes |0\rangle &\xrightarrow{H\otimes I} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \\ &\xrightarrow{S} \frac{1}{\sqrt{2}}\big(\,|0\rangle \otimes |1\rangle + |1\rangle \otimes |-1\rangle\,\big). \end{aligned} \qquad (2.2.16)$$

O resultado é uma superposição da partícula tanto na posição $n = 1$ como na posição $n = -1$. Podemos ver que a moeda H é não-viciada pois a amplitude da parte que foi para a direita é igual a amplitude da parte que foi para esquerda. A superposição de direções é consequência da superposição produzida pelo operador moeda.

Qual é o próximo passo? No caso quântico, precisamos medir o estado (2.2.16) para saber qual é a posição da partícula. Se medirmos usando a base computacional de $\mathcal{H}_P$, teremos 50% de chance de encontrarmos a partícula

na posição $n = 1$ e 50% de chance de encontrarmos na posição $n = -1$. Tal resultado é igual ao primeiro passo do passeio aleatório clássico. Se repetirmos o mesmo procedimento sucessivamente, isto é, aplicarmos o operador moeda e, em seguida, aplicarmos o operador de deslocamento e, logo após, medirmos usando a base computacional, re-obteremos o passeio aleatório clássico. Nosso objetivo é usar fenômenos quânticos para obter resultados novos, que não poderão ser obtidos no contexto clássico. Quando medimos a posição da partícula após o primeiro passo, destruímos as correlações entre diferentes posições, que são típicas de sistemas quânticos. Se não medirmos e aplicarmos sucessivamente o operador moeda seguido do operador de deslocamento, as correlações quânticas entre diferentes posições podem ter interferência construtiva ou destrutiva, gerando um comportamento efetivamente diferente do contexto clássico, característico de passeios quânticos. Veremos que a distribuição de probabilidades não tende à distribuição normal e que o desvio padrão não é $\sqrt{t}$.

O passeio quântico consiste na aplicação do operador unitário

$$U = S\,(H \otimes I), \tag{2.2.17}$$

um certo número de vezes sem medições intermediárias. Um passo consiste em aplicar U uma vez, que é equivalente a aplicar o operador moeda seguido do operador de deslocamento. No passo seguinte, aplicamos U novamente sem medições intermediárias. No instante t, o estado do passeio quântico é dado por

$$|\psi(t)\rangle = U^t\,|\psi(0)\rangle\,. \tag{2.2.18}$$

Vamos calcular os passos iniciais explicitamente para comparar com o passeio aleatório clássico. Tomaremos a condição inicial da Eq. (2.2.14). O primeiro passo será igual ao da Eq. (2.2.16). O segundo passo pode ser calculado através da fórmula $|\psi(2)\rangle = U\,|\psi(1)\rangle$ e assim por diante.

$$\begin{aligned}
|\psi(1)\rangle &= \frac{1}{\sqrt{2}}\big(\,|1\rangle\,|-1\rangle + |0\rangle\,|1\rangle\,\big) \\
|\psi(2)\rangle &= \frac{1}{2}\Big(-|1\rangle\,|-2\rangle + (|0\rangle + |1\rangle)\,|0\rangle + |0\rangle\,|2\rangle\,\Big) \\
|\psi(3)\rangle &= \frac{1}{2\sqrt{2}}\Big(\,|1\rangle\,|-3\rangle - |0\rangle\,|-1\rangle + (2\,|0\rangle + |1\rangle)\,|1\rangle + |0\rangle\,|3\rangle\,\Big)
\end{aligned} \tag{2.2.19}$$

Esses poucos passos iniciais já mostram que o passeio quântico difere do passeio randômico clássico em vários aspectos. Usamos uma moeda não viciada, porém o estado $|\psi(3)\rangle$ não é simétrico em relação a origem. A tabela da Fig. 2.3 mostra a distribuição de probabilidades até o quinto passo, sem medições intermediárias. Além de ser assimétrica, a distribuição

de probabilidades não é concentrada nos pontos centrais. A comparação com a tabela da Fig. 2.1 mostra isso.

t \ n	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					$\frac{1}{2}$		$\frac{1}{2}$				
2				$\frac{1}{4}$		$\frac{1}{2}$		$\frac{1}{4}$			
3			$\frac{1}{8}$		$\frac{1}{8}$		$\frac{5}{8}$		$\frac{1}{8}$		
4		$\frac{1}{16}$		$\frac{1}{8}$		$\frac{1}{8}$		$\frac{5}{8}$		$\frac{1}{16}$	
5	$\frac{1}{32}$		$\frac{5}{32}$		$\frac{1}{8}$		$\frac{1}{8}$		$\frac{17}{32}$		$\frac{1}{32}$

Figura 2.3: Probabilidade de encontrar a partícula quântica na posição n no instante t, supondo que ela começa o passeio quântico na origem com a moeda na posição "coroa".

Gostaríamos de encontrar a distribuição de probabilidades para um número de passos bem maior que 5. No entanto, o método de cálculo que estamos usando é trabalhoso demais para ser feito manualmente. Vamos supor que nosso objetivo seja calcular $p(100, n)$, isto é, a distribuição de probabilidades no centésimo passo. Primeiro temos que calcular $|\psi(100)\rangle$. Podemos seguir três caminhos para fazer uma implementação computacional.

O primeiro caminho é calcular explicitamente a matriz U. Temos que calcular o produto tensorial $H \otimes I$ segundo a fórmula do Apêndice A. O produto tensorial também é necessário para a obtenção da representação matricial do operador de deslocamento conforme definido na Eq. (2.2.13). Esses operadores atuam em vetores de um espaço vetorial infinito, no entanto, o número de componentes não-nulas é finito. Portanto, essas matrizes devem ter dimensões um pouco maior que 200×200. Após calcular U, devemos calcular o produto matricial de U^{100} com a condição inicial $|\psi(0)\rangle$ escrita como um vetor coluna com um número de componentes compatível. O resultado é $|\psi(100)\rangle$ e, finalmente, podemos calcular a distribuição de probabilidades.

O segundo caminho usa uma fórmula recursiva obtida da seguinte forma: o estado genérico do passeio quântico pode ser escrito pela combinação linear da base computacional como

$$|\psi(t)\rangle = \sum_{n=-\infty}^{\infty} \left(A_n(t)\,|0\rangle + B_n(t)\,|1\rangle \right) |n\rangle\,, \tag{2.2.20}$$

onde os coeficientes satisfazem ao vínculo

$$\sum_{n=-\infty}^{\infty} |A_n(t)|^2 + |B_n(t)|^2 = 1, \tag{2.2.21}$$

garantindo que $|\psi(t)\rangle$ tenha norma igual a 1 em todos os passos. Através de uma aplicação de $H \otimes I$ seguido do operador de deslocamento na expressão (2.2.20), podemos obter fórmulas recursivas envolvendo os coeficientes A e B, que são dadas por

$$\begin{aligned} A_n(t+1) &= \frac{A_{n-1}(t) + B_{n-1}(t)}{\sqrt{2}}, \\ B_n(t+1) &= \frac{A_{n+1}(t) - B_{n+1}(t)}{\sqrt{2}}. \end{aligned}$$

Usando as condições iniciais

$$A_n(0) = \begin{cases} 1, & \text{se } n = 0; \\ 0, & \text{caso contrário,} \end{cases}$$

$B_n(0) = 0$ podemos calcular a distribuição de probabilidades através da fórmula

$$p(t,n) = |A_n(t)|^2 + |B_n(t)|^2 . \tag{2.2.22}$$

O terceiro caminho é fazer o *download* do programa *QWalk* da página `http://qubit.lncc.br/qwalk` e seguir as instruções de como escolher a condição inicial e o operador moeda adequados.

Usando qualquer um desses caminhos obtemos o gráfico da Fig. 2.4 para a distribuição de probabilidades após 100 passos. Semelhante ao caso clássico, ignoramos os valores nulos da probabilidade. Para $t = 100$, todos os valores ímpares de n têm probabilidade nula. A assimetria da distribuição de probabilidades é evidente. A probabilidade de encontrar a partícula do lado direito da origem é maior do que do lado esquerdo. Em particular, para n em torno de $100/\sqrt{2}$ a probabilidade é bem maior do que na origem. Esse fato não é exclusivo do valor $t = 100$. Ele é válido para qualquer valor de t. Isso sugere um comportamento *balístico* do passeio quântico. A partícula pode ser encontrada longe da origem como se tivesse executando um movimento uniforme para direita. É natural perguntar se esse comportamento se manteria caso a distribuição fosse simétrica em torno da origem.

Para obtermos uma distribuição simétrica, é necessário entender porque o exemplo anterior tem a tendência de ir mais para a direita. A moeda H introduz um sinal negativo quando aplicada no estado $|1\rangle$. Isso faz com que haja mais cancelamento de termos, cujo valor da moeda é descrito por $|1\rangle$

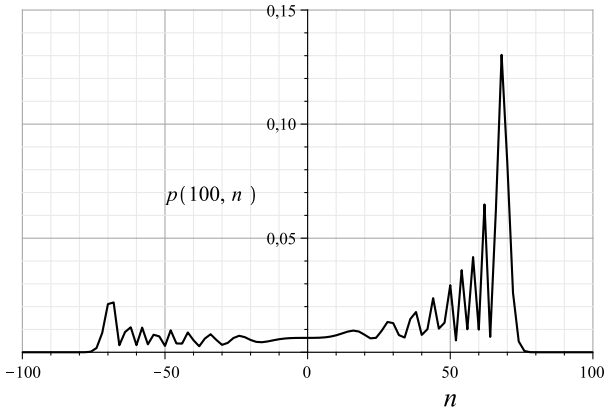

Figura 2.4: Distribuição de probabilidades após 100 passos de um passeio quântico com a moeda de Hadamard iniciando a partir da condição inicial $|\psi(0)\rangle = |0\rangle\,|n=0\rangle$. Os pontos onde a probabilidade são nulas foram excluídos (n ímpares).

do que termos com a moeda em $|0\rangle$. Como o estado $|0\rangle$ induz movimento para a direita e $|1\rangle$ para a esquerda, o efeito final é a assimetria. Podemos confirmar essa análise, calculando o passeio quântico resultante da condição inicial

$$|\psi(0)\rangle \;=\; -\,|1\rangle\,|n=0\rangle\,.$$

Nesse caso, o número de termos negativo será maior do que os positivos e haverá mais cancelamento de termos com o estado da moeda em $|0\rangle$. O resultado final é o espelho da distribuição da Fig. 2.4 em relação ao eixo vertical. Para obtermos uma distribuição simétrica, é preciso sobrepor os passeios quânticos resultantes dessas duas condições iniciais. O problema é um cancelamento fora de controle antes do cálculo da distribuição de probabilidades e, portanto, não temos a garantia de uma distribuição simétrica. Outra opção é multiplicar a segunda condição inicial pelo número complexo imaginário i e somar com a primeira condição inicial da seguinte forma

$$|\psi(0)\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}\,|n=0\rangle\,. \tag{2.2.23}$$

As componentes da moeda de Hadamard são reais. Portanto, os termos com a unidade imaginária não são convertidos em termos sem a unidade imaginária e vice-versa. Desse modo, não haverá cancelamento de nenhum termo do passeio dominante para direita com termos do passeio dominante

para a esquerda. No cálculo final, as distribuições de probabilidade se somam. De fato, o resultado é o gráfico da Fig. 2.5.

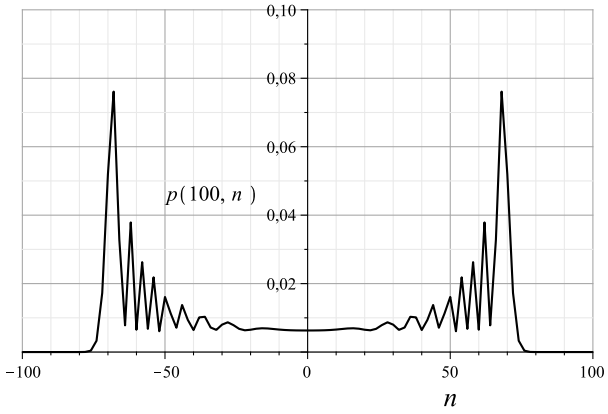

Figura 2.5: Distribuição de probabilidades após 100 passos de um passeio quântico com a moeda de Hadamard iniciando com a condição inicial dada pela Eq. (2.2.23).

Se a distribuição de probabilidades do passeio quântico for simétrica, o valor esperado da posição será zero, isto é, $\langle n \rangle = 0$. A questão agora é determinar como o desvio padrão $\sigma(t)$ se comporta em função do tempo. A fórmula do desvio padrão da posição é

$$\sigma(t) \quad = \quad \sqrt{\sum_{n=-\infty}^{\infty} n^2\, p(t,n)}, \tag{2.2.24}$$

onde $p(t,n)$ é a distribuição de probabilidades do passeio quântico com a condição inicial dada pela Eq. (2.2.23). O cálculo analítico é bastante elaborado e será feito em outro capítulo. No momento, vamos calcular numericamente o somatório da Eq. (2.2.24). Os gráficos da Fig. 2.6 mostram o desvio padrão em função do tempo tanto para o passeio quântico (pontos em forma de cruz) quanto para o passeio aleatório clássico (pontos em forma de círculo). Mostramos apenas os tempos pares para não sobrecarregar os gráficos. No caso clássico, temos $\sigma(t) = \sqrt{t}$. No caso quântico, obtemos nitidamente uma reta cuja inclinação é em torno de 0.54, isto é, $\sigma(t) = 0.54\, t$.

A dependência linear do desvio padrão com o tempo é impressionante. Considere a situação extrema. Suponha que a partícula tenha probabilidade

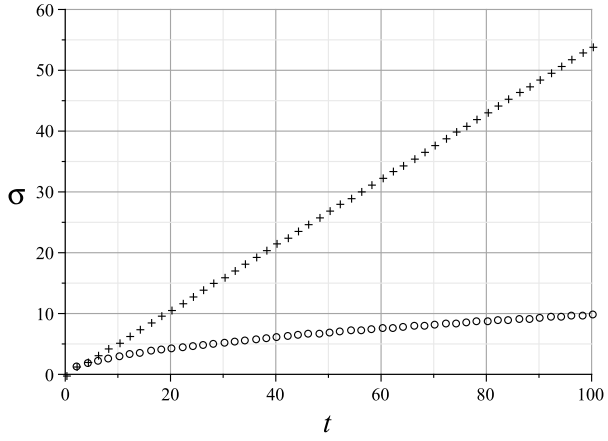

Figura 2.6: Desvio padrão da posição do passeio quântico (ponto-cruz) e do passeio aleatório clássico (círculos) em função do tempo.

exatamente igual a 1 de ir para a direita. No instante t, ela será encontrada com certeza na posição $n = t$. Esse movimento é chamado de *balístico*. É o movimento de uma partícula livre com velocidade unitária. O desvio padrão, nesse caso, é obtido substituindo $p(t, n)$ por $\delta_{t\,n}$ na Eq. (2.2.24). O resultado é $\sigma(t) = t$. O passeio quântico é balístico, porém a velocidade de afastamento da partícula é quase a metade da velocidade da partícula livre. Contudo, no caso quântico, a partícula poderá ser encontrada tanto à direita da origem quanto à esquerda de forma randômica, caracterizando um passeio aleatório. A distribuição de probabilidades quântica é espalhada no intervalo $\left[-t/\sqrt{2}, t/\sqrt{2}\right]$, enquanto que a distribuição clássica é uma Gaussiana concentrada na origem.

Exercício 2.4. *Calcule os estados $|\psi(4)\rangle$ e $|\psi(5)\rangle$ continuação dos estados das Eqs. (2.2.19) e verifique que a distribuição de probabilidades coincide com a descrita na tabela da Fig. 2.3.*

Sugestões para Leitura

Passeios aleatórios clássicos foram apresentados em inúmeros livros. Tratamentos bastante completos podem ser encontrados nas Refs. [19, 27, 28]. As fórmulas de somatório de expressões binomiais usadas no Exercício 2.2 podem ser deduzidas pelos métodos apresentados na Ref. [20] ou podem ser

encontradas na Ref. [11]. A *aproximação de Stirling* pode ser encontrada na Ref. [19].

O problema de determinar se um conjunto tem todos elementos distintos foi resolvido usando passeios quânticos na Ref. [6]. Uma boa referência para um contato inicial com a área de passeios quânticos é o artigo de revisão da *Julia Kempe* [31], de grande repercução. A noção de passeios aleatórios quânticos foi introduzida na Ref. [3] com o objetivo de apresentar novos fenômenos quânticos nitidamente diferentes dos clássicos. A Ref. [18] foi também bastante inovadora quando introduziu o conceito de *passeio quântico a tempo contínuo*. A aplicação desses novos conceitos para a área de algoritmos foi fortemente influenciada por essa referência. A análise de passeios quânticos na reta foi feita na Ref. [48]. A Ref. [1] promoveu um forte avanço na área de passeios quânticos em grafos. O programa *QWalk* está descrito na Ref. [43].

Capítulo 3

Algoritmo de Grover e sua Generalização

O *algoritmo de Grover* é um *algoritmo de busca* inicialmente idealizado para procurar um elemento em um banco de dados não-ordenado. Se o conteúdo de um banco de dados for armazenado de forma aleatória, o único método disponível para encontrar um elemento específico é uma busca exaustiva. Usualmente, esse não é o melhor método de usar bancos de dados, principalmente se ele for consultado diversas vezes. É melhor ordenar o conteúdo, tarefa custosa, mas feita uma única vez. No contexto quântico, armazenar dados em superposição ou emaranhados por um período longo não é uma tarefa fácil. Por essas razões, vamos apresentar o algoritmo de Grover de outra forma, tornando mais evidente sua grande aplicabilidade.

Na sequência, vamos mostrar que o algoritmo de Grover é *ótimo*, isto é, não é possível melhorar a *complexidade computacional*. Depois, trataremos da generalização do algoritmo de Grover para buscas em bancos de dados com elementos repetidos.

3.1 Algoritmo de Grover

Suponha que f é uma função cujo domínio é $\{0, \cdots, N-1\}$ onde $N = 2^n$ para algum inteiro positivo n e cuja imagem é

$$f(x) = \begin{cases} 1, & \text{se } x = x_0; \\ 0, & \text{caso contrário.} \end{cases} \tag{3.1.1}$$

Ou seja, a imagem da função f só é 1 para um único ponto x_0, para todos os outros pontos a imagem é 0. Suponha que tenhamos a função f a nossa

disposição. Podemos avaliar f em qualquer ponto do domínio, mas não conhecemos o ponto x_0. O problema é encontrar o ponto do domínio cuja imagem é 1, isto é, encontrar x_0. Esse é um problema de busca cuja relação com busca em banco de dados é evidente.

Qual é a *complexidade computacional* do melhor algoritmo clássico que resolve esse problema? Nesse problema em particular, o parâmetro usado para medir a complexidade é o número de vezes que a função f foi usada. Já que não conhecemos nenhuma equação para a função f nem qualquer detalhe da sua implementação, só nos resta uma busca exaustiva pelo ponto x_0. Consequentemente, a complexidade de tempo do algoritmo clássico é $\Omega(N)$. A função f é chamada de *oráculo* ou *caixa-preta*. Avaliar a função em um ponto também é referido como uma consulta ao oráculo. O ponto x_0 também é chamado de *elemento marcado*.

Uma maneira concreta de descrever esse problema é pedir a um programador que escolha aleatoriamente o ponto x_0 e implemente a função f usando uma linguagem de programação em um computador clássico com um único processador. Ele deve compilar o programa de forma a não termos acesso direto ao valor de x_0. Conhecemos o domínio da função que obedece à seguinte "promessa": apenas um ponto do domínio tem imagem 1, todos os outros pontos tem imagem 0. Um programa que resolve esse problema está descrito no Algoritmo 1.

Algoritmo 1: Algoritmo de Busca Clássico

```
for x = 0 to N − 1 do
    if f(x) = 1 then
        print x
        stop
```

Qual é a complexidade computacional do melhor algoritmo *quântico* que resolve o mesmo problema? O algoritmo de Grover encontra x_0 usando $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ consultas a função f. Esse é o algoritmo ótimo. Há um ganho quadrático na complexidade computacional na passagem do contexto clássico para o quântico. Como podemos colocar de maneira concreta esse problema? Podemos fazer um programa quântico equivalente ao Algoritmo 1?

No contexto quântico, devemos escolher um operador unitário que faça o papel da função f. Existe um método padrão de construir um operador unitário que implemente uma função. O computador quântico deve ter dois *registradores*. O primeiro registrador armazena os pontos do domínio e o segundo armazena os pontos da imagem da função f. A descrição completa

do operador, que chamaremos de $\mathcal{R}_f$, na base computacional é

$$\mathcal{R}_f \left|x\right\rangle \left|i\right\rangle = \left|x\right\rangle \left|i \oplus f(x)\right\rangle, \tag{3.1.2}$$

onde a operação $\oplus$ é a *soma binária*, ou *xor* bit-a-bit. O método padrão é: repetir o valor de x por questões de *reversibilidade* e fazer a soma binária da imagem de x com o valor do segundo registrador. Qualquer que seja a função f, o operador resultante será unitário.

Para a função f dada pela Eq. (3.1.1), o primeiro registrador deve ter n qubits e o segundo deve ter 1 qubit. Se o estado do segundo registrador for $\left|0\right\rangle$, podemos ver que $\mathcal{R}_f$ é similar à avaliação da função f:

$$\mathcal{R}_f \left|x\right\rangle \left|0\right\rangle = \begin{cases} \left|x_0\right\rangle \left|1\right\rangle, & \text{se } x = x_0; \\ \left|x\right\rangle \left|0\right\rangle, & \text{caso contrário.} \end{cases} \tag{3.1.3}$$

Agora pedimos a um programador quântico que implemente $\mathcal{R}_f$. Ele vai usar uma *porta Toffoli generalizada*. Por exemplo, se ele tiver em mãos $x_0 = 5$, o circuito da Fig. 3.1 implementará $\mathcal{R}_f$ para $n = 3$. Note que o estado do segundo registrador só mudará de $\left|0\right\rangle$ para $\left|1\right\rangle$ se a entrada do primeiro registrador for 5, caso contrário permanecerá no estado $\left|0\right\rangle$.

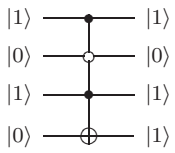

Figura 3.1: Circuito do operador $\mathcal{R}_f$ no caso $x_0 = 5$. O valor de x_0 determina quais bits de controle devem ser brancos e quais devem ser pretos. Apenas o programador quântico sabe onde estão os controles pretos e brancos.

Não podemos ver os detalhes da implementação de $\mathcal{R}_f$, porém podemos usar esse operador tantas vezes quanto desejarmos. Qual é o algoritmo que determina x_0 usando $\mathcal{R}_f$ o menor número de vezes?

O algoritmo de Grover usa um segundo operador definido por

$$\mathcal{R}_{\mathrm{D}} = \left(2 \left|\mathrm{D}\right\rangle \left\langle\mathrm{D}\right| - I_N\right) \otimes I_2, \tag{3.1.4}$$

onde $\left|\mathrm{D}\right\rangle$ é o *estado diagonal* do primeiro registrador (ver Apêndice). O *operador de evolução* para um passo do algoritmo é

$$U = \mathcal{R}_{\mathrm{D}}\, \mathcal{R}_f. \tag{3.1.5}$$

A condição inicial é

$$|\psi_0\rangle = |\mathrm{D}\rangle\,|-\rangle\,. \tag{3.1.6}$$

O algoritmo consiste em aplicar U no estado inicial $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ vezes. Medimos o primeiro registrador na base computacional e o resultado é x_0 com probabilidade maior ou igual a $1 - \frac{1}{N}$.

3.1.1 Análise através de Operadores de Reflexão

As componentes tanto do operador de evolução U como da condição inicial são reais. Isso quer dizer que toda a evolução se passa em um subespaço vetorial real do espaço de Hilbert $\mathcal{H}^{2N}$. No algoritmo de Grover, podemos visualizar geometricamente a evolução do algoritmo. A chave para entender o funcionamento do algoritmo é notar que o operador U é o produto de dois *operadores de reflexão*. Primeiro vamos verificar que $\mathcal{R}_f$ é uma reflexão em torno do espaço vetorial ortogonal ao espaço vetorial gerado por $|x_0\rangle$, que é um elemento da base computacional de $\mathcal{H}^{2N}$. Considere a ação de $\mathcal{R}_f$ no vetor $|x_0\rangle\,|-\rangle$. Usando a Eq. (3.1.3) obtemos

$$\begin{aligned} \mathcal{R}_f\ |x_0\rangle\,|-\rangle &= \frac{\mathcal{R}_f\,|x_0\rangle\,|0\rangle - \mathcal{R}_f\,|x_0\rangle\,|1\rangle}{\sqrt{2}} \\ &= \frac{|x_0\rangle\,|1\rangle - |x_0\rangle\,|0\rangle}{\sqrt{2}} \\ &= -\,|x_0\rangle\,|-\rangle\,. \end{aligned} \tag{3.1.7}$$

Logo $\mathcal{R}_f$ reflete $|x_0\rangle\,|-\rangle$ no espaço vetorial ortogonal a $|x_0\rangle\,|-\rangle$. Agora considere a ação de $\mathcal{R}_f$ em um vetor ortogonal à $|x_0\rangle\,|-\rangle$. Tome $|x\rangle\,|-\rangle$ onde $x \neq x_0$. Fazendo um cálculo análogo ao da Eq. (3.1.7) concluímos que

$$\mathcal{R}_f\ |x\rangle\,|-\rangle = |x\rangle\,|-\rangle\,,\ \ x \neq x_0. \tag{3.1.8}$$

Considere uma combinação linear com coeficientes reais de $|x_0\rangle\,|-\rangle$ com um vetor ortogonal à $|x_0\rangle\,|-\rangle$. A aplicação de $\mathcal{R}_f$ nessa soma inverte a componente de $|x_0\rangle\,|-\rangle$ e preserva a componente ortogonal à $|x_0\rangle\,|-\rangle$. A interpretação geométrica é uma reflexão.

$\mathcal{R}_\mathrm{D}$ também é uma reflexão, porém em torno do espaço vetorial gerado por $|\mathrm{D}\rangle$. Usando a Eq. (3.1.4) concluímos que

$$\mathcal{R}_\mathrm{D}\ |\mathrm{D}\rangle\,|-\rangle = |\mathrm{D}\rangle\,|-\rangle\,. \tag{3.1.9}$$

Tome um vetor ortogonal a $|\mathrm{D}\rangle\,|-\rangle$. Usando novamente a Eq. (3.1.4), concluímos que o resultado da aplicação de $\mathcal{R}_\mathrm{D}$ é o negativo do vetor original.

Considere uma combinação linear com coeficientes reais de $|\mathrm{D}\rangle\,|-\rangle$ com um vetor ortogonal à $|\mathrm{D}\rangle\,|-\rangle$. A componente ortogonal à $|\mathrm{D}\rangle\,|-\rangle$ inverte de sinal enquanto que a outra permanece invariante. A interpretação geométrica é uma reflexão análoga à ação de $\mathcal{R}_f$.

É possível simplificar a análise do algoritmo do seguinte modo: descartamos o segundo registrador, pois seu estado se mantém inalterado durante todo o algoritmo. Pela Fig. 3.2, podemos ver que uma aplicação de U no estado inicial resulta em um vetor que está no espaço vetorial gerado por $|x_0\rangle$ e $|\mathrm{D}\rangle$. O mesmo argumento vale para as próximas aplicações de U. Portanto, toda a evolução se passa em um plano real. Nesse caso R_f pode ser interpretado como uma reflexão em torno do espaço vetorial gerado pelo vetor ortogonal à $|x_0\rangle$ que pertence ao plano do algoritmo. Vamos chamar de $\left|x_0^{\perp}\right\rangle$ o vetor unitário ortogonal à $|x_0\rangle$ pertencente ao plano gerado por $|x_0\rangle$ e $|\mathrm{D}\rangle$ que tem o menor ângulo com $|\mathrm{D}\rangle$. A expressão para $\left|x_0^{\perp}\right\rangle$ na base computacional é

$$\left|x_0^{\perp}\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle\,. \tag{3.1.10}$$

Quando analisamos a evolução do algoritmo no plano gerado pelos vetores $|x_0\rangle$ e $|\mathrm{D}\rangle$, podemos substituir o operador $\mathcal{R}_f$ pelo seguinte operador

$$\mathcal{R}_{x_0^{\perp}} = 2\,\left|x_0^{\perp}\right\rangle\left\langle x_0^{\perp}\right| - I_N, \tag{3.1.11}$$

que mantém $\left|x_0^{\perp}\right\rangle$ inalterado e inverte o sinal de um vetor ortogonal a $\left|x_0^{\perp}\right\rangle$. Como descartamos o segundo registrador, vamos redefinir o operador $\mathcal{R}_{\mathrm{D}}$ para

$$\mathcal{R}_{\mathrm{D}} = 2\,|\mathrm{D}\rangle\,\langle\mathrm{D}| - I_N. \tag{3.1.12}$$

Em resumo, $\mathcal{R}_{x_0^{\perp}}$ é uma reflexão em torno do espaço vetorial gerado por $\left|x_0^{\perp}\right\rangle$ e $\mathcal{R}_{\mathrm{D}}$ é uma reflexão em torno do espaço vetorial gerado por $|\mathrm{D}\rangle$. Um passo da evolução é dado pelo operador

$$U = \mathcal{R}_{\mathrm{D}}\mathcal{R}_{x_0^{\perp}}, \tag{3.1.13}$$

que substitui o operador definido pela Eq. (3.1.5). A condição inicial é $|\mathrm{D}\rangle$.

Em espaços vetoriais reais, a ação de duas reflexões sucessivas sobre um vetor real $|\psi\rangle$ gira $|\psi\rangle$ de um ângulo que é o dobro do ângulo entre os espaços invariantes. A direção da rotação depende da ordem da aplicação das reflexões. No caso de $\mathcal{R}_{x_0^{\perp}}$ e $\mathcal{R}_{\mathrm{D}}$, a ação de U gira $|\psi\rangle$ de um ângulo que é o dobro do ângulo entre $\left|x_0^{\perp}\right\rangle$ e $|\mathrm{D}\rangle$. Como $\mathcal{R}_{x_0^{\perp}}$ é aplicado primeiro, o ângulo de rotação é positivo quando vai de $\left|x_0^{\perp}\right\rangle$ para $|\mathrm{D}\rangle$.

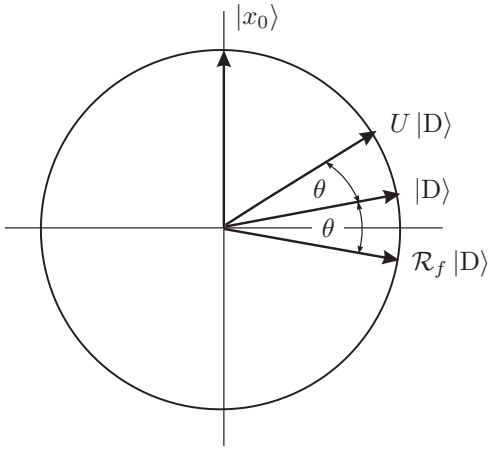

Figura 3.2: A condição inicial do algoritmo de Grover é o estado $|\mathrm{D}\rangle$. Após a aplicação do operador $\mathcal{R}_f$, o estado $|\mathrm{D}\rangle$ é refletido em torno do plano ortogonal ao vetor $|x_0\rangle$. Após a aplicação do operador $\mathcal{R}_\mathrm{D}$, o vetor $\mathcal{R}_f\,|\mathrm{D}\rangle$ é refletido em torno de $|\mathrm{D}\rangle$. Ou seja, uma aplicação de U gira o vetor inicial de θ graus em direção ao vetor $|x_0\rangle$.

Seja $\theta/2$ o ângulo entre $\left|x_0^\perp\right\rangle$ para $|\mathrm{D}\rangle$, tal ângulo é o complemento do ângulo entre $|x_0\rangle$ para $|\mathrm{D}\rangle$. Assim

$$\begin{aligned}\sin\frac{\theta}{2} &= \cos\left(\frac{\pi}{2}-\frac{\theta}{2}\right)\\ &= \left\langle x_0\middle|\mathrm{D}\right\rangle\\ &= \frac{1}{\sqrt{N}}.\end{aligned} \tag{3.1.14}$$

O ângulo θ é muito pequeno para uma função f que tenha $N \gg 1$. Quanto maior for o domínio de f, menor será o ângulo θ. Resolvendo a Eq. (3.1.14) para θ e tomando a expansão assintótica obtemos

$$\theta = \frac{2}{\sqrt{N}} + \frac{1}{3\,N\sqrt{N}} + O\left(\frac{1}{N^2}\right). \tag{3.1.15}$$

A condição inicial é $|\mathrm{D}\rangle$. Uma aplicação de U gira $|\mathrm{D}\rangle$ cerca de $\frac{2}{\sqrt{N}}$ graus na direção de $|x_0\rangle$. No instante

$$t_f = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor, \tag{3.1.16}$$

$|\mathrm{D}\rangle$ terá girado cerca de $\frac{\pi}{2}$ graus radianos. Na verdade, terá girado um pouco menos, pois o próximo termo na expansão (3.1.15) é positivo. O ângulo entre o estado final e $|x_0\rangle$ é cerca de $\frac{2}{\sqrt{N}}$ e é no máximo $\frac{\theta}{2}$. A probabilidade de encontrarmos o valor x_0 quando medimos o primeiro registrador é

$$\begin{aligned} p_{x_0} &= \left| \langle x_0 | \, U^{t_f} \, |\mathrm{D}\rangle \right|^2 \\ &\geq \cos^2 \frac{\theta}{2} \\ &= 1 - \frac{1}{N}. \end{aligned} \tag{3.1.17}$$

O limite inferior para a probabilidade de acerto mostra que o algoritmo de Grover tem uma probabilidade de sucesso muito alta quando N é grande.

Exercício 3.1. *Mostre que na base* $\left\{ |x_0\rangle \, , \left|x_0^{\perp}\right\rangle \right\}$, *$U$ é a matriz de rotação*

$$U = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Quais são as expressões de $\cos\theta$ *e* $\sin\theta$ *em função de N?*

Exercício 3.2. *Mostre que*

$$U^t \, |D\rangle = \sin\left(t\,\theta + \frac{\theta}{2}\right) |x_0\rangle + \cos\left(t\,\theta + \frac{\theta}{2}\right) \left|x_0^{\perp}\right\rangle .$$

Exercício 3.3. *Mostre que a probabilidade de acerto no algoritmo de Grover é 121/128 quando $N = 8$.*

Exercício 3.4. *Mostre que após descartar o segundo registrador, o operador $\mathcal{R}_f$ dado pela Eq. (3.1.2) pode ser escrito como*

$$\mathcal{R}_f = I - 2 \, |x_0\rangle \langle x_0| \, , \tag{3.1.18}$$

ou equivalentemente como

$$\mathcal{R}_f = 2 \sum_{x \neq x_0} |x\rangle \langle x| - I. \tag{3.1.19}$$

Qual é a decomposição espectral de R_f?

3.1.2 Análise através da Decomposição Espectral

Outra forma de analisar a evolução do algoritmo de Grover é através da *decomposição espectral* de U. O polinômio característico de U é

$$|\lambda I - U| = (\lambda + 1)^{N-2} \left(\lambda^2 - \frac{2(N-2)}{N} \lambda + 1 \right), \tag{3.1.20}$$

Portanto, os autovalores são -1 e $\mathrm{e}^{\pm i\omega}$ onde

$$\cos \omega = 1 - \frac{2}{N}. \tag{3.1.21}$$

O autovalor -1 tem multiplicidade $N-2$ e um conjunto não-ortogonal de autovetores associados é

$$|\alpha_j\rangle = \frac{|1\rangle - |j-1\rangle}{\sqrt{2}}, \quad 3 \leq j \leq N, \tag{3.1.22}$$

supondo que o elemento marcado é $x_0 = 0$. Os dois autovetores restantes associados aos autovalores $\mathrm{e}^{i\omega}$ e $\mathrm{e}^{-i\omega}$ são respectivamente

$$|\alpha_1\rangle = \frac{1}{\sqrt{2}} \left(\left|x_0^{\perp}\right\rangle - i \, |x_0\rangle \right), \tag{3.1.23}$$

$$|\alpha_2\rangle = \frac{1}{\sqrt{2}} \left(\left|x_0^{\perp}\right\rangle + i \, |x_0\rangle \right), \tag{3.1.24}$$

onde $\left|x_0^{\perp}\right\rangle$ é dado pela Eq. (3.1.10). A obtenção desses autovetores está orientada nos exercícios.

Autovetores de operadores unitários associados a autovalores distintos são ortogonais entre si. Portanto, $|\alpha_1\rangle$ e $|\alpha_2\rangle$ são ortogonais entre si e são ortogonais a $|\alpha_j\rangle$ para $3 \leq j \leq N$. Para analisar a evolução do algoritmo de Grover, temos que encontrar a expressão da condição inicial $|\mathrm{D}\rangle$ na base de autovetores de U. Usando a Eq. (3.1.22), vemos que $|\mathrm{D}\rangle$ é ortogonal a $|\alpha_j\rangle$ para $3 \leq j \leq N$. Portanto, a condição inicial está no espaço vetorial gerado por $|\alpha_1\rangle$ e $|\alpha_2\rangle$. Assim

$$|\mathrm{D}\rangle = a \, |\alpha_1\rangle + a^* \, |\alpha_2\rangle, \tag{3.1.25}$$

onde

$$\begin{aligned} a &= \langle \alpha_1 | \mathrm{D} \rangle \\ &= \frac{\sqrt{N-1} + i}{\sqrt{2N}}. \end{aligned} \tag{3.1.26}$$

Toda evolução do algoritmo se passa no espaço gerado por $|\alpha_1\rangle$ e $|\alpha_2\rangle$. A aplicação de U^t no estado $|\mathrm{D}\rangle$ dado pela Eq. (3.1.25) pode ser calculada explicitamente, pois $|\alpha_1\rangle$ e $|\alpha_2\rangle$ são autovetores de U com autovalores $\mathrm{e}^{\pm i\omega}$. Portanto, no instante t o estado do computador quântico é

$$U^t\,|\mathrm{D}\rangle = a\,\mathrm{e}^{i\omega t}\;|\alpha_1\rangle + a^*\mathrm{e}^{-i\omega t}\;|\alpha_2\rangle\,. \tag{3.1.27}$$

Por construção, as sucessivas aplicações do operador U giram o estado do computador quântico em direção ao estado $|x_0\rangle$, que é quase ortogonal ao estado inicial $|\mathrm{D}\rangle$ quando N é grande. Para $t_f = \pi/2\omega$ temos que $\mathrm{e}^{i\omega t_t} = i$ e $\mathrm{e}^{-i\omega t_f} = -i$, ou seja,

$$U^{t_f}\,|\mathrm{D}\rangle = i\,(a\;|\alpha_1\rangle - a^*\;|\alpha_2\rangle) \tag{3.1.28}$$

que é ortogonal a $|\mathrm{D}\rangle$. Esse é o primeiro valor de t tal que $U^t\,|\mathrm{D}\rangle$ é ortogonal à $|\mathrm{D}\rangle$.

Usando a equação acima para $U^{t_f}\,|\mathrm{D}\rangle$ e as Eqs. (3.1.23), (3.1.24) e (3.1.26), a probabilidade da medida do primeiro registrador na base computacional retornar o valor x_0 é

$$\begin{aligned} p_{x_0}(t_f) &= \left|\,\langle x_0|\,U^{t_f}\,|\mathrm{D}\rangle\,\right|^2 \\ &= 1 - \frac{1}{N}. \end{aligned} \tag{3.1.29}$$

Como o número de aplicações de U deve ser um número inteiro, temos que tomar $\lfloor \pi/2\omega \rfloor$ como instante de parada. Usando a Eq. (3.1.21) e tomando a *expansão assintótica* em N obtemos

$$\begin{aligned} \lfloor t_f \rfloor &= \left\lfloor \frac{\pi}{2\arccos\left(1-\frac{2}{N}\right)} \right\rfloor \\ &= \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor + O\left(\frac{1}{\sqrt{N}}\right). \end{aligned} \tag{3.1.30}$$

A expressão (3.1.29) é um limite inferior para $p_{x_0}(\lfloor t_f \rfloor)$.

Exercício 3.5. *Mostre que a matriz $\mathcal{R}_f$ dada pela Eq. (3.1.18) tem componentes $(\mathcal{R}_f)_{ij} = (-1)^{\delta_{ix_0}}\delta_{ij}$ e a matriz $\mathcal{R}_D$ dada pela Eq. (3.1.12) tem componentes $(\mathcal{R}_D)_{ij} = \frac{2}{N} - \delta_{ij}$. Mostre que as componentes de U são*

$$U_{ij} = (-1)^{\delta_{jx_0}}\left(\frac{2}{N} - \delta_{ij}\right).$$

Exercício 3.6. *Usando o Exercício 3.5, mostre que o polinômio característico de U é a expressão dada pela Eq. (3.1.20). Mostre que os autovalores são -1 e $e^{\pm i\omega}$ onde $\omega = \arccos\left(1-\frac{2}{N}\right)$.*

Exercício 3.7. *Use a matriz U dada no Exercício 3.5 e mostre que, se o elemento marcado é $x_0 = 0$, então a matriz $U + I$ é dada por*

$$U + I = \begin{pmatrix} \frac{2(N-1)}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ -\frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix}.$$

Por inspeção das componentes de $U + I$ obtenha uma base para o autoespaço associado ao autovalor -1. Mostre que os vetores $|\alpha_j\rangle$ descritos pela Eq. (3.1.22) formam uma base para este autoespaço. Generalize essa descrição para um elemento marcado genérico x_0 e mostre que o subespaço gerado por estes vetores não participa da dinâmica do processo.

3.1.3 Comparação entre as Análises

Apresentamos duas formas de analisar a evolução do algoritmo de Grover. Na primeira usamos o fato de que U é um operador real e produto de dois operadores de reflexão. U pode ser visto como uma matriz de rotação em um espaço vetorial bi-dimensional cujo ângulo de rotação é o dobro do ângulo entre os vetores invariantes pelos operadores de reflexão. O estado procurado $|x_0\rangle$ e a condição inicial $|\mathrm{D}\rangle$ são quase ortogonais para N grande. A estratégia do algoritmo é girar a condição inicial de $\pi/2$ radianos e medir usando a base computacional. Como o ângulo entre o estado final e o estado procurado é pequeno, a probabilidade de obter x_0 como resultado da medida é próxima de 1. Toda a interpretação da evolução do algoritmo nessa forma usa um subespaço real do espaço de Hilbert. Essa primeira forma de ver a evolução do algoritmo é bastante atraente pela sua simplicidade, porém não tem o mesmo grau de generalidade da segunda forma.

Na segunda forma, usamos a decomposição espectral de U. Toda a evolução se passa no autoespaço gerado por 2 autovetores, que são os únicos autovetores não-reais. Por definição, os autovetores não giram devido a ação de U. Porém, a condição inicial é uma combinação linear de autovetores e os coeficientes mudam devido a ação de U. A estratégia é igual a da primeira forma, ou seja, girar a condição inicial de $\pi/2$ radianos. Embora a primeira forma tenha uma interpretação geométrica atraente, a segunda forma permite estender a idéia por trás do algoritmo de Grover para outros algoritmos de busca, em particular, para o *algoritmo de busca abstrato*, que visa a encontrar um vértice especialmente marcado em um grafo.

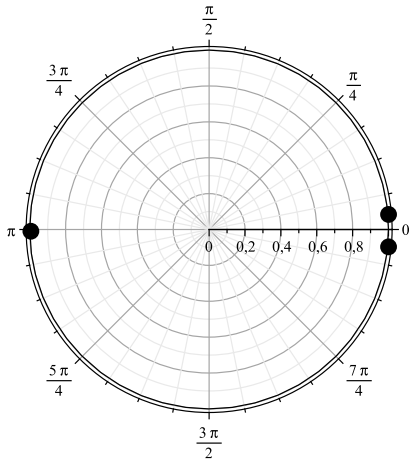

Figura 3.3: Autovalores do operador de evolução do algoritmo de Grover para $n = 9$.

Para ajudar na compreensão do algoritmo de busca abstrato futuramente, vamos analisar mais alguns detalhes da decomposição espectral de U do algoritmo de Grover. A Fig. 3.3 mostra a configuração geométrica dos autovalores de U para $N = 512$. Os autovalores não-reais são simétricos e tendem a 1 quando N cresce. Apesar deles estarem próximos, os autovetores associados são ortogonais. Note que U não tem 1 como autovalor. Se o estado inicial tivesse uma componente não desprezível no autoespaço associado a um autovalor 1, o algoritmo não funcionaria como desejado, pois não conseguiríamos girar o estado inicial de $\pi/2$ radianos. Assim, é necessário que o estado inicial não tenha componente no autoespaço associado ao autovalor 1 de U. No algoritmo de Grover, isso é válido automaticamente.

Outros detalhes importantes: o operador de evolução U é o produto de dois operadores $\mathcal{R}_{\mathrm{D}}$ e $\mathcal{R}_f$ e o estado inicial $|\mathrm{D}\rangle$ é autovetor com autovalor 1 do primeiro operador. O segundo operador deve ser uma reflexão. Essas exigências caracterizam um algoritmo de busca abstrato.

3.2 Otimalidade do Algoritmo de Grover

Mostramos que o algoritmo de Grover acha o elemento marcado fazendo $O\big(\sqrt{N}\big)$ consultas ao oráculo. É possível construir um algoritmo mais rápido do que o algoritmo de Grover? Nesta seção vamos mostrar que o algoritmo

de Grover é *ótimo*, isto é, nenhum algoritmo quântico pode encontrar o elemento marcado do domínio da função f fazendo menos do que $\Omega(\sqrt{N})$ consultas a função f.

Esse tipo de prova deve ser genérica. Usaremos o modelo de computação quântica padrão no qual um algoritmo genérico consiste em uma sequência de aplicações de operadores unitários a partir de uma condição inicial seguida de uma medida do estado final. Queremos mostrar que se o oráculo for consultado menos que $\Omega(\sqrt{N})$ vezes, o elemento marcado não será achado. Vamos supor que a forma do oráculo seja $\mathcal{R}_f = I - 2\,|x_0\rangle\,\langle x_0|$ como dado na Eq. (3.1.18), onde x_0 é o elemento marcado. Isso não é uma restrição, pois o oráculo deve distinguir de algum modo o elemento marcado e, para que outros oráculos possam ser usados, vamos admitir o uso de quaisquer operadores unitários U_a e U_b que transformam $\mathcal{R}_f$ em $U_a\mathcal{R}_f U_b$ durante a execução do algoritmo. Mais do que isso, U_a e U_b podem variar a cada passo. Sendo $|\psi_0\rangle$ o estado inicial, o estado do computador quântico após t passos é dado por

$$|\psi_t\rangle = U_t\mathcal{R}_f \cdots U_1\mathcal{R}_f\,|\psi_0\rangle\,, \tag{3.2.31}$$

onde $U_1, \cdots, U_t$ são operadores unitários genéricos, que são aplicados a cada passo após o oráculo. Não há nenhuma restrição com relação a eficiência desses operadores.

A estratégia da prova é comparar o estado $|\psi_t\rangle$ com o estado

$$|\phi_t\rangle = U_t \cdots U_1\,|\psi_0\rangle\,, \tag{3.2.32}$$

isto é, o estado equivalente sem a aplicação dos oráculos. Para fazer essa comparação, vamos definir a quantidade

$$D_t = \sum_{x_0=0}^{N-1} \big\|\,|\psi_t\rangle - |\phi_t\rangle\,\big\|^2, \tag{3.2.33}$$

que mede o desvio entre $|\psi_t\rangle$ e $|\phi_t\rangle$ após t passos. O somatório em x_0 é para fazer uma média sobre todos os valores possíveis de x_0 para não privilegiar nenhum valor especial. Note que $|\psi_t\rangle$ depende de x_0 e, em princípio, $|\phi_t\rangle$ não depende. Se D_t for muito pequeno após t passos, não conseguiremos distinguir o elemento marcado.

Vamos mostrar que valem as seguintes desigualdades

$$c\,N \leq D_t \leq 4\,t^2, \tag{3.2.34}$$

onde c é uma constante estritamente positiva. A partir desse resultado podemos concluir que se tomarmos o número de passos t com uma dependência

funcional em N menor que $\Omega\big(\sqrt{N}\big)$, por exemplo $N^{\frac{1}{4}}$, a primeira desigualdade será violada. Isso quer dizer que D_t não é grande o suficiente para que possamos distinguir o elemento marcado. No limite assintótico, a violação da desigualdade fica mais dramática mostrando que, para esse número de passos, uma sequência de operadores que distingue o elemento marcado é equivalente a uma sequência que não distingue.

Vamos começar pela desigualdade $D_t \leq 4\,t^2$. Essa desigualdade é válida para $t = 0$. Usando o método de prova por indução, supomos que ela é válida para t e mostraremos que ela será válida para $t+1$. Note que

$$\begin{aligned} D_{t+1} &= \sum_{x_0=0}^{N-1} \big\| U_{t+1}\mathcal{R}_f\,|\psi_t\rangle - U_{t+1}\,|\phi_t\rangle\,\big\|^2 \\ &= \sum_{x_0=0}^{N-1} \big\| \mathcal{R}_f\,|\psi_t\rangle - |\phi_t\rangle\,\big\|^2 \\ &= \sum_{x_0=0}^{N-1} \big\| \mathcal{R}_f(|\psi_t\rangle - |\phi_t\rangle) + (R_f - I)\,|\phi_t\rangle\,\big\|^2. \end{aligned} \tag{3.2.35}$$

Usando o quadrado da *desigualdade triangular*

$$\big\|\,|\alpha\rangle + |\beta\rangle\,\big\|^2 \leq \big\|\,|\alpha\rangle\,\big\|^2 + 2\,\|\,|\alpha\rangle\,\|\,\|\,|\beta\rangle\,\| + \big\|\,|\beta\rangle\,\big\|^2 \tag{3.2.36}$$

onde

$$|\alpha\rangle = \mathcal{R}_f(|\psi_t\rangle - |\phi_t\rangle)$$

e

$$\begin{aligned} |\beta\rangle &= (R_f - I)\,|\phi_t\rangle \\ &= -2\,\big\langle x_0\big|\phi_t\big\rangle\,|x_0\rangle\,, \end{aligned}$$

obtemos

$$\begin{aligned} D_{t+1} \leq \sum_{x_0=0}^{N-1} \Big(&\big\|\,|\psi_t\rangle - |\phi_t\rangle\,\big\|^2 + 4\,\big\|\,|\psi_t\rangle - |\phi_t\rangle\,\big\|\;\big|\big\langle x_0\big|\phi_t\big\rangle\big| + \\ &4\,\big|\big\langle x_0\big|\phi_t\big\rangle\big|^2\Big)\,. \end{aligned} \tag{3.2.37}$$

Usando a *desigualdade de Cauchy-Schwarz*

$$\big|\big\langle\alpha\big|\beta\big\rangle\big| \leq \|\,|\alpha\rangle\,\|\,\|\,|\beta\rangle\,\| \tag{3.2.38}$$

no segundo termo da desigualdade (3.2.37), onde

$$|\alpha\rangle = \sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |\phi_t\rangle \, \big\| \; |x_0\rangle$$

e

$$|\beta\rangle = \sum_{x_0=0}^{N-1} \big|\langle x_0|\phi_t\rangle\big| \; |x_0\rangle$$

e também usando o fato de que

$$\sum_{x_0=0}^{N-1} \big|\langle x_0|\phi_t\rangle\big|^2 = \langle \phi_t|\phi_t\rangle = 1,$$

obtemos

$$\begin{aligned} D_{t+1} &\leq D_t + 4 \left(\sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |\phi_t\rangle \, \big\|^2 \right)^{\frac{1}{2}} \left(\sum_{x_0'=0}^{N-1} \big|\langle x_0'|\phi_t\rangle\big|^2 \right)^{\frac{1}{2}} + 4 \\ &\leq D_t + 4\sqrt{D_t} + 4. \end{aligned} \tag{3.2.39}$$

Como estamos supondo que $D_t \leq 4\,t^2$ pela hipótese indutiva, obtemos $D_{t+1} \leq 4\,(t+1)^2$.

Vamos agora mostrar a desigualdade mais trabalhosa $c\,N \leq D_t$. Vamos definir duas novas quantidades dadas por

$$E_t = \sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |x_0\rangle \, \big\|^2, \tag{3.2.40}$$

$$F_t = \sum_{x_0=0}^{N-1} \big\| \, |\phi_t\rangle - |x_0\rangle \, \big\|^2. \tag{3.2.41}$$

Podemos obter uma desigualdade envolvendo D_t, E_t e F_t da seguinte forma:

$$\begin{aligned} D_t &= \sum_{x_0=0}^{N-1} \Big\| \, (|\psi_t\rangle - |x_0\rangle) + (|x_0\rangle - |\phi_t\rangle) \, \Big\|^2 \\ &\geq E_t + F_t - 2 \sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |x_0\rangle \, \big\| \, \big\| \, |\phi_t\rangle - |x_0\rangle \, \big\| \\ &\geq E_t + F_t - 2\sqrt{E_t\,F_t} \\ &= \left(\sqrt{F_t} - \sqrt{E_t} \right)^2, \end{aligned} \tag{3.2.42}$$

onde, na primeira desigualdade, usamos o quadrado da *desigualdade triangular reversa*

$$\big\| \, |\alpha\rangle + |\beta\rangle \, \big\|^2 \geq \big\| \, |\alpha\rangle \, \big\|^2 - 2 \, \| \, |\alpha\rangle \, \| \, \| \, |\beta\rangle \, \| + \big\| \, |\beta\rangle \, \big\|^2 \tag{3.2.43}$$

e, na segunda desigualdade, usamos Cauchy-Schwarz com os vetores

$$\begin{aligned} |\alpha\rangle &= \sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |x_0\rangle \, \big\| \;\; |x_0\rangle \, , \\ |\beta\rangle &= \sum_{x_0=0}^{N-1} \big\| \, |\phi_t\rangle - |x_0\rangle \, \big\| \;\; |x_0\rangle \, . \end{aligned}$$

Vamos agora mostrar que $F_t \geq 2N - 2\sqrt{N}$. Defina θ_{x_0} como sendo a fase de $\big\langle x_0 \big| \phi_t \big\rangle$, isto é,

$$\big\langle x_0 \big| \phi_t \big\rangle = \mathrm{e}^{i\theta_{x_0}} \, \big| \big\langle x_0 \big| \phi_t \big\rangle \big| \, .$$

Defina o estado

$$|\theta\rangle = \frac{1}{\sqrt{N}} \sum_{x_0=0}^{N-1} \mathrm{e}^{i\theta_{x_0}} \, |x_0\rangle \, . \tag{3.2.44}$$

Então,

$$\begin{aligned} \big\langle \theta \big| \phi_t \big\rangle &= \frac{1}{\sqrt{N}} \sum_{x_0=0}^{N-1} \mathrm{e}^{-i\theta_{x_0}} \, \big\langle x_0 \big| \phi_t \big\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{x_0=0}^{N-1} \big| \big\langle x_0 \big| \phi_t \big\rangle \big| \, . \end{aligned} \tag{3.2.45}$$

Pela desigualdade de Cauchy-Schwarz, obtemos $\big| \big\langle \theta \big| \phi_t \big\rangle \big| \leq 1$, portanto,

$$\sum_{x_0=0}^{N-1} \big| \big\langle x_0 \big| \phi_t \big\rangle \big| \leq \sqrt{N}. \tag{3.2.46}$$

Para obter o resultado desejado, vamos usar a desigualdade acima e o fato

de que a a parte real de $\langle x_0|\phi_t\rangle$ é menor ou igual a $|\langle x_0|\phi_t\rangle|$

$$\begin{aligned} F_t &= \sum_{x_0=0}^{N-1} \big\| \, |\phi_t\rangle - |x_0\rangle \, \big\|^2 \\ &= 2\,N - 2\sum_{x_0=0}^{N-1} \mathrm{Re}\left\{\langle x_0|\phi_t\rangle\right\} \\ &\geq 2\,N - 2\sum_{x_0=0}^{N-1} |\langle x_0|\phi_t\rangle| \\ &\geq 2\,N - 2\sqrt{N}. \end{aligned} \tag{3.2.47}$$

Vamos agora mostrar que $E_t \leq (2-\sqrt{2})N$. Após t passos, o estado do computador quântico com a aplicação dos oráculos é $|\psi_t\rangle$. Vamos supor que a probabilidade de uma medida retornar o valor x_0 seja maior ou igual a $1/2$, isto é, $|\langle x_0|\psi_t\rangle|^2 \geq 1/2$ para todo x_0. O valor $1/2$ é arbitrário. De fato, podemos escolher qualquer valor fixo entre 0 e 1, como mostra o Execício 3.8. Usando um desenvolvimento similar ao usado para F_t, temos

$$\begin{aligned} E_t &= \sum_{x_0=0}^{N-1} \big\| \, |\psi_t\rangle - |x_0\rangle \, \big\|^2 \\ &\geq 2\,N - 2\sum_{x_0=0}^{N-1} |\langle x_0|\psi_t\rangle| \\ &\geq 2\,N - 2\sum_{x_0=0}^{N-1} \frac{1}{\sqrt{2}} \\ &= (2-\sqrt{2})N. \end{aligned} \tag{3.2.48}$$

Usando $E_t \leq (2-\sqrt{2})N$ e $F_t \geq 2N - 2\sqrt{N}$ obtemos

$$\begin{aligned} D_t &\geq \left(\sqrt{F_t} - \sqrt{E_t}\right)^2 \\ &\geq \left(\sqrt{2N - 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N}\right)^2 \\ &= \left(\sqrt{2} - \sqrt{2-\sqrt{2}}\right)^2 N + O(\sqrt{N}). \end{aligned} \tag{3.2.49}$$

Completando a prova da desigualdade $c\,N \leq D_t$ para N suficientemente

grande. A constante c deve obedecer a

$$0 < c < \left(\sqrt{2} - \sqrt{2 - \sqrt{2}}\right)^2 .$$

Podemos concluir que um algoritmo que tenha condições de achar o elemento marcado deve satisfazer às desigualdades (3.2.34). Portanto $cN \leq 4t^2$ ou equivalentemente $t = \Omega\big(\sqrt{N}\big)$. Este resultado implica que o algoritmo de Grover acha o elemento marcado com a complexidade de número de consultas dado por $\Theta(\sqrt{N})$.

Exercício 3.8. *Mostre que se a probabilidade de uma medida retornar o valor x_0 for maior ou igual a p, o valor da constante c deve satisfazer a*

$$0 < c < \left(\sqrt{2} - \sqrt{2 - 2\sqrt{p}}\right)^2 .$$

Para que o algoritmo tenha uma probabilidade de sucesso próxima de 1, ele deve ser rodado $1/p$ vezes. Como p é constante, isto não altera o custo total de $\Omega\big(\sqrt{N}\big)$.

3.3 Busca com Elementos Repetidos

Na Sec. 3.1 descrevemos o algoritmo de Grover que resolve o seguinte problema: dada uma função booleana f, cujo domínio é $\big\{0, \cdots, N-1\big\}$ onde $N = 2^n$ para algum inteiro positivo n, ache o elemento x_0 tal que que $f(x_0) = 1$ assumindo que x_0 é o único ponto do domínio de f com imagem igual a 1. Nesta seção, vamos atacar um problema mais geral. Vamos supor que a função f é uma função booleana como antes, porém m pontos do domínio têm imagens iguais a 1. Se $m = 1$, recaímos no caso anterior. Suponha que M seja o conjunto dos pontos cujas imagens são iguais a 1. O problema consiste em achar um elemento de M com o menor número de consultas a f. Se compararmos esse problema com busca em banco de dados, temos um caso de banco de dados com elementos repetidos. Podemos colocar esse problema de forma concreta, como fizemos no início da Sec. 3.1. Pedimos a um programador quântico para escolher m pontos no domínio de f sem nos passar qualquer informação sobre quais foram os pontos escolhidos. Sabemos o valor de m, mas não sabemos quais foram os pontos. Por exemplo, se ele escolher os pontos 5 e 6, ele usará duas portas Toffoli generalizadas, como no circuito da Fig. 3.4. Note que o estado do segundo registrador mudará de $|0\rangle$ para $|1\rangle$ somente se a entrada do primeiro registrador for 5 ou 6, do contrário permanecerá no estado $|0\rangle$.

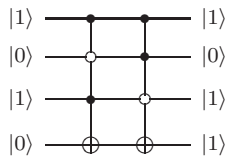

Figura 3.4: Circuito que implementa o caso $f(5) = 1$ e $f(6) = 1$. Apenas o programador quântico sabe onde estão os controles pretos e brancos. No entanto, temos conhecimento de quantas portas Toffoli foram usadas, que é dado por m.

O algoritmo quântico ótimo que resolve esse problema é uma extensão direta do algoritmo de Grover. Como antes, usamos 2 registradores com o total de $n + 1$ qubits. A forma do operador $\mathcal{R}_f$ é igual ao da Eq. (3.1.2), porém ele retorna m valores iguais a 1 no segundo registrador enquanto que o operador anterior retornava um único valor. O operador $\mathcal{R}_{\mathrm{D}}$ é exatamente o mesmo da Eq. (3.1.4), cada passo da evolução é feito aplicando $U = \mathcal{R}_{\mathrm{D}}\,\mathcal{R}_f$ e a condição inicial é dada pela Eq. (3.1.6) como no algoritmo de Grover. O número de vezes que o operador U é aplicado muda para $\left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{m}} \right\rfloor$. O algoritmo termina quando medimos o primeiro registrador na base computacional e o resultado é um elemento de M com probabilidade maior ou igual a $1 - \frac{m}{N}$.

3.3.1 Análise através de Operadores de Reflexão

A análise do algoritmo pode ser feita da seguinte forma: considere um subespaço de dimensão m gerado pelos vetores $|x\rangle$, $x \in M$. O estado

$$|M\rangle = \frac{1}{\sqrt{m}} \sum_{x \in M} |x\rangle \tag{3.3.50}$$

pertence a esse espaço. Ele substitui o vetor $|x_0\rangle$ quando o número de elementos marcados é maior que 1. Defina o vetor ortogonal $\left|M^{\perp}\right\rangle$ como

$$\left|M^{\perp}\right\rangle = \frac{1}{\sqrt{n-m}} \sum_{x \notin M} |x\rangle\,. \tag{3.3.51}$$

Todo o algoritmo se passa no espaço vetorial bidimensional gerado por $|M\rangle$ e $\left|M^{\perp}\right\rangle$. No espaço de Hilbert $\mathcal{H}^N$ do primeiro registrador, o operador $\mathcal{R}_f$

tem uma expressão similar a expressão dada pela Eq. (3.1.11), isto é

$$\mathcal{R}_{M^\perp} = 2\left|M^\perp\right\rangle\left\langle M^\perp\right| - I_N. \tag{3.3.52}$$

A mesma interpretação geométrica usada no algoritmo de Grover se aplica agora, porém o ângulo entre $\left|M^\perp\right\rangle$ e $|\mathrm{D}\rangle$ é

$$\begin{aligned}\frac{\theta}{2} &= \arcsin\left(\left\langle M|\mathrm{D}\right\rangle\right) \\ &= \sqrt{\frac{m}{N}} + O\left(\frac{1}{N}\right),\end{aligned} \tag{3.3.53}$$

no caso em que $N \gg m$. Esse resultado explica porque o número de passos do algoritmo é $t_f = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{m}} \right\rfloor$. A probabilidade de acerto pode ser calculada da mesma forma que antes

$$\begin{aligned}p_M &\geq \cos^2\left(\frac{\theta}{2}\right) \\ &= 1 - \frac{m}{N}.\end{aligned} \tag{3.3.54}$$

Exercício 3.9. *Mostre que a generalização do Execício 3.2 quando f tem M elementos marcados é*

$$U^t\left|D\right\rangle = \sin\left(t\,\theta + \frac{\theta}{2}\right)|M\rangle + \cos\left(t\,\theta + \frac{\theta}{2}\right)\left|M^\perp\right\rangle,$$

onde θ é dado pela Eq. (3.3.53). A partir desta expressão, ache o melhor ponto de parada t_f do algoritmo e mostre que a probabilidade de acerto p_M satisfaz à Eq. (3.3.54).

3.3.2 Análise através da Decomposição Espectral

A generalização da decomposição espectral quando há mais de 1 elemento marcado é direta. O polinômio característico de U passa a ser

$$\left|\lambda I - U\right| = (\lambda+1)^{N-m-1}(\lambda-1)^{m-1}\left(\lambda^2 - 2\left(1 - \frac{2m}{N}\right)\lambda + 1\right), \tag{3.3.55}$$

Portanto, os autovalores passam a ser ± 1 e $\mathrm{e}^{\pm i\omega}$ onde

$$\cos\omega = 1 - \frac{2m}{N}. \tag{3.3.56}$$

A estrutura geral da análise feita para um elemento marcado se mantém quando m é maior que 1. A condição inicial está no espaço vetorial gerado pelos autovetores associados aos autovalores $\mathrm{e}^{\pm i\omega}$. O número de iterações do algoritmo é $\lfloor \pi/2\omega \rfloor$. Como a expressão de ω é dada agora pela Eq. (3.3.56), o número de iterações passa a ser

$$\begin{aligned} t_f &= \left\lfloor \frac{\pi}{2\arccos\left(1-\frac{2m}{N}\right)} \right\rfloor \\ &= \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{m}} \right\rfloor + O\left(\frac{1}{\sqrt{N}}\right) \end{aligned} \tag{3.3.57}$$

quando $N \gg m$.

Os detalhes da análise e o cálculo de um limite inferior da probabilidade de acerto estão orientados nos exercícios a seguir.

Exercício 3.10. *Mostre a Eq. (3.3.55).*

Exercício 3.11. *Mostre que os autovetores de U associados aos autovalores $e^{\pm i\omega}$ são*

$$\frac{\left|M^{\perp}\right\rangle \mp i\left|M\right\rangle}{\sqrt{2}},$$

onde $|M\rangle$ e $\left|M^{\perp}\right\rangle$ estão definidos pelas Eqs. (3.3.50) e (3.3.51) respectivamente. Mostre que a condição inicial $|D\rangle$ está no espaço gerado por esses autovetores.

Exercício 3.12. *Mostre que $U^t\left|D\right\rangle$ é ortogonal a $|D\rangle$ para $t = \frac{\pi}{2\omega}$.*

Sugestões para Leitura

O algoritmo de Grover original está descrito na Ref. [23]. As Refs. [24, 22] também são influentes. A extensão do algoritmo para busca em banco de dados com elementos repetidos e uma primeira versão do algoritmo de contagem estão descritos na Ref. [12]. A versão do algoritmo de contagem usando estimativa de fase está descrita na Ref. [46]. A interpretação geométrica do algoritmo de Grover está descrita na Ref. [2]. Sua análise usando decomposição espectral é abordada na Ref. [46] e sua ligação com o *algoritmo de busca abstrato* está descrito sucintamente na Ref. [7]. A prova de *otimalidade* do algoritmo de Grover está na Ref. [10]. Uma versão mais legível está na Ref. [12] e seguimos de perto a prova apresentada na Ref. [49]. A Ref. [64] apresenta uma prova mais detalhada. A Ref. [53] pode ser usada como uma introdução ao algoritmo de Grover. As Refs. [30, 13] descrevem a técnica de *amplificação de amplitudes* em detalhes.

Capítulo 4

Passeios Quânticos em Grafos

Neste capítulo, apresentamos em detalhes o cálculo do estado do passeio quântico para dois grafos importantes: reta e hipercubo. O passeio sobre a reta foi introduzido na Sec. 2.2 com o objetivo de apresentar algumas características dos passeios quânticos, que são nitidamente diferentes dos passeios aleatórios clássicos. O hipercubo é um grafo finito com propriedades muito interessantes. O passeio quântico nesse grafo tem um papel de destaque na área. Nesses dois casos é possível obter resultados analíticos contrario à regra a geral.

4.1 Reta

Suponha que a parte espacial para o deslocamento do passeio quântico sejam os pontos nas posições inteiras de uma reta. A parte espacial está associada a um espaço de Hilbert $\mathcal{H}_P$ de dimensão infinita cuja base computacional é $\left\{ |n\rangle \, : \, n \in \mathbb{Z} \right\}$. O espaço da moeda tem dimensão 2 e sua base computacional é $\left\{ |0\rangle , |1\rangle \right\}$ correspondendo aos dois possíveis sentidos de movimento, para direita ou para esquerda. Assim, o espaço de Hilbert associado ao passeio quântico é $\mathcal{H}^2 \otimes \mathcal{H}_P$, cuja base computacional é $\big\{ |s, n\rangle$, $0 \leq s \leq 1$, $-\infty \leq n \leq \infty \big\}$, onde tomamos $s = 0$ correspondendo ao sentido para direita e $s = 1$ para esquerda. Dentro dessas convenções, o operador de deslocamento é

$$S = \sum_{s=0}^{1} \sum_{n=-\infty}^{\infty} |s, n + (-1)^s\rangle \langle s, n| \, . \tag{4.1.1}$$

Se $s = 0$, o valor de n será incrementado de uma unidade após uma aplicação de S, enquanto que se $s = 1$, n será decrementado de uma unidade. Essa expressão para S é igual a expressão da Eq. (2.2.13) da Sec. 2.2. Basta expandir o somatório em s para verificar esse fato.

O estado genérico do caminhante no instante de tempo t é descrito por

$$|\Psi(t)\rangle = \sum_{s=0}^{1} \sum_{n=-\infty}^{\infty} \psi_{s,n}(t) \, |s, n\rangle \, , \tag{4.1.2}$$

onde os coeficientes $\psi_{s,n}(t)$ são funções complexas, que obedecem à condição de normalização

$$\sum_{s=0}^{1} \sum_{n=-\infty}^{\infty} |\psi_{s,n}(t)|^2 = 1, \tag{4.1.3}$$

para todo instante t.

Vamos usar como moeda o operador de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{4.1.4}$$

Aplicando o operador de evolução

$$U = S \, (H \otimes I) \tag{4.1.5}$$

no estado genérico, obtemos

$$\begin{aligned} |\Psi(t+1)\rangle &= \sum_{n=-\infty}^{\infty} S \left(\psi_{0,n}(t) H \, |0\rangle \, |n\rangle + \psi_{1,n}(t) H \, |1\rangle \, |n\rangle \right) \\ &= \sum_{n=-\infty}^{\infty} \frac{\psi_{0,n}(t) + \psi_{1,n}(t)}{\sqrt{2}} S \, |0\rangle \, |n\rangle + \frac{\psi_{0,n}(t) - \psi_{1,n}(t)}{\sqrt{2}} S \, |1\rangle \, |n\rangle \\ &= \sum_{n=-\infty}^{\infty} \frac{\psi_{0,n}(t) + \psi_{1,n}(t)}{\sqrt{2}} \, |0\rangle \, |n+1\rangle + \\ &\qquad \frac{\psi_{0,n}(t) - \psi_{1,n}(t)}{\sqrt{2}} \, |1\rangle \, |n-1\rangle \, . \end{aligned}$$

Usando a Eq. (4.1.2) no lado esquerdo da equação acima, isto é, expandindo o lado esquerdo na base computacional, e igualando aos coeficientes correspondentes do lado direito, obtemos as equações de evolução do caminhante

$$\psi_{0,n}(t+1) = \frac{\psi_{0,n-1}(t) + \psi_{1,n-1}(t)}{\sqrt{2}}, \tag{4.1.6}$$

$$\psi_{1,n}(t+1) = \frac{\psi_{0,n+1}(t) - \psi_{1,n+1}(t)}{\sqrt{2}}. \tag{4.1.7}$$

Estas equações foram usadas na Sec. 2.2 para gerar os gráficos das distribuições de probabilidades através de simulação numérica. A distribuição de probabilidade é dada por

$$p_n(t) = |\psi_{0,n}(t)|^2 + |\psi_{1,n}(t)|^2 . \tag{4.1.8}$$

Nosso objetivo é calcular a distribuição de probabilidades analiticamente. No entanto, as Eqs. (4.1.6) e (4.1.7) não são fáceis de serem resolvidas do jeito que estão. Felizmente, nesse caso, há uma forma alternativa de atacar o problema. Existe uma base especial, chamada *base de Fourier*, que diagonaliza o operador de deslocamento. Isso vai facilitar a *diagonalização* do operador de evolução. Essa nova base pode ser encontrada aplicando a transformada de Fourier na base computacional da parte espacial do espaço de Hilbert.

A *transformada de Fourier* de uma função discreta $f : \mathbb{Z} \to \mathbb{C}$ é uma função contínua $\widetilde{f} : [-\pi, \pi] \to \mathbb{C}$ definida por

$$\widetilde{f}(k) = \sum_{n=-\infty}^{\infty} \mathrm{e}^{-ink} f(n), \tag{4.1.9}$$

onde $i = \sqrt{-1}$. A transformada inversa é dada por

$$f(n) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \mathrm{e}^{ink} \widetilde{f}(k)\ \mathrm{d}k. \tag{4.1.10}$$

Esse é um caso particular de um classe mais geral de transformadas de Fourier que se aplica diretamente ao nosso contexto. Observe que se n tivesse unidade (por exemplo metro), k deveria ter a unidade inversa, pois o produto nk está no expoente da função exponencial e, portanto, deve ser adimensional. A interpretação física da variável k é o *número de onda*.

Na Eq. (4.1.2), os coeficientes $\psi_{s,n}(t)$ são funções discretas na variável n. Podemos calcular a transformada de Fourier de $\psi_{s,n}(t)$ com relação ao índice n da seguinte forma:

$$\widetilde{\psi}_s(k,t) = \sum_{n=-\infty}^{\infty} \mathrm{e}^{-ink} \psi_{s,n}(t), \tag{4.1.11}$$

onde k é uma variável contínua definida no intervalo $[-\pi, \pi]$. O objetivo agora é obter a equação de evolução para $\widetilde{\psi}_s(k,t)$. Se conseguirmos resolver essa nova equação, poderemos obter $\psi_{s,n}(t)$ através da transformada inversa.

Existe outra forma de usar a transformada de Fourier. Em vez de transformar a função $f : \mathbb{Z} \to \mathbb{C}$, vamos transformar a base computacional de

$\mathcal{H}_{\mathcal{P}}$. Para que esse processo funcione adequadamente, vamos usar a fórmula

$$|\kappa_k\rangle = \sum_{n=-\infty}^{\infty} \mathrm{e}^{ink} |n\rangle , \tag{4.1.12}$$

para definir os vetores $|\kappa_k\rangle$, onde k é uma variável contínua definida no intervalo $[-\pi, \pi]$. Note que estamos usando o sinal positivo dentro da exponencial. O problema desse método é que $|\kappa_k\rangle$ tem norma infinita. Isto pode ser resolvido redefinindo $|\kappa_k\rangle$ da seguinte maneira

$$|\kappa_k\rangle = \lim_{L\to\infty} \frac{1}{\sqrt{2L+1}} \sum_{n=-L}^{L} \mathrm{e}^{ink} |n\rangle . \tag{4.1.13}$$

A mesma modificação deve ser aplicada na Eq. (4.1.11) por questão de consistência. Como a constante de normalização não será relevante, vamos continuar usando a Eq. (4.1.12) como definição de $|\kappa_k\rangle$ e a Eq. (4.1.11) como definição de $\widetilde{\psi}_s(k,t)$ para simplificar as contas. Essa transformada define uma nova base ortonormal $\Big\{ |\kappa_k\rangle : -\pi \leq k \leq \pi \Big\}$. Nessa base podemos expressar o estado do passeio quântico como

$$|\Psi(t)\rangle = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \sum_{s=0}^{1} \widetilde{\psi}_s(k,t)\ |s\rangle\, |\kappa_k\rangle . \tag{4.1.14}$$

As Eqs. (4.1.2) e (4.1.14) são equivalentes. A primeira decompõe $|\psi(t)\rangle$ na base computacional e a segunda na base $|s\rangle\,|\kappa_k\rangle$. Os coeficientes da primeira são $\psi_{s,n}(t)$ e os da segunda são $\widetilde{\psi}_s(k,t)$.

Vamos calcular a ação do operador de deslocamento na nova base, isto é, sua ação em $|s\rangle\,|\kappa_k\rangle$. Usando a Eq. (4.1.12) e a definição de S temos que

$$\begin{aligned} S\,|s\rangle\,|\kappa_k\rangle &= \sum_{n=-\infty}^{\infty} \mathrm{e}^{ink} S\,|s,n\rangle \\ &= \sum_{n=-\infty}^{\infty} \mathrm{e}^{ink}\,|s\rangle\,|n+(-1)^s\rangle . \end{aligned}$$

Renomeando o índice mudo n da forma $n' = n + (-1)^s$ obtemos

$$\begin{aligned} S\,|s\rangle\,|\kappa_k\rangle &= \sum_{n'=-\infty}^{\infty} \mathrm{e}^{i\,(n'-(-1)^s)\,k}\,|s\rangle\,|n'\rangle \\ &= \mathrm{e}^{-(-1)^s\,i\,k}\,|s\rangle\,|\kappa_k\rangle . \end{aligned} \tag{4.1.15}$$

O resultado mostra que o operador de deslocamento ao atuar em um estado da nova base muda apenas sua fase, ou seja, $|s\rangle\,|\kappa_k\rangle$ é um autovetor de S associado ao autovalor $\mathrm{e}^{-(-1)^s\,i\,k}$. A próxima tarefa é encontrar os autovetores do operador de evolução U. Se diagonalizarmos U, teremos condições de encontrar uma expressão analítica para o estado do passeio quântico em função do tempo.

Aplicando U no vetor $|s'\rangle\,|\kappa_k\rangle$ e usando a Eq. (4.1.15), temos

$$\begin{aligned} U\,|s'\rangle\,|\kappa_k\rangle &= S\left(\sum_{s=0}^{1} H_{s,s'}\,|s\rangle\,|\kappa_k\rangle\right) \\ &= \sum_{s=0}^{1} \mathrm{e}^{-(-1)^s\,i\,k} H_{s,s'}\,|s\rangle\,|\kappa_k\rangle\,. \end{aligned} \tag{4.1.16}$$

As componentes de U na nova base são

$$\langle s,\kappa_k|\,U\,|s',\kappa_{k'}\rangle = \mathrm{e}^{-(-1)^s\,i\,k} H_{s,s'}\,\delta_{k,k'}. \tag{4.1.17}$$

Para cada k, vamos definir o operador $\widetilde{H}_k$ cujas componentes são

$$\widetilde{H}_{s,s'} = \mathrm{e}^{-(-1)^s\,i\,k} H_{s,s'}. \tag{4.1.18}$$

No formato matricial temos

$$\begin{aligned} \widetilde{H}_k &= \begin{bmatrix} \mathrm{e}^{-i\,k} & 0 \\ 0 & \mathrm{e}^{i\,k} \end{bmatrix} \cdot H \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} \mathrm{e}^{-i\,k} & \mathrm{e}^{-i\,k} \\ \mathrm{e}^{i\,k} & -\mathrm{e}^{i\,k} \end{bmatrix} \end{aligned} \tag{4.1.19}$$

A Eq. (4.1.17) mostra uqe a parte não-diagonal do operador U está associada ao espaço da moeda. O objetivo agora é diagonalizar o operador $\widetilde{H}_k$. O produto tensorial de um autovetor de $\widetilde{H}_k$ com o vetor $|\kappa_k\rangle$ é um autovetor de U. Para verificar esse fato, note que a Eq. (4.1.16) pode ser escrita como

$$U\,|s\rangle\,|\kappa_k\rangle = \left(\widetilde{H}_k\,|s\rangle\,\right)|\kappa_k\rangle\,. \tag{4.1.20}$$

Toda ação do operador de deslocamento S foi absorvida em $\widetilde{H}_k$ quando U atua em $|\kappa_k\rangle$. Se $|\alpha_k\rangle$ for um autovetor de $\widetilde{H}_k$ com autovalor α_k, teremos

$$\begin{aligned} U\,|\alpha_k\rangle\,|\kappa_k\rangle &= \left(\widetilde{H}_k\,|\alpha_k\rangle\,\right)|\kappa_k\rangle \\ &= \alpha_k\,|\alpha_k\rangle\,|\kappa_k\rangle\,. \end{aligned} \tag{4.1.21}$$

Portanto, $|\alpha_k\rangle\,|\kappa_k\rangle$ é autovetor de U associado ao autovalor α_k. Esse resultado mostra que a diagonalização do operador de evolução se reduz à

diagonalização de $\widetilde{H}_k$. U está definido em um espaço vetorial de dimensão infinita, enquanto que $\widetilde{H}_k$ está definido em um espaço de dimensão 2.

O polinômio característico de $\widetilde{H}_k$ é

$$\lambda^2 + i\,\sqrt{2}\,\lambda \sin k - 1. \tag{4.1.22}$$

Os autovalores são

$$\alpha_k = \mathrm{e}^{-i\,\omega_k}, \tag{4.1.23}$$
$$\beta_k = \mathrm{e}^{i\,(\pi+\omega_k)}, \tag{4.1.24}$$

onde ω_k é um ângulo no intervalo $[-\pi/2, \pi/2]$, que satisfaz à equação

$$\sin\omega_k = \frac{1}{\sqrt{2}} \sin k. \tag{4.1.25}$$

Os autovetores normalizados são

$$|\alpha_k\rangle = \frac{1}{\sqrt{c^-}} \begin{pmatrix} \mathrm{e}^{-i\,k} \\ \sqrt{2}\,\mathrm{e}^{-i\,\omega_k} - \mathrm{e}^{-i\,k} \end{pmatrix}, \tag{4.1.26}$$

$$|\beta_k\rangle = \frac{1}{\sqrt{c^+}} \begin{pmatrix} \mathrm{e}^{-i\,k} \\ -\sqrt{2}\,\mathrm{e}^{i\,\omega_k} - \mathrm{e}^{-i\,k} \end{pmatrix}, \tag{4.1.27}$$

onde

$$c^{\pm} = 2\left(1 + \cos^2 k\right) \pm 2\,\cos k\,\sqrt{1 + \cos^2 k}. \tag{4.1.28}$$

A decomposição espectral de U é

$$U = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \left(\mathrm{e}^{-i\,\omega_k}\ |\alpha_k, \kappa_k\rangle\,\langle\alpha_k, \kappa_k| + \mathrm{e}^{i\,(\pi+\omega_k)}\ |\beta_k, \kappa_k\rangle\,\langle\beta_k, \kappa_k| \right). \tag{4.1.29}$$

A t-ésima potência de U é

$$U^t = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \left(\mathrm{e}^{-i\,\omega_k\,t}\ |\alpha_k, \kappa_k\rangle\,\langle\alpha_k, \kappa_k| + \mathrm{e}^{i\,(\pi+\omega_k)\,t}\ |\beta_k, \kappa_k\rangle\,\langle\beta_k, \kappa_k| \right). \tag{4.1.30}$$

Vamos tomar o estado inicial com a partícula localizada na origem e o valor da moeda com o spin para cima $|0\rangle$. Assim, a condição inicial na base computacional é

$$|\psi(0)\rangle = |0\rangle\,|0\rangle\,. \tag{4.1.31}$$

Usando a Eq. (4.1.30) obtemos

$$\begin{aligned} |\psi(t)\rangle &= U^t\,|\psi(0)\rangle \\ &= \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \left(\mathrm{e}^{-i\,\omega_k\,t}\ |\alpha_k, \kappa_k\rangle\,\langle\alpha_k, \kappa_k|0, 0\rangle + \right. \\ &\qquad \left. \mathrm{e}^{i\,(\pi+\omega_k)\,t}\ |\beta_k, \kappa_k\rangle\,\langle\beta_k, \kappa_k|0, 0\rangle \right). \end{aligned} \tag{4.1.32}$$

Usando as Eqs. (4.1.26), (4.1.27) e (4.1.12), obtemos

$$\langle \alpha_k, \kappa_k | 0, 0 \rangle = \frac{\mathrm{e}^{i\,k}}{\sqrt{c^-}}, \tag{4.1.33}$$

$$\langle \beta_k, \kappa_k | 0, 0 \rangle = \frac{\mathrm{e}^{i\,k}}{\sqrt{c^+}}. \tag{4.1.34}$$

Portanto,

$$|\psi(t)\rangle = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \left(\frac{\mathrm{e}^{-i\,(\omega_k t - k)}}{\sqrt{c^-}} |\alpha_k, \kappa_k\rangle + \frac{\mathrm{e}^{i\,(\pi+\omega_k)\,t + i\,k}}{\sqrt{c^+}} |\beta_k, \kappa_k\rangle \right). \tag{4.1.35}$$

O estado do passeio está escrito na base dos autovetores de U. É conveniente expressar o resultado na base computacional. Como um passo intermediário, vamos expressar os autovetores $|\alpha_k\rangle$ e $|\beta_k\rangle$ na base computacional através das Eqs. (4.1.26), (4.1.27) mantendo intacto os vetores $|\kappa_k\rangle$. Dessa forma podemos determinar os coeficientes $\widetilde{\psi}_s(k,t)$ da Eq. (4.1.14), que são dados por

$$\widetilde{\psi}_0(k,t) = \frac{1}{2}\left(1 + \frac{\cos k}{\sqrt{1+\cos^2 k}}\right) \mathrm{e}^{-i\,\omega_k t} + \frac{(-1)^t}{2}\left(1 - \frac{\cos k}{\sqrt{1+\cos^2 k}}\right) \mathrm{e}^{i\,\omega_k t}, \tag{4.1.36}$$

$$\widetilde{\psi}_1(k,t) = \frac{i\mathrm{e}^{ik}}{2\sqrt{1+\cos^2 k}} \left(\mathrm{e}^{-i\,\omega_k t} - (-1)^t \mathrm{e}^{i\,\omega_k t}\right). \tag{4.1.37}$$

Usando a Eq. (4.1.12), podemos calcular os coeficientes $\psi_{0,n}$ e $\psi_{1,n}$ da Eq. (4.1.2). Eles são dados por

$$\psi_{0,n}(t) = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \left(1 + \frac{\cos k}{\sqrt{1+\cos^2 k}}\right) \mathrm{e}^{-i\,(\omega_k t + kn)}, \tag{4.1.38}$$

$$\psi_{1,n}(t) = \int_{-\pi}^{\pi} \frac{\mathrm{d}k}{2\pi} \frac{\mathrm{e}^{ik}}{\sqrt{1+\cos^2 k}} \mathrm{e}^{-i\,(\omega_k t + kn)}. \tag{4.1.39}$$

Essas equações são válidas quando $n+t$ é par, caso contrário os coeficientes são iguais a zero.

4.2 Hipercubo

O hipercubo de dimensão n é um grafo regular de grau n com $N = 2^n$ vértices. Os rótulos dos vértices são n-tuplas binárias. Dois vértices são

adjacentes se e somente se as suas n-tuplas correspondentes diferem apenas em um bit, isto é, a distância de Hamming é igual a 1. As arestas também têm rótulos. O rótulo indica qual componente tem bits diferentes, ou seja, se dois vértices diferem em 1 bit na a-ésima componente, o rótulo da aresta que liga esses vértices é a. O passeio quântico tem associado o espaço de Hilbert $\mathcal{H} = \mathcal{H}^n \otimes \mathcal{H}^{2^n}$. Os vetores da forma $|a\rangle\,|\vec{v}\rangle$, onde $1 \leq a \leq n$ e $\vec{v}$ é uma n-tupla binária, formam a base computacional para $\mathcal{H}$. O vetor $|a\rangle$ representa uma aresta e indica o estado da moeda ou da direção do movimento e nesta seção, excepcionalmente usamos o vetor $|1\rangle$ representando o primeiro vetor da base computacional do espaço da moeda; o vetor $|\vec{v}\rangle$ é um vetor da base computacional de $\mathcal{H}^{2^n}$ e indica em qual vértice o caminhante está.

Exercício 4.1. *Faça um esboço de um hipercubo de dimensão $n = 3$ e rotule todos os vértices e todas as arestas.*

O operador de deslocamento deve levar o estado $|a\rangle\,|\vec{v}\rangle$ para $|a\rangle\,|\vec{v} \oplus \vec{e}_a\rangle$, onde $\vec{e}_a$ é a n-tupla binária que tem todas componentes iguais a zero exceto a a-ésima componente, cujo valor é 1, e a operação $\oplus$ é a soma binária bit-a-bit. Esse deslocamento tem o seguinte significado: se o valor da moeda for a e a posição do caminhante $\vec{v}$, ele vai se deslocar para o vértice adjacente ao vértice $\vec{v}$ através da aresta a. O valor da moeda após o deslocamento fica inalterado. Assim

$$S\,|a\rangle\,|\vec{v}\rangle = |a\rangle\,|\vec{v} \oplus \vec{e}_a\rangle\,. \tag{4.2.40}$$

Outra forma equivalente de escrever o operador de deslocamento é

$$S = \sum_{a=1}^{n} \sum_{\vec{v}=0}^{2^n-1} |a, \vec{v} \oplus \vec{e}_a\rangle\,\langle a, \vec{v}|\,. \tag{4.2.41}$$

O intervalo de variação da variável $\vec{v}$ no somatório está escrito na base decimal. Por exemplo, a notação $\vec{v} = 2^n - 1$ quer dizer $\vec{v} = (1, \cdots, 1)$. Usaremos esta notação se ficar claro pelo contexto o significado real dela.

Usaremos por diversas razões a moeda de Grover, isto é

$$G = 2\,|\mathrm{D}\rangle\,\langle \mathrm{D}| - I, \tag{4.2.42}$$

onde $|\mathrm{D}\rangle$ é o estado diagonal. Em termos matriciais temos

$$G = \begin{bmatrix} \frac{2}{n} - 1 & \frac{2}{n} & \cdots & \frac{2}{n} \\ \frac{2}{n} & \frac{2}{n} - 1 & \cdots & \frac{2}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{n} & \frac{2}{n} & \cdots & \frac{2}{n} - 1 \end{bmatrix}. \tag{4.2.43}$$

Ou seja, as componentes de G são $G_{ij} = \frac{2}{n} - \delta_{ij}$. A moeda de Grover é invariante por permutação de direções. Isto é, se os rótulos das arestas forem permutados em todos os vértices simultaneamente, a estrutura do hipercubo não se altera, porém, em princípio o operador moeda faria o caminhante seguir um caminho diferente. Seria equivalente a manter os rótulos como eram e a permutar as linha e colunas da matriz G correspondentes a permutação de rótulos. No entanto, a matriz de Grover fica inalterada por permutação simultânea de linhas e colunas.

Um estado genérico do caminhante no instante de tempo t é descrito por

$$|\Psi(t)\rangle = \sum_{a=1}^{n} \sum_{\vec{v}=0}^{2^n-1} \psi_{a,\vec{v}}(t)\, |a, \vec{v}\rangle\,, \tag{4.2.44}$$

onde o coeficiente $\psi_{a,\vec{v}}(t)$ é uma função complexa que obedece à condição de normalização

$$\sum_{a=1}^{n} \sum_{\vec{v}=0}^{2^n-1} |\psi_{a,\vec{v}}(t)|^2 = 1. \tag{4.2.45}$$

Aplicando o operador de evolução

$$U = S\ (G \otimes I) \tag{4.2.46}$$

no estado genérico, obtemos

$$\begin{aligned} |\Psi(t+1)\rangle &= \sum_{b=1}^{n} \sum_{\vec{v}=0}^{2^n-1} \psi_{b,\vec{v}}(t)\, S\Big(G\,|b\rangle\,|\vec{v}\rangle\Big) \\ &= \sum_{b=1}^{n} \sum_{\vec{v}=0}^{2^n-1} \psi_{b,\vec{v}}(t)\, S\Big(\sum_{a=1}^{n} G_{ab}\,|a\rangle\,|\vec{v}\rangle\Big) \\ &= \sum_{a,b=1}^{n} \sum_{\vec{v}=0}^{2^n-1} \psi_{b,\vec{v}}(t)\, G_{ab}\,|a\rangle\,|\vec{v} \oplus \vec{e}_a\rangle \end{aligned}$$

Podemos renomear o índice do somatório de $\vec{v}$ para $\vec{v} \oplus \vec{e}_a$ de forma que

$$|\Psi(t+1)\rangle = \sum_{a,b=1}^{n} \sum_{\vec{v}=0}^{2^n-1} G_{ab}\, \psi_{b,\vec{v}\oplus\vec{e}_a}(t)\ |a\rangle\,|\vec{v}\rangle\,. \tag{4.2.47}$$

Expandindo o lado esquerdo da equação acima na base computacional e igualando os coeficientes obtemos a equação de evolução do caminhante

$$\psi_{a,\vec{v}}(t+1) = \sum_{b=1}^{n} G_{ab}\, \psi_{b,\vec{v}\oplus\vec{e}_a}(t). \tag{4.2.48}$$

Essa equação é muito complexa para ser resolvida do jeito que está. No caso unidimensional, vimos que tomando a transformada de Fourier na parte espacial conseguimos diagonalizar o operador de deslocamento. Isso permitiu resolver analiticamente a equação de evolução. A mesma técnica funciona aqui.

O hipercubo é um grafo de Cayley do grupo $\mathbb{Z}_2^n$, portanto a transformada de Fourier atua na base computacional da seguinte forma:

$$\left|\beta_{\vec{k}}\right\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_{\vec{v}=0}^{2^n-1} (-1)^{\vec{k}\cdot\vec{v}} \left|\vec{v}\right\rangle, \tag{4.2.49}$$

onde $\vec{k}\cdot\vec{v}$ é o produto interno entre os vetores binários $\vec{k}$ e $\vec{v}$. O intervalo de variação da variável $\vec{k}$ é o mesmo da variável $\vec{v}$. Como antes, a transformada de Fourier define uma nova base ortonormal $\left\{\left|\beta_{\vec{k}}\right\rangle : 0 \leq \vec{k} \leq 2^n - 1\right\}$ chamada de base de Fourier. Nessa nova base, o estado genérico do caminhante é

$$\left|\Psi(t)\right\rangle = \sum_{a=1}^{n} \sum_{\vec{k}=0}^{2^n-1} \widetilde{\psi}_{a,\vec{k}}(t) \left|a\right\rangle \left|\beta_{\vec{k}}\right\rangle, \tag{4.2.50}$$

onde os coeficientes são dados por

$$\widetilde{\psi}_{a,\vec{k}} = \frac{1}{\sqrt{2^n}} \sum_{\vec{v}=0}^{2^n-1} (-1)^{\vec{k}\cdot\vec{v}} \psi_{a,\vec{v}}. \tag{4.2.51}$$

A interpretação dessa última equação é que as amplitudes de um estado na base de Fourier são a transformada de Fourier das amplitudes na base computacional.

Exercício 4.2. *Mostre as seguintes propriedades da transformada de Fourier:*

1. $\left|\beta_{\vec{0}}\right\rangle$ *é o estado diagonal do espaço de Hilbert* $\mathcal{H}^{2^n}$.
2. $\left\{\left|\beta_{\vec{k}}\right\rangle : 0 \leq \vec{k} \leq 2^n - 1\right\}$ *é uma base ortonormal para o espaço de Hilbert* $\mathcal{H}^{2^n}$.
3. $\left|\vec{0}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{k}=0}^{2^n-1} \left|\beta_{\vec{k}}\right\rangle$.

Vamos mostrar que o operador de deslocamento é diagonal na base $\left\{\left|a\right\rangle \left|\beta_{\vec{k}}\right\rangle : 1 \leq a \leq n,\ 0 \leq \vec{k} \leq 2^n - 1\right\}$, ou seja, vamos mostrar que

$|a\rangle \left|\beta_{\vec{k}}\right\rangle$ é um autovetor de S. De fato, usando a Eq. (4.2.49) temos

$$\begin{aligned} S\,|a\rangle \left|\beta_{\vec{k}}\right\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\vec{v}=0}^{2^n-1} (-1)^{\vec{k}\cdot\vec{v}}\, S\,|a,\vec{v}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{\vec{v}=0}^{2^n-1} (-1)^{\vec{k}\cdot\vec{v}}\ |a,\vec{v}\oplus\vec{e}_a\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{\vec{v}=0}^{2^n-1} (-1)^{\vec{k}\cdot(\vec{v}\oplus\vec{e}_a)}\ |a,\vec{v}\rangle \\ &= (-1)^{\vec{k}\cdot\vec{e}_a}\,|a\rangle \left|\beta_{\vec{k}}\right\rangle . \end{aligned} \tag{4.2.52}$$

O produto interno $\vec{k}\cdot\vec{e}_a$ é a a-ésima componente de $\vec{k}$, que denotamos por k_a. Portanto $(-1)^{k_a}$ é o autovalor associado ao autovetor $|a\rangle \left|\beta_{\vec{k}}\right\rangle$.

Mostramos que o operador S é diagonal na nova base, porém isso não implica que o operador de evolução seja diagonal. Uma vez que o operador moeda não é diagonal, o operador de evolução também não o será. No entanto, desejamos diagonalizar o operador de evolução para calcular o estado do passeio quântico no instante t de forma explícita. Apesar de ser uma tarefa árdua, vamos obter expressões explícitas para os autovalores e autovetores de U.

Aplicando U no vetor $|b\rangle \left|\beta_{\vec{k}}\right\rangle$ e usando a Eq. (4.2.52) temos

$$\begin{aligned} U\,|b\rangle \left|\beta_{\vec{k}}\right\rangle &= S\left(\sum_{a=1}^{n} G_{ab}\ |a\rangle \left|\beta_{\vec{k}}\right\rangle\right) \\ &= \sum_{a=1}^{n} (-1)^{k_a} G_{ab}\ |a\rangle \left|\beta_{\vec{k}}\right\rangle \end{aligned} \tag{4.2.53}$$

As componentes de U na base de Fourier espacial são

$$\left\langle a,\beta_{\vec{k}'}\right| U \left|b,\beta_{\vec{k}}\right\rangle = (-1)^{k_a} G_{ab}\,\delta_{\vec{k},\vec{k}'}. \tag{4.2.54}$$

Vamos definir o operador $\widetilde{G}$ cujas componentes são $\widetilde{G}_{ab} = (-1)^{k_a} G_{ab}$ para um vetor $\vec{k}$ genérico.

O objetivo agora é diagonalizar o operador $\widetilde{G}$. Vamos começar com o caso mais simples que é $\vec{k} = \vec{0}$, ou seja, $\vec{k} = (0,\cdots,0)$. Nesse caso $\widetilde{G}$ se reduz ao operador de Grover G. Primeiramente, note que $G^2 = I$, portanto os autovalores são ± 1. Sabemos que $|\mathrm{D}\rangle$ é um autovetor de G associado ao autovalor 1. Vamos nos concentrar agora nos autovetores associados ao autovalor -1. Devemos achar vetores $|\alpha\rangle$ tais que $(G+I)\,|\alpha\rangle = 0$. Usando

a Eq. (4.2.42) vemos que $G+I$ é a matrix com todas a componentes iguais a $2/n$. Segue que qualquer vetor da forma

$$\left|\alpha_a^{\vec{0}}\right\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle - |a\rangle\right) \tag{4.2.55}$$

com $1 < a \leq n$ é um autovetor de G associado ao autovalor -1. Por um argumento de dimensionalidade, segue que o conjunto $\left\{\left|\alpha_a^{\vec{0}}\right\rangle : 1 \leq a \leq n\right\}$ onde $\left|\alpha_1^{\vec{0}}\right\rangle = |\mathrm{D}\rangle$ é uma base não-ortogonal de autovetores de G para o espaço $\mathcal{H}^n$. A partir desse resultado, podemos fazer a decomposição espectral quando $\vec{k} = (1, \cdots, 1)$. Nesse caso $\widetilde{G} = -G$, consequentemente, os autovetores de G associados ao autovalor -1 são autovetores $\widetilde{G}$ associados ao autovalor $+1$ e vice-versa. Em resumo, os autovetores

$$\left|\alpha_a^{\vec{1}}\right\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle - |n\rangle\right) \tag{4.2.56}$$

onde $1 \leq a \leq n-1$ estão associados ao autovalor $+1$ e $\left|\alpha_n^{\vec{1}}\right\rangle = |\mathrm{D}\rangle$ está associado ao autovalor -1.

Agora vamos tomar um vetor $\vec{k}$ com peso de Hamming $0 < k < n$, isto é, com k componentes iguais a 1 e $n-k$ iguais a 0. A matriz $\widetilde{G}$ é obtida a partir de G trocando o sinal das linhas correspondentes às componentes de $\vec{k}$ que são iguais a 1. Portanto, k linhas de $\widetilde{G}$ trocaram de sinal em relação a G. Para encontrar os autovetores associados aos autovalores ± 1, podemos ver o espaço de Hilbert como uma soma de dois espaços vetoriais, o primeiro associado às linhas que não trocaram de sinal e o segundo associado às linhas que trocaram de sinal. Por permutação das linhas e colunas, a matriz $\widetilde{G}$ assume a seguinte forma:

$$\widetilde{G} = \left[\begin{array}{ccc|ccc} \frac{2}{n}-1 & \frac{2}{n} & \cdots & & & \\ \frac{2}{n} & \frac{2}{n}-1 & & & \frac{2}{n} & \\ \vdots & & \ddots & & & \\ \hline & & & -\frac{2}{n}+1 & -\frac{2}{n} & \cdots \\ & -\frac{2}{n} & & -\frac{2}{n} & -\frac{2}{n}+1 & \\ & & & \vdots & & \ddots \end{array}\right], \tag{4.2.57}$$

onde o primeiro bloco na diagonal é uma matriz quadrada com dimensão $n-k$ e o segundo bloco tem de dimensão k. Para achar os autovalores

associados ao autovalor 1 devemos achar vetores $|\alpha\rangle$ tais que $(\widetilde{G}-I)\,|\alpha\rangle = 0$. Note que

$$\widetilde{G}-I = \left[\begin{array}{ccc|ccc} \frac{2}{n}-2 & \frac{2}{n} & \cdots & & & \\ \frac{2}{n} & \frac{2}{n}-2 & & & \frac{2}{n} & \\ \vdots & & \ddots & & & \\ \hline & & & -\frac{2}{n} & -\frac{2}{n} & \cdots \\ & -\frac{2}{n} & & -\frac{2}{n} & -\frac{2}{n} & \\ & & & \vdots & & \ddots \end{array}\right]. \tag{4.2.58}$$

Portanto, um vetor da forma $|\alpha\rangle = (0,\cdots,0\,|\,1,-1,0,\cdots,0)/\sqrt{2}$ com as componentes nulas, exceto em duas posições correspondentes às linhas que trocaram de sinal, uma com valor $+1$ e a outra -1, é um autovetor de autovalor 1. Podemos construir $k-1$ vetores desta forma. Seguindo um raciocínio análogo para os autovetores associados aos autovalores -1, concluímos que podemos construir $n-k-1$ autovetores com as componentes nulas exceto em duas posições correspondentes às linhas que não trocaram de sinal, cujos valores são novamente $+1$ e -1. O total parcial de autovetores encontrados até agora é $(k-1)+(n-k-1) = n-2$. Portanto, faltam 2 autovetores associados a autovalores complexos não-reais.

Os dois autovetores restantes podem ser encontrados da seguinte forma: se uma matriz tiver a propriedade de que a soma das componentes de uma linha é invariante para todas as linhas, o vetor com componentes iguais a 1 será um autovetor, como na matriz G. No caso da matriz $\widetilde{G}$, essa propriedade vale em 2 blocos de linhas. O primeiro bloco consiste nas primeiras $n-k$ linhas e o segundo bloco nas k linhas restantes. Portanto, a forma do autovetor deve ser $|\alpha\rangle = (a,\cdots,a\,|\,b,\cdots,b)$, ou seja, as primeiras $n-k$ componentes devem ter um valor, e as k componentes restantes devem ter outro valor. Sem perda de generalidade podemos tomar $b=1$. Seja $e^{i\omega_k}$ o autovalor. Note que o autovalor depende de k, isto é, do peso de Hamming de $\vec{k}$, mas ele não depende explicitamente de $\vec{k}$. Devemos resolver a equação

matricial

$$\left[\begin{array}{ccc|cccc} \frac{2}{n}-1-e^{i\omega_k} & \frac{2}{n} & \cdots & & & & \\ \frac{2}{n} & \frac{2}{n}-1-e^{i\omega_k} & & \frac{2}{n} & & & \\ \vdots & & \ddots & & & & \\ \hline & & & -\frac{2}{n}+1-e^{i\omega_k} & -\frac{2}{n} & \cdots & \\ & -\frac{2}{n} & & -\frac{2}{n}+1-e^{i\omega_k} & -\frac{2}{n} & & \\ & & & \vdots & & \ddots & \end{array}\right] \left[\begin{array}{c} a \\ \vdots \\ a \\ \hline 1 \\ \vdots \\ 1 \end{array}\right] = 0,$$

que se reduz a

$$\begin{cases} \left(1-\frac{2k}{n}-e^{i\omega_k}\right)a+\frac{2k}{n}=0, \\ -2\left(1-\frac{k}{n}\right)a+1-\frac{2k}{n}-e^{i\omega_k}=0. \end{cases} \tag{4.2.59}$$

Resolvendo esse sistema de equações, obtemos

$$\begin{cases} a=\pm i\frac{\sqrt{\frac{k}{n}}}{\sqrt{1-\frac{k}{n}}}, \\ e^{i\omega_k}=1-\frac{2k}{n}\mp 2i\sqrt{\frac{k}{n}\left(1-\frac{k}{n}\right)}. \end{cases} \tag{4.2.60}$$

Consequentemente

$$\begin{cases} \cos\omega_k=1-\frac{2k}{n}, \\ \sin\omega_k=\mp 2\sqrt{\frac{k}{n}\left(1-\frac{k}{n}\right)}. \end{cases} \tag{4.2.61}$$

Encontramos os dois autovetores restantes. Na forma normalizada, o autovetor associado ao autovalor $e^{i\omega_k}$ se escreve como

$$\left|\alpha_1^{\vec{k}}\right\rangle = \frac{1}{\sqrt{2}}\left[\begin{array}{c} \frac{-i}{\sqrt{n-k}} \\ \vdots \\ \frac{-i}{\sqrt{n-k}} \\ \hline \frac{1}{\sqrt{k}} \\ \vdots \\ \frac{1}{\sqrt{k}} \end{array}\right], \tag{4.2.62}$$

e o autovetor $\left|\alpha_n^{\vec{k}}\right\rangle$ associado ao autovetor $e^{-i\omega_k}$ é o complexo conjugado do vetor $\left|\alpha_1^{\vec{k}}\right\rangle$.

Esses autovetores foram descritos separando as linhas que trocaram de sinal das linhas que permaneceram inalteradas. Devemos permutar as componentes dos autovetores para que elas correspondam às linhas nas posições originais. A variável que indica se a linha trocou ou não de sinal é $\vec{k}$. Se a componente k_a for zero, significa que não houve troca de sinal na a-ésima linha, se $k_a = 1$, então, houve troca. Os autovetores $\left|\alpha_1^{\vec{k}}\right\rangle$ e $\left|\alpha_n^{\vec{k}}\right\rangle$ associados aos autovalores $e^{\pm i\omega_k}$ se escrevem na base original como

$$\left|\alpha_1^{\vec{k}}\right\rangle = \frac{1}{\sqrt{2}}\sum_{a=1}^{n}\left(\frac{k_a}{\sqrt{k}} - i\frac{1-k_a}{\sqrt{n-k}}\right)|a\rangle\,, \tag{4.2.63}$$

$$\left|\alpha_n^{\vec{k}}\right\rangle = \frac{1}{\sqrt{2}}\sum_{a=1}^{n}\left(\frac{k_a}{\sqrt{k}} + i\frac{1-k_a}{\sqrt{n-k}}\right)|a\rangle\,, \tag{4.2.64}$$

para $0 < k < n$.

Concluímos que o conjunto $\left\{\left|\phi_{a,\vec{k}}\right\rangle := \left|\alpha_a^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle : 1 \le a \le n,\, 0 \le \vec{k} \le 2^n - 1\right\}$ forma uma base não-ortogonal de autovetores de U para o espaço de Hilbert $\mathcal{H}^n \otimes \mathcal{H}^{2^n}$. Os autovalores são ± 1 e $e^{\pm i\omega_k}$. As expressões de $\left|\alpha_a^{\vec{k}}\right\rangle$ na base computacional são dadas pelas Eqs. (4.2.55), (4.2.56) para $k = 0$ e $k = n$ e com os casos particulares $\left|\alpha_1^{\vec{0}}\right\rangle = \left|\alpha_n^{\vec{1}}\right\rangle = |\mathrm{D}\rangle$. Para $0 < k < n$, $a = 1$ ou $a = n$, $\left|\alpha_a^{\vec{k}}\right\rangle$ estão descritos nas Eqs. (4.2.63) e (4.2.64). Os vetores $\left|\beta_{\vec{k}}\right\rangle$ estão descritos na Eq. (4.2.49).

Exercício 4.3. *Obtenha expressões explícitas para os autovetores* $\left|\alpha_a^{\vec{k}}\right\rangle$ *quando* $0 < k < n$ *e* $0 < a < n$ *associados aos autovalores* $e^{\pm i\omega_k}$.

Exercício 4.4. *Mostre explicitamente que os autovetores associados aos autovalores* $e^{\pm i\omega_k}$ *são ortogonais entre si e ortogonais aos outros autovetores.*

Exercício 4.5. *Mostre que os autovetores das Eqs. (4.2.63) e (4.2.64) são unitários.*

Exercício 4.6. *Seja* $\phi_{a,\vec{k}}$ *o autovalor associado ao autovetor* $\left|\phi_{a,\vec{k}}\right\rangle$. *Faça uma tabela de todos os valores de* $\phi_{a,\vec{k}}$ *para todos os valores de* a *e* $\vec{k}$.

Podemos agora calcular o estado do passeio quântico num instante de tempo genérico. Vamos tomar como condição inicial o estado

$$|\Psi(0)\rangle = |\mathrm{D}\rangle \left|\vec{0}\right\rangle, \tag{4.2.65}$$

ou seja, um caminhante localizado no vértice $\vec{v} = \vec{0}$ com o estado diagonal no espaço da moeda. Essa condição inicial é invariante por permutação de arestas do hipercubo. Suponha que $\phi_{a,\vec{k}}$ seja o autovalor associado ao autovetor $\left|\phi_{a,\vec{k}}\right\rangle$. Usando a decomposição espectral de U, temos

$$U = \sum_{a,\vec{k}} \phi_{a,\vec{k}} \left|\phi_{a,\vec{k}}\right\rangle \left\langle\phi_{a,\vec{k}}\right|. \tag{4.2.66}$$

No instante t, o estado do passeio será dado por

$$\begin{aligned} |\Psi(t)\rangle &= U^t |\Psi(0)\rangle \\ &= \sum_{a,\vec{k}} (\phi^t_{a,\vec{k}} \left\langle\phi_{a,\vec{k}}|\Psi(0)\right\rangle \left|\phi_{a,\vec{k}}\right\rangle, \end{aligned} \tag{4.2.67}$$

Usando a equação acima, temos

$$\begin{aligned} |\Psi(t)\rangle &= \sum_{a,\vec{k}} (\phi_{a,\vec{k}})^t \left\langle\phi_{a,\vec{k}}|\Psi(0)\right\rangle \left|\phi_{a,\vec{k}}\right\rangle \\ &= \sum_{a,\vec{k}} (\phi_{a,\vec{k}})^t \left\langle\alpha^{\vec{k}}_a|\mathrm{D}\right\rangle \left\langle\beta_{\vec{k}}|\vec{0}\right\rangle \left|\alpha^{\vec{k}}_a\right\rangle |\beta_{\vec{k}}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{a,\vec{k}} (\phi_{a,\vec{k}})^t \left\langle\alpha^{\vec{k}}_a|\mathrm{D}\right\rangle \left|\alpha^{\vec{k}}_a\right\rangle |\beta_{\vec{k}}\rangle. \end{aligned} \tag{4.2.68}$$

Na última passagem, usamos a Eq. (4.2.49) para simplificar $\left\langle\beta_{\vec{k}}|\vec{0}\right\rangle$. Somente os autovetores $\left|\alpha^{\vec{0}}_1\right\rangle = |\mathrm{D}\rangle$, $\left|\alpha^{\vec{1}}_n\right\rangle = |\mathrm{D}\rangle$ associados aos autovalores $+1$ e -1 e autovetores do tipo $\left|\alpha^{\vec{k}}_1\right\rangle$ e $\left|\alpha^{\vec{k}}_n\right\rangle$ para $0 < k < 2^n - 1$ associados ao autovalores $e^{\pm i\omega_k}$ não são ortogonais ao vetor $|\mathrm{D}\rangle$. Portanto a Eq. (4.2.68)

se reduz a

$$\begin{aligned}|\Psi(t)\rangle &= \frac{1}{\sqrt{2^n}}\Big((1)^t\left|\alpha_1^{\vec{0}}\right\rangle|\beta_{\vec{0}}\rangle + (-1)^t\left|\alpha_n^{\vec{1}}\right\rangle|\beta_{\vec{1}}\rangle + \\ &\sum_{\vec{k}=1}^{2^n-2}(e^{i\omega_k})^t\left\langle\alpha_1^{\vec{k}}|\mathrm{D}\right\rangle\left|\alpha_1^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle + \\ &\sum_{\vec{k}=1}^{2^n-2}(e^{-i\omega_k})^t\left\langle\alpha_n^{\vec{k}}|\mathrm{D}\right\rangle\left|\alpha_n^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle\Big). \qquad (4.2.69)\end{aligned}$$

Usando as Eq. (4.2.63) temos

$$\left\langle\alpha_1^{\vec{k}}|\mathrm{D}\right\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{k}{n}} + i\sqrt{1-\frac{k}{n}}\right), \qquad (4.2.70)$$

$$\left\langle\alpha_n^{\vec{k}}|\mathrm{D}\right\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\frac{k}{n}} - i\sqrt{1-\frac{k}{n}}\right), \qquad (4.2.71)$$

para $1 < k < n$. O estado do passeio quântico no hipercubo para um instante de tempo t é então dado por

$$\begin{aligned}|\Psi(t)\rangle &= \frac{1}{\sqrt{2^n}}\Big(|\mathrm{D}\rangle|\beta_{\vec{0}}\rangle + (-1)^t|\mathrm{D}\rangle|\beta_{\vec{1}}\rangle\Big) + \\ &\frac{1}{\sqrt{2^{n+1}}}\sum_{\vec{k}=1}^{2^n-2}e^{i\omega_k t}\left(\sqrt{\frac{k}{n}} + i\sqrt{1-\frac{k}{n}}\right)\left|\alpha_1^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle + \\ &\frac{1}{\sqrt{2^{n+1}}}\sum_{\vec{k}=1}^{2^n-2}e^{-i\omega_k t}\left(\sqrt{\frac{k}{n}} - i\sqrt{1-\frac{k}{n}}\right)\left|\alpha_n^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle \qquad (4.2.72)\end{aligned}$$

É notável que possamos obter uma expressão analítica para o estado quântico para qualquer instante de tempo. Esse resultado abre caminho para se obter diversos outros resultados como a distribuição estacionária e o tempo de mistura no hipercubo. O resultado analítico só foi possível porque temos em mãos a decomposição espectral do operador de evolução. Note que apenas os autovetores não-ortogonais a $|\mathrm{D}\rangle \otimes I$ contribuem para a expressão de $|\Psi(t)\rangle$. Isso é consequência da escolha da condição inicial $|\mathrm{D}\rangle\left|\vec{0}\right\rangle$. Se a condição inicial estiver em um subespaço gerado apenas por alguns dos autovetores de U, o estado permanecerá nesse subespaço durante toda a evolução. No caso de $|\Psi(t)\rangle$, o subespaço tem dimensão $2^{n+1}-2$ e é gerado por uma base ortonormal dada por $\left\{\left|\alpha_1^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle : 0 \leq \vec{k} < 2^n - 1,\right.$

$\left|\alpha_n^{\vec{k}}\right\rangle |\beta_{\vec{k}}\rangle : 0 < \vec{k} \leq 2^n - 1\Big\}$. Vamos mostrar na próxima seção que, na verdade, a evolução do passeio quântico com essa condição inicial se dá em um subespaço bem menor.

Antes de concluir esta seção, vamos obter uma expressão mais simples para $|\Psi(t)\rangle$, que será útil em aplicações futuras. Note que a expressão

$$\sqrt{\frac{k}{n}} + i\sqrt{1 - \frac{k}{n}}$$

é um número complexo de módulo 1. Vamos redefinir os vetores $\left|\alpha_1^{\vec{k}}\right\rangle$ e $\left|\alpha_n^{\vec{k}}\right\rangle$ da seguinte forma:

$$\left|\widetilde{\alpha}_1^{\vec{k}}\right\rangle = \left(\sqrt{\frac{k}{n}} + i\sqrt{1 - \frac{k}{n}}\right)\left|\alpha_1^{\vec{k}}\right\rangle, \tag{4.2.73}$$

$$\left|\widetilde{\alpha}_n^{\vec{k}}\right\rangle = \left(\sqrt{\frac{k}{n}} - i\sqrt{1 - \frac{k}{n}}\right)\left|\alpha_n^{\vec{k}}\right\rangle, \tag{4.2.74}$$

para $0 < k < n$. Os vetores $\left|\widetilde{\alpha}_1^{\vec{k}}\right\rangle$ e $\left|\widetilde{\alpha}_n^{\vec{k}}\right\rangle$ são unitários e obedecem às mesmas propriedades de $\left|\alpha_1^{\vec{k}}\right\rangle$ e $\left|\alpha_n^{\vec{k}}\right\rangle$. Porém, o produto interno desses novos vetores com $|\mathrm{D}\rangle$ é $1/\sqrt{2}$ e a expressão de $|\Psi(t)\rangle$ se reduz a

$$\begin{aligned} |\Psi(t)\rangle = {} & \frac{1}{\sqrt{2^n}}\Big(|\mathrm{D}\rangle\left|\beta_{\vec{0}}\right\rangle + (-1)^t|\mathrm{D}\rangle\left|\beta_{\vec{1}}\right\rangle\Big) + \\ & \frac{1}{\sqrt{2^{n+1}}}\sum_{\vec{k}=1}^{2^n-2}\left(e^{i\omega_k t}\left|\widetilde{\alpha}_1^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle + e^{-i\omega_k t}\left|\widetilde{\alpha}_n^{\vec{k}}\right\rangle|\beta_{\vec{k}}\rangle\right) \end{aligned} \tag{4.2.75}$$

Sugestões para Leitura

O passeio sobre a reta é analisado em uma vasta quantidade de artigos. O artigo pioneiro é o [48], que obteve as Eqs. (4.1.38) e (4.1.39). Uma análise mais completa é apresentada nas Refs. [5, 33, 34, 14]. Mais referências podem ser encontradas no livro [63]. O artigo pioneiro na análise do passeio quântico no hipercubo é a Ref. [45]. A Ref. [41] corrige a distribuição estacionária apresentada na Ref. [45]. A Ref. [32] mostra que o tempo de alcance quântico entre dois vértices opostos do hipercubo é exponencialmente menor que o tempo de alcance clássico. Mais referências sobre o passeio no hipercubo podem ser encontradas na Ref. [17]. Passeios quânticos também

foram analisados em diversos outros grafos, como no ciclo [1] e na malha bidimensional [36, 61]. As teses de doutorado [42, 50] também são referências úteis.

Capítulo 5

Tempo de Alcance Quântico

Como é usual, antes de entrar no contexto quântico, apresentamos as noções clássicas que foram quantizadas. O foco é o *tempo de alcance quântico*, por isso vamos nos restringir à teoria clássica básica. A fórmula mais conhecida para o cálculo do tempo de alcance clássico em grafos usa a *distribuição estacionária*. No entanto, existe uma fórmula alternativa sem usar a distribuição estacionária, porém ela requer a definição de um grafo direcionado obtido a partir do grafo original. No contexto quântico, o processo é um pouco mais extenso. A partir do grafo original, definimos um grafo bipartido associado e depois um grafo bipartido direcionado. Para definir o tempo de alcance quântico no grafo original, o passeio quântico se processa no grafo bipartido direcionado. Mostramos como o operador de evolução é obtido a partir da matriz estocástica do grafo original e exemplificamos todo o processo no grafo completo. O modelo de passeio quântico deste capítulo tem uma estrutura diferente dos outros modelos que vimos até agora.

5.1 Tempo de Alcance Clássico

Considere um *grafo* $\Gamma(X, E)$ conexo, não-direcionado e não-bipartido onde $X = \{x_1, \cdots, x_n\}$ é o conjunto dos vértices e E é o conjunto das arestas. O *tempo de alcance* de um passeio randômico *clássico* nesse grafo é o tempo esperado para o caminhante atingir pela primeira vez um vértice marcado, uma vez dada as condições iniciais. Podemos ter mais que um vértice marcado formando um subconjunto de vértices M. Nesse caso, o tempo de

alcance é o tempo esperado para o caminhante atingir um dos vértices do conjunto M pela primeira vez, não importa qual seja o vértice desde que ele pertença a M e desde seja o primeiro vértice de M.

Se $p_{x\,x'}(t)$ é a probabilidade do caminhante atingir x' pela primeira vez no instante t tendo saído de x, o tempo de alcance do vértice x para x' será

$$H_{x\,x'} = \sum_{t=0}^{\infty} t\, p_{x\,x'}(t). \tag{5.1.1}$$

Definimos $H_{x\,x} = 0$ quando os vértices de saída e chegada são os mesmos.

Por exemplo, a probabilidade $p_{x\,x'}(t)$ no instante $t = 1$ com $x \neq x'$ para um *grafo completo* de n vértices é $1/(n-1)$, pois o caminhante tem $n-1$ possíveis vértices para ir no primeiro passo. Para o caminhante chegar no vértice x' no instante $t = 2$ pela primeira vez, ele deve visitar um dos $n-2$ vértices distintos de x e x'. A probabilidade disso ocorrer é $(n-2)/(n-1)$. Após essa visita, ele deve ir direto para o vértice x', que ocorre com probabilidade $1/(n-1)$. Portanto, $p_{x\,x'}(2) = (n-2)/(n-1)^2$. Generalizando esse raciocínio, obtemos $p_{x\,x'}(t) = (n-2)^{t-1}/(n-1)^t$. Assim

$$\begin{aligned} H_{x\,x'} &= \sum_{t=0}^{\infty} t\, \frac{(n-2)^{t-1}}{(n-1)^t} \\ &= n-1. \end{aligned} \tag{5.1.2}$$

Usamos a identidade $\sum_{t=0}^{\infty} t\omega^t = 1/(1-\omega)^2$ válida para $0 < \omega < 1$. Usualmente, o tempo de alcance depende de x e x', porém no grafo completo os pontos de partida ou de chegada são equivalentes. No caso geral, $H_{x\,x'}$ pode ser diferente de $H_{x'x}$.

A noção de tempo de alcance de um vértice para um subconjunto pode ser formalizada da seguinte maneira: suponha que M seja um subconjunto não-vazio de X com cardinalidade m e seja $p_{xM}(t)$ a probabilidade do caminhante atingir qualquer um dos vértices de M pela primeira vez no instante t tendo saído x, o tempo de alcance para atingir o subconjunto M partindo de x será

$$H_{xM} = \sum_{t=0}^{\infty} t\, p_{xM}(t). \tag{5.1.3}$$

Novamente definimos que $H_{xM} = 0$ se $x \in M$.

Vamos usar uma noção mais ampla de tempo de alcance quando o caminhante sai de uma distribuição de probabilidades nos vértices. No caso anterior, a probabilidade do caminhante sair do vértice x é 1 e nos outros vértices a probabilidade é 0. Suponha que o caminhante saia de uma distribuição σ, isto é, no instante inicial, a probabilidade do caminhante estar no

vértice x é σ_x. Usualmente a distribuição inicial é a distribuição estacionária ou a *distribuição uniforme* $\sigma_x = 1/n$. Em qualquer caso, a distribuição inicial tem que satisfazer a $\sum_{x\in X} \sigma_x = 1$. O tempo de alcance para atingir o subconjunto M partindo da distribuição σ é

$$H_{\sigma M} = \sum_{x\in X} \sigma_x \, H_{xM}. \tag{5.1.4}$$

Isto é, $H_{\sigma M}$ é o *valor esperado* segundo a distribuição σ dos tempos de alcance de cada passeio.

Exercício 5.1. *Mostre que no grafo completo*

$$H_{xM} = \frac{n-1}{m}$$

se $x \notin M$.

Exercício 5.2. *Mostre que no grafo completo*

$$H_{\sigma M} = \frac{(n-m)(n-1)}{mn}$$

se σ *for a distribuição uniforme. Por que* $H_{\sigma M} \approx H_{xM}$ *para* $n \gg m$*?*

5.1.1 Tempo de alcance clássico usando a distribuição estacionária

As Eqs. (5.1.1) e (5.1.3) são ingratas para o cálculo prático do tempo de alcance em grafos. Felizmente existem métodos alternativos. O método mais conhecido usa um raciocínio recursivo. Por exemplo, no grafo completo podemos calcular o tempo de alcance $H_{x\,x'}$ da seguinte forma: o caminhante sai de x; com probabilidade $1/(n-1)$ ele vai direto para x' e portando leva um tempo igual a 1; com probabilidade $(n-2)/(n-1)$ ele vai para um vértice x'' diferente de x' e, logo, vai levar um tempo igual a 1 mais o tempo esperado de ir de x'' para x', que é $H_{x\,x'}$. Assim, estabelecemos a seguinte equação recursiva:

$$H_{x\,x'} = \frac{1}{n-1} + \frac{n-2}{n-1}\left(1 + H_{x\,x'}\right), \tag{5.1.5}$$

cuja solução é igual a da Eq. (5.1.2).

Esse método funciona para um grafo genérico. Se V_x é a *vizinhança* de x, a cardinalidade de V_x será o grau de x denotado por d_x. Para facilitar a dedução, vamos supor que a distância entre x e x' é maior que 1. Então,

o caminhante sairá de x e irá para o vértice vizinho x'' com probabilidade $1/d_x$ levando um tempo igual a 1. Agora, devemos somar o tempo esperado de ir de x'' para x'. Isso tem que ser feito para todos vértices x'' vizinhos de x. Assim obtemos

$$H_{x\,x'} = \frac{1}{d_x} \sum_{x'' \in V_x} \big(1 + H_{x''\,x'}\big). \tag{5.1.6}$$

A Eq. (5.1.5) é um caso particular da Eq. (5.1.6), pois para o grafo completo $d_x = 1/(n-1)$ e $H_{x''\,x'} = H_{x\,x'}$ exceto se $x'' = x'$. Esse último caso gera o primeiro termo da Eq. (5.1.5). Os restantes $n-2$ casos geram o segundo termo. Isso mostra que a Eq. (5.1.6) é geral e a distância entre x e x' não precisa ser maior que 1. No entanto, não podemos ter $x = x'$, pois o lado esquerdo é zero e o lado direito não é.

O objetivo agora é resolver a Eq. (5.1.6) para obter o tempo de alcance. Esta tarefa é facilitada se a Eq. (5.1.6) for convertida para a forma matricial. Se H é a matriz de dimensão $n \times n$ cujas componentes são $H_{x\,x'}$, o lado esquerdo será convertido em H e o lado direito deverá ser expandido, considerando que

$$p_{x\,x'} = \begin{cases} \frac{1}{d_x}, & \text{se } x' \text{ é adjacente a } x; \\ 0, & \text{caso contrário,} \end{cases} \tag{5.1.7}$$

obtemos a seguinte equação matricial:

$$H = J + PH + D, \tag{5.1.8}$$

onde J é uma matriz com todas as componentes iguais a 1, P é a *matriz estocástica à direita* do grafo e D é uma matriz diagonal que deve ser introduzida para que a equação matricial seja igualmente válida para os elementos da diagonal. P também é conhecida como *matriz de transição* ou *matriz de probabilidades*.

A matriz D pode ser encontrada a partir da distribuição estacionária π. A distribuição estacionária satisfaz a $\pi^T \cdot P = \pi^T$. Multiplicando a Eq. (5.1.8) pela esquerda por π^T, obtemos

$$D_{x\,x} = -\frac{1}{\pi_x},$$

onde π_x é a x-ésima componente de π.

A Eq. (5.1.8) pode ser escrita como $(I-P)H = J+D$. Quando tentamos encontrar H a partir dessa equação, lidamos com o fato de que $I-P$ é uma matriz não-inversível, pois $I-P$ tem o autovalor 0 associado ao autovetor

com todas as componentes iguais a 1, que denotaremos por $\mathbf{1}$. Isso quer dizer que a equação $(I - P)X = J + D$ tem mais de uma solução X. De fato, se a matriz X é uma solução, então $X + \mathbf{1} \cdot v^T$ também é uma solução para qualquer vetor v. Contudo, ter em mãos uma solução X da equação não garante que achamos H. Há uma forma de verificar se X é uma solução correta, pois $H_{x\,x}$ deve ser nulo para todo x. Uma solução da equação $(I - P)X = J + D$ é

$$X = (I - P + \mathbf{1} \cdot \pi^T)^{-1}(J + D), \tag{5.1.9}$$

como pode ser verificada através do Exercício 5.3. Agora temos que anular a diagonal de X somando um termo do tipo $\mathbf{1} \cdot v^T$. Finalmente obtemos

$$H = X - \mathbf{1} \cdot v^T, \tag{5.1.10}$$

onde o vetor v tem como componentes a diagonal de X, isto é, $v_x = X_{x\,x}$.

Exercício 5.3. *Seja*

$$M = I - P + \boldsymbol{1} \cdot \pi^T.$$

1. *Mostre que M é inversível.*
2. *Usando as relações $\pi^T \cdot P = \pi^T$, $P \cdot \boldsymbol{1} = \boldsymbol{1}$ e*

$$M^{-1} = \sum_{t=0}^{\infty} (I - M)^t,$$

mostre que

$$M^{-1} = \sum_{t=0}^{\infty} P^t - \boldsymbol{1} \cdot \pi^T.$$

3. *Mostre que a solução (5.1.9) satisfaz à equação $(I - P)X = J + D$.*
4. *Mostre que a matriz H dada pela Eq. (5.1.10) satisfaz $H_{x\,x} = 0$.*

5.1.2 Tempo de alcance sem usar a distribuição estacionária

Existe um método alternativo para o cálculo do tempo de alcance que não usa a distribuição estacionária. Apresentaremos o método para o cálculo de $H_{\sigma M}$ como definido na Eq. (5.1.4). Vamos denominar os vértices do conjunto M de *vértices marcados*. Definiremos um grafo direcionado modificado a partir do grafo $\Gamma(X, E)$ não-direcionado original. Cada aresta de um grafo não-direcionado pode ser vista como duas arestas direcionadas opostas. As

arestas direcionadas estão fundidas formando a aresta não-direcionada. O grafo direcionado modificado é obtido do grafo original removendo todas as arestas direcionadas que saem dos vértices marcados, porém mantendo as arestas direcionadas que chegam. Isso quer dizer que se o caminhante atingir um vértice marcado, ele ficará preso nesse vértice nos passos seguintes. Para o cálculo do tempo de alcance, o grafo não-direcionado original e o grafo direcionado modificado são equivalentes. No entanto, as matrizes de probabilidades são diferentes. Vamos denotar a matriz estocástica do grafo modificado por P'. As componentes de P' são

$$p'_{xy} = \begin{cases} p_{xy}, & x \notin M; \\ \delta_{xy}, & x \in M. \end{cases} \tag{5.1.11}$$

Seja $\sigma^{(0)}$ a distribuição de probabilidades inicial nos vértices do grafo original vista como um vetor linha, a distribuição depois de t passos é

$$\sigma^{(t)} = \sigma^{(0)} \cdot P^t. \tag{5.1.12}$$

Seja $\mathbf{1}$ o vetor coluna com todas as n componentes iguais a 1, vamos definir $\mathbf{1}_{X-M}$ como o vetor coluna com as $n-m$ componentes fora de M iguais a 1 e a m componentes em M iguais a zero. A probabilidade de encontrarmos o caminhante no conjunto $X - M$ no instante t é $\sigma^{(t)} \cdot \mathbf{1}_{X-M}$. No entanto, essa expressão não é útil nesse contexto, pois o caminhante terá passado no conjunto M anteriormente. Queremos achar a probabilidade do caminhante estar no conjunto $X - M$ no instante t sem ter passado pelo conjunto M. Esse resultado é obtido se usarmos a matriz P' no lugar de P na Eq. (5.1.12). De fato, se a evolução é feita com a matriz P' e o caminhante entrou em M, ele ficará preso em M nos passos seguintes. Portanto, se o caminhante for encontrado em $X - M$, certamente ele não entrou ainda em M. A probabilidade de encontrarmos o caminhante no conjunto $X-M$ no instante t sem ter passado por M é $\sigma^{(0)} \cdot (P')^t \cdot \mathbf{1}_{X-M}$.

Na Eq. (5.1.3), calculamos o tempo médio para atingir um vértice marcado através da fórmula usual para cálculo de médias ponderadas. Quando a variável em questão assume os valores inteiros não negativos $\{0, 1, 2, \cdots\}$, existe uma fórmula alternativa de cálculo da média. Essa fórmula se aplica nesse contexto pois o tempo é o número de passos. Seja T o número de passos para atingir um vértice marcado pela primeira vez em uma instância de execução de um passeio randômico e seja $p(T \geq t)$ a probabilidade de atingir M pela primeira vez para qualquer número de passos T maior ou igual a t tendo como condição inicial a distribuição σ, o tempo de alcance pode ser definido de forma equivalente usando a fórmula

$$H_{\sigma\, M} = \sum_{t=1}^{\infty} p(T \geq t). \tag{5.1.13}$$

Para verificar a equivalência dessa nova fórmula com a anterior, note que

$$p(T \geq t) = \sum_{j=t}^{\infty} p(T = j), \tag{5.1.14}$$

onde $p(T = t)$ é a probabilidade de atingir M pela primeira vez com exatamente t passos. Substituindo a Eq. (5.1.14) na Eq. (5.1.13) e invertendo a ordem do somatório, obtemos

$$\begin{aligned} H_{\sigma\, M} &= \sum_{j=1}^{\infty} \sum_{t=1}^{j} p(T = j) \\ &= \sum_{j=1}^{\infty} j\, p(T = j). \end{aligned} \tag{5.1.15}$$

Esta última equação é equivalente a Eq. (5.1.3).

A probabilidade $p(T \geq t)$ pode ser entendida de outra forma. Se o caminhante atinge M para $T \geq t$, então nos primeiros $t-1$ passos ele está ainda no conjunto $X - M$, isto é, em um dos vértices não-marcados sem ter passado por M. Vimos em um parágrafo anterior que a probabilidade do caminhante estar em um dos vértices do conjunto $X - M$ no instante t sem ter passado por M anteriormente é $\sigma^{(0)} \cdot (P')^{t-1} \cdot \mathbf{1}_{X-M}$. Portanto,

$$p(T \geq t) = \sigma^{(0)} \cdot (P')^{t-1} \cdot \mathbf{1}_{X-M}. \tag{5.1.16}$$

Vamos definir $P_{\overline{M}}$ como a matriz quadrada de dimensão $n-m$ obtida a partir de P eliminando as linhas e colunas referentes aos vértices de M. Vamos definir $\sigma_{\overline{M}}$ e $\mathbf{1}_{\overline{M}}$ de maneira equivalente. Examinando as componentes que não se anulam na multiplicação matricial da Eq. (5.1.16), concluímos que

$$p(T \geq t) = \sigma^{(0)}_{\overline{M}} \cdot P^{t-1}_{\overline{M}} \cdot \mathbf{1}_{\overline{M}}. \tag{5.1.17}$$

Substituindo a equação acima na Eq. (5.1.13) obtemos

$$\begin{aligned} H_{\sigma\, M} &= \sigma^{(0)}_{\overline{M}} \cdot \left(\sum_{t=0}^{\infty} P^{t}_{\overline{M}} \right) \cdot \mathbf{1}_{\overline{M}} \\ &= \sigma^{(0)}_{\overline{M}} \cdot (I - P_{\overline{M}})^{-1} \cdot \mathbf{1}_{\overline{M}}. \end{aligned} \tag{5.1.18}$$

A matriz $I - P_{\overline{M}}$ tem sempre inversa para grafos do tipo conexo, não-direcionado e não-bipartido. A razão por trás deste resultado é o fato de que $P_{\overline{M}}$ não tem autovalor igual a 1, portanto $I - P_{\overline{M}}$ não possui autovalor igual a 0.

As sugestões de leitura no final do capítulo descrevem referências úteis sobre as *Cadeias de Markov Ergódicas* e o *Teorema de Perron-Frobenius*, que são úteis neste contexto. Dos resultados apresentados aqui, o mais importante é a estratégia usada para gerar a Eq. (5.1.18), pois ela também será usada para definir a versão *quântica* do tempo de alcance.

5.2 Operadores de Reflexão em um Grafo Bipartido

Para definir o *tempo de alcance quântico*, vamos usar um processo de duplicação para obter um *grafo bipartido* associado ao grafo original, como será explicado em detalhes na Sec. 5.6. No momento definiremos os operadores quânticos no grafo bipartido. A partir desses operadores, definiremos o tempo de alcance quântico no grafo original na Sec. 5.6.

Considere um grafo bipartido entre os conjunto de vértices X e Y de cardinalidades iguais. Vamos denotar por x e y vértices genéricos dos conjuntos X e Y. Vamos definir p_{xy} como o inverso do grau de saída do vértice x, se y for *adjacente* a x, do contrário, $p_{xy} = 0$. Por exemplo, se x for adjacente a apenas dois vértices y_1 e y_2 do conjunto Y, então $p_{xy_1} = p_{xy_2} = 1/2$. Equivalentemente vamos definir q_{yx} como o inverso do grau de saída do vértice y. As variáveis p_{xy} e q_{yx} satisfazem a

$$\sum_{y\in Y} p_{xy} = 1 \qquad \forall x \in X, \tag{5.2.19}$$

$$\sum_{x\in X} q_{yx} = 1 \qquad \forall y \in Y. \tag{5.2.20}$$

Para definir um passeio quântico no grafo bipartido, vamos associar ao grafo o espaço de Hilbert $\mathcal{H}^{n^2} = \mathcal{H}^n \otimes \mathcal{H}^n$, onde $n = |X| = |Y|$. A base computacional da primeira componente é $\left\{ |x\rangle : x \in X \right\}$ e a da segunda é $\left\{ |y\rangle : y \in Y \right\}$. Evidentemente a base computacional de $\mathcal{H}^{n^2}$ é $\left\{ |x, y\rangle : x \in X, y \in Y \right\}$. Em vez de usar as matrizes de probabilidades P e Q do passeio aleatório clássico, cujas componentes são p_{xy} e q_{yx}, vamos definir os operadores $A : \mathcal{H}^n \to \mathcal{H}^{n^2}$ e $B : \mathcal{H}^n \to \mathcal{H}^{n^2}$ da seguinte forma:

$$A = \sum_{x\in X} |\alpha_x\rangle \langle x| , \tag{5.2.21}$$

$$B = \sum_{y\in Y} |\beta_y\rangle \langle y| , \tag{5.2.22}$$

onde

$$|\alpha_x\rangle = |x\rangle \otimes \left(\sum_{y \in Y} \sqrt{p_{xy}}\, |y\rangle \right), \tag{5.2.23}$$

$$|\beta_y\rangle = \left(\sum_{x \in X} \sqrt{q_{yx}}\, |x\rangle \right) \otimes |y\rangle . \tag{5.2.24}$$

As dimensões de A e B são $n^2 \times n$. Outra forma de escrever as Eqs. (5.2.21) e (5.2.22) é

$$A\,|x\rangle = |\alpha_x\rangle , \tag{5.2.25}$$

$$B\,|y\rangle = |\beta_y\rangle , \tag{5.2.26}$$

cuja interpretação é a seguinte: o resultado da multiplicação da matriz A pelo x-ésimo vetor da base computacional de $\mathcal{H}^n$ é a x-ésima coluna de A. Portanto, as colunas da matriz A são os vetores $|\alpha_x\rangle$ e as colunas da matriz B são os vetores $|\beta_y\rangle$. Usando as Eqs. (5.2.23) e (5.2.24) junto com as Eqs. (5.2.19) e (5.2.20), obtemos

$$\langle \alpha_x | \alpha'_x \rangle = \delta_{x,x'}, \tag{5.2.27}$$

$$\langle \beta_y | \beta'_y \rangle = \delta_{y,y'}. \tag{5.2.28}$$

Consequentemente temos

$$A^T A = I_n, \tag{5.2.29}$$

$$B^T B = I_n. \tag{5.2.30}$$

Essas equações implicam que A e B preservam a norma de vetores, assim se $|\mu\rangle$ for um vetor unitário de $\mathcal{H}^n$ então $A\,|\mu\rangle$ será um vetor unitário de $\mathcal{H}^{n^2}$. O mesmo em relação a B.

Naturalmente vamos investigar o produto na ordem inversa. Usando as Eqs. (5.2.21) e (5.2.22) obtemos

$$AA^T = \sum_{x \in X} |\alpha_x\rangle \langle \alpha_x| , \tag{5.2.31}$$

$$BB^T = \sum_{y \in Y} |\beta_y\rangle \langle \beta_y| . \tag{5.2.32}$$

Usando as Eqs. (5.2.29) e (5.2.30) temos $(AA^T)^2 = AA^T$ e $(BB^T)^2 = BB^T$. Assim vamos definir os projetores

$$\Pi_A = AA^T, \tag{5.2.33}$$

$$\Pi_B = BB^T. \tag{5.2.34}$$

As Eqs. (5.2.31) e (5.2.32) mostram que Π_A projeta um vetor genérico de $\mathcal{H}^{n^2}$ no subespaço $\mathcal{H}_A$ gerado por $\left\{ |\alpha_x\rangle : x \in X \right\}$ e Π_B no subespaço $\mathcal{H}_B$ gerado por $\left\{ |\beta_y\rangle : y \in Y \right\}$.

Uma vez definidos dois projetores, podemos definir os *operadores de reflexão* associados

$$\mathcal{R}_A = 2\,\Pi_A - I_{n^2}, \tag{5.2.35}$$
$$\mathcal{R}_B = 2\,\Pi_B - I_{n^2}. \tag{5.2.36}$$

$\mathcal{R}_A$ reflete um vetor genérico de $\mathcal{H}^{n^2}$ em torno do subespaço $\mathcal{H}_A$. A verificação pode ser feita como se segue: $\mathcal{R}_A$ deixa invariante um vetor de $\mathcal{H}_A$, ou seja, se $|\psi\rangle \in \mathcal{H}_A$, então $\mathcal{R}_A\,|\psi\rangle = |\psi\rangle$, como pode ser confirmado através da Eq. (5.2.35). Por outro lado, $\mathcal{R}_A$ inverte um vetor ortogonal a $\mathcal{H}_A$, isto é, se $|\psi\rangle \in \mathcal{H}_A^{\perp}$, então $\mathcal{R}_A\,|\psi\rangle = -\,|\psi\rangle$. Um vetor genérico de $\mathcal{H}^{n^2}$ pode ser escrito como uma combinação linear de um vetor de $\mathcal{H}_A$ com um de $\mathcal{H}_A^{\perp}$. A ação de $\mathcal{R}_A$ faz com que a componente em $\mathcal{H}_A$ fique inalterada e com que a componente em $\mathcal{H}_A^{\perp}$ tenha o sinal invertido. Isso significa geometricamente uma *reflexão* em torno de $\mathcal{H}_A$, como se $\mathcal{H}_A$ fosse o espelho e $\mathcal{R}_A\,|\psi\rangle$ a imagem de $|\psi\rangle$. O mesmo vale para $\mathcal{R}_B$ em relação ao subespaço $\mathcal{H}_B$.

Agora vamos relacionar os subespaços $\mathcal{H}_A$ e $\mathcal{H}_B$. Podemos analisar os ângulos entre os vetores da base $\left\{ |\alpha_x\rangle : x \in X \right\}$ com os da base $\left\{ |\beta_y\rangle : y \in Y \right\}$. Para isso vamos definir a *matriz dos produtos internos* C da forma $C_{xy} = \langle \alpha_x | \beta_y \rangle$. Usando as Eqs. (5.2.23) e (5.2.24) podemos expressar as componentes de C em termos das probabilidades de transição como $C_{xy} = \sqrt{p_{xy} q_{yx}}$. E, em termos matriciais, podemos escrever C como

$$C = A^T B, \tag{5.2.37}$$

que pode ser deduzido através das Eqs. (5.2.21) e (5.2.22). C é uma matriz de dimensão n. Ela fornece informações essenciais sobre o passeio quântico que vamos definir no grafo bipartido. Se ela fosse uma matriz normal, seus autovalores e autovetores seriam as grandezas mais relevantes. Uma vez que C não é normal em geral, vamos analisar seus valores e vetores singulares, que são as grandezas conceitualmente mais próximas de autovalores e autovetores.

Exercício 5.4. *Considere o grafo bipartido completo entre os conjuntos X e Y ambos de cardinalidade 2. Encontre os vetores $|\alpha_x\rangle$ e $|\beta_y\rangle$. Eliminado a última componente, esses vetores podem ser vistos no $\mathbb{R}^3$. Esboce um cubo com um vértice na origem e o vértice oposto no ponto $(1,1,1)$ e com 3 arestas sobre os eixos x, y e z. Mostre que o espaço vetorial real $\mathbb{R}^3_A$ gerado*

pelas colunas de A é um plano vertical que contém o eixo z e corta o cubo ao meio. Mostre que o espaço vetorial real $\mathbb{R}^3_B$ gerado pelas colunas de B é um plano inclinado de $45°$ que contém o eixo y e também corta o cubo ao meio. Mostre que a intersecção desses espaços vetoriais é gerado pelo vetor

$$|\mu\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Encontre um vetor $|\psi_A\rangle$ ortogonal a $|\mu\rangle$ pertencente a $\mathbb{R}^3_A$. Encontre um vetor $|\psi_B\rangle$ ortogonal a $|\mu\rangle$ pertencente a $\mathbb{R}^3_B$. Qual é o ângulo entre $|\psi_A\rangle$ e $|\psi_B\rangle$? Seja $|\psi\rangle$ um vetor ortogonal a $|\mu\rangle$ pertencente a $\mathbb{R}^3$. Mostre que $\mathcal{R}_B\mathcal{R}_A$ gira $|\psi\rangle$ de $2\pi/3$ radianos no plano ortogonal a $|\mu\rangle$.

Exercício 5.5. *O objetivo desse exercício é generalizar as fórmulas desta seção quando a cardinalidade do conjunto X é diferente da cardinalidade do conjunto Y. Seja $|X| = m$ e $|Y| = n$, quais são as dimensões das matrizes A, B e C nesse caso? Quais fórmulas desta seção que mudam explicitamente?*

Exercício 5.6. *Considere o grafo bipartido completo onde X tem um único elemento e Y tem 2 elementos. Mostre que $\mathcal{R}_A$ é a matriz de Pauli σ_x e que $\mathcal{R}_B$ é a matriz identidade I_2.*

5.3 Valores e Vetores Singulares

O teorema da decomposição em *valores singulares* afirma que existem matrizes unitárias U e V tal que

$$C = UDV^\dagger, \tag{5.3.38}$$

onde D é uma matriz diagonal de dimensão n com componentes reais não-negativas. Usualmente os elementos na diagonal são ordenados com o maior elemento ocupando a primeira posição. Esses elementos são chamados de valores singulares e são univocamente determinados uma vez dada a matriz C. No caso geral as matrizes U e V não são univocamente determinadas. Elas podem ser determinadas através da aplicação do teorema espectral na matriz $C^\dagger C$. $C^\dagger C$ é uma matriz Hermitiana positiva semidefinida, ou seja, seus autovalores são números reais não-negativos. Consequentemente, $C^\dagger C$ admite uma decomposição espectral e a raíz quadrada $\sqrt{C^\dagger C}$ está bem definida. Na base dos autovetores de $C^\dagger C$, $\sqrt{C^\dagger C}$ é uma matriz diagonal em que cada elemento da diagonal é a raíz quadrada do autovalor correspondente de $C^\dagger C$.

Suponha que λ_i^2 e $|\nu_i\rangle$ sejam os *autovalores* e *autovetores* de $C^\dagger C$, então

$$C^\dagger C = \sum_{i=1}^{n} \lambda_i^2 \, |\nu_i\rangle \langle \nu_i| \tag{5.3.39}$$

e, consequentemente,

$$\sqrt{C^\dagger C} = \sum_{i=1}^{n} \lambda_i \, |\nu_i\rangle \langle \nu_i| \, . \tag{5.3.40}$$

Vamos mostrar como achar U e V. Para cada i tal que $\lambda_i > 0$ defina

$$|\mu_i\rangle = \frac{1}{\lambda_i} C \, |\nu_i\rangle \, . \tag{5.3.41}$$

Uma vez que tomamos $\left\{ |\nu_i\rangle : 1 \leq i \leq n \right\}$ como uma base ortonormal segue que

$$\langle \mu_i | \mu_j \rangle = \delta_{ij} \tag{5.3.42}$$

para todo i, j tal que λ_i e λ_j sejam positivos. Para os autovetores no *núcleo* de $\sqrt{C^\dagger C}$, definimos $|\mu'_j\rangle = |\nu_j\rangle$. Porém, com essa extensão perdemos no caso geral a ortogonalidade entre os vetores $|\mu_i\rangle$ e $|\mu'_j\rangle$. Podemos aplicar o procedimento de Gram-Schmidt para redefinir os vetores $|\mu'_j\rangle$ de forma que sejam ortogonais aos vetores que não pertencem ao núcleo e chamá-los de $|\mu_j\rangle$. No final, podemos obter um conjunto completo satisfazendo à condição de ortonormalidade (5.3.42). Com os vetores $|\nu_i\rangle$ e $|\mu_i\rangle$ em mãos, podemos obter U e V através das equações

$$U = \sum_{i=1}^{n} |\mu_i\rangle \langle i| \, , \tag{5.3.43}$$

$$V = \sum_{i=1}^{n} |\nu_i\rangle \langle i| \, . \tag{5.3.44}$$

$|\nu_i\rangle$ e $|\mu_i\rangle$ são os vetores singulares e λ_i os valores singulares correspondentes. Eles obedecem às seguintes equações:

$$C \, |\nu_i\rangle = \lambda_i \, |\mu_i\rangle \, , \tag{5.3.45}$$

$$C^T \, |\mu_i\rangle = \lambda_i \, |\nu_i\rangle \, , \tag{5.3.46}$$

para $1 \leq i \leq n$. Note que $|\mu_i\rangle$ e $|\nu_i\rangle$ têm um comportamento dual. De fato, eles são chamados de vetores singulares à esquerda e à direita.

Multiplicando a Eq. (5.3.45) por A e a Eq. (5.3.46) por B obtemos

$$\Pi_A B |\nu_i\rangle = \lambda_i A |\mu_i\rangle , \tag{5.3.47}$$
$$\Pi_B A |\mu_i\rangle = \lambda_i B |\nu_i\rangle . \tag{5.3.48}$$

Vimos anteriormente que a ação dos operadores A e B preservam a norma dos vetores. Como os vetores $|\mu_i\rangle$ e $|\nu_i\rangle$ são unitários, $A|\mu_i\rangle$ e $B|\nu_i\rangle$ também são unitários. A ação de projetores ou diminui a norma dos vetores ou mantém a norma invariante. Usando a Eq. (5.3.47) concluímos que os valores singulares satisfazem às inequações $0 \leq \lambda_i \leq 1$. Portanto, podem ser escritos como $\lambda_i = \cos\theta_i$ onde $0 \leq \theta_i \leq \pi/2$. A interpretação geométrica de θ_i é o ângulo entre os vetores $A|\mu_i\rangle$ e $B|\nu_i\rangle$. De fato usando as Eqs. (5.2.37) e (5.3.45) obtemos que o produto interno entre $A|\mu_i\rangle$ e $B|\nu_i\rangle$ é

$$\cos\theta_i = \langle\mu_i| A^T B |\nu_i\rangle . \tag{5.3.49}$$

Exercício 5.7. *Verifique se U e V dados pelas Eqs. (5.3.43) e (5.3.44) são unitários. Mostre que a Eq. (5.3.38) é satisfeita para esses U e V.*

Exercício 5.8. *Mostre que se $\lambda_i \neq \lambda_j$ então o espaço vetorial gerado por $A|\mu_i\rangle$ e $B|\nu_i\rangle$ será ortogonal ao espaço vetorial gerado por $A|\mu_j\rangle$ e $B|\nu_j\rangle$.*

5.4 Operador de Evolução

Agora estamos prontos para definir um passeio quântico em um grafo bipartido. Vamos definir o *operador de evolução* como

$$U_P := \mathcal{R}_B \mathcal{R}_A, \tag{5.4.50}$$

onde $\mathcal{R}_A$ e $\mathcal{R}_B$ são os operadores de reflexão dados pelas Eqs. (5.2.35) e (5.2.36). No instante t, o estado do passeio quântico será U^t aplicado ao estado inicial. Esse passeio tem uma estrutura diferente do passeio padrão descrito por um operador moeda e um operador de deslocamento. Essa nova definição tem vantagens. Em especial, o tempo de alcance quântico pode ser definido de uma forma natural como uma generalização do tempo de alcance clássico. É possível mostrar de forma genérica que o tempo de alcance para esse passeio quântico é pelo menos quadraticamente menor do que o tempo de alcance do passeio aleatório clássico no grafo equivalente.

A análise da evolução do passeio requer a obtenção da *decomposição espectral* de U_P. Sabemos que a tarefa de calcular U^t é simplificada com a decomposição espectral. Nessa nova definição de passeio quântico, a decomposição espectral associada aos autovalores não triviais pode ser calculada a partir dos valores e vetores singulares da matriz C definida na Eq. (5.2.37).

Note que apesar da definição de U_P ser nova, definições semelhantes já apareceram em outros lugares. Mostramos no Capítulo 3.1 que o operador de evolução do *algoritmo de Grover* é o produto de duas reflexões.

Exercício 5.9. *O objetivo desse exercício é analisar em que condições o estado*

$$|\psi(0)\rangle = \frac{1}{\sqrt{n}} \sum_{\substack{x\in X \\ y\in Y}} \sqrt{p_{xy}}\,|x,y\rangle$$

é autovetor de U_P associado ao autovalor 1. Mostre que a ação de $\mathcal{R}_A$ deixa $|\psi(0)\rangle$ invariante. A ação de $\mathcal{R}_B$ deixa $|\psi(0)\rangle$ invariante? Em que condições?

5.5 Decomposição Espectral do Operador de Evolução

As Eqs. (5.3.47) e (5.3.48) mostram que os projetores Π_A e Π_B têm uma ação simétrica nos vetores $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$ para cada j. É de se esperar que a ação dos operadores de reflexão $\mathcal{R}_A$ e $\mathcal{R}_B$ sobre uma combinação linear entre os vetores $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$ resulte em um vetor no plano gerado por $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$. Isto é, esse plano é invariante sob a ação de U_P. Portanto, vamos tentar o seguinte *Ansatz* para os autovetores de U_P:

$$U\big(a\,A\,|\mu_j\rangle + b\,B\,|\nu_j\rangle\big) = \lambda'_j\big(a\,A\,|\mu_j\rangle + b\,B\,|\nu_j\rangle\big). \tag{5.5.51}$$

O objetivo é encontrar a, b e λ'_j que obedeçam à Eq. (5.5.51). Usando as Eqs. (5.4.50), (5.2.35) e (5.2.36) obtemos

$$(2\,\Pi_B - I)(2\,\Pi_A - I)\big(a\,A\,|\mu_j\rangle + b\,B\,|\nu_j\rangle\big) = \lambda'_j\big(a\,A\,|\mu_j\rangle + b\,B\,|\nu_j\rangle\big). \tag{5.5.52}$$

Usando as Eqs. (5.3.47) e (5.3.48) obtemos o seguinte sistema de equações:

$$\lambda'_j\,a \;=\; -a \;-\; 2\lambda_j b, \tag{5.5.53}$$

$$\lambda'_j\,b \;=\; 2\lambda_j a + (4\lambda_j^2 - 1)b, \tag{5.5.54}$$

desde que $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$ sejam linearmente independentes, isto é, não-colineares. Vamos impor que $\theta_j \neq 0$, pois da Eq. (5.3.49) sabemos que θ_j é o ângulo entre $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$. Usando $\lambda_j = \cos\theta_j$, o sistema de equações acima impõe que

$$\lambda'_j = \mathrm{e}^{\pm 2i\theta_j}. \tag{5.5.55}$$

Usando a Eq. (5.5.53), obtemos

$$\begin{aligned} \frac{b}{a} &= -\frac{1+\mathrm{e}^{\pm 2\,i\theta_j}}{2\cos(\theta_j)} \\ &= -\mathrm{e}^{\pm\, i\theta_j}. \end{aligned} \tag{5.5.56}$$

Portanto, os vetores

$$\left|\theta_j^{\pm}\right\rangle = \frac{A\left|\mu_j\right\rangle - \mathrm{e}^{\pm\, i\theta_j} B\left|\nu_j\right\rangle}{\sqrt{2}\sin\theta_j} \tag{5.5.57}$$

são autovetores normalizados de U_P associados aos autovalores $\mathrm{e}^{\pm 2i\theta_j}$ quando $0 < \theta_j \leq \pi/2$.

Os vetores $A\left|\mu_j\right\rangle$ e $B\left|\nu_j\right\rangle$ só serão linearmente independentes se $\lambda_j \neq 1$. Quando $A\left|\mu_j\right\rangle$ e $B\left|\nu_j\right\rangle$ são colineares, a Eq. (5.5.57) não fornece a expressão para os autovetores associados a $\lambda_j = 1$. No entanto, como $A\left|\mu_j\right\rangle$ é invariante por Π_A, $B\left|\nu_j\right\rangle$ também é. E vice-versa, como $B\left|\nu_j\right\rangle$ é invariante por Π_B, $A\left|\mu_j\right\rangle$ também é. Portanto, $A\left|\mu_j\right\rangle$ e $B\left|\nu_j\right\rangle$ são invariantes por $\mathcal{R}_A$ e $\mathcal{R}_B$ e são autovetores de U_P com autovalor 1. O número de autovetores de autovalor 1 que podemos encontrar por esse método vai depender da multiplicidade do valor singular 1. Seja k a multiplicidade do valor singular 1, a Tabela 5.1 compila os resultados sobre a decomposição espectral de U_P obtidos até agora. Já encontramos $2n-k$ autovetores de U_P, onde os $2(n-k)$ primeiros estão associados aos autovalores $\mathrm{e}^{\pm 2i\theta_j}$ e os k autovetores restantes estão associados ao autovalor 1.

$\mathcal{H}_A$ e $\mathcal{H}_B$ são os espaços vetoriais gerados pelas colunas da matriz A e B, respectivamente, ou seja, $\mathcal{H}_A$ é gerado pelos vetores $\left|\alpha_x\right\rangle$, $x \in X$ e $\mathcal{H}_B$ é gerado pelos vetores $\left|\beta_y\right\rangle$, $y \in Y$. Tanto $\mathcal{H}_A$ quanto $\mathcal{H}_B$ são subespaços de $\mathcal{H}^{n^2}$ de dimensão n. Seja $\mathcal{H}_{A,B}$ o espaço vetorial gerado pelos vetores $\left|\alpha_x\right\rangle$ e $\left|\beta_y\right\rangle$, a dimensão de $\mathcal{H}_{A,B}$ é no máximo $2n$. A dimensão de $\mathcal{H}_{A,B}$ será exatamente $2n$ se $A\left|\mu_j\right\rangle$ e $B\left|\nu_j\right\rangle$ forem linearmente independentes para todo j. Para cada j tal que $\lambda_j = 1$, a dimensão de $\mathcal{H}_{A,B}$ é reduzida de 1. Por outro lado, a dimensão de $\mathcal{H}_{A,B}$ é $2n$ menos a dimensão de $\mathcal{H}_A \cap \mathcal{H}_B$. Portanto, os autovetores $\left|\theta_j\right\rangle$, para $1 \leq j \leq k$, geram o subespaço $\mathcal{H}_A \cap \mathcal{H}_B$ e $\left|\theta_j^{\pm}\right\rangle$, para $k+1 \leq j \leq n$, geram o espaço ortogonal a $\mathcal{H}_A \cap \mathcal{H}_B$ em $\mathcal{H}_{A,B}$.

O conjunto de autovetores encontrados não forma uma *base*. Faltam $n^2 - 2n + k$ autovetores que pertencem ao espaço vetorial ortogonal a $\mathcal{H}_{A,B}$, isto é, $\mathcal{H}_A^{\perp} \cap \mathcal{H}_B^{\perp}$. Esses autovetores estão associados aos autovalores 1, pois tanto o projetor Π_A como Π_B anulam um vetor $\left|\psi\right\rangle$ que esteja no espaço ortogonal tanto a $\mathcal{H}_A$ como $\mathcal{H}_B$. Consequentemente, $\mathcal{R}_A\left|\psi\right\rangle = -\left|\psi\right\rangle$ e $\mathcal{R}_B\left|\psi\right\rangle = -\left|\psi\right\rangle$. Como $U = \mathcal{R}_B\mathcal{R}_A$, segue que $U\left|\psi\right\rangle = \left|\psi\right\rangle$. Uma base de vetores ortonormais para espaço $\mathcal{H}_A^{\perp} \cap \mathcal{H}_B^{\perp}$ completa a decomposição espectral de

Autovalor	Autovetor	Intervalo
$\mathrm{e}^{\pm 2i\theta_j}$	$\left\|\theta_j^{\pm}\right\rangle = \frac{A\|\mu_j\rangle - \mathrm{e}^{\pm\, i\theta_j} B\|\nu_j\rangle}{\sqrt{2}\sin\theta_j}$	$1 \leq j \leq n-k$
1	$\|\theta_j\rangle = A\,\|\mu_j\rangle$	$n-k+1 \leq j \leq n$
1	$\|\theta_j\rangle =$ sem expr.	$2n-k+1 \leq j \leq n$

Tabela 5.1: Autovalores e autovetores normalizados de $U_{P'}$ obtidos a partir dos valores e vetores singulares de C, onde k é a multiplicidade do valor singular 1 de C e n é a dimensão de C. Os ângulos θ_j são obtidos a partir dos valores singulares λ_j através da fórmula $\cos\theta_j = \lambda_j$. Os autovetores $|\theta_j\rangle$ para $2n-k+1 \leq j \leq n$ não podem ser obtidos pelo método desta seção, porém sabemos que estão associados ao autovalor 1.

U_P. O método dos valores e vetores singulares não serve para calcular esses autovetores restantes, no entanto, vamos mostrar adiante que somente os autovetores associados aos autovalores diferentes de 1 contribuem para o cálculo do tempo de alcance.

Exercício 5.10. *Mostre que se o valor singular λ_j for igual a 0, então $A\,|\mu_j\rangle$ e $B\,|\nu_j\rangle$ serão autovetores ortonormais associados ao autovalor -1 de U_P.*

Exercício 5.11. *Usando os autovetores da Tabela 5.1, calcule uma base de autovetores do operador de evolução U_P associado ao grafo do Exercício 5.4 referente ao subespaço $\mathcal{H}_{A,B}$. Ache uma base para $\mathcal{H}_{A,B}^{\perp}$ e verifique se os vetores dessa base são autovetores de U_P associado ao autovalor 1. Verifique se algum autovalor tem multiplicidade maior que 1 e caracterize completamente os autovetores de U_P.*

5.6 Tempo de Alcance Quântico

Vamos definir o *tempo de alcance quântico* no *grafo* $\Gamma(X, E)$ conexo, não-direcionado e não-bipartido como uma generalização natural do conceito clássico. Para isto, vamos definir um grafo bipartido associado a $\Gamma(X, E)$ através de um processo de duplicação. X e Y são os conjuntos de vértices de mesma cardinalidade do grafo bipartido. Cada aresta $\{x_i, x_j\}$ pertencente

a E do grafo original, que liga os vértices adjacentes x_i e x_j, corresponde a duas arestas no grafo bipartido $\{x_i, y_j\}$ e $\{y_i, x_j\}$. Na Fig. 5.1 temos um exemplo de um grafo não-direcionado (primeiro grafo) e seu grafo bipartido associado (segundo grafo). Em relação a notação usada na Sec. 5.2, temos que $p_{xy} = q_{xy}$ e $p_{xy} = p_{yx}$, pois o grafo bipartido é não-direcionado e existe uma identificação entre X e Y.

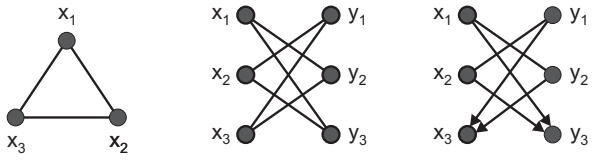

Figura 5.1: Exemplo de um grafo conexo com 3 vértices, seu grafo bipartido gerado pelo processo de duplicação e o grafo bipartido direcionado supondo que x_3 é o único vértice marcado. O tempo de alcance quântico é definido para o primeiro grafo, porém o passeio quântico se processa no terceiro grafo.

O passeio quântico no grafo bipartido é definido pelo operador de evolução U_P dado pela Eq. (5.4.50). No grafo bipartido, uma aplicação de U_P corresponde a dois passos do passeio quântico, de X para Y e de Y para X. Temos que tomar o traço parcial sobre o espaço associado a Y para obtermos o estado do passeio quântico no conjunto X.

Para definir o tempo de alcance quântico, vamos usar um segundo operador de evolução associado a um grafo bipartido direcionado modificado a partir do grafo bipartido original. Esse processo é semelhante ao método usado para o cálculo do tempo de alcance clássico sem usar a distribuição estacionária descrito na Sec. 5.1.2. O grafo direcionado modificado é obtido a partir do grafo bipartido original removendo-se todas as arestas direcionadas que saem dos vértices marcados, porém mantendo as arestas direcionadas que chegam. O terceiro grafo da Fig. 5.1 é um exemplo onde o conjunto $M = \{x_3\}$ tem um único elemento. Note que se x_3 for um vértice marcado, y_3 também será pelo processo de duplicação. Todas as arestas que saem de x_3 e y_3 foram removidas. Isto quer dizer que se o caminhante atingir um vértice marcado, ele ficará preso neste vértice marcado nos passos seguintes.

Vimos na Sec. 5.1.2 que o grafo não-direcionado original e o grafo direcionado modificado são equivalentes para o cálculo do tempo de alcance clássico. No caso quântico, para definir o tempo de alcance no grafo original, o passeio quântico se processa no grafo direcionado modificado através do operador de evolução U_P, onde P é a matriz de probabilidades modificada

dada por

$$p_{xy} = \begin{cases} p'_{xy}, & x \notin M; \\ \delta_{xy}, & x \in M, \end{cases} \tag{5.6.58}$$

onde p'_{xy} são as componentes da matriz de probabilidades P' do grafo bipartido não-direcionado. Como estamos usando o operador U_P do grafo direcionado, se a condição inicial for a *distribuição uniforme*, as probabilidades associadas aos vértices marcados aumentam periodicamente. Para achar um vértice marcado, devemos medir a posição do caminhante no primeiro instante em que a probabilidade aumenta. O tempo de alcance é adequado para quantificar em que instante devemos medir a posição do caminhante.

A condição inicial do passeio quântico é

$$|\psi(0)\rangle = \frac{1}{\sqrt{n}} \sum_{\substack{x \in X \\ y \in Y}} \sqrt{p'_{xy}}\, |x, y\rangle \,. \tag{5.6.59}$$

Note que $|\psi(0)\rangle$ é definido usando a matriz de probabilidades do grafo original e portanto é invariante sob a ação de $U_{P'}$ referente ao grafo original, quando a distribuição de probabilidades p'_{xy} é simétrica, isto é, $|\psi(0)\rangle$ é um autovetor de $U_{P'}$ associado ao autovalor 1. No entanto, $|\psi(0)\rangle$ não é um autovetor de U_P em geral. Agora vamos definir o tempo de alcance quântico.

Definição 5.1. *(Tempo de Alcance Quântico) O tempo de alcance quântico $H_{P',M}$ de um passeio quântico em um grafo com o operador de evolução associado $U_{P'}$ partindo da condição inicial $|\psi(0)\rangle$ é definido como o menor número de passos T tal que*

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

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

$$F(T) = \frac{1}{T+1} \sum_{t=0}^{T} \Big\| \, |\psi(t)\rangle - |\psi(0)\rangle \, \Big\|^2, \tag{5.6.60}$$

onde $|\psi(t)\rangle$ é o estado quântico no passo t do passeio no grafo modificado com a matriz de probabilidades P, isto é, $|\psi(t)\rangle = (U_P)^t \, |\psi(0)\rangle$.

5.7 Tempo de Alcance no Grafo Completo

O objetivo desta seção é calcular o tempo de alcance quântico no *grafo completo* de n vértices. O grafo completo tem todos os vértices adjacentes entre si. Se o caminhante está em um dos vértices, ele pode ir para $n-1$ vértices. Portanto, a matriz de probabilidades do grafo é

$$P' = \frac{1}{n-1}\begin{bmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 0 \end{bmatrix}. \tag{5.7.61}$$

A matriz $(n-1)P'$ é igual a uma matriz com componentes iguais a 1 menos a matriz identidade. Portanto, podemos escrever P' da seguinte forma

$$P' = \frac{1}{n-1}\left(n\left|u^{(n)}\right\rangle\left\langle u^{(n)}\right| - I_n\right), \tag{5.7.62}$$

onde $\left|u^{(j)}\right\rangle$ é o vetor

$$\left|u^{(j)}\right\rangle = \frac{1}{\sqrt{j}}\sum_{i=1}^{j}|i\rangle\,. \tag{5.7.63}$$

Vamos numerar os vértices de 1 até n, de forma que nesta seção a base computacional do espaço de Hilbert $\mathcal{H}^n$ seja $\left\{\,|1\rangle\,,\cdots,|n\rangle\,\right\}$. Os vértices marcados serão os m últimos vértices, isto é, $x \in M$ se e somente se $n-m < x \leq n$.

Na definição de tempo de alcance quântico, o operador de evolução usa a matriz de probabilidades modificada P definida na Eq. (5.6.58) em vez da matriz original P'. As componentes da matriz P são

$$p_{xy} = \begin{cases} \frac{1-\delta_{xy}}{n-1}, & 1 \leq x \leq n-m; \\ \delta_{xy}, & n-m < x \leq n. \end{cases} \tag{5.7.64}$$

Todos os vetores e operadores da Sec. 5.2 devem ser calculados usando P. O operador C da Eq. (5.2.37) é o mais importante, pois seus valores e vetores singulares são usados para calcular uma parte dos autovetores do operador de evolução U_P. Na Sec. 5.2 vimos que as componentes C_{xy} são dadas por $\sqrt{p_{xy}q_{yx}}$. Aqui estamos tomando $q_{yx} = p_{yx}$. No grafo completo temos que $p'_{xy} = p'_{yx}$. No entanto, $p_{xy} \neq p_{yx}$ se x e y estão em M. Usando a Eq. (5.7.64) e analisando os valores das componentes de C concluímos que

$$C = \begin{bmatrix} P_{\overline{M}} & 0 \\ 0 & I_m \end{bmatrix}, \tag{5.7.65}$$

onde $P_{\overline{M}}$ é obtida da matriz P' da Eq. (5.7.61) eliminando-se as m linhas e colunas correspondentes aos m vértices marcados. Podemos encontrar os valores e vetores singulares de C através da decomposição espectral de $P_{\overline{M}}$.

A expressão algébrica de $P_{\overline{M}}$ é

$$P_{\overline{M}} = \frac{1}{n-1}\left((n-m)\left|u^{(n-m)}\right\rangle\left\langle u^{(n-m)}\right| - I_{n-m}\right), \tag{5.7.66}$$

onde $\left|u^{(n-m)}\right\rangle$ é obtido através da Eq. (5.7.63). Seu polinômio característico é

$$\det(P_{\overline{M}} - \lambda I) = \left(\lambda - \frac{n-m-1}{n-1}\right)\left(\lambda + \frac{1}{n-1}\right)^{n-m-1}. \tag{5.7.67}$$

Os autovalores são $\frac{n-m-1}{n-1}$ com multiplicidade 1 e $\frac{-1}{n-1}$ com multiplicidade $n-m-1$. Note que se $m \geq 1$, então 1 não é autovalor de $P_{\overline{M}}$. O autovetor associado ao autovalor $\frac{n-m-1}{n-1}$ é

$$|\nu_{n-m}\rangle := \left|u^{(n-m)}\right\rangle \tag{5.7.68}$$

e os autovetores associados ao autovalor $\frac{-1}{n-1}$ são

$$|\nu_i\rangle := \frac{1}{\sqrt{i+1}}\left(\left|u^{(i)}\right\rangle - \sqrt{i}\,|i+1\rangle\right), \tag{5.7.69}$$

onde $1 \leq i \leq n-m-1$. O conjunto $\left\{|\nu_i\rangle, 1 \leq i \leq n-m\right\}$ forma uma base ortonormal de autovetores de $P_{\overline{M}}$. A verificação está orientada no Exercício 5.12.

Exercício 5.12. *O objetivo deste exercício é verificar explicitamente a ortonormalidade da decomposição espectral de $P_{\overline{M}}$.*

1. *Use a Eq. (5.7.66) para verificar que $P_{\overline{M}}|u^{n-m}\rangle = \frac{n-m-1}{n-1}|u^{n-m}\rangle$.*

2. *Mostre que $\left\langle u^{(n-m)}\middle|\nu_i\right\rangle = 0$, para $1 \leq i \leq n-m-1$. Use este fato e a Eq. (5.7.66) para verificar que $P_{\overline{M}}|\nu_i\rangle = \frac{-1}{n-1}|\nu_i\rangle$.*

3. *Mostre que $\left\langle u^{(i)}\middle|i+1\right\rangle = 0$ e conclua que $\left\langle u^{(i)}\middle|u^{(i)}\right\rangle = 1$, para $1 \leq i \leq n-m-1$. Use este fato para mostrar que $\left\langle \nu_i\middle|\nu_i\right\rangle = 1$.*

4. *Suponha que $i < j$. Mostre que $\left\langle u^{(i)}\middle|u^{(j)}\right\rangle = \sqrt{\frac{i}{j}}$ e que $\left\langle u^{(i)}\middle|j+1\right\rangle = 0$. Use estes fatos para mostrar que $\left\langle \nu_i\middle|\nu_j\right\rangle = 0$.*

A matriz C é hermitiana. Portanto, os valores singulares λ_i não-triviais de C definidos na Eq. (5.3.40) são obtidos tomando o módulo dos autovalores de $P_{\overline{M}}$. O vetores singulares à direita $|\nu_i\rangle$ são os autovetores de $P_{\overline{M}}$ e os vetores singulares à esquerda são obtidos a partir da Eq. (5.3.41). Se o autovalor de $P_{\overline{M}}$ for negativo, o vetor singular à esquerda é o negativo do autovetor de $P_{\overline{M}}$. Estes vetores devem ser aumentados com m zeros para terem a dimensão compatível com C. Finalmente, a submatriz I_m na Eq. (5.7.65) acrescenta à lista o valor singular 1 com multiplicidade m com os vetores singulares associados $|j\rangle$, onde $n-m+1 \leq j \leq n$. A Tabela 5.2 resume estes resultados.

Valor singular	Vetor singular à direita	Vetor singular à esquerda	Intervalo
$\cos\theta_1 = \frac{1}{n-1}$	$\|\nu_j\rangle$	$-\|\nu_j\rangle$	$1 \leq j \leq n-m-1$
$\cos\theta_2 = \frac{n-m-1}{n-1}$	$\|\nu_{n-m}\rangle$	$\|\nu_{n-m}\rangle$	$j = n-m$
$\cos\theta_3 = 1$	$\|j\rangle$	$\|j\rangle$	$n-m+1 \leq j \leq n$

Tabela 5.2: Valores e vetores singulares à direita e esquerda da matriz C. Os vetores $|\nu_{n-m}\rangle$ e $|\nu_i\rangle$ são dados pelas Eqs. (5.7.68) e (5.7.69). Os ângulos θ_1, θ_2 e θ_3 são definidos a partir dos valores singulares.

Autovalores e autovetores de U_P, que podem obtidos a partir dos valores e vetores singulares de C, são dados pela Tabela 5.1. A Tabela 5.3 reproduz estes resultados para o grafo completo. Ficam faltando $n^2 - 2n + m$ autovetores todos associados ao autovalor 1.

A condição inicial é dada pela Eq. (5.6.59), que no grafo completo se reduz a

$$|\psi(0)\rangle = \frac{1}{\sqrt{n(n-1)}} \sum_{x,y=1}^{n} (1-\delta_{xy})\,|x\rangle\,|y\rangle\,. \tag{5.7.70}$$

Apenas os autovetores de U_P que não são ortogonais à condição inicial $|\psi(0)\rangle$ participam da dinâmica. O Exercício 5.13 orienta a prova de que os autovetores $|\theta_j\rangle$, onde $n-m+1 \leq j \leq n$ são ortogonais à condição inicial. O Exercício 5.14 orienta a prova de que os autovetores $\left|\theta_j^{\pm}\right\rangle$, onde $1 \leq j \leq n-m-1$ também são ortogonais à condição inicial. Sobram apenas os dois autovetores $\left|\theta_{n-m}^{\pm}\right\rangle$ associados ao autovalor positivo de $P_{\overline{M}}$ e os autovetores associados ao autovalor 1 que ainda não foram considerados.

Autovalor	Autovetor	Intervalo
$\mathrm{e}^{\pm 2i\theta_1}$	$\left\|\theta_j^{\pm}\right\rangle = \frac{-\left(A+\mathrm{e}^{\pm i\theta_1}B\right)\|\nu_j\rangle}{\sqrt{2}\sin\theta_1}$	$1 \leq j \leq n-m-1$
$\mathrm{e}^{\pm 2i\theta_2}$	$\left\|\theta_{n-m}^{\pm}\right\rangle = \frac{\left(A-\mathrm{e}^{\pm i\theta_2}B\right)\|\nu_{n-m}\rangle}{\sqrt{2}\sin\theta_2}$	$j = n-m$
1	$\|\theta_j\rangle = A\,\|j\rangle$	$n-m+1 \leq j \leq n$

Tabela 5.3: Autovalores e autovetores normalizados de U_P obtidos a partir dos valores e vetores singulares de C.

Portanto, a condição inicial $|\psi(0)\rangle$ pode ser escrita como

$$|\psi(0)\rangle = c^+\left|\theta_{n-m}^+\right\rangle + c^-\left|\theta_{n-m}^-\right\rangle + |\beta\rangle\,, \tag{5.7.71}$$

onde os coeficientes $c^{\pm}$ são dados por (ver Exercício 5.15)

$$c^{\pm} = \frac{\sqrt{n-m}\,\left(1-\mathrm{e}^{\mp i\theta_2}\right)}{\sqrt{2n}\,\sin\theta_2}, \tag{5.7.72}$$

onde o ângulo θ_2 é definido por

$$\cos\theta_2 = \frac{n-m-1}{n-1}. \tag{5.7.73}$$

O vetor $|\beta\rangle$ é a componente de $|\psi(0)\rangle$ no autoespaço de autovalor 1. O cálculo da base de autovetores para este autoespaço é trabalhoso, vamos adiar este cálculo por enquanto.

Exercício 5.13. *Para mostrar que* $\langle\theta_j|\psi(0)\rangle = 0$ *quando* $n-m+1 \leq j \leq n$, *use a expressão de A dada pela Eq. (5.2.21) e a expressão de* $|\alpha_x\rangle$ *dada pela Eq. (5.2.23), onde* p_{xy} *e* q_{xy} *são dados pela Eq. (5.7.64). Mostre que*

$$\langle\theta_j|\psi(0)\rangle = \sum_{x\in M}\langle\alpha_x|\psi(0)\rangle\,.$$

Use a Eq. (5.7.70) e mostre que $\langle\alpha_x|\psi(0)\rangle = 0$ *se* $x \in M$.

Exercício 5.14. *Para mostrar que* $\langle\theta_j^{\pm}|\psi(0)\rangle = 0$ *para* $1 \leq j \leq n-m-1$*, use as expressões de A e B dadas pelas Eqs. (5.2.21) e (5.2.22) e as expressões de* $|\alpha_x\rangle$ *e* $|\beta_y\rangle$ *dadas pelas Eqs. (5.2.23) e (5.2.24), onde* p_{xy} *e* q_{xy} *são dados pela Eq. (5.7.64). A Eq. (5.7.69) e o Exercício 5.12 também devem ser usados. A expressão de* $|\psi(0)\rangle$ *é dada pela Eq. (5.7.70).*

Exercício 5.15. *O objetivo deste exercício é orientar o cálculo dos coeficientes* $c^{\pm}$ *da Eq. (5.7.71), que são definidos por*

$$c^{\pm} = \langle\theta_{n-m}^{\pm}|\psi(0)\rangle\,.$$

Use as Eqs. (5.7.70) e (5.7.80), cancele os termos ortogonais e simplifique o resultado.

Aplicando U_P^t em $|\psi(0)\rangle$, dado pela Eq. (5.7.71) e usando o fato de que $|\theta_{n-m}^{\pm}\rangle$ são autovetores associados aos autovalores $\mathrm{e}^{\pm 2i\theta_2}$ e $|\beta\rangle$ está no autoespaço associado ao autovalor 1 obtemos

$$\begin{aligned} |\psi(t)\rangle &= U_P^t\,|\psi(0)\rangle \\ &= c^{+}\mathrm{e}^{2i\theta_2 t}\,|\theta_{n-m}^{+}\rangle + c^{-}\mathrm{e}^{-2i\theta_2 t}\,|\theta_{n-m}^{-}\rangle + |\beta\rangle\,, \end{aligned} \tag{5.7.74}$$

A partir da expressão de $|\psi(t)\rangle$ podemos calcular a seguinte quantidade que é usada para obter o tempo de alcance

$$F(T) = \frac{1}{T+1}\sum_{t=0}^{T}\Big\|\,|\psi(t)\rangle - |\psi(0)\rangle\,\Big\|^2. \tag{5.7.75}$$

A diferença $|\psi(t)\rangle - |\psi(0)\rangle$ pode ser calculada da seguinte forma. Usando as Eqs. (5.7.71) e (5.7.74) obtemos

$$|\psi(t)\rangle - |\psi(0)\rangle = c^{+}(\mathrm{e}^{2i\theta_2 t}-1)\,|\theta_{n-m}^{+}\rangle + c^{-}(\mathrm{e}^{-2i\theta_2 t}-1)\,|\theta_{n-m}^{-}\rangle \tag{5.7.76}$$

e usando a Eq. (5.7.72) obtemos

$$\begin{aligned} \Big\|\,|\psi(t)\rangle - |\psi(0)\rangle\,\Big\|^2 &= \big|c^{+}(\mathrm{e}^{2i\theta_2 t}-1)\big|^2 + \big|c^{-}(\mathrm{e}^{-2i\theta_2 t}-1)\big|^2 \\ &= \frac{4(n-1)(n-m)}{n(2n-m-2)}\left(1 - T_{2t}\left(\frac{n-m-1}{n-1}\right)\right), \end{aligned}$$

onde T_n são os *polinômios de Chebyshev* do primeiro tipo definidos por $T_n(\cos\theta) = \cos n\theta$. Tomando a média e usando que

$$\sum_{t=0}^{T} T_{2t}\left(\frac{n-m-1}{n-1}\right) = \frac{1}{2} + \frac{1}{2}\,U_{2T}\left(\frac{n-m-1}{n-1}\right) \tag{5.7.77}$$

obtemos

$$F(T) = \frac{2\,(n-1)\,(n-m)\left(2\,T+1-U_{2T}\left(\frac{n-m-1}{n-1}\right)\right)}{n\,(2\,n-m-2)\,(T+1)}, \tag{5.7.78}$$

onde U_n são os polinômios de Chebyshev do segundo tipo definidos por $U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}$. O gráfico da Fig. 5.2 mostra o comportamento da função $F(T)$. $F(T)$ cresce rapidamente passando pela linha tracejada, depois oscila em torno do valor limite que é dado por $\frac{4(n-1)(n-m)}{n(2\,n-m-2)}$.

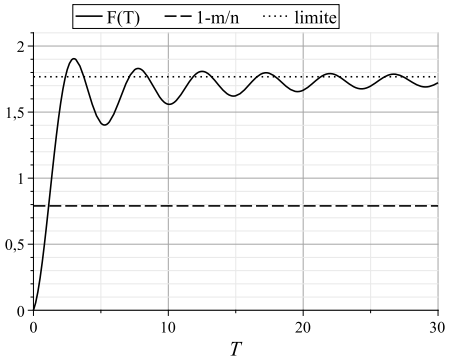

Figura 5.2: Gráficos da função $F(T)$ (linha contínua), da reta $1-\frac{m}{n}$ (linha tracejada) e da reta $\frac{4(n-1)(n-m)}{n(2\,n-m-2)}$ (linha pontilhada) para $n = 100$ e $m = 21$. O tempo de alcance pode ser visto no gráfico pelo instante T tal que $F(T) = 1-\frac{m}{n}$, que é aproximadamente 1.13.

Para $n \gg m$, podemos obter o tempo de alcance $H_{P',M}$ por inversão de séries de Laurent a partir da equação $F(T) = 1-\frac{m}{n}$. Os primeiros termos são

$$H_{P',M} = \frac{j_0^{-1}\left(\frac{1}{2}\right)}{2}\sqrt{\frac{n}{2\,m}} - \frac{\sqrt{1-\frac{1}{4}\,j_0^{-1}\left(\frac{1}{2}\right)^2}}{1+2\sqrt{1-\frac{1}{4}\,j_0^{-1}\left(\frac{1}{2}\right)^2}} + O\left(\frac{1}{\sqrt{n}}\right) \tag{5.7.79}$$

onde j_0 é a primeira função de Bessel esférica ou a função *sinc* não-normalizada. O valor de $j_0^{-1}\left(\frac{1}{2}\right)$ é aproximadamente 1.9.

Exercício 5.16. *O objetivo deste exercício é obter a Eq. (5.7.77). Use a representação trigonométrica de T_n e converta o cosseno em termos de uma soma de exponenciais com argumentos complexos. Use a fórmula da progressão geométrica $\sum_{t=0}^{T} a^t = \frac{a^{T+1}-1}{a-1}$ para simplificar o somatório. Converta o resultado na forma de polinômios de Chebyshev do segundo tipo.*

5.7.1 Probabilidade de achar um elemento marcado

O tempo de alcance é usado em algoritmos de busca como o instante de parada. É importante calcular a probabilidade de sucesso quando usamos o tempo de alcance. O cálculo da probabilidade de encontrarmos um elemento marcado em função do tempo é mais elaborado do que o cálculo do tempo de alcance, pois temos que calcular $|\psi(t)\rangle$ explicitamente, ou seja, temos que calcular os vetores $\left|\theta_{n-m}^{\pm}\right\rangle$ e $|\beta\rangle$.

Usando as Eqs. (5.2.21) e (5.2.22) obtemos

$$\begin{aligned}\left|\theta_{n-m}^{\pm}\right\rangle &= \frac{1}{\sqrt{2}\sin\theta_2}\left(A - \mathrm{e}^{\pm i\theta_2}B\right)\left|u^{(n-m)}\right\rangle \\ &= \frac{1}{\sqrt{2(n-m)}\sin\theta_2}\left(\sum_{x=1}^{n-m}|\alpha_x\rangle - \mathrm{e}^{\pm i\theta_2}\sum_{y=1}^{n-m}|\beta_y\rangle\right)\end{aligned}$$

Usando as Eqs. (5.2.23), (5.2.24) e (5.7.64) obtemos

$$\begin{aligned}\left|\theta_{n-m}^{\pm}\right\rangle = \frac{1}{\sqrt{2(n-1)(n-m)}\,\sin\theta_2}\Bigg(&\left(1-\mathrm{e}^{\pm i\theta_2}\right)\sum_{x,y=1}^{n-m}\left(1-\delta_{xy}\right)|x\rangle\,|y\rangle + \\ &\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}|x\rangle\,|y\rangle - \mathrm{e}^{\pm i\theta_2}\sum_{x=n-m+1}^{n}\sum_{y=1}^{n-m}|x\rangle\,|y\rangle\Bigg). \qquad (5.7.80)\end{aligned}$$

Usando as Eqs. (5.7.72) e (5.7.73), a expressão para a função de onda no instante t se reduz a

$$\begin{aligned}|\psi(t)\rangle = \frac{1}{\sqrt{n(n-1)}}\Bigg(&\frac{2(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2}\sum_{x,y=1}^{n-m}\left(1-\delta_{xy}\right)|x\rangle\,|y\rangle + \\ &\left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2} - U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}|x\rangle\,|y\rangle + \\ &\left(\frac{(n-1)T_{2t}\left(\frac{n-m-1}{n-1}\right)}{2\,n-m-2} + U_{2t-1}\left(\frac{n-m-1}{n-1}\right)\right)\sum_{x=n-m+1}^{n}\sum_{y=1}^{n-m}|x\rangle\,|y\rangle\Bigg) + \\ &\sum_{j=n-k+1}^{n^2-n+k}c_j\,|\alpha_j\rangle\,. \qquad (5.7.81)\end{aligned}$$

O vetor $|\beta\rangle$ como um todo ser determinado por tentativa e erro analisando

diretamente a estrutura da matriz U_P. O resultado é

$$\begin{aligned}|\beta\rangle &= \frac{1}{\sqrt{n(n-1)}}\left(\frac{-m}{2n-m-2}\sum_{x,y=1}^{n-m}(1-\delta_{xy})\,|x\rangle\,|y\rangle + \right.\\ &\quad \frac{n-m-1}{2n-m-2}\sum_{x=1}^{n-m}\sum_{y=n-m+1}^{n}\left(\,|x\rangle\,|y\rangle + |y\rangle\,|x\rangle\,\right) + \\ &\quad \left.\sum_{x,y=n-m+1}^{n}(1-\delta_{xy})\,|x\rangle\,|y\rangle\right). \qquad (5.7.82)\end{aligned}$$

A probabilidade de encontrarmos um elemento marcado é calculada com uma medida que usa o *projetor* $\mathcal{P}_{\overline{M}}$ no espaço vetorial gerado pelos elementos marcados, isto é

$$\begin{aligned}\mathcal{P}_{\overline{\mathcal{M}}} &= \sum_{x=n-m+1}^{n}|x\rangle\,\langle x|\otimes I \\ &= \sum_{x=n-m+1}^{n}\sum_{y=1}^{n}|x,y\rangle\,\langle x,y|\,. \qquad (5.7.83)\end{aligned}$$

A probabilidade é dada por $\langle\psi(t)|\,\mathcal{P}_{\overline{\mathcal{M}}}|\psi(\sqcup)\rangle$. Usando a Eq. (5.7.81) obtemos

$$\begin{aligned}p_M(t) &= \frac{m(m-1)}{n(n-1)}+\frac{m(n-m)}{n(n-1)}\left(\frac{n-1}{2\,n-m-2}T_{2t}\left(\frac{n-m-1}{n-1}\right)+\right.\\ &\quad \left.U_{2t-1}\left(\frac{n-m-1}{n-1}\right)+\frac{n-m-1}{2n-m-2}\right)^2 \qquad (5.7.84)\end{aligned}$$

cujo gráfico está mostrado na Fig. 5.3 para $n = 100$ e $m = 21$.

Derivando a função $p_M(t)$ em função do tempo, podemos determinar os pontos críticos. O primeiro ponto de máximo ocorre no instante

$$t_{\max}=\frac{\arctan\left(\dfrac{\sqrt{2n-m-2}}{\sqrt{m}}\right)}{2\arccos\left(\dfrac{n-m-1}{n-1}\right)}, \qquad (5.7.85)$$

cuja expansão assintótica é

$$t_{\max}=\frac{\pi}{4}\sqrt{\frac{n}{2\,m}}-\frac{1}{4}+O\left(\sqrt{\frac{m}{n}}\right). \qquad (5.7.86)$$

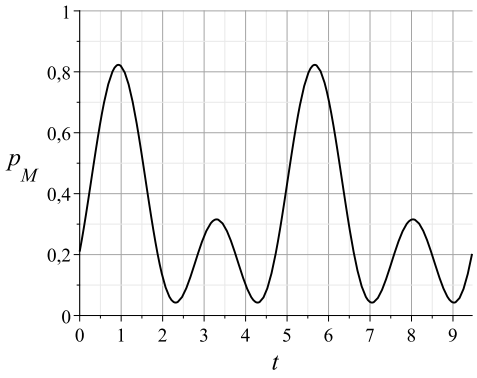

Figura 5.3: Gráfico da probabilidade de achar um vértice marcado em função do tempo para $n = 100$ e $m = 21$. O valor inicial é $\frac{m}{n}$ e a função tem período $\frac{\pi}{\theta_2}$.

Substituindo na expressão da probabilidade obtemos

$$p_M(t_{\max}) = \frac{1}{2} + \sqrt{\frac{m}{2\,n}} + O\left(\frac{m}{n}\right). \tag{5.7.87}$$

Para quaisquer valores de n e m, a probabilidade de encontrar o vértice marcado é maior que $\frac{1}{2}$ caso a medida seja realizada no instante $t_{\max}$. O instante $t_{\max}$ é menor que o tempo de alcance dado pela Eq. (5.7.79), pois $\frac{\pi}{4\sqrt{2}} \approx 0.56$ enquanto que $\frac{j_0^{-1}\left(\frac{1}{2}\right)}{2\sqrt{2}} \approx 0.67$. O valor da probabilidade de acerto em um algoritmo que use o tempo de alcance como ponto de parada será menor que a probabilidade no instante $t_{\max}$. Avaliando p_M no instante H e tomando a expansão assintótica obtemos

$$p_M(H_{P,M}) = \frac{1}{8}\, j_0^{-1} \left(\frac{1}{2}\right)^2 + O\left(\frac{1}{\sqrt{n}}\right). \tag{5.7.88}$$

O primeiro termo é aproximadamente 0.45 e não depende de n ou m. Isto mostra que o tempo de alcance no grafo completo é um bom parâmetro para o ponto de parada do algoritmo de busca.

Exercício 5.17. *Usando a Eq. (5.7.84) mostre que*

1. *$p_M(t)$ é uma função periódica com período $\frac{\pi}{\theta_2}$.*
2. *os pontos de máximos para $t \geq 0$ são dados por*

$$t_j = \frac{1}{2\theta_2} \arctan\left(\frac{1+\cos\theta_2}{\sin\theta_2}\right) + \frac{j\pi}{2\theta_2}$$

onde $j = 0, 1, \cdots$.

Sugestões para Leitura

A teoria de cadeias de Markov clássicas pode ser encontrada nas Refs. [47, 35, 4]. A definição de tempo de alcance quântico apresentada na Sec. 5.6 foi retirada da Ref. [59]. A Ref. [60] também é útil. O passeio quântico definido por *Mario Szegedy* foi inspirado no algoritmo para distinção de elementos desenvolvido por *Andris Ambainis* [6]. Uma extensão dos trabalhos de Szegedy para cadeias de Markov ergódicas, porém não-simétricas foi apresentada nas Refs. [39, 38]. A Ref. [38] usa o algoritmo de *Tulsi* [62] para amplificar a probabilidade do caminhante encontrar um elemento marcado. As idéias de Szegedy ajudaram o desenvolvimento de novos algoritmos quânticos com ganhos em relação aos equivalentes clássicos. A Ref. [40] apresenta um algoritmo para encontrar triângulos em um grafo. A Ref. [37] apresenta um algoritmo para testar a comutatividade de grupos *black-box*. O cálculo do tempo de alcance no grafo completo foi apresentado no *preprint* [56] e na tese de mestrado [57]. A tese de mestrado [29] apresenta uma revisão sobre o tempo de alcance de Szegedy e sobre o algoritmo para testar a comutatividade de grupos.

Apêndice A

Álgebra Linear

O objetivo deste apêndice é compilar as definições, notações e fatos da Álgebra Linear que são importantes neste livro. Este apêndice também serve de referência rápida para as propriedades das operações em espaços vetoriais como, por exemplo, o produto interno e o produto tensorial. A Computação Quântica herdou da Mecânica Quântica a Álgebra Linear como a linguagem para a descrição da área. Portanto, é fundamental um conhecimento sólido dos resultados básicos da Álgebra Linear para a compreensão da Computação Quântica e de algoritmos quânticos. Caso o leitor não tenha essa base, sugerimos a leitura de alguma das referências básicas do final deste apêndice.

A.1 Espaços Vetoriais

Um *espaço vetorial* V sobre o corpo dos números complexos $\mathbb{C}$ é um conjunto não-vazio de elementos chamados de vetores. Em V, estão definidas as operações de soma de vetores e multiplicação de um vetor por um escalar em $\mathbb{C}$. A operação de soma é associativa e comutativa. Além disso satisfaz às propriedades

- Há um elemento $\mathbf{0} \in V$, tal que, para cada $\mathbf{v} \in V$, $\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}$ (existência de elemento neutro)
- Para cada $\mathbf{v} \in V$, existe $\mathbf{u} = (-1)\mathbf{v}$ em V tal que $\mathbf{v} + \mathbf{u} = \mathbf{0}$ (existência de elemento oposto)

$\mathbf{0}$ é chamado de vetor nulo. A operação de multiplicação por escalar satisfaz às propriedades

- $a.(b.\mathbf{v}) = (a.b).\mathbf{v}$ (associatividade)
- $1.\mathbf{v} = \mathbf{v}$ (1 é o elemento neutro da multiplicação)
- $(a+b).\mathbf{v} = a.\mathbf{v} + b.\mathbf{v}$ (distributividade sobre soma de escalares)
- $a.(\mathbf{v}+\mathbf{w}) = a.\mathbf{v} + a.\mathbf{w}$ (distributividade em V)

onde $\mathbf{v}, \mathbf{w} \in V$ e $a, b \in \mathbb{C}$.

Um espaço vetorial pode ser infinito, porém na maior parte das aplicações em Computação Quântica, são usados espaços vetoriais finitos que são denotados por $\mathbb{C}^n$. Nesse caso os vetores têm n componentes complexas. Neste livro, raramente vamos usar espaços infinitos e, nesses poucos casos, estaremos interessados apenas em subespaços finitos. No contexto da Mecânica Quântica, os espaços vetoriais infinitos são usados com mais frequência do que os finitos.

Uma *base* de $\mathbb{C}^n$ é constituída por exatamente n vetores linearmente independentes. Se $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ é uma base de $\mathbb{C}^n$, então um vetor genérico $\mathbf{v}$ pode ser escrito como

$$\mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{v}_i,$$

onde os coeficientes a_i são números complexos. A *dimensão* de um espaço vetorial é o número de vetores da base.

A.2 Produtos Internos

O *produto interno* é uma operação binária $(\cdot,\cdot) : V \times V \mapsto \mathbb{C}$ que satisfaz às seguintes propriedades

1. $(\cdot,\cdot)$ é linear no segundo argumento

$$\left(\mathbf{v}, \sum_{i=1}^{n} a_i \mathbf{v}_i\right) = \sum_{i=1}^{n} a_i \left(\mathbf{v}, \mathbf{v}_i\right).$$

2. $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_2, \mathbf{v}_1)^*$.

3. $(\mathbf{v}, \mathbf{v}) \geq 0$ com a igualdade se, e somente se $\mathbf{v} = \mathbf{0}$.

Em geral, o produto interno não é linear no primeiro argumento, e sim conjugado-linear.

Existe mais de uma forma de definir um produto interno em um espaço vetorial. Em $\mathbb{C}^n$, o produto interno mais usado é definido da seguinte maneira: sejam

$$\mathbf{v} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

então

$$(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^{n} a_i^* b_i.$$

Essa expressão equivale ao produto matricial do vetor transposto-conjugado cuja notação usual é $\mathbf{v}^\dagger$, por $\mathbf{w}$.

Se um produto interno foi introduzido em um espaço vetorial, podemos definir a noção de ortogonalidade. Dois vetores são ortogonais se o produto interno for zero. Podemos também introduzir a noção de norma de vetores via o produto interno. A norma de $\mathbf{v}$, denotado por $\|\mathbf{v}\|$ é definida como

$$\|\mathbf{v}\| = \sqrt{(\mathbf{v}, \mathbf{v})}.$$

Um vetor é dito normalizado se sua norma é igual a 1. Uma base é dita ortonormal se todos os vetores da base são normalizados e ortogonais entre si.

Um espaço vetorial finito com um produto interno é dito um *espaço de Hilbert*. Para um espaço vetorial infinito ser um espaço de Hilbert, ele deve satisfazer a propriedades adicionais além de ter um produto interno. Como lidaremos basicamente com espaços vetoriais finitos, usaremos o termo espaço de Hilbert como sinônimo de espaço vetorial com um produto interno. Um *subespaço* W de um espaço de Hilbert V finito também é um espaço de Hilbert. O conjunto de vetores ortogonais a todos os vetores de W é o espaço de Hilbert $W^\perp$ chamado de *complemento ortogonal*. V é a soma direta de W e $W^\perp$, isto é $V = W \oplus W^\perp$.

A.3 Notação de Dirac

Nesta revisão dos principais conceitos de Álgebra Linear usados na Computação Quântica, vamos usar a notação de Dirac que foi introduzida pelo físico inglês Paul A.M. Dirac no início da Mecânica Quântica para facilitar a execução de cálculos aplicados. Essa notação é muito simples. Diversas notações são usada para vetores, como $\mathbf{v}$ e $\vec{v}$. Na notação de Dirac temos

$$\mathbf{v} \equiv |v\rangle .$$

Até esse ponto, em vez de usar negrito ou colocar uma seta sobre a letra, colocamos a letra entre a barra vertical e o sinal de maior. Se temos uma base indexada, como por exemplo $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$, na notação de Dirac usamos a forma $\{|v_1\rangle, \cdots, |v_n\rangle\}$ ou $\{|1\rangle, \cdots, |n\rangle\}$. Note que se usarmos uma única base, a letra $\mathbf{v}$, em princípio, será desnecessária. Na área da computação, é muito comum começar a numeracão pelo zero, assim o primeiro vetor da base usualmente é chamado de $\mathbf{v}_0$. Na notação de Dirac temos

$$\mathbf{v}_0 \equiv |0\rangle .$$

O vetor $|0\rangle$ não é o vetor nulo, ele é apenas o primeiro vetor de uma coleção de vetores. Na notação de Dirac, o vetor nulo é uma exceção, cuja notação não é modificada. Aqui vamos usar a notação $\mathbf{0}$.

Suponha que o vetor $|v\rangle$ tenha as seguintes componentes em uma determinada base

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} .$$

O vetor dual é denotado por $\langle v|$ e é definido por

$$\langle v| = \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix} .$$

Os vetores usuais e os duais podem ser vistos como matrizes colunas e matrizes linhas, respectivamente, para fins de cálculo. O produto matricial de $\langle v|$ por $|v\rangle$ é denotado por $\langle v|v\rangle$ e seu valor em termos das componentes é

$$\langle v|v\rangle = \sum_{i=1}^{n} a_i^* a_i .$$

Esse é um exemplo de um produto interno, implicitamente usado na notação de Dirac. Se $\{|v_1\rangle, \cdots, |v_n\rangle\}$ é uma base ortonormal então

$$\langle v_i|v_j\rangle = \delta_{ij},$$

onde δ_{ij} é o delta de Kronecker. A norma de um vetor nessa notação é

$$\| \, |v\rangle \, \| = \sqrt{\langle v|v\rangle}.$$

Usa-se a terminologia *ket* para o vetor $|v\rangle$ e *bra* para o vetor dual $\langle v|$. Mantendo a concistência, usa-se a terminologia *braket* para $\langle v|v\rangle$, pois *braket* é similar a palavra da língua inglesa *bracket*.

É muito comum também o produto matricial de $|v\rangle$ por $\langle v|$, denotado por $|v\rangle\langle v|$, conhecido como produto externo cujo resultado é uma matriz $n \times n$

$$\begin{aligned} |v\rangle\langle v| &= \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix} \\ &= \begin{pmatrix} a_1 a_1^* & \cdots & a_1 a_n^* \\ & \ddots & \\ a_n a_1^* & \cdots & a_n a_n^* \end{pmatrix}. \end{aligned}$$

A chave para a notação de Dirac é sempre visualizar o *ket* como uma matriz coluna, o *bra* como uma matriz linha e reconhecer que uma sequência de *bras* e *kets* é um produto matricial, portanto associativo, porém não-comutativo.

A.4 Base Computacional

A *base computacional* de $\mathbb{C}^n$, denotada por $\{|0\rangle, \cdots, |n-1\rangle\}$, é dada por

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \cdots, \ |n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Essa base também é conhecida por *base canônica*. Algumas poucas vezes vamos usar a numeração da base computacional começando por $|1\rangle$ e terminando com $|n\rangle$. Neste livro, quando usarmos uma letra latina minúscula dentro de um *ket* ou um *bra*, estaremos nos referindo à base computacional, portanto sempre será válida a relação

$$\langle i|j\rangle = \delta_{ij}.$$

A soma normalizada de todos os vetores da base computacional define o vetor

$$|\mathrm{D}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle,$$

que chamaremos de *estado diagonal*. Quando $n = 2$, o estado diagonal é dado por $|\mathrm{D}\rangle = |+\rangle$ onde

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

A.5 Qubit e a Esfera de Bloch

O *qubit* é um vetor unitário no espaço vetorial $\mathbb{C}^2$. Um qubit genérico $|\psi\rangle$ é representado por

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

onde os coeficientes complexos α e β satisfazem ao vínculo

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

O conjunto $\{|0\rangle\,,\,|1\rangle\}$ é a base computacional de $\mathbb{C}^2$ e α, β são chamados de amplitudes do estado $|\psi\rangle$. O termo *estado* (ou *vetor de estado*) é usado como sinônimo de vetor unitário em um espaço de Hilbert.

Em princípio, precisamos de quatro números reais para descrever um qubit, dois para especificar α e dois para β. O vínculo $|\alpha|^2 + |\beta|^2 = 1$ reduz para três números. Na Mecânica Quântica, dois vetores que diferem de um fator de fase global são considerados equivalentes. Uma fase global é um número complexo de módulo unitário multiplicado ao estado. Eliminando a fase global, um qubit pode ser descrito por dois números reais θ e ϕ da seguinte forma:

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

onde $0 \leq \theta \leq \pi/2$ e $0 \leq \phi < 2\pi$. Na notação acima, o estado $|\psi\rangle$ pode ser representado por um ponto na superfície de uma esfera de raio unitário, chamada *esfera de Bloch*. Colocando o estado $|0\rangle$ como o polo norte da esfera, os números θ e ϕ são os ângulos esféricos que situam o ponto que descreve $|\psi\rangle$, como na Fig. A.1. O vetor indicado na figura é dado por

$$\begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix}.$$

Existe uma correspondência bi-unívoca entre os estados quânticos de um qubit e os pontos na esfera de Bloch. Os estados

$$|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

ficam nos pontos de encontro do eixo x com a esfera e os estados $(|0\rangle \pm i\,|1\rangle)/\sqrt{2}$ ficam nos pontos de encontro do eixo y com a esfera.

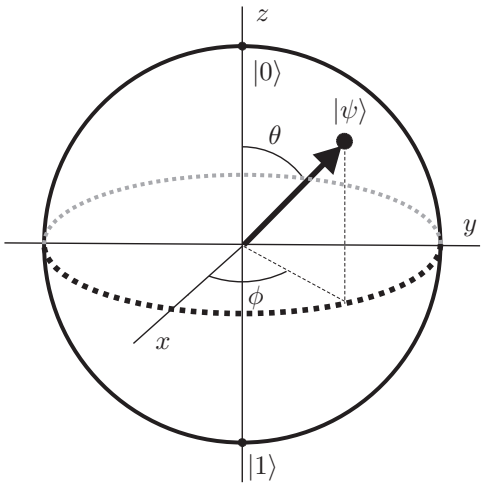

Figura A.1: Esfera de Bloch. O estado $|\psi\rangle$ de um qubit é representado por um ponto sobre a esfera.

A.6 Operadores Lineares

Sejam V, W espaços vetoriais; $\{|v_1\rangle, \cdots, |v_n\rangle\}$ uma base para V; $\mathcal{A}$ uma função $\mathcal{A} : V \mapsto W$ que satisfaz à

$$\mathcal{A}\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i \mathcal{A}(|v_i\rangle),$$

para quaisquer números complexos a_i. $\mathcal{A}$ é dito um *operador linear* de V em W. O termo operador linear em V quer dizer que tanto o domínio como o contradomínio de $\mathcal{A}$ é V. A composição de operadores lineares $\mathcal{A} : V_1 \mapsto V_2$ e $\mathcal{B} : V_2 \mapsto V_3$ é também um operador linear $\mathcal{C} : V_1 \mapsto V_3$ obtido através da composição das respectivas funções: $\mathcal{C}(|v\rangle) = \mathcal{B}(\mathcal{A}(|v\rangle))$. A soma de dois operadores lineares, ambos de V em W, é naturalmente definida através da fórmula $(A + B)(|v\rangle) = A(|v\rangle) + B(|v\rangle)$.

O operador identidade I em V é um operador linear em V tal que $I(|v\rangle) = |v\rangle$ para todo $|v\rangle \in V$. O operador nulo O em V é um operador linear tal que $O(|v\rangle) = \mathbf{0}$ para todo $|v\rangle \in V$.

Fato

Se especificarmos a ação de um operador linear em uma base do espaço

vetorial V, sua ação em qualquer vetor de V estará automaticamente determinada.

A.7 Representação Matricial

Os operadores lineares podem ser representados por matrizes. Sejam $\mathcal{A} : V \mapsto W$ um operador linear; $\{|v_1\rangle, \cdots, |v_n\rangle\}$ e $\{|w_1\rangle, \cdots, |w_m\rangle\}$ bases ortonormais para V e W, respectivamente. A *representação matricial* de $\mathcal{A}$ é obtida aplicando $\mathcal{A}$ a cada vetor da base de V e expressando o resultado como uma combinação linear de vetores da base de W, da seguinte forma:

$$\mathcal{A}(|v_j\rangle) = \sum_{i=1}^{m} A_{ij} |w_i\rangle ,$$

onde o sub-índice j corre de 1 até n. Portanto, A_{ij} são componentes de uma matriz de dimensão $m \times n$ que chamaremos de A. Quando fixamos as bases dos espaços vetoriais envolvidos, um operador linear pode ser substituído pela sua representação matricial. Nesse caso, a expressão $\mathcal{A}(|v_j\rangle)$ que significa a função $\mathcal{A}$ aplicada ao argumento $|v_j\rangle$ é equivalente ao produto matricial $A|v_j\rangle$. Usando a notação de produto externo, temos

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij} |w_i\rangle \langle v_j| .$$

Usando a equação acima e a ortonormalidade da base de V, podemos verificar que o produto matricial de A por $|v_j\rangle$ é igual a $\mathcal{A}(|v_j\rangle)$. A chave para esse cálculo é usar a associatividade da multiplicação matricial, pois

$$\begin{aligned} \left(|w_i\rangle \langle v_j| \right) |v_k\rangle &= |w_i\rangle \left(\langle v_j | v_k \rangle \right) \\ &= \delta_{jk} |w_i\rangle . \end{aligned}$$

Se o operador linear $\mathcal{C}$ for a composição do operador linear $\mathcal{B}$ com $\mathcal{A}$, a representação matricial de $\mathcal{C}$ será obtida por multiplicação da representação matricial de $\mathcal{B}$ com a de $\mathcal{A}$, ou seja, $C = BA$.

Uma vez fixadas as bases ortonormais para os espaços vetoriais em questão, existe uma identificação entre operadores lineares e matrizes. Em $\mathbb{C}^n$, temos a base computacional como referência, portanto podemos usar os termos operadores lineares e matrizes como sinônimos. Vamos também usar o termo operador como sinônimo de operador linear.

A.8 Representação Diagonal

Seja $\mathcal{O}$ um operador em V. Se existir uma base $\{|v_1\rangle, \cdots, |v_n\rangle\}$ ortonormal de V tal que

$$O = \sum_{i=1}^{n} \lambda_i |v_i\rangle \langle v_i| ,$$

dizemos que $\mathcal{O}$ admite uma *representação diagonal* ou, equivalentemente, $\mathcal{O}$ é *diagonalizável*. Os números complexos λ_i são os *autovalores* de $\mathcal{O}$ e $|v_i\rangle$ os seus *autovetores* associados. Qualquer múltiplo de um autovetor também é um autovetor. Se dois autovetores estão associados ao mesmo autovalor, então qualquer combinação linear desses autovetores é um autovetor. O número de autovetores linearmente independentes associados a um mesmo autovalor é a multiplicidade desse autovalor.

Quando há autovalores com multiplicidade maior que 1, a representação diagonal pode ser fatorada da seguinte forma

$$O = \sum_{\lambda} \lambda P_\lambda,$$

onde o índice λ do somatório corre apenas nos autovalores distintos e P_λ é o projetor no auto-espaço de $\mathcal{O}$ associado ao autovalor λ. Se λ tiver multiplicidade 1, $P_\lambda = |v\rangle \langle v|$, onde $|v\rangle$ é o autovetor unitário associado a λ. Se λ tiver multiplicidade 2 e $|v_1\rangle, |v_2\rangle$ são os autovetores unitários associados linearmente independentes, $P_\lambda = |v_1\rangle \langle v_1| + |v_2\rangle \langle v_2|$ e assim por diante.

Uma definição alternativa de um operador diagonalizável é exigir que O é *similar* a uma matriz diagonal por uma transformação de similaridade com uma matriz unitária. Uma *transformação de similaridade* é do tipo $O \to M^{-1}OM$ onde M é uma matriz inversível. A definição do termo *diagonalizável* é mais restrita do que usualmente aparece na literatura, pois estamos exigindo que M seja uma matriz unitária.

A.9 Relação de Completeza

A *relação de completeza* é tão útil que merece destaque. Seja $\{|v_1\rangle, \cdots, |v_n\rangle\}$ uma base ortonormal de V, então

$$I = \sum_{i=1}^{n} |v_i\rangle \langle v_i| .$$

A relação de completeza é uma representação diagonal da matriz identidade.

A.10 Desigualdade de Cauchy-Schwarz

Seja V um espaço de Hilbert e $|v\rangle, |w\rangle \in V$, então

$$|\langle v|w\rangle| \leq \sqrt{\langle v|v\rangle \langle w|w\rangle}.$$

Uma forma mais explícita de apresentar a desigualdade de Cauchy-Schwarz é

$$\left|\sum_i v_i w_i\right|^2 \leq \left(\sum_i |v_i|^2\right)\left(\sum_i |w_i|^2\right),$$

que é obtida quando tomamos $|v\rangle = \sum_i v_i^* |i\rangle$ e $|w\rangle = \sum_i w_i |i\rangle$.

A.11 Operadores Especiais

Seja A um operador linear no espaço de Hilbert V, então existe um único operador linear $A^\dagger$ em V, chamado de *operador ajunto*, que satisfaz à

$$(|v\rangle, A|w\rangle) = \left(A^\dagger |v\rangle, |w\rangle\right),$$

para todos $|v\rangle, |w\rangle \in V$.

A representação matricial de $A^\dagger$ é a matriz transposta-conjugada de A. As principais propriedades da operação *adaga* ou *transposta-conjugada* são

1. $(AB)^\dagger = B^\dagger A^\dagger$
2. $|v\rangle^\dagger = \langle v|$
3. $A|v\rangle^\dagger = \langle v| A^\dagger$
4. $\left(|w\rangle\langle v|\right)^\dagger = |v\rangle\langle w|$
5. $\left(A^\dagger\right)^\dagger = A$
6. $(\sum_i a_i A_i)^\dagger = \sum_i a_i^* A_i^\dagger$

A última propriedade mostra que a operação adaga é conjugada-linear.

Operador Normal

Um operador A em V é *normal* se $A^\dagger A = AA^\dagger$.

Teorema Espectral

Um operador A em V é diagonalizável se, e somente se A for normal.

Operador Unitário

Um operador U em V é *unitário* se $U^\dagger U = UU^\dagger = I$.

Fatos sobre Operadores Unitários

Operadores unitários são normais, portanto são diagonalizáveis com relação a uma base ortonormal. Autovetores de um operador unitário associados a autovalores diferentes são ortogonais. Os autovalores têm módulo iguais a 1. A aplicação de um operador unitário sobre um vetor preserva a norma.

Operador Hermitiano

Um operador A em V é *hermitiano* ou *auto-adjunto* se $A^\dagger = A$.

Fatos sobre Operadores Hermitianos

Operadores hermitianos são normais, portanto são diagonalizáveis com relação a uma base ortonormal. Autovetores de um operador hermitiano associados a autovalores diferentes são ortogonais. Os autovalores de um operador hermitiano são reais. Uma matriz real simétrica é hermitiana.

Projetor

Um operador P em V é um *projetor* se $P^2 = P$.

Fatos sobre Projetores

Projetores são hermitianos. Os autovalores são iguais a 0 ou 1. Se P é um projetor, então o *complemento ortogonal* $I - P$ também é um projetor. A aplicação de um projetor sobre um vetor ou diminui a sua norma ou a mantém invariante.

Operador Positivo

Um operador A em V é dito *positivo* se $\langle v|A|v\rangle \geq 0$ para todo $|v\rangle \in V$. Se a desigualdade for estrita para todo vetor não-nulo de V, então o operador

é dito *positivo definido*.

Fatos sobre Operadores Positivos

Os operadores positivos são hermitianos.

Exercício A.1. *Considere a matrix*

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

1. *Mostre que M não é normal.*
2. *Mostre que os autovetores de M geram um espaço unidimensional.*

Exercício A.2. *Considere a matrix*

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

1. *Mostre os autovalores de M são ± 1.*
2. *Mostre que M não é unitária e não é hermitiana.*
3. *Mostre que os autovetores de M associados a autovalores distintos não são ortogonais.*
4. *Mostre que M não tem uma representação diagonal.*

A.12 Matrizes de Pauli

As *matrizes de Pauli* são

$$\begin{aligned} \sigma_0 &= I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\ \sigma_1 &= \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 &= \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\ \sigma_3 &= \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned}$$

Essas matrizes são unitárias e hermitianas, portanto seus autovalores são iguais a 1 ou -1.

A.13 Funções de Operadores

Se temos um operador A em V, podemos perguntar se é possível calcular $\sqrt{A}$, isto é, achar um operador cujo quadrado é A? De modo geral, podemos nos perguntar se faz sentido usar um operador como argumento de uma função, como a função exponencial ou logaritmo? Se o operador A é normal, ele tem uma representação diagonal, ou seja, pode ser escrito na forma

$$A = \sum_i a_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

onde a_i são os autovalores e o conjunto $\{|v_i\rangle\}$ é uma base ortonormal de autovetores de A. Podemos estender a aplicação de uma função $f : \mathbb{C} \mapsto \mathbb{C}$ para A da seguinte forma

$$f(A) = \sum_i f(a_i) \left|v_i\right\rangle \left\langle v_i\right| .$$

O resultado é um operador definido no mesmo espaço vetorial V e é independente da escolha da base de V.

Se o objetivo é calcular $\sqrt{A}$, primeiramente diagonalizamos A, isto é, determinamos uma matriz unitária U tal que $A = UDU^\dagger$, onde D é uma matriz diagonal. Depois usamos o fato que $\sqrt{A} = U\sqrt{D}U^\dagger$, onde $\sqrt{D}$ é calculada tomando a raíz quadrada de cada elemento da diagonal.

Se U é o operador de evolução de um sistema quântico isolado que está inicialmente no estado $|\psi(0)\rangle$, o estado no instante t será dado por

$$\left|\psi(t)\right\rangle \; = \; U^t \left|\psi(0)\right\rangle .$$

A maneira mais eficiente de calcular o estado $|\psi(t)\rangle$ é obter a representação diagonal do operador unitário U

$$U \; = \; \sum_i \lambda_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

e calcular a t-ésima potência de U, ou seja

$$U^t \; = \; \sum_i \lambda_i^t \left|v_i\right\rangle \left\langle v_i\right| .$$

O estado do sistema no instante t será

$$\left|\psi(t)\right\rangle \; = \; \sum_i \lambda_i^t \left\langle v_i|\psi(0)\right\rangle \; \left|v_i\right\rangle .$$

O traço de uma matriz é outro tipo de função de operadores. Nesse caso, o resultado da aplicação da função é um número complexo definido como

$$\mathrm{tr}(A) = \sum_i A_{ii},$$

onde A_{ii} são os elementos diagonais de A. A função traço satisfaz às seguintes propriedades

1. $\mathrm{tr}(aA + bB) = a\,\mathrm{tr}(A) + b\,\mathrm{tr}(B)$, (linearidade)
2. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$,
3. $\mathrm{tr}(A\,B\,C) = \mathrm{tr}(C\,A\,B)$. (propriedade cíclica)

A propriedade 3 é consequência imediata da 2.

A função traço é invariante por transformações de similaridade, isto é, $\mathrm{tr}(M^{-1}AM)$=$\mathrm{tr}(A)$, onde M é uma matriz inversível. Isso implica que o traço não depende da base escolhida para obter a representação matricial do operador.

Uma fórmula bastante útil envolvendo o traço de operadores é

$$\mathrm{tr}(A\,|\psi\rangle\,\langle\psi|) = \langle\psi|A|\psi\rangle\,,$$

para qualquer $|\psi\rangle \in V$ e qualquer A em V.

Exercício A.3. *Usando o método de avaliação de funções sobre matrizes descrito nesta seção, encontre a matriz M tal que*

$$M^2 = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix}.$$

A.14 Produto Tensorial

Sejam V e W espaços de Hilbert finitos com as base $\{|v_1\rangle, \cdots, |v_m\rangle\}$ e $\{|w_1\rangle, \cdots, |w_n\rangle\}$, respectivamente. O *produto tensorial* de V com W, denotado por $V \otimes W$, é um espaço de Hilbert de dimensão mn, que tem o conjunto $\{|v_1\rangle \otimes |w_1\rangle, |v_1\rangle \otimes |w_2\rangle, \cdots, |v_m\rangle \otimes |w_n\rangle\}$ como uma base. O produto tensorial de um vetor de V por um vetor de W, $|v\rangle \otimes |w\rangle$, também denotado por $|v\rangle\,|w\rangle$ ou $|v, w\rangle$ ou $|v\,w\rangle$, pode ser calculado explicitamente via o produto de Kronecker, definido logo adiante. Um vetor genérico de $V \otimes W$ é uma combinação linear de vetores do tipo $|v_i\rangle \otimes |w_j\rangle$, ou seja, se $|\psi\rangle \in V \otimes W$ então

$$|\psi\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\,|v_i\rangle \otimes |w_j\rangle\,.$$

O produto tensorial é *bilinear*, isto é, linear em cada argumento. Portanto

1. $|v\rangle \otimes \big(a\,|w_1\rangle + b\,|w_2\rangle\big) \;=\; a\,|v\rangle \otimes |w_1\rangle + b\,|v\rangle \otimes |w_2\rangle\,,$
2. $\big(a\,|v_1\rangle + b\,|v_2\rangle\big) \otimes |w\rangle \;=\; a\,|v_1\rangle \otimes |w\rangle + b\,|v_2\rangle \otimes |w\rangle\,.$

Um escalar pode sempre ser fatorado para o início da expressão, pois

$$a\big(\,|v\rangle \otimes |w\rangle\,\big) \;=\; \big(a\,|v\rangle\,\big) \otimes |w\rangle \;=\; |v\rangle \otimes \big(a\,|w\rangle\,\big).$$

O produto tensorial dos operadores lineares A em V e B em W, denotado por $A \otimes B$, é o operador linear em $V \otimes W$ definido por

$$\big(A \otimes B\big)\big(\,|v\rangle \otimes |w\rangle\,\big) \;=\; \big(A\,|v\rangle\,\big) \otimes \big(B\,|w\rangle\,\big).$$

Um operador linear genérico em $V \otimes W$ pode ser escrito como combinação linear de operadores da forma $A \otimes B$, porém um operador em $V \otimes W$ não precisa admitir a forma fatorada. Essa definição pode ser facilmente estendida para operadores do tipo $A : V \mapsto V'$ e $B : W \mapsto W'$. Nesse caso, o produto tensorial desses operadores é do tipo $(A \otimes B) : (V \otimes W) \mapsto (V' \otimes W')$.

Na Mecânica Quântica é muito comum usar operadores na forma de produto externo, por exemplo, $A = |v\rangle\langle v|$ e $B = |w\rangle\langle w|$. O produto tensorial de A por B pode ser representado das seguintes maneiras equivalentes entre si:

$$\begin{aligned} A \otimes B &= \big(\,|v\rangle\langle v|\,\big) \otimes \big(\,|w\rangle\langle w|\,\big) \\ &= |v\rangle\langle v| \otimes |w\rangle\langle w| \\ &= |v, w\rangle\langle v, w|\,. \end{aligned}$$

Se A_1, A_2 são operadores em V e B_1, B_2 são operadores em W então a composição ou o produto matricial das representações matriciais obedecem à propriedade

$$(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = (A_1 \cdot A_2) \otimes (B_1 \cdot B_2).$$

O produto interno de $|v_1\rangle \otimes |w_1\rangle$ por $|v_2\rangle \otimes |w_2\rangle$ é definido como

$$\big(\,|v_1\rangle \otimes |w_1\rangle\;,\; |v_2\rangle \otimes |w_2\rangle\,\big) \;=\; \big\langle v_1\big|v_2\big\rangle\,\big\langle w_1\big|w_2\big\rangle\,.$$

O produto interno entre vetores escritos como combinação lineares de vetores da base são calculados aplicando-se a propriedade de linearidade no

segundo argumento do produto interno e a propriedade de conjugação-linear no primeiro argumento. Por exemplo,

$$\left(\left(\sum_{i=1}^{n} a_i \left|v_i\right\rangle\right) \otimes \left|w_1\right\rangle \ , \ \left|v\right\rangle \otimes \left|w_2\right\rangle\right) \ = \ \left(\sum_{i=1}^{n} a_i^* \left\langle v_i\middle|v\right\rangle\right) \left\langle w_1\middle|w_2\right\rangle .$$

A definição do produto interno implica que

$$\left\| \left|v\right\rangle \otimes \left|w\right\rangle \right\| \ = \ \left\| \left|v\right\rangle \right\| \cdot \left\| \left|w\right\rangle \right\|.$$

Em particular, a norma do produto tensorial de vetores de norma unitária é um vetor de norma unitária.

Quando usamos representações matriciais para os operadores, o produto tensorial pode ser calculado explicitamente via o *produto de Kronecker*. Seja A uma matriz de dimensão $m \times n$ e B uma matriz de dimensão $p \times q$, então

$$A \otimes B = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ & \ddots & \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix}.$$

A matriz $A \otimes B$ tem dimensão $mp \times nq$. O produto de Kronecker pode ser usado para matrizes de qualquer dimensão, em particular para dois vetores,

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ \\ b_2 \end{pmatrix} \\ \\ a_2 \begin{pmatrix} b_1 \\ \\ b_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ \\ a_1 b_2 \\ \\ a_2 b_1 \\ \\ a_2 b_2 \end{pmatrix}.$$

O produto tensorial é uma operação associativa e distributiva, porém não-comutativa, de modo que $\left|v\right\rangle \otimes \left|w\right\rangle \neq \left|w\right\rangle \otimes \left|v\right\rangle$. A maioria das operações sobre um produto tensorial de vários termos é feita termo a termo:

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

Por sua vez, o traço de um produto de Kronecker de matrizes é

$$\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\,\mathrm{tr}(B).$$

Se ambos operadores A e B são operadores especiais do mesmo tipo, como definidos na Sec. A.11, então o produto tensorial $A \otimes B$ também é um operador especial desse tipo. Por exemplo, o produto tensorial de operadores hermitianos é um operador hermitiano.

A soma direta de um espaço vetorial V consigo mesmo n vezes é um caso particular de produto tensorial. De fato, $V \oplus \cdots \oplus V$ é igual a $I \otimes V$, onde I é a matriz identidade de dimensão $n \times n$. Isso mostra que, de certa forma, o produto tensorial é uma construção a partir da soma direta de espaços vetoriais, assim como o produto de números é uma construção a partir da soma de números. No entanto, o produto tensorial é mais rico do que a simples repetição de soma direta de espaços vetoriais. É natural definir potenciação tensorial, de fato $V^{\otimes n}$ quer dizer $V \otimes \cdots \otimes V$ com n termos.

Se o estado diagonal do espaço vetorial V é $|\mathrm{D}\rangle_V$ e do espaço W é $|\mathrm{D}\rangle_W$, o estado diagonal do espaço $V \otimes W$ é $|\mathrm{D}\rangle_V \otimes |\mathrm{D}\rangle_W$. Portanto, o estado diagonal do espaço $V^{\otimes n}$ é $|\mathrm{D}\rangle^{\otimes n}$.

A.15 Registradores

Um *registrador* é um conjunto de qubits tratados como um sistema composto. Suponha que temos um registrador com 2 qubits. A base computacional é

$$|0,0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0,1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |1,0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1,1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Um estado genérico desse registrador é

$$|\psi\rangle = \sum_{i=0}^{1} \sum_{j=0}^{1} a_{ij} \, |i,j\rangle$$

onde os coeficientes a_{ij} são números complexos que satisfazem ao vínculo

$$\left|a_{00}\right|^2 + \left|a_{01}\right|^2 + \left|a_{10}\right|^2 + \left|a_{11}\right|^2 = 1.$$

Para facilitar a generalização para n qubits, é usual compactar a notação convertendo de base binária para base decimal. A base computacional para um registrador de 2 qubits na notação decimal é $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. Na base binária podemos determinar o número de qubits contando o número de dígitos dentro do *ket*, por exemplo, $|011\rangle$ ser refere a três qubits. Na base decimal não podemos determinar a princípio qual é o número de qubits. Essa informação deve estar implícita. Podemos sempre voltar atrás, escrever o número decimal na base binária e recuperar a notação explícita. Nessa

notação compacta, um estado genérico de um registrador com n qubits é

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

onde os coeficientes a_i são números complexos que satisfazem ao vínculo

$$\sum_{i=0}^{2^n-1} \left|a_i\right|^2 \, = \, 1.$$

O estado diagonal de um registrador de n qubits é o produto tensorial dos estados diagonais de cada qubit, ou seja, $|\mathrm{D}\rangle = |+\rangle^{\otimes n}$.

Sugestões para Leitura

A quantidade de bons livros de Álgebra Linear é muito grande. Para um contato inicial, sugerimos as Refs. [58, 8, 9, 26]; para uma abordagem mais avançada sugerimos a Ref. [25]; para quem já domina os conceitos básicos e está interessado apenas na aplicação da Álgebra Linear na Computação Quântica, sugerimos a Ref. [49].

Bibliografia

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. *Proc. 33th STOC*, pág. 50–59, New York, NY, 2001. ACM.

[2] Dorit Aharonov. Quantum computation – a review. *Annual Review of Computational Physics*, pág. 1–77, ed. Dietrich Stauffer, vol. VI, World Scientific, 1998.

[3] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48(2):1687–1690, 1993.

[4] David J. Aldous and James A. Fill. *Reversible Markov Chains and Random Walks on Graphs.* Livro em preparação, `http://www.stat.berkeley.edu/~aldous/book.html`, 200X.

[5] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. *Proc. 33th STOC*, pág. 60–69, New York, NY, 2001. ACM.

[6] Andris Ambainis. Quantum walk algorithm for element distinctness. *FOCS '04: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pág. 22–31, Washington, DC, USA, 2004. IEEE Computer Society.

[7] Andris Ambainis, Julia Kempe, and Alexander Rivosh. Coins make quantum walks faster. *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA*, pág. 1099–1108, 2005.

[8] Tom M. Apostol. *Calculus, vol. 1: One-Variable Calculus with an Introduction to Linear Algebra.* Wiley, New York, 1967.

[9] Sheldon Axler. *Linear Algebra Done Right.* Springer, New York, 1997.

[10] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[11] G. Boros and V. Moll. *Irresistible integrals: symbolics, analysis and experiments in the evaluation of integrals*. Cambridge University Press, Cambridge, England, 2004.

[12] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Forstschritte Der Physik*, 4:820–831, 1998.

[13] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Quantum Computation and Quantum Information Science, AMS Contemporary Mathematics Series*, 305:53–74, 2002, quant-ph/0005055.

[14] H. A. Carteret, M. E. H. Ismail, and B. Richmond. Three routes to the exact asymptotics for the one-dimensional quantum walk. *Journal of Physics A: Mathematical and General*, 36(33):8775 – 8795, August 2003.

[15] Bernard Diu Claude Cohen-Tannoudji and Frank Laloe. *Quantum Mechanics*. Wiley-Interscience, 2006.

[16] Bernard d'Espagnat. *Conceptual foundations of quantum mechanics*. Westview Press, 1999.

[17] Milosh Drezgich, Andrew P. Hines, Mohan Sarovar, and Shankar Sastry. Complete characterization of mixing time for the continuous quantum walk on the hypercube with markovian decoherence model. *Quantum Inf. & Comp.*, 9:856, 2009.

[18] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998.

[19] William Feller. *An Introduction to Probability Theory and Its Applications, Vol. 1*. Wiley, 3a. edição, January 1968.

[20] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science (2nd Edition)*. Addison-Wesley Professional, segunda edição, 1994.

[21] David Griffiths. *Introduction to Quantum Mechanics*. Benjamin Cummings, segunda edição, 2005.

[22] Lov K. Grover. Quantum computers can search arbitrarily large databases by a single query. *Phys. Rev. Lett.*, 79(23):4709–4712, Dec 1997.

[23] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, Jul 1997.

[24] Lov K. Grover. Quantum computers can search rapidly by using almost any transformation. *Phys. Rev. Lett.*, 80(19):4329–4332, May 1998.

[25] Kenneth M. Hoffman and Ray Kunze. *Linear Algebra*. Prentice Hall, New York, 1971.

[26] Roger Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[27] Barry D. Hughes. *Random Walks and Random Environments: Random Walks (Vol 1)*. Clarendon Press, March 1995.

[28] Barry D. Hughes. *Random Walks and Random Environments: Random Environments (Vol 2)*. Oxford University Press, USA, August 1996.

[29] Yuki Kelly Itakura. Quantum algorithm for commutativity testing of a matrix set. Dissertação de Mestrado, University of Waterloo, Waterloo, 2005.

[30] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Inc., New York, NY, USA, 2007.

[31] Julia Kempe. Quantum random walks - an introductory overview. *Contemporary Physics*, 44(4):302–327, 2003. quant-ph/0303081.

[32] Julia Kempe. Discrete quantum walks hit exponentially faster. *Probability Theory and Related Fields*, 133(2):215–235, 2005, quant-ph/0205083.

[33] Norio Konno. Quantum random walks in one dimension. *Quantum Information Processing*, 1(5):345–354, 2002.

[34] Jozef Košík. Two models of quantum random walk. *Central European Journal of Physics*, 4:556–573, 2003.

[35] László Lovász. Random walks on graphs: A survey. *Combinatorics, Paul Erdös is Eighty (Volume 2)*, pág. 1–46, 1993.

[36] T D Mackay, S D Bartlett, L T Stephenson, and B C Sanders. Quantum walks in higher dimensions. *Journal of Physics A: Mathematical and General*, 35(12):2745, 2002.

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

[38] F. Magniez, A. Nayak, P. Richter, and M. Santha. On the hitting times of quantum versus random walks. *Proceedings of 20th ACM-SIAM Symposium on Discrete Algorithms*, 2009.

[39] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. *Proceedings of 39th ACM Symposium on Theory of Computing*, pág. 575–584, 2007.

[40] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):413–424, 2007.

[41] F. L. Marquezino, R. Portugal, G. Abal, and R. Donangelo. Mixing times in quantum walks on the hypercube. *Physical Review A*, 77:042312, 2008.

[42] Franklin L. Marquezino. *Análise, simulações e aplicação algorítmicas de caminhadas quânticas*. Tese de Doutorado, LNCC, 2010.

[43] Franklin L. Marquezino and Renato Portugal. The QWalk simulator of quantum walks. *Computer Physics Communications*, 179(5):359–369, 2008, arXiv:0803.3459.

[44] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, New York, NY, USA, 2007.

[45] C. Moore and A. Russell. Quantum walks on the hypercube. J. D. P. Rolim and S. Vadhan, editors, *Proc. Random 2002*, pág. 164–178, Cambridge, MA, 2002. Springer.

[46] Michele Mosca. Counting by quantum eigenvalue estimation. *Theor. Comput. Sci.*, 264(1):139–153, 2001.

[47] Rajeev Motwani and Prabhakar Raghavan. Randomized algorithms. *ACM Comput. Surv.*, 28(1):33–37, 1996.

[48] A. Nayak and A. Vishwanath. Quantum walk on a line, 2000. DIMACS Technical Report 2000-43, quant-ph/0010117.

[49] Michael A. Nielsen and Isaac L. Chuang. *Computação Quântica e Informação Quântica*. Editora Bookman, 2005.

[50] Amanda C. Oliveira. *Simulação de Caminhos Quânticos em Redes Bidimensionais*. Tese de Doutorado, LNCC, 2007.

[51] Roland Omnès. *Understanding Quantum Mechanics*. Princeton University Press, 1999.

[52] Asher Peres. *Quantum Theory: Concepts and Methods*. Springer, 1995.

[53] Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho e Nelson Maculan. *Uma Introdução à Computação Quântica*, vol. 8 das *Notas em Matemática Aplicada*. Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), São Carlos, primeira edição, 2004.

[54] Jonh Preskill. *Lecture Notes on Quantum Computation*. `http://-www.theory.caltech.edu/~preskill/ph229`, 1998.

[55] J. J. Sakurai. *Modern Quantum Mechanics*. Addison Wesley, 1993.

[56] R. A. M. Santos and R. Portugal. Quantum hitting time on the complete graph. 2009, arXiv:0912.1217.

[57] Raqueline M. A. Santos. Cadeias de Markov Quânticas. Dissertação de Mestrado, LNCC, 2010.

[58] Gilbert Strang. *Linear Algebra and Its Applications*. Brooks Cole, 1988.

[59] Mario Szegedy. Quantum speed-up of Markov chain based algorithms. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:32–41, 2004.

[60] Mario Szegedy. Spectra of quantized walks and a $\sqrt{\delta\epsilon}$ rule. 2004, quant-ph/0401053.

[61] Ben Tregenna, Will Flanagan, Rik Maile, and Viv Kendon. Controlling discrete quantum walks: coins and initial states. *New Journal of Physics*, 5(1):83, 2003, quant-ph/0304204.

[62] Avatar Tulsi. Faster quantum-walk algorithm for the two-dimensional spatial search. *Physical Review A*, 78(1):012310, 2008.

[63] Salvador Elias Venegas-Andraca. *Quantum Walks for Computer Scientists*. Morgan and Claypool Publishers, 2008.

[64] Christof Zalka. Grover's quantum searching algorithm is optimal. 1997, quant-ph/9711070.

Índice

Notas em Matemática Aplicada

Arquivos em pdf disponíveis em http://www.sbmac.org.br/notas.php

1. Restauração de Imagens com Aplicações em Biologia e Engenharia
   Geraldo Cidade, Antônio Silva Neto e Nilson Costa Roberty
2. Fundamentos, Potencialidades e Aplicações de Algoritmos Evolutivos
   Leandro dos Santos Coelho
3. Modelos Matemáticos e Métodos Numéricos em Águas Subterrâneas
   Edson Wendlander
4. Métodos Numéricos para Equações Diferenciais Parciais
   Maria Cristina de Castro Cunha e Maria Amélia Novais Schleicher
5. Modelagem em Biomatemática
   Joyce da Silva Bevilacqua, Marat Rafikov e Cláudia de Lello Courtouke Guedes
6. Métodos de Otimização Randômica: algoritmos genéticos e "simulated annealing"
   Sezimária F. Pereira Saramago
7. "Matemática Aplicada à Fisiologia e Epidemiologia"
   H.M. Yang, R. Sampaio e A. Sri Ranga
8. Uma Introdução à Computação Quântica
   Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho e Nelson Maculan
9. Aplicações de Análise Fatorial de Correspondências para Análise de Dados
   Homero Chaib Filho

10. Modelos Matemáticos baseados em autômatos celulares para Geoprocessamento

    Marilton Sanchotene de Aguiar, Fábia Amorim da Costa, Graçaliz Pereira Dimuro e Antônio Carlos da Rocha Costa

11. Computabilidade: os limites da Computação

    Regivan H. N. Santiago e Benjamín R. C. Bedregal

12. Modelagem Multiescala em Materiais e Estruturas

    Fernando Rochinha e Alexandre Madureira

13. Modelagem em Biomatemática (Coraci Malta ed.)

    1 - "Modelagem matemática do comportamento elétrico de neurônios e algumas aplicações"

    Reynaldo D. Pinto

    2 - "Redes complexas e aplicações nas Ciências"

    José Carlos M. Mombach

    3 - "Possíveis níveis de complexidade na modelagem de sistemas biológicos"

    Henrique L. Lenzi, Waldemiro de Souza Romanha e Marcelo Pelajo- Machado

14. A lógica na construção dos argumentos

    Angela Cruz e José Eduardo de Almeida Moura

15. Modelagem Matemática e Simulação Numérica em Dinâmica dos Fluidos

    Valdemir G. Ferreira, Hélio A. Navarro, Magda K. Kaibara

16. Introdução ao Tratamento da Informação nos Ensinos Fundamental e Médio

    Marcilia Andrade Campos, Paulo Figueiredo Lima

17. Teoria dos Conjuntos Fuzzy com Aplicações

    Rosana Sueli da Motta Jafelice, Laércio Carvalho de Barros, Rodney Carlos Bassanezi

18. Introdução à Construção de Modelos de Otimização Linear e Inteira

    Socorro Rangel

19. Observar e Pensar, antes de Modelar
    Flavio Shigeo Yamamoto, Sérgio Alves, Edson P. Marques Filho, Amauri P. de Oliveira
20. Frações Contínuas: Propriedades e Aplicações
    Eliana Xavier Linhares de Andrade, Cleonice Fátima Bracciali
21. Uma Introdução à Teoria de Códigos
    Carlile Campos Lavor, Marcelo Muniz Silva Alves, Rogério Monteiro de Siqueira, Sueli Irene Rodrigues Costa
22. Análise e Processamento de Sinais
    Rubens Sampaio, Edson Cataldo, Alexandre de Souza Brandão
23. Introdução aos Métodos Discretos de Análise Numérica de EDO e EDP
    David Soares Pinto Júnior
24. Representações Computacionais de Grafos
    Lílian Markenzon, Oswaldo Vernet
25. Ondas Oceânicas de Superfície
    Leandro Farina
26. Técnicas de Modelagem de Processos Epidêmicos e Evolucionários
    Domingos Alves, Henrique Fabrício Gagliardi
27. Introdução à teoria espectral de grafos com aplicações
    Nair Maria Maia de Abreu, Renata Raposo Del-Vecchio, Cybele Tavares Maia Vinagre e Dragan Stevanović
28. Modelagem e convexidade
    Eduardo Cursi e Rubens Sampaio
29. Modelagem matemática em finanças quantitativas em tempo discreto
    Max Oliveira de Souza e Jorge Zubelli
30. Programação não linear em dois níveis: aplicação em Engenharia Mecânica
    Ana Friedlander e Eduardo Fancello

31. Funções simétricas e aplicações em Combinatória
    José Plinio de Oliveira Santos e Robson da Silva
32. Semigrupos aplicados a sistemas dissipativos em EDP
    Carlos Raposo da Cunha
33. Introdução à Simulação Estocástica para Atuária e Finanças Usando R
    Hélio Côrtes Vieira, Alejandro C. Frery e Luciano Vereda
34. Modelos de Sustentabilidade nas Paisagens Amazônicas Alagáveis
    Maurício Vieira Kritz, Jaqueline Maria da Silva e Cláudia Mazza
35. Uma Introdução à Dinâmica Estocástica de Populações
    Leonardo Paulo Maia
36. Geometria de Algoritmos Numéricos
    Gregorio Malajovich
37. Equações Diferenciais, Teorema do Resíduo e as Transformadas Integrais
    Edmundo Capelas de Oliveira e Jayme Vaz Júnior
38. Métodos Matemáticos e Computacionais em Música
    Paulo Cezar Carvalho,Luiz Velho, Marcelo Cicconet e Sergio Krakowski
39. Métodos para Problemas Inversos de Grande Porte
    Fermín S. Viloche Bazán e Leonardo Silveira Borges
40. TerraME : Suporte a Modelagem Ambiental Multi-Escalas Integrada a Bancos de Dados Geográficos
    Tiago Garcia de Senna Carneiro e Gilberto Camara
41. Técnicas de Inteligência Computacional Inspiradas na Natureza - Aplicações em Problemas Inversos em Transferência Radiativa
    Antônio J. Silva Neto e José Carlos Becceneri
42. Avanços em Métodos de Krylov para Solução de Sistemas Lineares de Grande Porte
    Luiz Mariano Carvalho e Serge Gratton