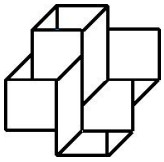


Laboratório Nacional de Computação Científica

Programa de Pós-Graduação em Modelagem Computacional

Algoritmo de Contagem Quântico Aplicado ao Grafo Bipartido Completo

Gustavo Alves Bezerra

Petrópolis, RJ - Brasil

Setembro de 2021

Gustavo Alves Bezerra

Algoritmo de Contagem Quântico Aplicado ao Grafo Bipartido Completo

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

Laboratório Nacional de Computação Científica

Programa de Pós-Graduação em Modelagem Computacional

Orientador(es): Renato Portugal e Raqueline Azevedo Medeiros Santos

Petrópolis, RJ - Brasil

Setembro de 2021

Ficha catalográfica elaborada por Patrícia Vieira Silva - CRB7 5822

B574a Bezerra, Gustavo Alves

Algoritmo de contagem quântico aplicado ao grafo bipartido completo / Gustavo Alves Bezerra. - Petrópolis, RJ: Laboratório Nacional de Computação Científica, 2021.
100 f.: il.; 30 cm.

Dissertação (Mestrado em Modelagem Computacional) – Laboratório Nacional de Computação Científica, 2021.
Orientadores: Renato Portugal; Raqueline Azevedo Medeiros Santos.

1. Computação quântica. 2. Algoritmos (Computação). 3. Teoria dos grafos. 4. Fourier, Transformações de. I. Portugal, Renato. II. Santos, Raqueline Azevedo Medeiros. III. LNCC/MCTI. IV. Título.

CDD – 004.1

Gustavo Alves Bezerra

Algoritmo de Contagem Quântico Aplicado ao Grafo Bipartido Completo

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

Aprovada por:

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

Prof. Paulo César Marques Vieira, D.Sc.

Prof. Franklin de Lima Marquezino, D.Sc.

Petrópolis, RJ - Brasil
Setembro de 2021

Dedicatória

A todos que me apoiaram
durante minha trajetória.

Agradecimentos

Agradeço à minha família pelo apoio contínuo ao longo de toda minha trajetória educacional. Agradeço a Victor Santos e a Yuri Messias pelos CiViKs e Blue Days, contribuindo para a manutenção da minha sanidade mental. Agradeço a Raul Silva, Breno Viana, Felipe Barbalho, Débora Emili e Patrícia Cruz por motivos similares.

Agradeço também à todas as amizades que fiz ao longo da minha vivência no Laboratório Nacional de Computação Científica – pessoas também essenciais para minha sobrevivência nesses tempos pandêmicos. Em especial, ressalto os nomes de Dudu Hutter e Nana Grassi (por me fazerem sentir em casa em Petrópolis); Douglas Terra (pela companhia na república); Ana Néri e Roberta Machado (por aturarem minhas dúvidas na secretaria); Cauê Teixeira e Jalil Moqadam (pela recepção no grupo de pesquisa); Edlaine Fernandes, Haron Calegari, Ítalo Messias, João Vitor de Oliveira, Lucas dos Anjos e Weslley Pereira (membros do RPGzim); Alonso Alvarez, Ana Luiza Karl, Andressa Machado, Luís Cury, Matheus Müller e Rafael Terra (membros da comissão discente e organização do EAMC); Dayana Cristine, Felipe Otávio dos Santos, Frederico Cabral, Natanael Júnior, Pedro Lugão e Renato Borseti (pelos perrengues e contribuições compartilhados); e a Gabriele Iwashima (por iluminar meus dias desde que a conheci). Peço desculpas a todos aqueles que não foram mencionados pela falta de memória e de espaço.

Por fim, presto minha homenagem a algumas pessoas próximas que pereceram diante da COVID-19: Artur Ziviani, Flávio Bezerra e Gabriel Rocha. Agradeço também à CAPES e à FAPERJ pelo apoio financeiro.

"I saw an old man sitting with his head in hands
His eyes reflect the wisdom of his life
His words painted a new world
And my thoughts just followed him"
(Eloy)

Resumo

Estudos na Computação Quântica têm avançado desde a década de 1980, numa busca incessante por algoritmos melhores que qualquer algoritmo clássico concebível. Um exemplo desses algoritmos é o algoritmo de Grover, capaz de encontrar k elementos (marcados) num banco de dados desordenado com N elementos em $O\left(\sqrt{N/k}\right)$ passos. O algoritmo de Grover também pode ser interpretado como um passeio quântico num grafo completo (com laços) com N vértices dos quais k são marcados. Essa interpretação estimulou a análise de algoritmos de busca em outros tipos de grafo – e.g. grafo bipartido completo, malha e hipercubo. Utilizando o operador linear que descreve o algoritmo de Grover, o algoritmo de contagem quântico resulta numa estimativa do valor k com erro da ordem de $O\left(\sqrt{k}\right)$ e em $O\left(\sqrt{N}\right)$ passos. Neste trabalho, analisa-se o problema de usar o algoritmo de contagem quântico para estimar a quantidade k de elementos marcados em outros tipos de grafos; em particular no grafo bipartido completo. De fato, conclui-se que para um subcaso desse tipo de grafo, ao executar o algoritmo proposto no máximo t vezes, é possível obter uma estimativa de k com erro da ordem de $O\left(\sqrt{k}\right)$ em $O\left(t\sqrt{N}\right)$ passos e probabilidade de sucesso maior ou igual a $\left(1-2^{-t}\right)8/\pi^2$.

Palavras-chave: Passeios quânticos. Grafo bipartido completo. Algoritmo de contagem.

Abstract

Studies on Quantum Computing have been developed since the 1980s, motivating researches on quantum algorithms better than any classical algorithm possible. An example of such algorithms is Grover's algorithm, capable of finding k (marked) elements in an unordered database with N elements using $O\left(\sqrt{N/k}\right)$ steps. Grover's algorithm can be interpreted as a quantum walk in a complete graph (with loops) containing N vertices from which k are marked. This interpretation motivated search algorithms in other graphs – complete bipartite graph, grid, and hypercube. Using Grover's algorithm's linear operator, the quantum counting algorithm estimates the value of k with an error of $O\left(\sqrt{k}\right)$ using $O\left(\sqrt{N}\right)$ steps. This work tackles the problem of using the quantum counting algorithm for estimating the value k of marked elements in other graphs; more specifically, the complete bipartite graph. It is concluded that for a particular case, running the proposed algorithm at most t times wields an estimation of k with an error of $O\left(\sqrt{k}\right)$ using $O\left(t\sqrt{N}\right)$ steps and success probability of at least $\left(1-2^{-t}\right)8/\pi^2$.

Keywords: Quantum walks. Complete bipartite graphs. Counting algorithm.

Lista de figuras

Lista de tabelas

Sumário

1 Introdução

Os computadores clássicos foram um grande avanço na humanidade possibilitando automação de tarefas como cálculos complexos. A capacidade de processamento dos computadores depende dos transistores: quão maior a quantidade de transistores, mais cálculos um computador é capaz de fazer. Logo, diminuir o tamanho dos transistores é essencial para se obter maior poder computacional numa área cada vez menor. Os avanços tecnológicos até então permitiram que os transistores (logo processadores) evoluíssem de tal forma a obedecer a Lei de Moore, que afirma que o poder computacional dobra a cada 18 meses (MOORE et al., 1965; MACK, 2011). Tais avanços fizeram com que os transistores ficassem em escala nanométrica (YU et al., 2002), a ponto de serem influenciados pelas Leis da Mecânica Quântica (NIELSEN; CHUANG, 2002). Tal influencia impede que os transistores diminuam ainda mais de tamanho e realizem computação com baixa margem de erro (NIELSEN; CHUANG, 2002). Há duas formas de contornar esse problema: utilizar computação paralela, não sendo necessário diminuir o tamanho dos transistores para melhorar o desempenho (PATT et al., 1997); ou criar computadores que se aproveitem das propriedades da Mecânica Quântica, os computadores quânticos (NIELSEN; CHUANG, 2002).

Estudos na Computação Quântica têm avançado desde a década de 1980 (FEYNMAN, 1982; DEUTSCH, 1985), numa busca incessante por algoritmos melhores que qualquer computador clássico é capaz de executar. Exemplos desses algoritmos são os algoritmos que realizam consultas a um oráculo, *e.g.* o algoritmo de Deutsch-Jozsa (DEUTSCH; JOZSA, 1992), o algoritmo de Bernstein-Vazirani (BERNSTEIN; VAZIRANI, 1997), e o algoritmo de (busca de) Grover (GROVER, 1996; GROVER, 1997). Esse tipo de algoritmo consiste de um oráculo (uma caixa preta que implementa uma função com saída binária) e o objetivo do algoritmo é extrair alguma informação dessa caixa preta fazendo o mínimo de consultas possíveis ao oráculo. No algoritmo de Grover, por exemplo, dado um banco de dados não ordenado, o oráculo marca um elemento de N e o algoritmo é capaz de encontrar o elemento marcado em $O(\sqrt{N})$ consultas ao oráculo; enquanto um computador clássico precisaria de $O(N)$ chamadas ao oráculo.

Um outro tipo de algoritmo quântico bastante estudado são os algoritmos baseados em passeios quânticos (AHARONOV; DAVIDOVICH; ZAGURY, 1993; FARHI; GUTMANN, 1998). De fato, há uma equivalência entre passeios quânticos e qualquer algoritmo por um computador quântico. (LOVETT et al., 2010). Além disso, passeios quânticos permitem a implementação de algoritmos em laboratórios sem a necessidade de um computador quântico (PORTUGAL, 2013). Sendo assim, o algoritmo de Grover também pode ser interpretado como um passeio quântico em grafos.

Shenvi, Kempe e Whaley mostraram que o algoritmo de Grover pode ser interpretado aproximadamente como um passeio quântico num hipercubo com N vértices (SHENVI; KEMPE; WHALEY, 2003); impulsionando algoritmos de busca em outros tipos de grafos. De fato, mostrou-se que o algoritmo de Grover pode ser interpretado *exatamente* como um passeio quântico no grafo completo com N vértices e laços em todos os vértices (AMBAINIS; KEMPE; RIVOSH, 2005; WONG, 2015). Um algoritmo de busca em látices 2-dimensionais quadrados (malha) com N vértices foi apresentado com complexidade de $O(\sqrt{N}\log N)$ (AMBAINIS; KEMPE; RIVOSH, 2005) e posteriormente aprimorado para $O(\sqrt{N\log N})$ (TULSI, 2008). O algoritmo de busca em látices "colméia" com N vértices também pode ser feita em $O(\sqrt{N\log N})$ (ABAL et al., 2010). Um último exemplo (e o de mais interesse para este trabalho) é a busca realizada no grafo bipartido completo em $O(\sqrt{N})$ (RHODES; WONG, 2019).

Generalizações do algoritmo de Grover marcam k elementos e o algoritmo é capaz de encontrar um elemento marcado em $O(\sqrt{N/k})$ passos (BOYER et al., 1998). Entretanto, a generalização de busca para k elementos marcados em outros grafos não é trivial: existem algumas escolhas de elementos marcados para as quais o algoritmo quântico não apresenta ganho em comparação com os algoritmos clássicos – chamadas de configurações excepcionais. Exemplos de casos excepcionais são a diagonal na malha (AMBAINIS; RIVOSH, 2008) e qualquer quantidade de elementos marcados em grafos cíclicos (WONG; SANTOS, 2017). Nahimovs e Rivosh encontraram outras configurações excepcionais na malha (NAHIMOVS; RIVOSH, 2015). Bezerra *et al.* estendem para vários elementos marcados uma técnica usada para analisar algoritmos de busca com $N \to \infty$ e apenas um elemento marcado (BEZERRA; LUGÃO; PORTUGAL, 2021; SHENVI; KEMPE; WHALEY, 2003; AMBAINIS; KEMPE; RIVOSH, 2005; PORTUGAL, 2013). O trabalho não foca em casos excepcionais e a técnica exige que algumas pré-condições sejam verdadeiras; porém, conjecturaram que não há configurações excepcionais no hipercubo, encontrando um elemento marcado em $O(\sqrt{N/k})$ (BEZERRA; LUGÃO; PORTUGAL, 2021). Já a referência (RHODES; WONG, 2019) considera a busca no grafo bipartido completo com $k \ll N$ elementos marcados, nenhuma configuração excepcional foi encontrada.

O problema de contagem surge naturalmente a partir do problema de busca: ao invés do objetivo ser encontrar um dos k elementos marcados, o foco é descobrir o valor de k. Esse problema foi atacado em (BRASSARD et al., 2002; KAYE et al., 2007); onde o algoritmo de estimativa de fase é utilizado (como uma subrotina) junto com o operador que descreve o algoritmo de Grover para obter uma estimativa de k. Essa estimativa de k pode ser utilizada para determinar a quantidade de iterações necessárias para o algoritmo de busca (NIELSEN; CHUANG, 2002).

Surpreendentemente, não foram encontrados trabalhos que utilizem o algoritmo de estimativa de fase junto com o operador linear que descreve o passeio quântico em grafos

não completos para estimar o valor de k nesses grafos. Portanto, neste trabalho, propõe-se utilizar esse método para estimar a quantidade k de vértices marcados no grafo bipartido completo utilizando o operador linear descrito pelo passeio quântico discreto com moeda nesse grafo – o mesmo utilizado em (RHODES; WONG, 2019). Em particular, foca-se no caso em que ambos os conjuntos disjuntos do grafo possuem a mesma quantidade de vértices marcados e não marcados.

A estrutura deste trabalho é descrita a seguir. Capítulo 2 revisa conceitos necessários ao longo do trabalho, como Álgebra Linear, Postulados da Mecânica Quântica e Teoria dos Grafos. Capítulo 3 apresenta o conteúdo necessário para o entendimento do algoritmo quântico de contagem, além do próprio algoritmo. Capítulo 4 foca na explicação de passeios quânticos em grafos regulares e na junção do algoritmo quântico de contagem com o passeio quântico de busca no grafo bipartido completo (as contribuições originais desta dissertação são encontradas nesse capítulo). Capítulo 5 apresenta as conclusões e considerações finais.

2 Referencial Teórico

Esse Capítulo dedica-se a introduzir conceitos que serão necessários ao longo do documento. Espera-se que o leitor tenha conhecimento prévio de Álgebra Linear e números complexos. Seção 2.1 resume os conceitos necessários pra computação quântica e entendimento dos algoritmos apresentados posteriormente. Seção 2.2 aborda os conceitos de Teoria dos Grafos necessários.

2.1 Computação Quântica

Seção 2.1.1 revisa conceitos de Álgebra Linear utilizando a notação de Dirac; Seção 2.1.2 aborda como os conceitos de Álgebra Linear são utilizados para descrever a Mecânica Quântica e seus postulados; Seção 2.1.3 introduz a representação de circuitos utilizada na implementação ou explicação de algoritmos quânticos.

2.1.1 Álgebra Linear

Em Computação Quântica, trabalha-se normalmente com número complexos. Ressalta-se aqui algumas definições básicas de números complexos.

Definição 2.1. A unidade imaginária é representada por $\mathrm{i} = \sqrt{-1}$. —

Definição 2.2. Define-se um número complexo $z = a + \mathrm{i}b$, onde $a, b \in \mathbb{R}$, onde a é chamada de parte real e b de parte imaginária. Denota-se a parte real de z por $a = \Re(z)$. —

Definição 2.3. O complexo conjugado de $z \in \mathbb{C}$ é dado por

$$z^* = (a + \mathrm{i}b)^* = a - \mathrm{i}b. \tag{2.1}$$

—

O livro do Axler é uma referência consolidada em Álgebra Linear (AXLER, 2014). Seja $N \in \mathbb{N}$ tal que $N \geq 1$. Em Álgebra Linear, normalmente $\vec{v}$ denota um vetor e representa uma lista de N elementos complexos (ou entradas complexas); ou seja, $\vec{v} \in \mathbb{C}^N$. Esses N elementos podem ser explicitados através da representação

$$\vec{v} = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix}, \tag{2.2}$$

onde $v_0, v_1, \ldots, v_{N-1} \in \mathbb{C}$. Ao longo do restante desse trabalho, como usual na Mecânica e Computação Quântica, utiliza-se a notação de Dirac para representação de vetores. Então, o mesmo vetor $\vec{v}$ é representado como $|v\rangle$ – leia-se *ket v*.

Toda a análise em Álgebra Linear é feita num espaço denominado espaço vetorial. Para definir espaço vetorial, é necessário definir *adição* e *multiplicação por escalar* num conjunto V.

Definição 2.4. Seja V um conjunto de vetores em $\mathbb{C}^N$. Para todos $|u\rangle, |v\rangle \in V$, a adição é definida como uma função tal que $|u\rangle + |v\rangle \in V$. Para este trabalho, utiliza-se a adição

$$|u\rangle + |v\rangle = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{N-1} \end{bmatrix} + \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix} = \begin{bmatrix} u_0 + v_0 \\ u_1 + v_1 \\ \vdots \\ u_{N-1} + v_{N-1} \end{bmatrix}. \tag{2.3}$$

—

Definição 2.5. Seja V um conjunto de vetores em $\mathbb{C}^N$. Para todos $|v\rangle \in V$ e $c \in \mathbb{C}$, a multiplicação por escalar é uma função tal que $c\,|v\rangle \in V$. Para este trabalho, utiliza-se a multiplicação por escalar

$$c\,|v\rangle = c \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix} = \begin{bmatrix} cv_0 \\ cv_1 \\ \vdots \\ cv_{N-1} \end{bmatrix}. \tag{2.4}$$

—

Definição 2.6. Sejam V um conjunto de vetores em $\mathbb{C}^N$. Um espaço vetorial consiste do conjunto V munido de adição e multiplicação por escalar definidas em V de tal modo que as seguintes propriedades sejam verdadeiras; para todos $|t\rangle, |u\rangle, |v\rangle \in V$ e $c, c' \in \mathbb{C}$.

- Comutatividade: $|u\rangle + |v\rangle = |v\rangle + |u\rangle$;
- Associatividade: $(|t\rangle + |u\rangle) + |v\rangle = |t\rangle + (|u\rangle + |v\rangle)$;
- Identidade aditiva: existe um vetor nulo $\vec{0} \in V$ tal que $\vec{0} + |v\rangle = |v\rangle$. Para este trabalho, [1]

$$\vec{0} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}; \tag{2.5}$$

[1] Para o vetor nulo, utiliza-se $\vec{0}$ ao invés de $|0\rangle$, pois um significado distinto é normalmente atribuído para $|0\rangle$.

- Inverso aditivo: $\exists\,|v'\rangle \in V$ tal que $|v'\rangle = -\,|v\rangle$ e $|v'\rangle + |v\rangle = -\,|v\rangle + |v\rangle = \vec{0}$;
- Identidade multiplicativa: $1 \in \mathbb{C}$ tal que $1\,|v\rangle = |v\rangle$;
- Propriedades distributivas:
  - $c\,(|u\rangle + |v\rangle) = c\,|u\rangle + c\,|v\rangle$;
  - $(c + c')\,|v\rangle = c\,|v\rangle + c'\,|v\rangle$.

—

A definição de subespaço vetorial também é relevante para este trabalho.

Definição 2.7. Seja V' um subconjunto (não necessariamente próprio) de V. V' é dito um subespaço de V se V' também for um espaço vetorial usando a mesma adição e multiplicação por escalar definidas para V. —

Por exemplo,

$$V' = \left\{ \begin{bmatrix} v_0 \\ v_1 \\ 0 \end{bmatrix} \right\} \tag{2.6}$$

para todo $v_0, v_1 \in \mathbb{C}$ é um subespaço vetorial de $\mathbb{C}^3$, ou simplesmente um subespaço.

Deseja-se obter maneiras simplificadas para descrever um espaço vetorial. Para tanto, a definição de conjunto gerador é útil.

Definição 2.8. Seja V um espaço vetorial e S um subconjunto de vetores de V. S é um conjunto gerador de V se e somente se $\forall\,|v\rangle \in V$, $|v\rangle$ pode ser escrito como uma combinação linear dos vetores em S. Em outras palavras,

$$\text{span}\,(S) = V \iff \forall\,|v\rangle \in V, |v\rangle = \sum_{i=1}^{|S|} \alpha_i\,|S_i\rangle\,, \tag{2.7}$$

onde $\alpha_i \in \mathbb{C}$, $|S_i\rangle \in S$, e α_i é denominada amplitude de $|S_i\rangle$. —

Um exemplo de um conjunto gerador para $\mathbb{C}^2$ é o conjunto $\{\,|0\rangle\,, |1\rangle\,\}$, onde

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.8}$$

Note que qualquer vetor $|v\rangle \in \mathbb{C}^2$ pode ser escrito como

$$|v\rangle = \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} = v_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + v_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = v_0\,|0\rangle + v_1\,|1\rangle = \sum_{i=0}^{1} v_i\,|i\rangle\,, \tag{2.9}$$

onde $v_0, v_1 \in \mathbb{C}$.

Na definição 2.8 não restringiu-se a cardinalidade de S. Logo, é possível que um vetor tenha múltiplas representações dependendo de S. Por exemplo, se $S = \{ |0\rangle, |1\rangle, |+\rangle \}$, onde

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \tag{2.10}$$

existem no mínimo duas representações possíveis para $\vec{0}$:

$$0\,|0\rangle + 0\,|1\rangle + 0\,|+\rangle = \vec{0} = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle - |+\rangle\,. \tag{2.11}$$

De modo geral, é desejável que $|S|$ tenha o menor valor possível para simplificar essas representações. Esses pontos motivam as definições de vetores *linearmente independentes* e *base*.

Definição 2.9. Um conjunto $S \in V$ de vetores é dito linearmente independente se a única escolha de $\alpha_1, \ldots, \alpha_{|S|} \in \mathbb{C}$ tais que

$$\sum_{i=1}^{|S|} \alpha_i\,|S_i\rangle = \vec{0} \tag{2.12}$$

é $\alpha_1, \ldots, \alpha_{|S|} = 0$, onde $|S_i\rangle \in S$. —

Definição 2.10. Um conjunto $S \in V$ de vetores é uma base de V se e somente se S é linearmente independente e $\text{span}\,(S) = V$. Além disso, $V = \mathbb{C}^N \implies |S| = N$. —

Nesse âmbito, $\{ |0\rangle, |1\rangle, |+\rangle \}$ não são linearmente independentes (*i.e.* são linearmente dependentes), e tanto $\{ |0\rangle, |1\rangle \}$ quanto $\{ |0\rangle, |+\rangle \}$ são bases de $\mathbb{C}^2$. Como existe mais de uma base para um espaço vetorial, é desejável ter um modo sistemático para conversão entre bases (ou vetores) de um mesmo espaço vetorial ou até mesmo mapear vetores de um espaço vetorial para outro distinto; o que motiva a definição de *transformações lineares* e *operadores lineares*.

Definição 2.11. Sejam V e W espaços vetoriais. Uma transformação linear é uma função $T : V \to W$ que possui as propriedades de aditividade e homogeneidade. Ou seja, para $|v_i\rangle \in V$ e $\alpha_i \in \mathbb{C}$,

$$T \sum_i \alpha_i\,|v_i\rangle = T\left(\sum_i \alpha_i\,|v_i\rangle\right) = \sum_i \alpha_i T\,(|v_i\rangle) = \sum_i \alpha_i T\,|v_i\rangle\,. \tag{2.13}$$

—

Definição 2.12. Seja V um espaço vetorial e uma transformação linear $T : V \to V$, por ter imagem e domínio no mesmo espaço vetorial, chama-se T de um operador linear. —

Normalmente, omite-se os parênteses. Desse modo, sendo V_1, V_2 e V_3 espaços vetoriais e $T_1 : V_1 \to V_2$ e $T_2 : V_2 \to V_3$ transformações lineares; denota-se a composição de funções $T_2\left(T_1\left(|v\rangle\right)\right)$ simplesmente por $T_2 T_1 |v\rangle$, onde $|v\rangle \in V_1$. Um operador linear de interesse é o operador identidade.

Definição 2.13. Seja V um espaço vetorial. O operador identidade $I_V : V \to V$ é tal que $\forall\, |v\rangle \in V$,

$$I_V |v\rangle = |v\rangle\,. \tag{2.14}$$

O operador identidade é representado simplesmente por I quando não há ambiguidade no contexto. —

Para interpretar uma transformação linear como mudança de bases, considere os espaços vetoriais V e W espaços vetoriais cujas bases são $\{\, |V_j\rangle \,\}$, $\{\, |W_i\rangle \,\}$, respectivamente; e seja $T : V \to W$ uma transformação linear. Sendo assim, para $|w_j\rangle \in W$ existem valores $T_{i,j} \in \mathbb{C}$ tais que

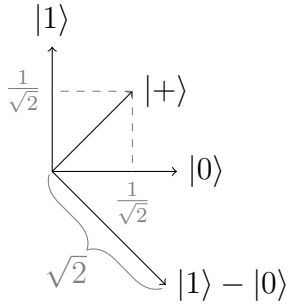
$$T |V_j\rangle = |w_j\rangle = \sum_i T_{i,j} |W_i\rangle\,. \tag{2.15}$$

Esse resultado sugere que T pode ser representado como uma matriz cujas entradas são $T_{i,j}$:

$$T = \begin{bmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,|V|} \\ T_{2,1} & T_{2,2} & \cdots & T_{2,|V|} \\ \vdots & \vdots & \ddots & \vdots \\ T_{|W|,1} & T_{|W|,2} & \cdots & T_{|W|,|V|} \end{bmatrix}, \tag{2.16}$$

onde $|V| = |\{\, |V_j\rangle \,\}|$ e $|W| = |\{\, |W_i\rangle \,\}|$. Para representar T utilizando notação de Dirac, é necessário saber como calcular os valores $T_{i,j}$. Para isso, introduz-se o conceito de *produto interno*.

Figura 1 – Projeção e comprimento de vetores.



Fonte: Produzido pelo autor.

Há mais motivos para formalizar produto interno. Considere os vetores $|0\rangle$, $|1\rangle$ e $|+\rangle$ representado no plano dos reais – Figura 1 (Fig. 1) – observa-se que $|0\rangle$ e $|1\rangle$ são vetores perpendiculares; logo, a projeção de $|0\rangle$ em $|1\rangle$ é 0 e vice-versa. Entretanto, o mesmo não acontece com a projeção de $|+\rangle$ em $|0\rangle$ ou $|1\rangle$, que é igual a $1/\sqrt{2}$. Outro valor escalar que é relavante é o comprimento dos vetores. Por exemplo, $|0\rangle$ tem comprimento 1, mas $|0\rangle - |1\rangle$ possui comprimento $\sqrt{2}$. Os cálculos dessas projeções e comprimentos foram obtidos facilmente, mas definir um modo sistemático e geral para calcular esses valores é mais útil. Isso pode ser feito utilizando-se *produto interno* e *norma*.

Definição 2.14. Seja V um espaço vetorial. O produto interno é uma função $(\cdot,\cdot) : V \times V \to \mathbb{C}$ tal que $\forall\, |u\rangle, |v_i\rangle \in V$ e $\alpha_i \in \mathbb{C}$ as seguintes propriedades são verdadeiras.

- Positividade: $(|u\rangle, |u\rangle) \geq 0$ com igualdade se e somente se $|u\rangle = \vec{0}$;
- Aditividade e homogeneidade no segundo argumento:

$$\left(|u\rangle, \sum_i \alpha_i |v_i\rangle\right) = \sum_i \alpha_i \left(|u\rangle, |v_i\rangle\right); \tag{2.17}$$

- Simetria Hermitiana: $(|u\rangle, |v_i\rangle) = (|v_i\rangle, |u\rangle)^*$.

—

Todo produto interno possui as propriedades de aditividade, e de homogeneidade conjugada no primeiro argumento:

$$\left(\sum_i \alpha_i |v_i\rangle, |u\rangle\right) = \left(|u\rangle, \sum_i \alpha_i |v_i\rangle\right)^* = \sum_i \alpha_i^* \left(|u\rangle, |v_i\rangle\right)^* = \sum_i \alpha_i^* \left(|v_i\rangle, |u\rangle\right). \tag{2.18}$$

Definição 2.15. Se V é um espaço vetorial munido de um produto interno, então é denominado *espaço de Hilbert* e denotado por $\mathcal{H}$. —

Ao longo deste trabalho, utiliza-se $\mathcal{H}^N$ para se referir ao espaço vetorial $\mathbb{C}^N$ munido de um produto interno.

Definição 2.16. A norma de um vetor $|v\rangle \in \mathcal{H}$ é dada por

$$|||v\rangle|| = \sqrt{(|v\rangle, |v\rangle)}. \tag{2.19}$$

Um vetor $|v\rangle$ é dito unitário se $|||v\rangle|| = 1$. —

Um produto interno em $\mathbb{C}^N$ é o produto escalar.

Definição 2.17. Sejam $|u\rangle, |v\rangle \in \mathbb{C}^N$. O produto escalar é definido por

$$(|u\rangle, |v\rangle) = \sum_{i=0}^{N-1} u_i^* v_i = \begin{bmatrix} u_0^*, u_1^*, \ldots, u_{N-1}^* \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix}. \tag{2.20}$$

—

Note que o produto escalar é equivalente a uma multiplicação de matrizes, mas antes de realizar essa multiplicação, tomou-se o transposto conjugado de $|u\rangle$. O vetor transposto conjugado também é chamado de vetor dual. Observe também que o vetor dual pode ser interpretado como uma transformação linear $\mathbb{C}^N \to \mathbb{C}$; de fato, ele é definido de tal forma.

Definição 2.18. Para todo $|u\rangle, |v\rangle \in \mathcal{H}^N$, o vetor dual (leia-se *bra u*) $\langle u| \equiv |u\rangle^\dagger$ é uma transformação linear $\mathbb{C}^N \to \mathbb{C}$ tal que

$$\langle u \,|\, v\rangle = \langle u| \, |v\rangle = (|u\rangle, |v\rangle). \tag{2.21}$$

—

Em posse da definição de produto interno e de norma, é possível definir ortogonalidade e ortonormalidade, que se relacionam com a perpendicularidade argumentada previamente.

Definição 2.19. Sejam $|u\rangle, |v\rangle \in \mathcal{H}$. Esses vetores são ditos ortogonais se $\langle u \,|\, v\rangle = 0$. —

Definição 2.20. Sejam $|u\rangle, |v\rangle \in \mathcal{H}$. Esses vetores são ditos ortonormais se $\langle u \,|\, v\rangle = 0$ e $|||u\rangle|| = |||v\rangle|| = 1$. —

Recorrendo novamente à Fig. 1 têm-se uma interpretação geométrica de vetores ortogonais ($|+\rangle$ e $|0\rangle - |1\rangle$) e vetores ortonormais ($|0\rangle$ e $|1\rangle$). Essas definições estendem-se facilmente para um conjunto de vetores. O conjunto $\{\, |V_i\rangle \,\} \in V$ é dito ortonormal se $\langle V_i \,|\, V_j\rangle = 0$ e $|||V_i\rangle|| = 1$ para todo $i \neq j$. Além disso, se o conjunto for uma base de V, diz-se que $\{\, |V_i\rangle \,\}$ é uma base ortonormal. Isso motiva a definição do delta de Kronecker.

Definição 2.21. Seja $\{\, |V_i\rangle \,\}$ um conjunto de vetores ortonormais indexados por i. O delta de Kronecker é uma função de duas variáveis tal que

$$\delta_{i,j} = \langle V_i \,|\, V_j\rangle = \begin{cases} 1 & \text{se } i = j; \\ 0 & \text{se } i \neq j. \end{cases} \tag{2.22}$$

—

Utilizando bases ortonormais, delta de Kronecker, e as propriedades de produto interno, é possível obter uma representação matricial para o vetor dual. Sejam dois vetores $|v\rangle = \sum_i v_i |S_i\rangle$ e $|u\rangle = \sum_i u_i |S_i\rangle$ onde $v_i, u_i, \in \mathbb{C}$,

$$\langle u \,|\, v\rangle = \left(\sum_i u_i |S_i\rangle \,, \sum_j v_j |S_j\rangle \right) \tag{2.23}$$

$$= \sum_{i,j} u_i^* v_j \langle S_i \,|\, S_j\rangle \tag{2.24}$$

$$= \sum_{i,j} u_i^* v_j \delta_{i,j} \tag{2.25}$$

$$= \sum_i u_i^* v_i. \tag{2.26}$$

Ou seja, se $|u\rangle$ e $|v\rangle$ forem representados com a mesma base, o vetor dual $\langle u|$ é o transposto conjugado de $|u\rangle$.

Retornando ao tópico de transformações lineares, é possível representar uma transformação linear entre espaços de Hilbert utilizando notação de Dirac. Essa transformação é representada através de *produtos externos*.

Definição 2.22. Sejam V e W espaços de Hilbert, e $|v\rangle, |v'\rangle \in V$ e $|w\rangle \in W$. Utiliza-se o produto externo $|w\rangle \langle v|$ para definir uma transformação linear $|w\rangle \langle v| : V \to W$ cuja ação é dada por

$$(|w\rangle \langle v|) |v'\rangle = |w\rangle \langle v| |v'\rangle = |w\rangle \langle v \,|\, v'\rangle = \langle v \,|\, v'\rangle |w\rangle \,. \tag{2.27}$$

—

Essa representação em produto externo sugere que uma transformação linear $T : V \to W$ descreve uma relação entre bases ortonormais $\{ |V_j\rangle \}$ de V e $\{ |W_i\rangle \}$ de W. Para dar continuidade, a *relação de completude* faz-se necessária

Definição 2.23. Seja $\{ |V_i\rangle \}$ uma base ortonormal de Hilbert V. A relação de completude assegura que

$$\sum_i |V_i\rangle \langle V_i| = I. \tag{2.28}$$

—

Note que isso é verdade já que $\forall\, |v\rangle \in V$,

$$|v\rangle = I\,|v\rangle = I \sum_{i'} v_{i'}\,|V_{i'}\rangle \tag{2.29}$$

$$= \sum_{i} |V_i\rangle\,\langle V_i| \sum_{i'} v_{i'}\,|V_{i'}\rangle \tag{2.30}$$

$$= \sum_{i,i'} |V_i\rangle\, v_{i'}\delta_{i,i'} \tag{2.31}$$

$$= \sum_{i'} v_{i'}\,|V_{i'}\rangle \tag{2.32}$$

$$= |v\rangle\,, \tag{2.33}$$

onde $v_{i'} \in \mathbb{C}$. Analogamente, considere o vetor dual $|v\rangle$, então $\forall\, |v'\rangle \in V$,

$$\langle v\,|\,v'\rangle = \langle v|\,I\,|v'\rangle \tag{2.34}$$

$$= \langle v| \left(\sum_{i} |V_i\rangle\,\langle V_i| \right) \sum_{i'} v_{i'}\,|V_{i'}\rangle \tag{2.35}$$

$$= \langle v| \sum_{i,i'} |V_i\rangle\, v_{i'}\delta_{i,i'} \tag{2.36}$$

$$= \langle v|\,|v'\rangle = \langle v\,|\,v'\rangle\,. \tag{2.37}$$

Sendo assim, denote por $\{\,|V_j\rangle\,\}$ e $\{\,|W_i\rangle\,\}$ bases ortonormais dos espaços de Hilbert V e W, respectivamente; e $T : V \to W$ uma transformação linear. Então,

$$T = I_W T I_V \tag{2.38}$$

$$= \sum_{i} |W_i\rangle\,\langle W_i|\,T \sum_{j} |V_j\rangle\,\langle V_j| \tag{2.39}$$

$$= \sum_{i,j} |W_i\rangle\,\langle W_i|\,T\,|V_j\rangle\,\langle V_j| \tag{2.40}$$

$$= \sum_{i,j} \langle W_i|\,T\,|V_j\rangle\,|W_i\rangle\,\langle V_j|\,. \tag{2.41}$$

Note que $\langle W_i|\,T\,|V_j\rangle \in \mathbb{C}$, já que as transformações lineares

$$T : V \to W \text{ e } \langle W_i| : W \to \mathbb{C} \implies \langle W_i|\,T : V \to \mathbb{C}. \tag{2.42}$$

A Equação 2.41 (Eq. 2.41) sugere que é possível obter uma representação matricial para T com respeito à base de entrada $\{\,|V_j\rangle\,\}$ e à base de saída $\{\,|W_i\rangle\,\}$. Ordene as bases

ortonormais pelos índices i e j, e denote $T_{i,j} = \langle W_i | T | V_j \rangle$. A matriz de T é dada por

$$T = T_{1,1} |W_1\rangle \langle V_1| + \sum_{\substack{i,j \\ (i,j)\neq(1,1)}} T_{i,j} |W_i\rangle \langle V_j| \tag{2.43}$$

$$= T_{1,1} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \end{bmatrix} + \sum_{\substack{i,j \\ (i,j)\neq(1,1)}} T_{i,j} |W_i\rangle \langle V_j| \tag{2.44}$$

$$= \begin{bmatrix} T_{1,1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} + \sum_{\substack{i,j \\ (i,j)\neq(1,1)}} T_{i,j} |W_i\rangle \langle V_j| \tag{2.45}$$

$$= \begin{bmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,|V|} \\ T_{2,1} & T_{2,2} & \cdots & T_{2,|V|} \\ \vdots & \vdots & \ddots & \vdots \\ T_{|W|,1} & T_{|W|,2} & \cdots & T_{|W|,|V|} \end{bmatrix}, \tag{2.46}$$

onde (i, j) representam tuplas; $|V| = |\{ |V_i\rangle \}|$; $|W| = |\{ |W_j\rangle \}|$; $1 \leq i \leq |V|$; $1 \leq j \leq |W|$; e os vetores linha $\begin{bmatrix} b_1 & \cdots & b_N \end{bmatrix}$ com $b_i = 1$ e $b_{i'} = 0$ caso $i' \neq i$ indicam que deve-se utilizar o dual de $|V_i\rangle$ (análogo para a relação entre vetores coluna com a utilização dos vetores $|W_j\rangle$).

Do mesmo modo que existem funções invertíveis, deseja-se saber se um operador linear T é invertível ou não. Uma transformação linear $T : V \to W$ é invertível se e somente se for injetiva e sobrejetiva (AXLER, 2014). De particular interesse para esse trabalho, são as transformações lineares invertíveis com imagem e domínio iguais, *e.g.* $T : V \to V$. Se T for invertível, então existe uma transformação linear T^{-1} tal que

$$TT^{-1} = T^{-1}T = I. \tag{2.47}$$

Para dar continuidade, é necessário definir transformações lineares adjuntas, análogo ao que foi feito na definição 2.18 (def. 2.18). Essa definição é consequência do Teorema de representação de Riesz (AXLER, 2014).

Definição 2.24. Sejam V, W espaços de Hilbert; denotando o produto interno de W por $(\cdot, \cdot)$ – def. 2.14 – e uma transformação linear $T : V \to W$. A transformação linear adjunta $T^\dagger : W \to V$ de $T : V \to W$ é tal que $\forall v \in V$ e $\forall |w\rangle \in W$,

$$(|w\rangle, T |v\rangle) = \left(T^\dagger |w\rangle, |v\rangle\right). \tag{2.48}$$

Sejam V, W e W' espaços de Hilbert; $T, T_1, T_2 : V \to W$, $T_1 : W' \to W$ e $T_2 : V \to W'$ transformações lineares tais que $T = L_1 + L_2$, $T = T_1 T_2$ e $T = T_{i,j} \left|W_i\right\rangle \left\langle V_j\right|$ para $T_{i,j} \in \mathbb{C}$ e bases ortonormais $\{ \left|V_j\right\rangle \}$, $\{ \left|W_i\right\rangle \}$ de V, W, respectivamente. Usando as propriedades de produtos internos, e a definição de transformação linear adjunta, conclui-se que as seguintes propriedades são verdadeiras.

- $(L_1 + L_2)^\dagger = L_1^\dagger + L_2^\dagger$:

$$\begin{aligned}
\left(\left|w\right\rangle, T\left|v\right\rangle\right) &= \left(\left|w\right\rangle, L_1\left|v\right\rangle\right) + \left(\left|w\right\rangle, L_2\left|v\right\rangle\right) && (2.49)\\
&= \left(L_1^\dagger\left|w\right\rangle, \left|v\right\rangle\right) + \left(L_2^\dagger\left|w\right\rangle, \left|v\right\rangle\right) && (2.50)\\
&= \left(\left(L_1^\dagger + L_2^\dagger\right)\left|w\right\rangle, \left|v\right\rangle\right) && (2.51)\\
&= \left(T^\dagger\left|w\right\rangle, \left|v\right\rangle\right); && (2.52)
\end{aligned}$$

- $(T_1 T_2)^\dagger = T_2^\dagger T_1^\dagger$:

$$\begin{aligned}
\left(\left|w\right\rangle, T\left|v\right\rangle\right) &= \left(\left|w\right\rangle, T_1 T_2\left|v\right\rangle\right) = \left(T_1^\dagger\left|w\right\rangle, T_2\left|v\right\rangle\right) && (2.53)\\
&= \left(T_2^\dagger T_1^\dagger\left|w\right\rangle, \left|v\right\rangle\right) = \left(T^\dagger\left|w\right\rangle, \left|v\right\rangle\right); && (2.54)
\end{aligned}$$

- Notando que $\left|v\right\rangle$ pode ser interpretado como uma transformação linear de $\mathbb{C}$ para V e relambrando que $\left\langle v\right| \equiv \left|v\right\rangle^\dagger$, obtém-se que $\left(T\left|v\right\rangle\right)^\dagger = \left\langle v\right| T^\dagger$:

$$\left(\left|w\right\rangle 1, \left(T\left|v\right\rangle\right) 1\right) = \left(T^\dagger\left|w\right\rangle 1, \left|v\right\rangle 1\right) = \left(\left\langle v\right| T^\dagger\left|w\right\rangle 1, 1\right) = \left(\left(T\left|v\right\rangle\right)^\dagger\left|w\right\rangle 1, 1\right); \quad (2.55)$$

- $\left(T^\dagger\right)^\dagger = T$:

$$\begin{aligned}
\left(\left|w\right\rangle, T\left|v\right\rangle\right) &= \left(T^\dagger\left|w\right\rangle, \left|v\right\rangle\right) = \left(\left|v\right\rangle, T^\dagger\left|w\right\rangle\right)^* && (2.56)\\
&= \left(\left(T^\dagger\right)^\dagger\left|v\right\rangle, \left|w\right\rangle\right)^* = \left(\left|w\right\rangle, \left(T^\dagger\right)^\dagger\left|v\right\rangle\right). && (2.57)
\end{aligned}$$

- $T^\dagger = \sum_{i,j} T_{i,j}^* \left|V_j\right\rangle \left\langle V_i\right|$ – *i.e.* representação de $T^\dagger$ em notação de Dirac:

$$\begin{aligned}
\left(\left|w\right\rangle, T\left|v\right\rangle\right) &= \left(\left|w\right\rangle, \sum_{i,j} T_{i,j}\left|V_i\right\rangle\left\langle V_j\right|\left|v\right\rangle\right) = \sum_{i,j} T_{i,j}\left(\left|w\right\rangle, \left|V_i\right\rangle\left\langle V_j\right|\left|v\right\rangle\right) && (2.58)\\
&= \sum_{i,j} T_{i,j}\left(\left\langle V_j\right|^\dagger\left|V_i\right\rangle^\dagger\left|w\right\rangle, \left|v\right\rangle\right) = \sum_{i,j} T_{i,j}\left(\left|V_j\right\rangle\left\langle V_i\right|\left|w\right\rangle, \left|v\right\rangle\right) && (2.59)\\
&= \left(\sum_{i,j} T_{i,j}^*\left|V_j\right\rangle\left\langle V_i\right|\left|w\right\rangle, \left|v\right\rangle\right) = \left(T^\dagger\left|w\right\rangle, \left|v\right\rangle\right); && (2.60)
\end{aligned}$$

- $I^\dagger = I$: segue da relação de completude e da propriedade anterior.

Essas propriedades permitem manipular transformações lineares adjuntas sem ter que recorrer à definição frequentemente.

A definição de adjunto leva à definição de outros tipos de operadores, *e.g.* Hermitiano, projetores, normais e unitários. Seja V um espaço de Hilbert com dimensão N, então,

Definição 2.25. Um operador $T : V \to V$ é Hermitiano se $T = T^\dagger$. —

Definição 2.26. Seja W um subespaço de V com bases ortonormais $\{ |W_i\rangle \} \subseteq \{ |V_j\rangle \}$, respectivamente. Define-se um projetor de V em W por

$$P = \sum_i |W_i\rangle \langle W_i| . \tag{2.61}$$

—

Um projetor P é Hermitiano já que

$$P^\dagger = \left(\sum_i |W_i\rangle \langle W_i| \right)^\dagger = \sum_i \langle W_i|^\dagger |W_i\rangle^\dagger = \sum_i |W_i\rangle \langle W_i| = P, \tag{2.62}$$

e $P^2 = P$ já que

$$P^2 = \left(\sum_i |W_i\rangle \langle W_i| \right) \left(\sum_j |W_j\rangle \langle W_j| \right) = \sum_{i,j} |W_i\rangle \delta_{i,j} \langle W_j| = \sum_i |W_i\rangle \langle W_i| = P. \tag{2.63}$$

Definição 2.27. Um operador $T : V \to V$ é normal se $T^\dagger T = T T^\dagger$. —

Note que operadores Hermitianos são normais. Operadores normais têm uma representação especial dada pelo Teorema Espectral.

Teorema 1. *Teorema Espectral: Um operador normal $T : V \to V$ é diagonalizável. Isto é, existem valores $\lambda_i \in \mathbb{C}$ e uma base ortonormal $\{ |\lambda_i\rangle \}$ de T tal que*

$$T = \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i| = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_N \end{bmatrix}. \tag{2.64}$$

—

Devido ao nome do Teorema, a base $\{ |\lambda_i\rangle \}$ é comumente chamada de *decomposição espectral* de T. Note que $\{ \lambda_i \}$ permite calcular a saída de T de modo simples, já que

$$T |\lambda_j\rangle = \sum_i \lambda_i |\lambda_i\rangle \langle \lambda_i | \lambda_j\rangle = \sum_i \lambda_i |\lambda_i\rangle \delta_{i,j} = \lambda_j |\lambda_j\rangle \tag{2.65}$$

e para qualquer vetor $|v\rangle$ de V, $|v\rangle = \sum_j v_j |\lambda_j\rangle$ com $v_j \in \mathbb{C}$,

$$T |v\rangle = T \sum_j v_j |\lambda_j\rangle = \sum_j v_j \lambda_j |\lambda_j\rangle . \tag{2.66}$$

Por proporcionarem tal simplicidade, atribui-se nomes específicos para esses valores e vetores.

Definição 2.28. Para uma transformação linear $T : V \to V$, seja um vetor $|\lambda\rangle \in V$ e um valor $\lambda \in \mathbb{C}$ tais

$$T\,|\lambda\rangle = \lambda\,|\lambda\rangle\,. \tag{2.67}$$

Então, diz-se λ é um *autovalor* de T e que $|\lambda\rangle$ é um *autovetor* de T associado ao autovalor λ. Alternativamente, diz-se que $|\lambda\rangle$ é um λ-autovetor de T. —

Um tipo especial de operador normal são os operadores unitários.

Definição 2.29. Um operador $U : V \to V$ é unitário se $U^\dagger U = UU^\dagger = I$. —

Da definição segue que U é invertível e sua inversa é $U^\dagger$. Operadores unitários têm a propriedade de preservar o produto interno entre dois vetores, consequentemente a norma se preserva. Sejam $|u\rangle$, $|v\rangle \in V$, então

$$(U\,|u\rangle\,, U\,|v\rangle) = \langle u|\,U^\dagger U\,|v\rangle = \langle u\,|\,v\rangle\,. \tag{2.68}$$

Já que o produto interno é preservado, ao tomar uma base $\{\,V_i\,\}$ de V e denotando $|U_i\rangle = U\,|V_i\rangle$, conclui-se que $U = \sum_i |U_i\rangle\,\langle V_i|$. Note que esse resultado é consistente com a eq. 2.41 e que $\langle V_i\,|\,V_j\rangle = \langle U_i\,|\,U_j\rangle$. Uma consequência da preservação de norma é que os autovalores de U também têm norma 1, *i.e.* se $|\lambda_j\rangle$ é um λ_j-autovetor de U, então $\lambda_j = e^{\mathrm{i}\theta_j} = \exp \mathrm{i}\theta_j$ onde e é o número de Euler e $\theta_j \in \mathbb{R}$. Note que

$$U\,|\lambda_j\rangle = e^{\mathrm{i}\theta_j}\,|\lambda_j\rangle \implies \left|\left|e^{\mathrm{i}\theta_j}\,|\lambda_j\rangle\right|\right|^2 = \langle\lambda_j|\,e^{-\mathrm{i}\theta_j}e^{\mathrm{i}\theta_j}\,|\lambda_j\rangle = \langle\lambda_j\,|\,\lambda_j\rangle = 1, \tag{2.69}$$

conforme desejado.

Sejam V_1 e V_2 espaços de Hilbert com dimensões N_1 e N_2, respectivamente. Analisa-se o problema de utilizar V_1 e V_2 para representar um espaço vetorial de maior dimensão. Mais especificamente, o espaço de Hilbert $V = V_1 \otimes V_2$ (leia-se V_1 tensor V_2) com dimensão N_1N_2. O símbolo $\otimes$ indica produto tensorial, cuja definição é dada a seguir.

Definição 2.30. Sejam V_1 e V_2 espaços vetoriais, $|v_1\rangle\,, |v_1'\rangle \in V_1$, $|v_2\rangle\,, |v_2'\rangle \in V_2$ e $c \in \mathbb{C}$. Então um produto tensorial $V_1 \otimes V_2$ satisfaz as seguintes propriedades.

- $c\,(|v_1\rangle \otimes |v_2\rangle) = (c\,|v_1\rangle) \otimes |v_2\rangle = |v_1\rangle \otimes (c\,|v_2\rangle)$;
- $(|v_1\rangle + |v_1'\rangle) \otimes |v_2\rangle = (|v_1\rangle \otimes |v_2\rangle) + (|v_1'\rangle \otimes |v_2\rangle)$;
- $|v_1\rangle \otimes (|v_2\rangle + |v_2'\rangle) = (|v_1\rangle \otimes |v_2\rangle) + (|v_1\rangle \otimes |v_2'\rangle)$.

—

Em outras palavras, o produtor tensorial mantém a linearidade em ambos os subespaços separados e "estende" a linearidade para $V_1 \otimes V_2$. Note também que

$$(|v_1\rangle + |v_1'\rangle) \otimes (|v_2\rangle + |v_2'\rangle) = |v_1\rangle \otimes |v_2\rangle + |v_1'\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |v_2'\rangle \quad (2.70)$$

é a combinação linear de quatro vetores em $V_1 \otimes V_2$. Seguindo esse mesmo raciocínio, para bases ortonormais $\{ V_{1,i} \}$ de V_1 e $\{ V_{2,j} \}$ de V_2, qualquer vetor $|v\rangle \in V$ pode ser escrito como uma combinação linear

$$\left(\sum_i v_{1,i} |V_{1,i}\rangle \right) \otimes \left(\sum_j v_{2,j} |V_{2,j}\rangle \right) = \sum_{i,j} v_{1,i} v_{2,j} |V_{1,i}\rangle \otimes |V_{2,j}\rangle , \quad (2.71)$$

onde $v_{1,i}, v_{2,j} \in \mathbb{C}$. Perceba que isso resulta numa base $N_1 N_2$-dimensional de V. A representação matricial pode ajudar no entendimento. Considerando $|v_1\rangle \otimes |v_2\rangle \in V$, então, para $v_{1,i}, v_{2,j} \in \mathbb{C}$,

$$|v_1\rangle \otimes |v_2\rangle = \left(\sum_i v_{1,i} \right) \otimes |v_2\rangle = \begin{bmatrix} v_{1,1} |v_2\rangle \\ \vdots \\ v_{1,N_1} |v_2\rangle \end{bmatrix} = \begin{bmatrix} v_{1,1} v_{2,1} \\ \vdots \\ v_{1,1} v_{2,N_2} \\ v_{1,2} v_{2,1} \\ \vdots \\ v_{1,2} v_{2,N_2} \\ \vdots \\ v_{1,N_1} v_{2,N_2} \end{bmatrix} . \quad (2.72)$$

Para simplificar a notação, é comum representar $|v_1\rangle \otimes |v_2\rangle = |v_1\rangle |v_2\rangle = |v_1, v_2\rangle = |v_1 v_2\rangle$.

É interessante também estender os conceitos vistos até então em V_1 e V_2 para o espaço V – *e.g.* transformações lineares e produtos internos – de modo que a linearidade seja mantida.

Sejam $T_1 : V_1 \to V_1'$ e $T_2 : V_2 \to V_2'$ transformações lineares, onde V_1' e V_2' possuem dimensão M_1 e M_2, respectivamente. Então, define-se a transformação linear $T = T_1 \otimes T_2 : V_1 \otimes V_2 \to V_1' \otimes V_2'$ conforme a equação

$$(T_1 \otimes T_2) (|v_1\rangle \otimes |v_2\rangle) = (T_1 |v_1\rangle) \otimes (T_2 \otimes |v_2\rangle) . \quad (2.73)$$

A representação matricial de $T_1 \otimes T_2$ é análoga à de vetores e é dada por

$$T_1 \otimes T_2 = \begin{bmatrix} T_{1,1,1} T_2 & T_{1,1,2} T_2 & \cdots & T_{1,1,N_1} T_2 \\ T_{1,2,1} T_2 & T_{1,2,2} T_2 & \cdots & T_{1,2,N_1} T_2 \\ \vdots & \vdots & \ddots & \vdots \\ T_{1,M_1,1} T_2 & T_{1,M_1,2} T_2 & \cdots & T_{1,M_1,N_1} T_2 \end{bmatrix} , \quad (2.74)$$

onde $T_{1,i,j}$ são as entradas de T_1. Note que nem toda transformação linear T pode ser representada usando um único produto tensorial. Por exemplo, seja

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.75}$$

e deseja-se encontrar $A, B : \mathcal{H}^2 \to \mathcal{H}^2$ tal que $\text{CNOT} = A \otimes B$. Isso implicaria que

$$\text{CNOT} = \begin{bmatrix} a_{1,1}B & a_{1,2}B \\ a_{2,1}B & a_{2,2}B \end{bmatrix} = \begin{bmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & a_{1,2}b_{1,1} & a_{1,2}b_{1,2} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & a_{1,2}b_{2,1} & a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} & a_{2,1}b_{1,2} & a_{2,2}b_{1,1} & a_{2,2}b_{1,2} \\ a_{2,1}b_{2,1} & a_{2,1}b_{2,2} & a_{2,2}b_{2,1} & a_{2,2}b_{2,2} \end{bmatrix}, \tag{2.76}$$

onde $a_{i,j}, b_{i,j} \in \mathbb{C}$ são respectivamente os elementos de A e B para $i, j \in \{1, 2\}$. Essa equação implica que $a_{1,1}b_{1,1} = a_{2,2}b_{1,2} = 1$ e $a_{2,2}b_{1,1} = 0$, o que gera a seguinte contradição: como $a_{2,2}b_{1,1} = 0$, $a_{2,2} = 0$ ou $b_{1,1} = 0$; se $a_{2,2} = 0$, então $a_{2,2}b_{1,2} \neq 1$. se $b_{1,1} = 0$, então $a_{1,1}b_{1,1} \neq 1$. Então conlui-se que $\text{CNOT} \neq A \otimes B$ para qualquer $A, B \in \mathcal{H}^2$.

O produto interno em V segue de uma maneira muito similar e utilizando os produtos internos que já foram definidos para V_1 e V_2. Sendo $|v\rangle = \sum_i v_i |v_{1,i}\rangle \otimes |v_{2,i}\rangle \in V$ e $|v'\rangle = \sum_j v'_j \left|v'_{1,j}\right\rangle \otimes \left|v'_{2,j}\right\rangle \in V$ onde $v_i, v'_j \in \mathbb{C}$, o produto interno $\langle v \,|\, v'\rangle$ é dado por

$$\left(\sum_i v_i |v_{1,i}\rangle \otimes |v_{2,i}\rangle , \sum_j v'_j \left|v'_{1,j}\right\rangle \otimes \left|v'_{2,j}\right\rangle\right) = \sum_{i,j} v_i^* v'_j \left\langle v_{1,i} \,\middle|\, v'_{1,j}\right\rangle \left\langle v_{2,i} \,\middle|\, v'_{2,j}\right\rangle . \tag{2.77}$$

A partir da qual seguem as definições de transformação linear adjunta, operadores Hermitianos e operadores unitários. Em particular, vale salientar que para uma transformação linear $T = T_1 \otimes T_2$ com domínio em $V_1 \otimes V_2$,

$$T^\dagger = (T_1 \otimes T_2)^\dagger = T_1^\dagger \otimes T_2^\dagger. \tag{2.78}$$

Além disso, se T_1 e T_2 forem operadores unitários, então T também é unitário. Uma notação útil utilizada no trabalho visa compactar múltiplos produtos tensoriais: sendo $|v\rangle , |v_i\rangle$ vetores de um espaço de Hilbert e $n \in \mathbb{N}$,

$$\bigotimes_{i=0}^{n-1} |v_i\rangle = |v_0\rangle \otimes |v_1\rangle \otimes \cdots \otimes |v_{n-1}\rangle ; \tag{2.79}$$

analogamente,

$$|v\rangle^{\otimes n} = \bigotimes_{i=0}^{n-1} |v\rangle . \tag{2.80}$$

O mesmo se aplica a transformações lineares.

Uma última definição que será necessária é a do operador $\oplus$, utilizado para representar soma direta.

Definição 2.31. Sejam V_1, V_2 e V espaços de Hilbert com o mesmo produto interno e com dimensões N_1, N_2, $N = N_1 + N_2$, respectivamente. É possível descrever V em termos da soma direta ($\oplus$) de V_1 e V_2. Para todo $|v\rangle \in V$ existem $|v_1\rangle \in V_1$ e $|v_2\rangle \in V_2$ tais que

$$|v\rangle = |v_1\rangle \oplus |v_2\rangle = \begin{bmatrix} |v_1\rangle \\ |v_2\rangle \end{bmatrix} = \begin{bmatrix} v_{1,1} \\ \vdots \\ v_{1,N_1} \\ v_{2,1} \\ \vdots \\ v_{2,N_2} \end{bmatrix}, \tag{2.81}$$

onde $v_{1,1}, \cdots v_{1,N_1} \in \mathbb{C}$ são os elementos de $|v_1\rangle$ e $v_{2,1}, \cdots v_{2,N_2} \in \mathbb{C}$ são os elementos de $|v_2\rangle$. —

2.1.2 Mecânica Quântica – Postulados

Nesta Seção são listados os postulados da Mecânica Quântica. Esses postulados descrevem como os conceitos da Seção 2.1.1 são utilizados para descrever a Mecânica Quântica. Um computador quântico precisa agir de acordo com as regras definidas por esses postulados.

O primeiro postulado diz respeito ao escopo onde a Mecânica Quântica atua.

Definição 2.32. Postulado do Espaço dos estados: Um sistema físico isolado é descrito por um espaço de Hilbert e o estado em que esse sistema se encontra é descrito por um vetor unitário nesse espaço de Hilbert. —

Como mencionado na seção 2.1.1, ao longo deste trabalho utiliza-se espaços de Hilbert com dimensão N. Esse espaço de estados é representado por $\mathcal{H}^N$ e vetores que pertecem a esse estado $|v\rangle \in \mathcal{H}^N$. Vetores $|v\rangle$ podem ser descritos unicamente como uma combinação linear $\sum_i v_i |V_i\rangle$ dados valores $v_i \in \mathbb{C}$ (denominados de amplitudes) e uma base $\{ |V_i\rangle \}$ de V. Normalmente utiliza-se uma base ortonormal. Quando um estado $|v\rangle$ é representado como uma combinação linear de outros estados – *e.g.* $|v\rangle = v_0 |V_0\rangle + v_1 |V_1\rangle$ para $v_0, v_1 \neq 0$ – diz-se que $|v\rangle$ é uma *sobreposição* dos estados $|V_0\rangle$ e $|V_1\rangle$.

Para realizar computação, é interessante que os estados mudem e que haja algum modo de descrever essa evolução.

Definição 2.33. Postulado da Evolução: A evolução de um sistema quântico isolado é descrita por um operador unitário U e dependendo do tempo. Seja $|\psi_0\rangle$ o estado correspondente ao instante de tempo t_0, o estado no instante de tempo seguinte t_1 é dado por $|\psi_1\rangle = U |\psi_0\rangle$. —

Esse postulado permite que a norma dos estados seja mantida (ou seja, trabalha-se apenas com estados unitários). Normalmente, para facilitar a análise, decompõ-se U em diversos operadores unitários – e.g $U = U_1 U_0$ – e a análise é feita passo a passo: sendo o estado inicial $|\psi_0\rangle$, o estado no passo 1 é $|\psi_1\rangle = U_0 |\psi_0\rangle$ e o estado no passo 2 é $|\psi_2\rangle = U_1 |\psi_1\rangle$; sendo $|\psi_f\rangle$ o estado final, nesse exemplo tem-se que $|\psi_f\rangle = U |\psi_0\rangle = |\psi_2\rangle$.

Para realizar computação, é necessário obter algum resultado, mas infelizmente, obter explicitamente o estado final $|\psi_f\rangle$ não é fácil. Inclusive, é comum $|\psi_f\rangle$ ser uma sobreposição de outros estados – *e.g.* sobreposição de $\{ |V_i\rangle \}$ – cuja obtenção é mais fácil.

Definição 2.34. Postulado da Medição: Medições de um estado são descritas por um conjunto de *operadores de medida* $\{ M_i \}$ e os índices i referem-se aos possíveis resultados. Dado um vetor $|\psi\rangle$, a probabilidade de obter i após a medição é dada por

$$\text{prob}\,(i) = \langle\psi| M_i^\dagger M_i |\psi\rangle \tag{2.82}$$

e o estado correspondente $|\psi_i\rangle$ obtido após a medida é dado por

$$|\psi_i\rangle = \frac{M_i |\psi\rangle}{\sqrt{\text{prob}\,(i)}}. \tag{2.83}$$

Como a soma das probabilidades precisa ser igual a 1,

$$1 = \sum_i \text{prob}\,(i) = \sum_i \langle\psi| M_i^\dagger M_i |\psi\rangle = \langle\psi \,|\, \psi\rangle\,, \tag{2.84}$$

conclui-se que que os operadores de medida satisfazem a relação de completude:

$$\sum_i M_i^\dagger M_i = I. \tag{2.85}$$

—

Note que o fato de $|\psi\rangle$ precisar ser unitário está intrinsecamente relacionado com a soma das probabilidades resultar em 1. Além disso, suponha que $|\psi\rangle = \sum_i v_i |V_i\rangle$ e note que $\{ M_i \} = \{ |V_i\rangle \langle V_i| \}$ é um conjunto de operadores de medida e que a relação de completude é respeitada:

$$\sum_i M_i^\dagger M_i = \sum_i \left(|V_i\rangle \langle V_i|\right)^\dagger \left(|V_i\rangle \langle V_i|\right) = \sum_i \left(|V_i\rangle \langle V_i|\right) \left(|V_i\rangle \langle V_i|\right) \tag{2.86}$$

$$= \sum_i |V_i\rangle\, 1\, \langle V_i| = I. \tag{2.87}$$

Espera-se que as amplitudes de $|V_i\rangle$ influenciem na probabilidade de obtenção de cada estado. De fato,

$$\begin{aligned}
\text{prob}\,(i) &= \sum_j v_j^* \langle V_j| M_i^\dagger M_i \sum_k v_k |V_k\rangle && (2.88)\\
&= \sum_j v_j^* \langle V_j| |V_i\rangle \langle V_i| \sum_k v_k |V_k\rangle && (2.89)\\
&= \sum_j v_j^* \delta_{j,i} \sum_k v_k \delta i, k && (2.90)\\
&= v_i^* v_i = |v_i|^2 . && (2.91)
\end{aligned}$$

Logo, o estado obtido após a medida é

$$\begin{aligned}
|\psi_i\rangle &= \frac{|V_i\rangle \langle V_i| \sum_j v_j |V_j\rangle}{|v_i|} && (2.92)\\
&= \frac{|V_i\rangle \sum_j v_j \delta_{i,j}}{|v_i|} && (2.93)\\
&= \frac{v_i |V_i\rangle}{|v_i|}. && (2.94)
\end{aligned}$$

Observe que esses operadores de medida foram definidos de forma a estarem diretamente relacionados com o estado obtido após a medição – *i.e.* $M_i \implies |V_i\rangle$. Além disso, $v_i/|v_i| = \exp(\mathrm{i}\theta_i)$ para algum $\theta_i \in \mathbb{R}$. Diz-se que $\exp(\mathrm{i}\theta_i)$ é a fase de $|V_i\rangle$ e dependendo do contexto, essa fase pode ser ignorada após a medida já que para dois vetores $|\psi\rangle$ e $e^{\mathrm{i}\theta}|\psi\rangle$, $e^{-\mathrm{i}\theta}\langle\psi| M_i^\dagger M_i e^{\mathrm{i}\theta}|\psi\rangle = \langle\psi| M_i^\dagger M_i |\psi\rangle$.

Considerando um exemplo mais concreto, considere a medição de $|+\rangle$ em relação aos operadores de medida $M_0 = |0\rangle\langle 0|$ e $M_1 = |1\rangle\langle 1|$:

$$\text{prob}\,(0) = \text{prob}\,(1) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}, \tag{2.95}$$

e os possíveis estados após a medição são

$$|\psi_0\rangle = \frac{\frac{1}{\sqrt{2}}|0\rangle}{\left|1/\sqrt{2}\right|} = |0\rangle \quad \text{e} \quad |\psi_1\rangle = |1\rangle . \tag{2.96}$$

Por último, resta analisar como sistemas quânticos compostos se comportam – *i.e.* dois ou mais sistemas distintos evoluindo concomitantemente. Para isso, utiliza-se a notação tensorial.

Definição 2.35. Postulado dos sistemas compostos: Sejam V_1, V_2 espaços de Hilbert. A composição desses sistemas é dada por $V = V_1 \otimes V_2$. Sendo assim, se $|v_1\rangle \in V_1$ e $|v_2\rangle \in V_2$, a composição desses estados pode ser representada como $|v\rangle = |v_1\rangle \otimes |v_2\rangle$, onde $|v\rangle \in V$. Estados $|v\rangle \in V$ que *não* podem ser descritos dessa forma são chamados de estados emaranhados – *i.e.* $|v\rangle \neq |v_1\rangle \otimes |v_2\rangle$ para qualquer $|v_1\rangle \in V_1$ e $|v_2\rangle \in V_2$. —

A evolução do sistema composto V também é dada por operadores unitários, o que inclui $U_1 \otimes U_2$ desde que U_1 seja unitário em V_1 e U_2 unitário em V_2. Para este trabalho, é útil analisar o que acontece ao realizar uma medição num subsistema de V. Considere que deseja-se fazer uma medição no primeiro subsistema do estado $|v\rangle = \sum_i c_i |v_i\rangle \otimes |w_i\rangle$ onde $c_i \in \mathbb{C}$, $|v_i\rangle \in V_1$ e $|w_i\rangle \in V_2$. Como não deseja-se medir o segunda subsistema, considere os operadores de medida $\{ M_k \} = \{ |v_k\rangle \langle v_k| \otimes I \}$. Então, a probabilidade de obter o resultado k é:

$$\begin{aligned}
\text{prob}(k) &= \langle v| M_k^\dagger M_k |v\rangle && (2.97)\\
&= \sum_i c_i^* \langle v_i| \otimes \langle w_i| \left(|v_k\rangle \langle v_k| \otimes I\right)^\dagger \left(|v_k\rangle \langle v_k| \otimes I\right) \sum_j c_j |v_j\rangle \otimes |w_j\rangle && (2.98)\\
&= \sum_{i,j} c_i^* c_j \langle v_i| \otimes \langle w_i| \left(|v_k\rangle \langle v_k| \otimes I\right) |v_j\rangle \otimes |w_j\rangle && (2.99)\\
&= \sum_{i,j} c_i^* c_j \langle v_i \,|\, v_k\rangle \langle v_k \,|\, v_j\rangle \langle w_i \,|\, w_j\rangle && (2.100)\\
&= |c_k|^2 ; && (2.101)
\end{aligned}$$

e o estado após a medida é

$$\begin{aligned}
\frac{M_k |v\rangle}{\sqrt{\text{prob}(k)}} &= \frac{1}{|c_k|} \left(|v_k\rangle \langle v_k| \otimes I\right) \sum_i c_i |v_i\rangle \otimes |w_i\rangle && (2.102)\\
&= \frac{1}{|c_k|} \sum_i \left(c_i |v_k\rangle \langle v_k \,|\, v_i\rangle\right) \otimes |w_i\rangle && (2.103)\\
&= \frac{c_k}{|c_k|} |v_k\rangle \otimes |w_k\rangle . && (2.104)
\end{aligned}$$

Perceba que nessa situação, os estados do primeiro subsistema estavam diretamente associados a estados do segundo subsistema e como consequência, ao realizar a medição do primeiro subsistema, o segundo também foi afetado.

2.1.3 Circuitos Quânticos

Nessa seção, introduz-se a notação de circuitos que é comum na Computação Quântica para descrever ou ilustrar algoritmos. A representação de circuitos é equivalente à representação de matrizes e é de sumo interesse para implementação de algoritmos em computadores quânticos, já que um circuito descreve um algoritmo.

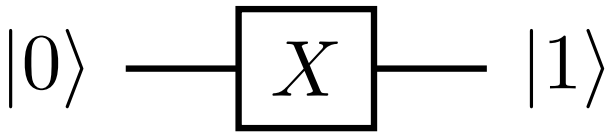
Num computador clássico a menor unidade de informação é representada por um *bit*. Um bit b pode codificar, por exemplo, se há ausência (valor 0) ou presença (valor 1) de corrente elétrica. O bit quântico (*qubit*) $|b\rangle$ é análogo, mas utiliza vetores: um paralelo é feito entre $|0\rangle$ e 0, e entre $|1\rangle$ e 1. Análogo a um circuito clássico, um circuito quântico possui um (ou mais) fio, representando um qubit. A informação flui da esquerda pra direita e pode ser alterada de acordo com uma *porta*.

Por exemplo, o circuito da Fig. 2 possui um qubit. A entrada do circuito está representada à esquerda do fio ($|0\rangle$). O bloco X no meio do circuito representa uma porta cuja ação no qubit é descrita por uma matriz unitária (conforme descrito nos postulados). No caso,

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \implies X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle . \tag{2.105}$$

Sendo assim, a ação da porta X no circuito da Fig. 2 é transformar $|0\rangle$ em $|1\rangle$, que é a saída do circuito, representada à direita do fio. Como X mapeia $|0\rangle \to |1\rangle$ e $|1\rangle \to |0\rangle$, invertendo a informação do qubit, X é chamada de porta NOT. Já que há uma equivalência entre portas e matrizes unitárias, o longo deste trabalho, os termos porta e operador unitário são usados como sinônimos.

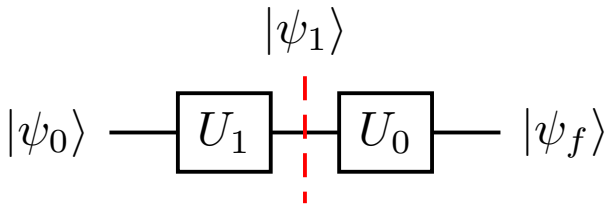
Figura 2 – Exemplo de circuito: porta NOT.



Fonte: Produzido pelo autor.

Um operador unitário U pode ser decomposto como um produto de vários operadores unitários – *e.g.* $U = U_0 U_1 \cdots U_n = \prod_{i=1}^{n} U_i$ onde $n \in \mathbb{N}$. Essa decomposição pode facilitar a análise e a concepção de circuitos quânticos. Considere o circuito apresentado na Fig. 3. A entrada do circuito é $|\psi_0\rangle$. Primeiro aplica-se a porta U_1, resultado no estado intermediário $|\psi_1\rangle = U_1 |\psi_0\rangle$ (estados intermediários são representados por linhas tracejadas que "cortam" o circuito na vertical para fins didáticos apenas). Posteriormente, aplica-se a porta U_0 em $|\psi_1\rangle$, resultando no estado final $|\psi_f\rangle = U_0 |\psi_1\rangle$. Note que $|\psi_f\rangle = U_0 U_1 |\psi_0\rangle$, portanto, a ordem em que as portas são representadas nos circuitos é a ordem inversa de sua representação algébrica.

Figura 3 – Exemplo de circuito com múltiplas portas e estados intermediários.

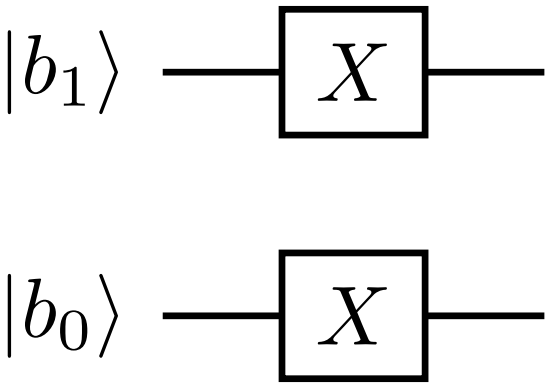


Fonte: Produzido pelo autor.

Em computação, normalmente se trabalha com múltiplos bits de modo a representar um número maior de informação. Considere um sistema composto de 2 qubits: $|b_1\rangle$ e $|b_0\rangle$.

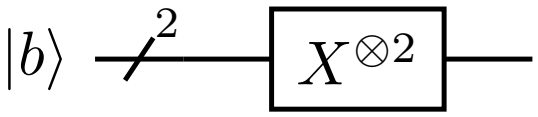
Pelos postulados, é possível representar o estado composto utilizando produto tensorial: $|b\rangle = |b_1\rangle \otimes |b_0\rangle$ (desde que $|b\rangle$ não seja um estado emaranhado). O circuito que inverte os dois qubits está representado na Fig. 4. Usando produto tensorial, é possível representar o mesmo circuito de forma mais compacta (Fig. 5): a linha na diagonal com rótulo 2 indica que estão sendo utilizados 2 qubits e $X^{\otimes 2}$ que aplica-se a porta X em ambos os qubits. Em ambos os circuitos, a saída foi omitida.

Figura 4 – Circuito que inverte 2 qubits.



Fonte: Produzido pelo autor.

Figura 5 – Circuito que inverte 2 qubits (compacto).



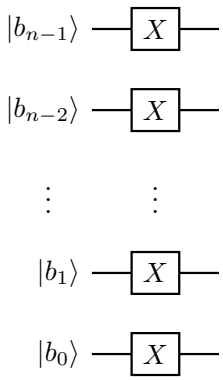
Fonte: Produzido pelo autor.

O exemplo anterior pode ser facilmente generalizado para n qubits ($n \in \mathbb{N}$ e $n \geq 1$) e tomando

$$|b\rangle = |b_{n-1}\rangle\,|b_{n-2}\rangle \cdots |b_1\rangle\,|b_0\rangle = \otimes_{i=1}^{n} |b_{n-i}\rangle\,. \tag{2.106}$$

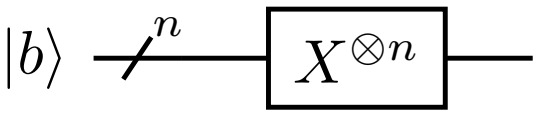
Fig. 6 ilustra o circuito que inverte n qubits e a Fig. 7 ilustra o mesmo circuito de maneira compacta usando produto tensorial.

Figura 6 – Circuito que inverte n qubits.



Fonte: Produzido pelo autor.

Figura 7 – Circuito que inverte n qubits (compacto).



Fonte: Produzido pelo autor.

Faz-se um paralelo dos qubits $|b\rangle$ com bits. Ao concatenar vários bits, é possível representar números naturais. Por exemplo, considere a sequência (ou cadeia) de bits

$b = b_{n-1}b_{n-2}\cdots b_1 b_0$ para $0 \leq i < n$. O número natural $b_{\mathbb{N}}$ representado por essa cadeia de bits é

$$b_{\mathbb{N}} = \sum_{i=0}^{n-1} b_i \cdot 2^i. \tag{2.107}$$

Diz-se que b é a representação binária de um número natural e $b_{\mathbb{N}}$ a representação decimal do mesmo número. Como b e $b_{\mathbb{N}}$ representam o mesmo número mudando apenas a representação, utiliza-se um único rótulo para representar ambos – *e.g.* b – desde que especificado pelo contexto qual representação está sendo utilizada. Desse modo, tanto b quanto $|b\rangle$ são capazes de representes 2^n valores e esses vetores possuem uma relação direta com a *base canônica* ou *base computacional*.

Definição 2.36. Seja $N \in \mathbb{N}$ tal que $N \geq 1$. Os N vetores da base canônica (ou base computacional) são dados por

$$|i\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_i \\ \vdots \\ b_{N-1} \end{bmatrix}, \tag{2.108}$$

onde $b_i = 1$, $b_j = 0$ se $j \neq i$, e $0 \leq i, j \leq N-1$. Por exemplo, o conjunto $\{\, |0\rangle, |1\rangle \,\}$ visto anteriormente é a base computacional de $\mathcal{H}^2$. —

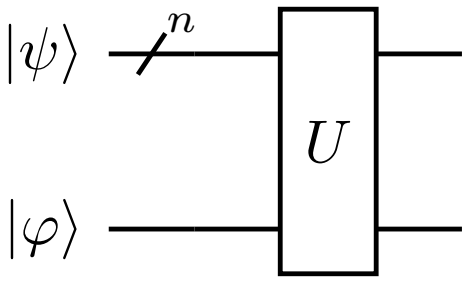
Normalmente, N é uma potência de 2, traçando-se um paralelo direto de um qubit com um bit e um fio de circuito por bit ou qubit (conforme retratado até aqui). Tomar um valor de N que não é potência de 2, entretanto, pode facilitar manipulações algébricas dependendo do problema. Nesse trabalho, ambas as situações são utilizadas (e, inclusive, combinadas).

Suponha que $N = 2^n$ mas N' não é uma potência de 2 e que deseja-se construir um circuito que atua em $\mathcal{H}^N \otimes \mathcal{H}^{N'}$. Como $\mathcal{H}^{N'}$ pode ser interpretado como uma generalização de qubit – *i.e.* um qudit [2] (THEW et al., 2002) – sua representação num circuito é feita através de um único fio. Suponha que $|\psi\rangle \in \mathcal{H}^N$ e $|\varphi\rangle \in \mathcal{H}^{N'}$ são vetores; e $U : \mathcal{H}^N \otimes \mathcal{H}^{N'} \to \mathcal{H}^N \otimes \mathcal{H}^{N'}$ um operador linear. Um circuito cuja ação é definida pela porta $U \otimes U'$ é ilustrado na Fig. 8. Nesse circuito, combina-se dois espaços de Hilbert e quando isso acontece, normalmente cada espaço de Hilbert tem uma função diferente, recebendo o nome de *registradores*. No caso da Fig. 8, $\mathcal{H}^N$ corresponde ao primeiro registrador e $\mathcal{H}^{N'}$ ao segundo.

Vale salientar que é possível representar $\mathcal{H}^{N'}$ usando um outro espaço de Hilbert $\mathcal{H}^{N'_2}$ sendo N'_2 uma potência de 2, desde que $\mathcal{H}^{N'}$ seja um subespaço de $\mathcal{H}^{N'_2}$. Isso é útil

[2] um qubit com mais de 2 níveis.

Figura 8 – Exemplo de circuito atuando em dois espaços de Hilbert ($\mathcal{H}^N \otimes \mathcal{H}^{N'}$).



Fonte: Produzido pelo autor.

principalmente para a implementação de algoritmos em computadores quânticos, tópico que foge do escopo do trabalho.

Retornando aos circuitos que usam apenas qubits, introduz-se alguma portas que serão utilizadas ao longo do trabalho. Especificamente: porta Hadamard, portas SWAP e portas controladas. Para o resto da seção, considere que $n \in \mathbb{N}$, $n \leq 1$ e $N = 2^n$.

Definição 2.37. A porta de Hadamard atua em $\mathcal{H}^2$ e é definida pela matriz

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.109}$$

A ação desse operador também pode ser entendida simplesmente por $|0\rangle \to |+\rangle$ e $|1\rangle \to |-\rangle$, onde $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. —

A porta de Hadamard é unitária já que $H^2 = I$. A porta de Hadamard é utilizada na maioria dos algoritmos, sendo responsável pelo paralelismo quântico: gera um estado que é uma sobreposição uniforme de todas as possíveis entradas do algoritmo. Note que para $\mathcal{H}^2$, tem-se $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; já para $\mathcal{H}^4$,

$$H^{\otimes 2}|0\rangle^{\otimes 2} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.110}$$

$$= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \tag{2.111}$$

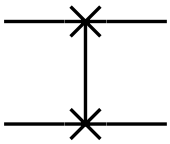
$$= \frac{1}{2} \sum_{i=0}^{3} |i\rangle . \tag{2.112}$$

De um modo geral,

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle . \tag{2.113}$$

Definição 2.38. A operação SWAP que atua nos qubits indexados por i e j é representada por $\text{SWAP}_{i,j}$. A ação da porta $\text{SWAP}_{i,j}$ é trocar a informação representada pelo i-ésimo qubit com a do j-ésima qubit. Fig. 9 ilustra uma porta SWAP. —

Figura 9 – Porta SWAP.



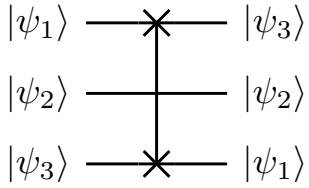
Fonte: Produzido pelo autor.

Por exemplo, suponha que $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle \in \mathcal{H}^2$ e que deseja-se trocar o conteúdo do primeiro e do terceiro qubit do estado $|\psi_1\rangle |\psi_2\rangle |\psi_3\rangle$. Sendo assim, o circuito desejado é dado pela porta $\text{SWAP}_{1,3}$ já que

$$\text{SWAP}_{1,3} |\psi_1\rangle |\psi_2\rangle |\psi_3\rangle = |\psi_3\rangle |\psi_2\rangle |\psi_1\rangle , \tag{2.114}$$

ilustrado na Fig. 10.

Figura 10 – Exemplo da ação de uma porta SWAP.



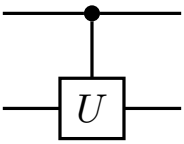
Fonte: Produzido pelo autor.

Definição 2.39. Seja U uma porta unitária que atua em $\mathcal{H}^2$. A porta U-controlada depende de dois qubits: um qubit de controle e um qubit alvo. Se o qubit de controle for $|0\rangle$, o estado permanece inalterado. Se o qubit de controle for $|1\rangle$, aplica-se a porta U no qubit alvo. A porta U-controlada com controle no qubit c-ésimo qubit e alvo no a-ésimo qubit é representada por

$$\mathcal{C}_{c,a}(U) . \tag{2.115}$$

Fig. 11 ilustra uma porta $U-$controlada.

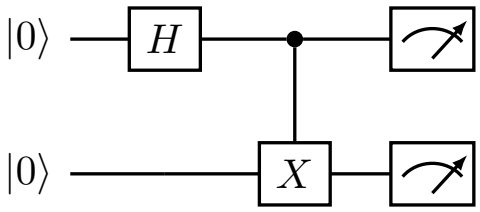
Figura 11 – Porta U-controlada.



Fonte: Produzido pelo autor.

Um exemplo de circuito que usa a portas controladas, é o circuito que gera estados de Bell, descrito por $\mathcal{C}_{1,2}(X)(H \otimes I)$. Esse circuito está ilustrado na Fig. 12 para entrada $|00\rangle$.

Figura 12 – Circuito gerador de estados de Bell.



Fonte: Produzido pelo autor.

Após executar esse circuito, obtém-se

$$\mathcal{C}_{1,2}(X)(H \otimes I)|00\rangle = \mathcal{C}_{1,2}(X)\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{2.116}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + (I \otimes X)|10\rangle) \tag{2.117}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.118}$$

Os ícones à direita (no final) do circuito indicam que está sendo feita uma medição na base computacional. Como resultado desse exemplo, uma medição na base computacional resulta no estado $|00\rangle$ ou no estado $|11\rangle$, ambos com probabilidade de $1/2$.

2.2 Teoria dos Grafos

O livro do West é uma referência consolidada em Teoria dos Grafos (WEST et al., 2001). Considere as seguintes definições.

Definição 2.40. Um grafo $\Gamma(V, E)$ consiste de dois conjuntos finitos: um de vértices V e um de arestas E. A cada vértice é associado um rótulo (normalmente um número natural) e cada aresta $a = (v_1, v_2)$ é uma tupla de dois vértices $v_1, v_2 \in V$. —

Definição 2.41. Seja $\Gamma(V, E)$ um grafo. Qualquer aresta $(v, v) \in E$ onde $v \in V$ é chamada de laço. —

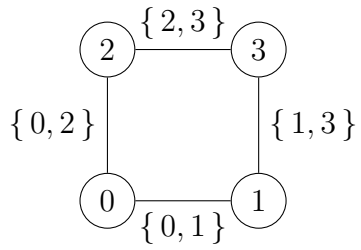
Definição 2.42. Seja $\Gamma(V, E)$ um grafo tal que $v_1, v_2 \in V$. Quaisquer arestas que possuam o mesmo par de vértices são chamadas de arestas múltiplas – *e.g.* (v_1, v_2) e (v_2, v_1). —

Definição 2.43. Um grafo $\Gamma(V, E)$ é um grafo simples se não possui laços ou arestas múltiplas. Nesse caso, as arestas podem ser representadas como um conjunto de vértices ao invés de tuplas ou até mesmo contatenando-se os vértices. Por exemplo, se $v_1, v_2 \in V$,

a aresta entre esses dois vértices pode ser representada equivalentemente como $\{ v_1, v_2 \}$, v_1v_2 ou v_2v_1. —

Ao longo deste trabalho, foca-se apenas em grafos simples. Um exemplo de grafo simples está ilustrado na Fig. 13. Esse grafo possui quatro vértices ($V = \{ 1, 2, 3, 4 \}$) e quatro arestas. Os rótulos dos vértices e arestas podem ser omitidos.

Figura 13 – Exemplo de grafo simples.



Fonte: produzido pelo autor.

Introduz-se agora alguns conceitos que relacionam vértices e arestas: incidência, grau e adjacência.

Definição 2.44. Seja $\Gamma(V, E)$ um grafo simples, $a \in E$ uma aresta tal que $a = \{ v_1, v_2 \}$ e $v_1, v_2 \in V$. Então, diz-se que a aresta a é *incidente* nos vértices v_1 e v_2. —

Definição 2.45. Seja $\Gamma(V, E)$ um grafo simples e um vértice $v \in V$, diz-se que v tem grau d se existem d arestas distintas incidentes a v. —

Definição 2.46. Seja $\Gamma(V, E)$ um grafo simples, $v_1, v_2 \in V$ e $\{ v_1, v_2 \} \in E$. Então, diz-se que os vértices v_1 e v_2 são *adjacentes*. —

Grafos podem ser conexos ou não conexos. Para definir grafos conexos, é necessário definir passeio e caminho.

Definição 2.47. Seja $\Gamma(V, E)$ um grafo simples. Um passeio em Γ é uma lista de vértices (não necessariamente distintos) $v_0, \ldots, v_n \in V$ tal que $\{ v_i, v_{i+1} \} \in E$ para $0 \leq i \leq n - 1$. Ou seja, uma lista de vértices adjacentes. —

Um exemplo de passeio no grafo da Fig. 13 é 0, 1, 3, 1, 3, 2.

Definição 2.48. Um caminho num grafo simples $\Gamma(V, E)$ é um passeio onde todos os vértices da lista são distintos. —

Um exemplo de caminho no grafo da Fig. 13 é 0, 1, 3, 2.

Definição 2.49. Um grafo simples $\Gamma(V, E)$ é dito conexo se para todo par distinto de vértices $v_1, v_2 \in V$ existe um caminho de v_1 até v_2. —

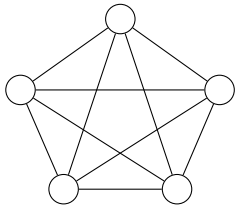
O grafo da Fig. 13 é um grafo conexo. Entretanto, ao se retirar duas arestas quaisquer desse grafo, ele se torna um grafo não-conexo. Ao longo deste trabalho, pressupõe-se que todos os grafos são conexos.

Foca-se agora em alguns tipos de grafo que estão relacionados com o trabalho.

Definição 2.50. Um grafo simples $\Gamma(V, E)$ é dito um grafo completo se todos os vértices distintos forem adjacentes entre si. —

Fig. 14 ilustra o grafo completo com 5 vértices.

Figura 14 – Grafo completo com cinco vértices.

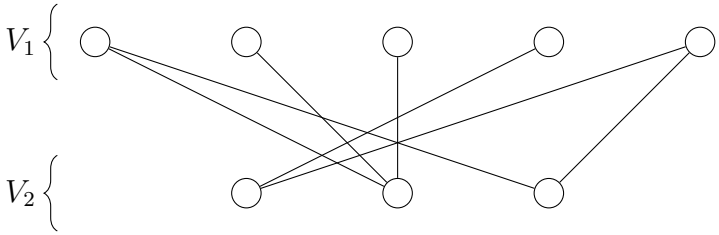


Fonte: produzido pelo autor.

Definição 2.51. Um grafo simples $\Gamma(V, E)$ é dito bipartido se V for a união de dois conjuntos disjuntos – *i.e.* $V = V_1 \cup V_2$ e $V_1 \cap V_2 = \emptyset$ – de tal forma que os vértices de um conjunto *não* são adjacentes a vértices do próprio conjunto – *i.e.* $v_j, u_j \in V_j \implies v_j u_j \notin E$ para $j \in 1, 2$. —

Fig. 15 ilustra um grafo bipartido com $|V_1| = 5$ e $|V_2| = 3$.

Figura 15 – Exemplo de grafo bipartido.

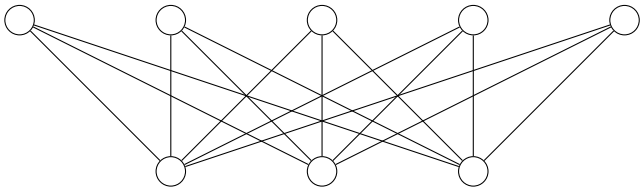


Fonte: produzido pelo autor.

Definição 2.52. Um grafo simples $\Gamma(V, E)$ é dito bipartido completo se ele for um grafo bipartido e todos os vértices de um conjunto disjunto forem adjacentes a todos os vértices do outro conjunto – *i.e.* $v_1 \in V_1$ e $v_2 \in V_2 \implies \{ v_1, v_2 \} \in E$. —

Fig. 16 ilustra um grafo bipartido completo com $|V_1| = 5$ e $|V_2| = 3$.

Figura 16 – Exemplo de grafo bipartido completo.



Fonte: produzido pelo autor.

Definição 2.53. Um grafo simples $\Gamma(V, E)$ é dito um grafo regular se todos os vértices possuem o mesmo grau. Se esse grau for d, chama-se o grafo de d-regular. —

Os grafos das Figs. 13 e 14 são exemplos de grafos regulares. Um último conceito que será necessário para o trabalho é o de coloração de arestas.

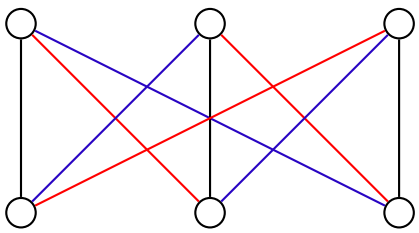
Definição 2.54. Dado um grafo simples $\Gamma(V, E)$, uma coloração de arestas é uma rotulação das arestas onde cada aresta é associada com uma cor (ou número). Várias arestas podem ser associadas com uma cor, compondo uma classe de cor. —

Definição 2.55. Um grafo simples $\Gamma(V, E)$ é d-colorível por arestas se existe uma coloração de arestas com d cores tais que $\forall v \in V$ todas as arestas incidentes em v possuem cores diferentes. —

Definição 2.56. O índice cromático de um grafo simples $\Gamma(V, E)$ é o menor valor d tal que Γ seja d-colorível por arestas. —

O grafo ilustrado na Fig. 17 possui índice cromático 3, logo, é 3-colorível, 4- colorível por arestas, etc.

Figura 17 – Exemplo de coloração de arestas.



Fonte: produzido pelo autor.

Em particular, este trabalho foca em grafos simples regulares com número par de vértices. Sabe-se que grafos d-regulares com número par de vértices possuem índice cromático d. Note que o grafo da Fig. 17 é um exemplo desse tipo de grafo com $d = 3$. Grafos d-regulares com número ímpar de vértices possuem índice cromático $d + 1$ e fogem do escopo do trabalho.

3 Algoritmo de Contagem

Seja $S_N = \{0, \ldots, N-1\}$ para $N = 2^n$ e $n \in \mathbb{N}$ e considere a função $f(x) : S_N \to \{0, 1\}$. O problema de contagem consiste em estimar o valor $k = |\{x \in S_N | f(x) = 1\}|$; *i.e.* estimar a quantidade de elementos que possuem a propriedade descrita pela função f. Esse problema foi estudado por Brassard, Høyer, Mosca e Tapp (BHMT) – na referência (BRASSARD et al., 2002) – e descrito nas próximas seções. Seção 3.1 descreve o problema de busca e o algoritmo de Grover (GROVER, 1996; GROVER, 1997), Seção 3.2 descreve a Transformada Quântica de Fourier, Seção 3.3 descreve o algoritmo de estimativa de fase, Seção 3.4 descreve o algoritmo de contagem, unindo todas as seções supracitadas.

3.1 Algoritmo de Busca

Considerando a função $f(x) : S_N \to \{0, 1\}$, o problema de busca consiste em encontrar um elemento $x \in S_N$ tal que $f(x) = 1$. Nesse tipo de problema, uma terceira pessoa é responsável por implementar a função f (chamada de oráculo) e o objetivo do problema é descobrir um elemento x fazendo a menor quantidade de consultas possíveis à f. Evidentemente, num computador clássico são necessárias $O(N)$ invocações à f, fazendo uma consulta para cada valor de x possível. Em contrapartida, num computador quântico podemos encontrar x realizando $O(\sqrt{N})$ invocações de f. Esse processo será descrito nas Seções a seguir.

3.1.1 Oráculo

Primeiramente, é necessário que uma terceira pessoa implemente uma porta que simule o comportamento do oráculo f. Assume-se que o oráculo age de acordo com

$$O_f : |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle , \tag{3.1}$$

onde $|x\rangle \in \mathcal{H}^N$, $|b\rangle \in \mathcal{H}^2$ e $\oplus$ é a operação binária XOR, detalhada na Tabela 1. O oráculo

Tabela 1 – Tabela verdade da operação XOR.

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Fonte: autor.

é unitário já que $O_f^\dagger = O_f$:

$$O_f^2 \left|x\right\rangle \left|b\right\rangle = \left|x\right\rangle \left|b \oplus f(x) \oplus f(x)\right\rangle \tag{3.2}$$

$$= \left|x\right\rangle \left|b \oplus 0\right\rangle = \left|x\right\rangle \left|b\right\rangle . \tag{3.3}$$

Para utilizar o oráculo no algoritmo de busca, faz-se uso de *phase kickback*. Suponha que $x_0, x_1 \in S_N$ tais que $f(x_0) = 0$ e $f(x_1) = 1$; então

$$O_f \left|x_0\right\rangle \otimes \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} = \left|x_0\right\rangle \otimes \frac{\left|0 \oplus 0\right\rangle - \left|1 \oplus 0\right\rangle}{\sqrt{2}} \tag{3.4}$$

$$= \left|x_0\right\rangle \otimes \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}, \tag{3.5}$$

e

$$O_f \left|x_1\right\rangle \otimes \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} = \left|x_1\right\rangle \otimes \frac{\left|1\right\rangle - \left|0\right\rangle}{\sqrt{2}} \tag{3.6}$$

$$= - \left|x_1\right\rangle \otimes \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}. \tag{3.7}$$

Esse fenômeno é uma consequência direta das propriedades de produto tensorial. Perceba que o segundo registrador permanece inalterado no estado $\left(\left|0\right\rangle - \left|1\right\rangle\right)/\sqrt{2}$ e sua fase é "transferida" para o primeiro registrador. Portanto é possível desconsiderar o segundo registrador no decorrer das contas.

3.1.2 Operador de Evolução de Grover

Para extrair informações de O_f em menos de $O(N)$ passos, é necessário realizar algum processamento entre invocações de O_f. Tal processamento é descrito pela matriz de Grover, definida por

$$G = H^{\otimes n} \left(2 \left|0\right\rangle \left\langle 0\right| - I\right) H^{\otimes n} \tag{3.8}$$

$$= 2H^{\otimes n} \left|0\right\rangle \left(H^{\otimes n} \left|0\right\rangle\right)^\dagger - \left(H^2\right)^{\otimes n} \tag{3.9}$$

$$= \frac{2}{N} \sum_{i,j=0}^{N-1} \left|i\right\rangle \left\langle j\right| - I. \tag{3.10}$$

A matriz de Grover também é chamada de operador de difusão devido ao seu comportamento de espalhar a amplitude de um dos estados da base computacional para os demais:

$$G \left|x\right\rangle = \frac{2}{N} \sum_{i,j=0}^{N-1} \left|i\right\rangle \left\langle j \,\middle|\, x\right\rangle - I \left|x\right\rangle \tag{3.11}$$

$$= \frac{2}{N} \sum_{i=0}^{N-1} \left|i\right\rangle - \left|x\right\rangle \tag{3.12}$$

$$= \left(\frac{2}{N} - 1\right) \left|x\right\rangle + \frac{2}{N} \sum_{i \neq x} \left|i\right\rangle . \tag{3.13}$$

Ao aplicar o oráculo seguido pela matriz de Grover, obtém-se o operador de evolução de Grover

$$U_G = GO_f, \tag{3.14}$$

que é chamado múltiplas vezes durante o algoritmo de busca. De fato, toda a análise do algoritmo de busca é focada em U_G.

3.1.3 O Algoritmo e Sua Análise

O algoritmo de busca está descrito em Algoritmo 1.

Algoritmo 1: Algoritmo de Busca

Entrada: O_f: Oráculo da função f; n: quantidade de qubits respeitando o domínio da função f

1: Preparar o estado $|\psi\rangle = H^{\otimes n}|0\rangle$
2: Aplicar $U_G^t|\psi\rangle$ onde $t = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{k}} \right\rfloor$
3: Realizar medição obtendo o resultado $|\psi_f\rangle$
4: **retorna** $|\psi_f\rangle$

Note que o estado inicial $|\psi_0\rangle$ é uma sobreposição uniforme de todos os valores de x pertencentes ao domínio de f,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle . \tag{3.15}$$

Portanto, é uma sobreposição de todos os valores $x_0 \in \{x \in S_N | f(x) = 0\}$ e $x_1 \in \{x \in S_N | f(x) = 1\}$ (com cardinalidades $N - k$ e k, respectivamente). Sejam

$$|x_0\rangle = \frac{1}{\sqrt{N-k}} \sum_{f(x)=0} |x\rangle \tag{3.16}$$

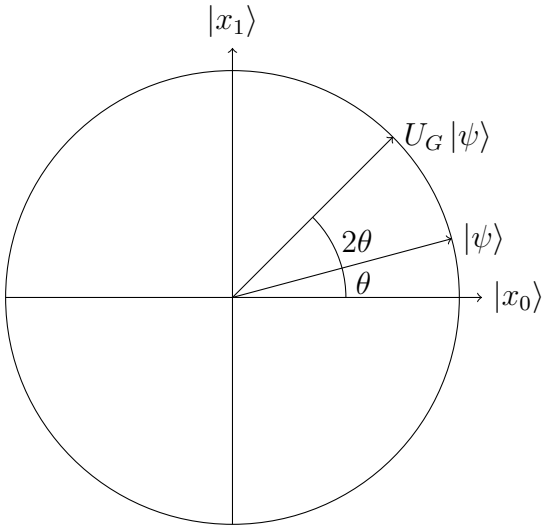
e

$$|x_1\rangle = \frac{1}{\sqrt{k}} \sum_{f(x)=1} |x\rangle . \tag{3.17}$$

Então o estado inicial pode ser representado como

$$|\psi\rangle = \sqrt{\frac{N-k}{N}}\,|x_0\rangle + \sqrt{\frac{k}{N}}\,|x_1\rangle . \tag{3.18}$$

Figura 18 – Rotação de 2θ no hiperplano definido por $|x_0\rangle$ e $|x_1\rangle$.



Fonte: Produzido pelo autor.

Denotando $\cos\theta = \sqrt{(N-k)/N}$ e $\sin\theta = \sqrt{k/N}$, aplicando U_G ao estado inicial, e usando as propriedades trigonométricas para $\cos(\alpha \pm \beta)$ e $\sin(\alpha \pm \beta)$, obtém-se

$$\begin{aligned}
U_G|\psi\rangle &= GO_f\left(\cos\theta|x_0\rangle + \sin\theta|x_1\rangle\right) && (3.19)\\
&= \left(2|\psi\rangle\langle\psi| - I\right)\left(\cos\theta|x_0\rangle - \sin\theta|x_1\rangle\right) && (3.20)\\
&= 2\left(\cos^2\theta - \sin^2\theta\right)|\psi\rangle - \cos\theta|x_0\rangle + \sin\theta|x_1\rangle && (3.21)\\
&= \cos\theta\left(2\cos(2\theta) - 1\right)|x_0\rangle + \sin\theta\left(2\cos(2\theta) + 1\right)|x_1\rangle && (3.22)\\
&= \left(\cos(3\theta) + \cos\theta - \cos\theta\right)|x_0\rangle + \left(\sin(3\theta) - \sin\theta + \sin\theta\right)|x_1\rangle && (3.23)\\
&= \cos(3\theta)|x_0\rangle + \sin(3\theta)|x_1\rangle. && (3.24)
\end{aligned}$$

Esse resultado levanta suspeitas de que U_G faz uma rotação de 2θ graus no hiperplano definido por $|x_0\rangle$ e $|x_1\rangle$ (conforme ilustrado na Figura 18). De fato, é possível fazer uma prova indutiva para isso. Tome como caso base $U_G|\psi\rangle = \cos(3\theta)|x_0\rangle + \sin(3\theta)$; e como hipótese indutiva $U_G^{t'}|\psi\rangle = \cos\theta_{t'}|x_0\rangle + \sin\theta_{t'}|x_1\rangle$, onde $\theta_{t'} = (2t'+1)\theta$ e $t' \in \mathbb{N}$. Deseja-se demonstrar que $U_G^{t'+1}|\psi\rangle = \cos\theta_{t'+1}|x_0\rangle + \sin\theta_{t'+1}|x_1\rangle$;

$$\begin{aligned}
U_G^{t'+1}|\psi\rangle &= U_G\left(\cos\theta_{t'}|x_0\rangle + \sin\theta_{t'}|x_1\rangle\right) && (3.25)\\
&= \left(2|\psi\rangle\langle\psi| - I\right)\left(\cos\theta_{t'}|x_0\rangle - \sin\theta_{t'}|x_1\rangle\right) && (3.26)\\
&= 2\cos(\theta + \theta_{t'})|\psi\rangle - \cos\theta_{t'}|x_0\rangle + \sin\theta_{t'}|x_1\rangle && (3.27)\\
&= \cos(2\theta + \theta_{t'})|x_0\rangle + \sin(2\theta + \theta_{t'})|x_1\rangle && (3.28)\\
&= \cos\theta_{t'+1}|x_0\rangle + \sin\theta_{t'+1}|x_1\rangle, && (3.29)
\end{aligned}$$

concluindo a demonstração.

Dessa forma, também é possível interpretar a matriz U_G como a matriz de rotação $R(2\theta)$ definida na base $|x_0\rangle, |x_1\rangle$; onde

$$R(\theta') = \begin{bmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{bmatrix}. \tag{3.30}$$

Matrizes de rotação têm autovetores e autovalores bem conhecidos. Especificamente,

$$|\mp \mathrm{i}\rangle = \frac{|0\rangle \mp \mathrm{i}\,|1\rangle}{\sqrt{2}} \tag{3.31}$$

são os autovetores de $R(\theta')$ associados aos autovalores $e^{\pm \mathrm{i}\theta'}$, respectivamente.

Resta agora analisar a quantidade de iterações t necessária no algoritmo. Observe que deseja-se maximizar a amplitude dos elementos marcados $|x_1\rangle$ de forma a maximizar a probabilidade de medir um desses elementos no passo subsequente. Ou seja, deseja-se maximizar $\sin((2t+1)\theta)$, que ocorre quando $(2t+1)\theta = \pi/2$. Primeiro encontra-se uma expressão para θ. Supondo que $k \ll N$ e expandindo $\arcsin(\alpha)$ no ponto $\alpha = 0$, obtém-se

$$\theta = \arcsin\left(\sqrt{\frac{k}{N}}\right) = \sqrt{\frac{k}{N}} + \frac{1}{6}\left(\frac{k}{N}\right)^{3/2} + O\left(\left(\frac{k}{N}\right)^{5/2}\right). \tag{3.32}$$

Por último, isola-se t na expressão $(2t+1)\theta = \pi/2$ e usando o termo mais dominante da eq. 3.32:

$$t = \frac{\pi}{4\theta} - \frac{1}{2} = \frac{\pi}{4}\sqrt{\frac{N}{k}} - \frac{1}{2}. \tag{3.33}$$

Já que deseja-se $t \in \mathbb{N}$, tome

$$t = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{k}} \right\rfloor. \tag{3.34}$$

Esse valor rotaciona a condição inicial em aproximadamente $\pi/2$ radianos no hiperplano descrito por $|x_0\rangle$ e $|x_1\rangle$ (Fig. 18). Ao final, obtém-se $|\psi_f\rangle \approx |x_1\rangle$, logo, há a probabilidade do algoritmo falhar. No pior caso, as t iterações rotacionam $|\psi_0\rangle$ em exatamente $\pi/2$ radianos – na prática, serão menos de $\pi/2$ radianos já que o segundo termo da expansão de θ é positivo (eq. 3.32). Nesse cenário, temos que a probabilidade de sucesso é dada por

$$|\langle \psi_f \,|\, x_1\rangle|^2 \geq |\langle \psi_0 \,|\, x_0\rangle|^2 = \cos^2\theta = 1 - \frac{k}{N}. \tag{3.35}$$

3.2 Transformada Quântica de Fourier

A Transformada de Fourier possui diversas aplicações na ciência, sendo responsável por mudar o domínio de uma função, *e.g.* domínio do tempo para domínio da frequência

temporal. O domínio da frequência é útil na representação e processamento de sinais digitais, no processamento de imagens, dentro outras aplicações. Era de se esperar que uma contrapartida quântica da Transformada de Fourier tivesse aplicações interessantes na Computação Quântica. De fato, a Transformada Quântica de Fourier (QFT [1]) tem um papel essencial em algoritmos quânticos (COPPERSMITH, 1994; NIELSEN; CHUANG, 2002), por exemplo o Algoritmo de Shor (SHOR, 1994), o algoritmo de estimativa de fase e o algoritmo de contagem; sendo os dois últimos o foco deste trabalho.

É possível definir a QFT em torno do seguinte estado.

Definição 3.1. Seja P a dimensão do espaço de Hilbert e $\omega \in \mathbb{R}$; o estado $|\mathcal{F}_P(\omega)\rangle$ é dado por

$$|\mathcal{F}_P(\omega)\rangle = \frac{1}{\sqrt{P}} \sum_{\ell=0}^{P-1} e^{2\pi \mathrm{i}\omega\ell/P} |\ell\rangle . \tag{3.36}$$

—

Note que é possível restringir os valores de ω no intervalo $0 \leq \omega < P$. Entretanto, em alguns casos, utiliza-se $0 \leq \omega \leq P$ pois a equivalência entre $|\mathcal{F}_P(0)\rangle$ e $|\mathcal{F}_P(P)\rangle$ facilita as demonstrações.

Essa definição genérica de $|\mathcal{F}_P(\omega)\rangle$ será útil para calcular a probabilidade de sucesso do algoritmo de estimativa de fase (seção 3.3). É possível utilizar os estados $|\mathcal{F}_P(\omega)\rangle$ para descrever uma base de $\mathcal{H}^P$.

Lema 1. *O conjunto de estados*

$$B_{\mathcal{F}} = \bigcup_{j=0}^{P-1} \{ |\mathcal{F}_P(j)\rangle \} \tag{3.37}$$

forma uma base ortonormal de $\mathcal{H}^P$, denominada base de Fourier. —

Demonstração. Primeiro, verifica-se a ortonormalidade dos estados de $B_{\mathcal{F}}$:

$$\langle \mathcal{F}_P(j) \,|\, \mathcal{F}_P(j')\rangle = \left(\frac{1}{\sqrt{P}} \sum_{\ell=0}^{P-1} e^{-2\pi \mathrm{i} j\ell/P} \langle \ell| \right) \left(\frac{1}{\sqrt{P}} \sum_{\ell'=0}^{P-1} e^{2\pi \mathrm{i} j'\ell'/P} |\ell'\rangle \right) \tag{3.38}$$

$$= \frac{1}{P} \sum_{\ell,\ell'=0}^{P-1} e^{2\pi \mathrm{i}(-j\ell + j'\ell')/P} \delta_{\ell\ell'} \tag{3.39}$$

$$= \frac{1}{P} \sum_{\ell=0}^{P-1} e^{2\pi \mathrm{i}(j'-j)\ell/P}. \tag{3.40}$$

Caso $j = j'$,

$$\langle \mathcal{F}_P(j) \,|\, \mathcal{F}_P(j')\rangle = \frac{1}{P} \sum_{k=0}^{P-1} e^0 \tag{3.41}$$

$$= \frac{1}{P} \cdot P = 1. \tag{3.42}$$

[1] Quantum Fourier Transform

Caso $j \neq j'$, é possível expressar a Eq. 3.40 como uma série geométrica. Denotando $j_\Delta = j' - j$ e notando que $j_\Delta \in \mathbb{Z}$, obtém-se

$$\langle \mathcal{F}_P(j) \,|\, \mathcal{F}_P(j') \rangle = \frac{1}{P} \cdot \frac{1 - e^{2\pi \mathrm{i} j_\Delta}}{1 - e^{2\pi \mathrm{i} j_\Delta / P}} \tag{3.43}$$

$$= \frac{1}{P} \cdot \frac{1 - 1}{1 - e^{2\pi \mathrm{i} j_\Delta / P}} \tag{3.44}$$

$$= 0. \tag{3.45}$$

Sendo assim os estados de $B_\mathcal{F}$ são ortonormais:

$$\langle \mathcal{F}_P(j) \,|\, \mathcal{F}_P(j') \rangle = \delta_{jj'}. \tag{3.46}$$

Por último,

$$|B_\mathcal{F}| = P \implies \mathrm{span}(B_\mathcal{F}) = \mathcal{H}^P. \tag{3.47}$$

Portanto, $B_\mathcal{F}$ é uma base ortonormal de $\mathcal{H}^P$. □

Agora, é possível definir a QFT e sua inversa.

Definição 3.2. A Transformada Quântica de Fourier é descrita pelo operador que realiza a transformação

$$\mathrm{QFT} \,|j\rangle = |\mathcal{F}_P(j)\rangle, \tag{3.48}$$

onde $|j\rangle$ são os estados da base canônica de $\mathcal{H}^P$. Analogamente, a Transformada Inversa de Fourier é descrita pelo operador que realiza a transformação

$$\mathrm{QFT}^{-1} \,|\mathcal{F}_P(j)\rangle = |j\rangle. \tag{3.49}$$

—

Note que QFT é unitário:

$$\mathrm{QFT}^{-1}\ \mathrm{QFT} = \mathrm{QFT}^\dagger\ \mathrm{QFT} \tag{3.50}$$

$$= \sum_{j=0}^{P-1} |j\rangle \langle \mathcal{F}_P(j)| \sum_{j'=0}^{P-1} |\mathcal{F}_P(j')\rangle \langle j'| \tag{3.51}$$

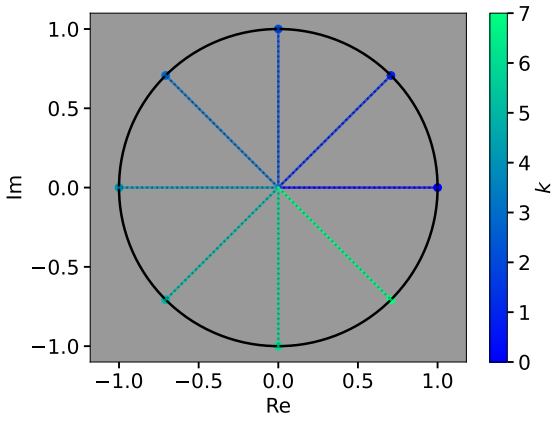
$$= \sum_{j,j'=0}^{P-1} \delta_{j,j'} \,|j\rangle \langle j'| \tag{3.52}$$

$$= I. \tag{3.53}$$

Antes de prosseguir, é importante interpretar os estados $|\mathcal{F}_P(\omega)\rangle$ geometricamente. Ao dividir o círculo unitário uniformemente em P partições, todas as entradas do vetor $|\mathcal{F}_P(\omega)\rangle$ podem ser representadas em termos dos ângulos que delimitam essas partições.

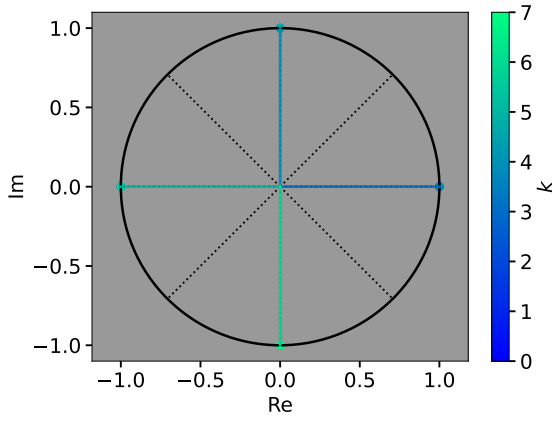
Denomine os P ângulos de $|\mathcal{F}_P(1)\rangle$ por *ângulos base de Fourier* (ou simplismente ângulos base), *i.e.* o k-ésimo ângulo base é dado por $2\pi k/P$. Fig. 19 ilustra os 8 ângulos (base) de $|\mathcal{F}_8(1)\rangle$. De agora em diante, esses ângulos serão representados nas figuras por linhas pontilhadas. Nessa interpretação, ω pode ser entendido como um multiplicador dos ângulos base. Um exemplo disso são os pontos de $|\mathcal{F}_8(2)\rangle$ na Fig. 20, onde o k-ésimo ângulo de $|\mathcal{F}_8(2)\rangle$ coincide com o $(k+4)$-ésimo ângulo de $|\mathcal{F}_8(1)\rangle$ (para $0 \leq k \leq 3$) e com alguns ângulos base. De fato, sempre que $\omega \in \mathbb{N}$, todos os ângulos $2\pi\omega k/P$ de $|\mathcal{F}_8(\omega)\rangle$ coincidirão com ângulos base.

Figura 19 – Valores de $\langle k \,|\, \mathcal{F}_8(1)\rangle$ no plano complexo (ângulos base).



Fonte: Produzido pelo autor.

Figura 20 – Valores de $\langle k \,|\, \mathcal{F}_8(2)\rangle$ no plano complexo.

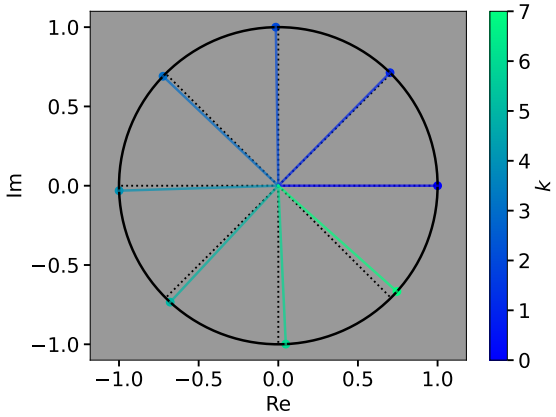


Fonte: Produzido pelo autor.

A definição genérica de $|\mathcal{F}_P(\omega)\rangle$ permite analisar o cenário em que $\omega \notin \mathbb{N}$, *i.e.* $|\mathcal{F}_P(\omega)\rangle \notin B_{\mathcal{F}}$. Nesse caso, ω é um multiplicador dos ângulos base tal que $\lfloor\omega\rfloor < \omega < \lceil\omega\rceil$, e espera-se que os ângulos de $|\mathcal{F}_P(\omega)\rangle$ estejam próximos dos ângulos de $|\mathcal{F}_P(\lfloor\omega\rfloor)\rangle$ e $|\mathcal{F}_P(\lceil\omega\rceil)\rangle$ – vale frisar a equivalência entre $|\mathcal{F}_P(0)\rangle$ e $|\mathcal{F}_P(P)\rangle$. De fato, é possível ver que isso acontece ao comparar os ângulos de $|\mathcal{F}_8(1.01)\rangle$ (Figura 21), $|\mathcal{F}_8(1.5)\rangle$ (Figura 22) e $|\mathcal{F}_8(1.99)\rangle$ (Figura 23) com os ângulos de $|\mathcal{F}_8(1)\rangle$ (Figura 19) e $|\mathcal{F}_8(2)\rangle$ (Figura 20). Perceba que os ângulos de $|\mathcal{F}_8(1.5)\rangle$ estão no meio do caminho entre os ângulos de $|\mathcal{F}_8(1)\rangle$ e $|\mathcal{F}_8(2)\rangle$, enquanto que os ângulos de $|\mathcal{F}_8(1.01)\rangle$ estão bem mais próximos dos ângulos de $|\mathcal{F}_8(1)\rangle$ do que de $|\mathcal{F}_8(2)\rangle$; análogo para os ângulos de $|\mathcal{F}_8(1.99)\rangle$. Analisando as Figs. 21 e 23, a interpretação de ω como multiplicador dos ângulos base fica mais clara. Como todos os ângulos dependem de ω, é possível simplificar os gráficos ao representar apenas o valor de $\langle 1 \,|\, \mathcal{F}_P(\omega)\rangle$, melhorando a visualização e facilitando interpretações futuras. A Fig. 24 ilustra a representação simplificada de $|\mathcal{F}_8(1.5)\rangle$.

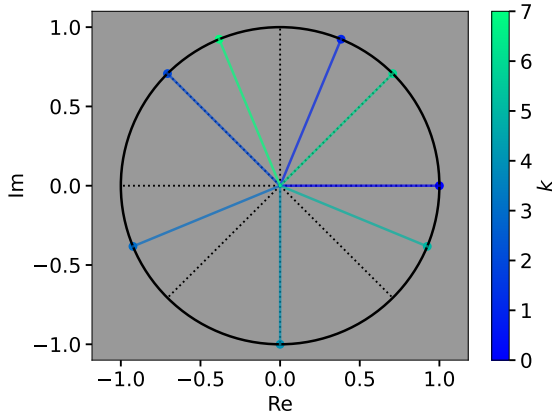
É interessante notar também que alguns ângulos de $|\mathcal{F}_8(1.5)\rangle$ e $|\mathcal{F}_8(1.99)\rangle$ não coincidem com os ângulos base – *i.e.* $|\mathcal{F}_8(1.5)\rangle$, $|\mathcal{F}_8(1.99)\rangle \notin B_{\mathcal{F}}$. Essa observação levanta as seguintes perguntas (correlacionadas):

Figura 21 – Valores de $\langle k \,|\, \mathcal{F}_8\,(1.01)\rangle$ no plano complexo.



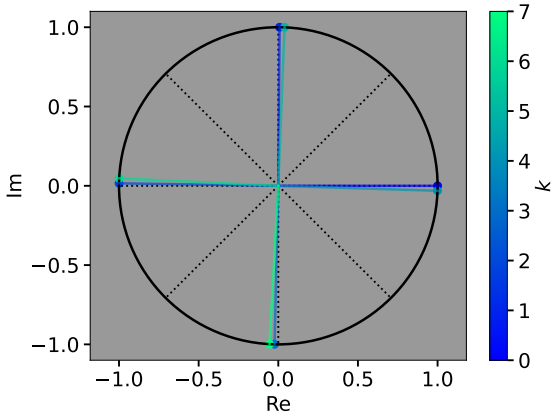
Fonte: Produzido pelo autor.

Figura 22 – Valores de $\langle k \,|\, \mathcal{F}_8\,(1.5)\rangle$ no plano complexo.



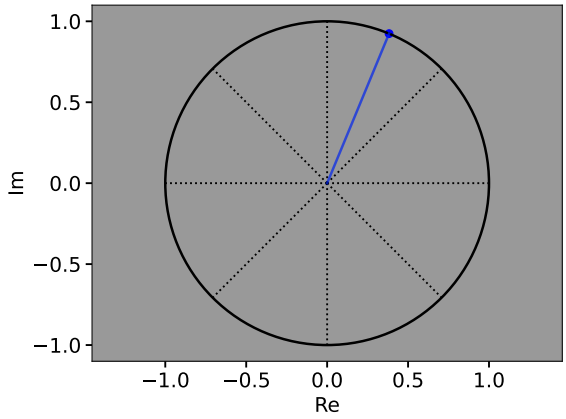
Fonte: Produzido pelo autor.

Figura 23 – Valores de $\langle k \,|\, \mathcal{F}_8\,(1.99)\rangle$ no plano complexo.



Fonte: Produzido pelo autor.

Figura 24 – Valor de $\langle 1 \,|\, \mathcal{F}_8\,(1.5)\rangle$ no plano complexo.



Fonte: Produzido pelo autor.

1. Sendo $|\mathcal{F}_P\,(\omega)\rangle$ representado na base $B_{\mathcal{F}}$, qual é o quadrado da norma das amplitudes de $|\mathcal{F}_P\,(\lfloor\omega\rfloor)\rangle$ e $|\mathcal{F}_P\,(\lceil\omega\rceil)\rangle$? Ou, de forma geral, qual o valor de $|\langle\mathcal{F}_P\,(\omega)\,|\,\mathcal{F}_P\,(\omega')\rangle|^2$ onde $\omega \neq \omega'$?

2. Ao fazer uma medição de $QFT^{-1}\,|\mathcal{F}_P\,(\omega)\rangle$ na base computacional, qual a probabilidade do resultado ser $|\lfloor\omega\rfloor\rangle$ ou $|\lceil\omega\rceil\rangle$?

A resposta da primeira pergunta é dada pelo Lema 10 de BHMT (BRASSARD et al., 2002), adaptado a seguir.

Lema 2. *Sejam $\mathcal{H}^P$ o espaço de Hilbert; ω e ω' valores reais tais que $0 \leq \omega, \omega' \leq P$ e*

$\omega \neq \omega'$; *e* $\omega_\Delta = \omega' - \omega$. *Então,*

$$|\langle \mathcal{F}_P(\omega) \,|\, \mathcal{F}_P(\omega')\rangle|^2 = \frac{\sin^2(\omega_\Delta \pi)}{P^2 \sin^2(\omega_\Delta \pi / P)}. \tag{3.54}$$

—

Demonstração. Análogo ao obtido na Eq. 3.40, obtém-se a série geométrica

$$|\langle \mathcal{F}_P(\omega) \,|\, \mathcal{F}_P(\omega')\rangle|^2 = \left| \frac{1}{P^2} \sum_{\ell=0}^{P-1} e^{2\pi i \omega_\Delta \ell / P} \right|^2 \tag{3.55}$$

$$= \frac{1}{P^2} \left(\frac{1 - e^{2\pi i \omega_\Delta}}{1 - e^{2\pi i \omega_\Delta / P}} \right) \left(\frac{1 - e^{-2\pi i \omega_\Delta}}{1 - e^{-2\pi i \omega_\Delta / P}} \right) \tag{3.56}$$

$$= \frac{1}{P^2} \left(\frac{2 - e^{2\pi i \omega_\Delta} - e^{-2\pi i \omega_\Delta}}{2 - e^{2\pi i \omega_\Delta / P} - e^{-2\pi i \omega_\Delta / P}} \right) \tag{3.57}$$

$$= \frac{1}{P^2} \left(\frac{2 - 2\cos(2\pi \omega_\Delta)}{2 - 2\cos(2\pi \omega_\Delta / P)} \right). \tag{3.58}$$

Usando a identidade trigonométrica $1 - \cos(2\theta) = 2\sin^2\theta$,

$$|\langle \mathcal{F}_P(\omega) \,|\, \mathcal{F}_P(\omega')\rangle|^2 = \frac{\sin^2(\pi \omega_\Delta)}{P^2 \sin^2(\pi \omega_\Delta / P)}, \tag{3.59}$$

como esperado.

Note que se $\omega, \omega' \in \mathbb{N}$, então $|\mathcal{F}_P(\omega)\rangle$, $|\mathcal{F}_P(\omega')\rangle \in B_{\mathcal{F}}$ e

$$\sin^2(\omega_\Delta \pi) = 0,\ \sin^2(\omega_\Delta \pi / P) \neq 0 \implies |\langle \mathcal{F}_P(\omega) \,|\, \mathcal{F}_P(\omega')\rangle|^2 = 0, \tag{3.60}$$

conforme desejado. □

Já a resposta da segunda pergunta é dada pelo Teorema 11 de BHMT (BRASSARD et al., 2002) – adaptado a seguir –, que utiliza o Lema 2.

Teorema 2. *Seja* X *a variável aleatória correspondente ao resultado da medição do estado* $\mathrm{QFT}_P^{-1} |\mathcal{F}_P(\omega)\rangle$ *na base computacional onde* $\omega \in \mathbb{R}$ *e* $0 \leq \omega \leq P$. *Se* ω *for um inteiro, então* $\mathrm{prob}(X = \omega) = 1$ *e o estado após a medição é* $|\omega\rangle$ *(denota-se* $|P\rangle = |0\rangle$*). Caso contrário,*

$$\mathrm{prob}(X = \lfloor \omega \rfloor) + \mathrm{prob}(X = \lceil \omega \rceil) = \mathrm{prob}(|X - \omega| \leq 1) \geq \frac{8}{\pi^2} \tag{3.61}$$

é a probabilidade associada a obter um dos estados $|\lfloor \omega \rfloor\rangle$ *ou* $|\lceil \omega \rceil\rangle$ *após a medição.*

—

Demonstração. Considere os operadores de medida da base computacional $\{ M_m \} = \{ |m\rangle \langle m| \}$ para $m \in \mathbb{N}$ tal que $0 \leq m < P$. Então, de modo geral,

$$\begin{aligned} \text{prob}\,(X = m) &= \left(\langle \mathcal{F}_P\,(\omega)| \,\text{QFT}_P\right) M_m^\dagger M_m \left(\text{QFT}_P^\dagger \,|\mathcal{F}_P\,(\omega)\rangle\right) && (3.62)\\ &= \langle \mathcal{F}_P\,(\omega)| \,\text{QFT}_P \,|m\rangle \,\langle m| \,\text{QFT}_P^\dagger \,|\mathcal{F}_P\,(\omega)\rangle && (3.63)\\ &= \langle \mathcal{F}_P\,(\omega) \,|\, \mathcal{F}_P\,(m)\rangle \,\langle \mathcal{F}_P\,(m) \,|\, \mathcal{F}_P\,(\omega)\rangle && (3.64)\\ &= |\langle \mathcal{F}_P\,(m) \,|\, \mathcal{F}_P\,(\omega)\rangle|^2 && (3.65) \end{aligned}$$

e após a medição o estado obtido ignorando-se a fase global é

$$\frac{(|m\rangle \langle m|)\ \ \text{QFT}^\dagger \,|\mathcal{F}_P\,(\omega)\rangle}{\sqrt{|\langle \mathcal{F}_P\,(m) \,|\, \mathcal{F}_P\,(\omega)\rangle|^2}} = \frac{|m\rangle \,\langle \mathcal{F}_P\,(m) \,|\, \mathcal{F}_P\,(\omega)\rangle}{|\langle \mathcal{F}_P\,(m) \,|\, \mathcal{F}_P\,(\omega)\rangle|} = |m\rangle\,. \tag{3.66}$$

Como $|\mathcal{F}_P\,(0)\rangle$ e $|\mathcal{F}_P\,(P)\rangle$ são equivalentes, ambos os estados geram os mesmos resultados; então denota-se $|P\rangle = |0\rangle$ e $\text{prob}\,(X = P) = \text{prob}\,(X = 0)$. Usando-se esses fatos sistematicamente, vários cenários são considerados.

Se $P = 1$, Lema 2 dá que

$$|\langle \mathcal{F}_P\,(\omega) \,|\, \mathcal{F}_P\,(\omega')\rangle|^2 = \frac{\sin^2\,(\pi\omega_\Delta)}{\sin^2\,(\pi\omega_\Delta)} = 1. \tag{3.67}$$

O caso $P = 2$ foi analisado no Apêndice A. Caso $P > 2$ e ω for um inteiro, então $|\mathcal{F}_P\,(\omega)\rangle \in B_\mathcal{F}$ e

$$\text{QFT}_P^{-1} \,|\mathcal{F}_P\,(\omega)\rangle = |\omega\rangle \tag{3.68}$$

é o estado obtido após a medida com probabilidade 1.

Caso contrário ($P > 2$ e $\omega \notin \mathbb{N}$), deseja-se calcular

$$\begin{aligned} \text{prob}\,(|X - \omega| \leq 1) &= \text{prob}\,(X = \lfloor\omega\rfloor) + \text{prob}\,(X = \lceil\omega\rceil) && (3.69)\\ &= |\langle \mathcal{F}_P\,(\lfloor\omega\rfloor) \,|\, \mathcal{F}_P\,(\omega)\rangle|^2 + |\langle \mathcal{F}_P\,(\lceil\omega\rceil) \,|\, \mathcal{F}_P\,(\omega)\rangle|^2\,. && (3.70) \end{aligned}$$

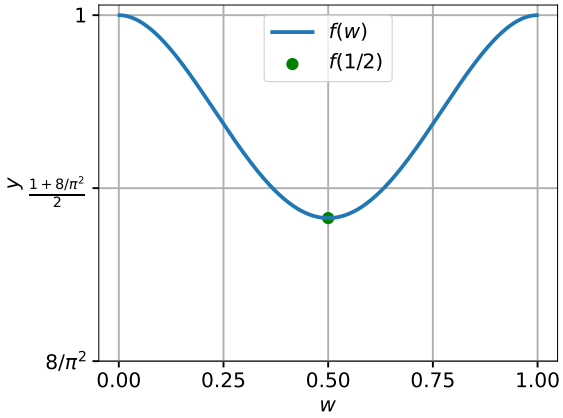
Usando o Lema 2 e donotando $w = |\omega - \lfloor\omega\rfloor\,|$ (note que $0 < w < 1$ e $|\omega - \lceil\omega\rceil| = 1 - w$), obtém-se

$$\text{prob}\,(|X - \omega| \leq 1) = f(w) = \frac{\sin^2\,(\pi w)}{P^2 \sin^2\,(\pi w/P)} + \frac{\sin^2\,(\pi(1-w))}{P^2 \sin^2\,(\pi(1-w)/P)}. \tag{3.71}$$

A função $f(w)$ tem mínimo quando $w = 1/2$, conforme ilustrado nas Figs. 25 e 26 para $P = 3$ e P $= 30$, respectivamente. Uma demonstração formal pode ser encontrada no Apêndice A. Usando também que $\sin^2\theta \leq \theta^2$, obtém-se

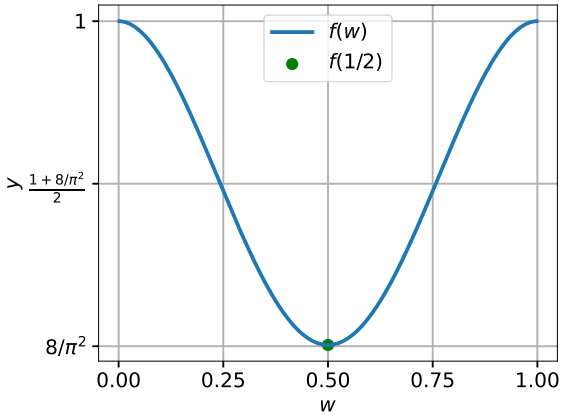
$$\begin{aligned} \text{prob}\,(|X - \omega| \leq 1) &\geq 2\frac{\sin^2\left(\frac{\pi}{2}\right)}{P^2 \sin^2\left(\frac{\pi}{2P}\right)} && (3.72)\\ &\geq \frac{2}{P^2} \cdot \frac{4P^2}{\pi^2} && (3.73)\\ &= \frac{8}{\pi^2}. && (3.74) \end{aligned}$$

Figura 25 – Gráfico de $f(w)$ com $P = 3$ e respectivo mínimo global.



Fonte: Produzido pelo autor.

Figura 26 – Gráfico de $f(w)$ com $P = 30$ e respectivo mínimo global.



Fonte: Produzido pelo autor.

Logo, uma medição de $\mathrm{QFT}_P^{-1} |\mathcal{F}_P(\omega)\rangle$ na base computacional e ignorando a fase global resulta em um dos estados $|\lfloor \omega \rfloor\rangle$ ou $|\lceil \omega \rceil\rangle$ com probabilidade maior ou igual a $8/\pi^2$.

□

3.2.1 Implementação da QFT e sua inversa

O foco dessa seção é a implementação da QFT (e sua inversa) em portas quânticas. Para tanto, considere ao longo dessa sessão que $P = 2^p$ onde $p \in \mathbb{N}$ é a quantidade de qubits. Quando $p = 1$, a porta H implementa a QFT, já que

$$|\mathcal{F}_2(0)\rangle = \frac{1}{\sqrt{2}} \sum_{\ell=0}^{1} e^0 |\ell\rangle \tag{3.75}$$

$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{3.76}$$

e

$$|\mathcal{F}_2(1)\rangle = \frac{1}{\sqrt{2}} \sum_{\ell=0}^{1} e^{\pi \mathrm{i} \ell} |\ell\rangle \tag{3.77}$$

$$= \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \tag{3.78}$$

ou, de forma geral,

$$|\mathcal{F}_2(d)\rangle = 2^{-p/2} \left(|0\rangle + e^{2\pi \mathrm{i} d/P} |1\rangle \right), \tag{3.79}$$

onde $d = \{ 0, 1 \}$.

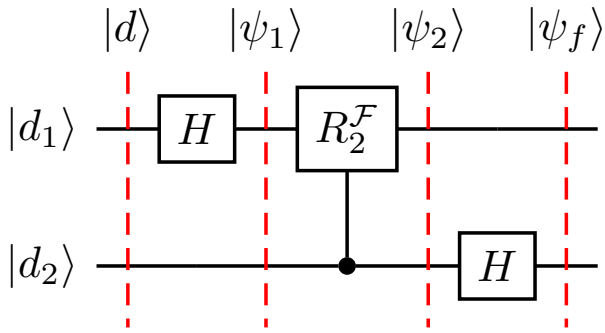
Para $p \geq 2$, será necessário utilizar a seguinte definição.

Definição 3.3. A porta $R_k^{\mathcal{F}}$ atua em vetores em $\mathcal{H}^2$ e é definida na base computacional como

$$R_k^{\mathcal{F}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi \mathrm{i}/2^k} \end{bmatrix}. \tag{3.80}$$

A ação dessa porta é multiplicar o segundo estado da base computacional pela fase $e^{2\pi \mathrm{i}/2^k}$. —

Figura 27 – Circuito básico para implementação da QFT.



Fonte: Produzido pelo autor.

Para $p = 2$, considere o circuito da Fig. 27 com entrada $|d\rangle = |d_1\rangle\,|d_2\rangle \in \mathcal{H}^4$ sendo $|d_1\rangle$ e $|d_2\rangle$ vetores da base computacional representando o valor d, *i.e.* $d_1 d_2$ é a representação binária de d. Primeiramente, aplica-se a porta H no primeiro qubit, resultando no estado

$$|\psi_1\rangle = (H \otimes I)\,|d\rangle \tag{3.81}$$
$$= 2^{-1/2}\left(|0\rangle + e^{2\pi \mathrm{i} d_1/2}\,|1\rangle\right) \otimes |d_2\rangle\,. \tag{3.82}$$

A aplicação da porta $R_2^{\mathcal{F}}$-controlada resulta em

$$|\psi_2\rangle = \mathcal{C}_{2,1}\left(R_2^{\mathcal{F}}\right)|\psi_1\rangle \tag{3.83}$$
$$= 2^{-1/2}\left(|0\rangle + e^{2\pi \mathrm{i} d_1/2} e^{2\pi \mathrm{i} d_2/4}\,|1\rangle\right) \otimes |d_2\rangle\,. \tag{3.84}$$

Note que a representação em binário da divisão $d/4$ é $(d_1 \cdot 2^1 + d_2 \cdot 2^0)/2^2 = d_1 \cdot 2^{-1} + d_2 \cdot 2^{-2}$. Logo, é possível reescrever o estado $|\psi_2\rangle$ como

$$|\psi_2\rangle = 2^{-1/2}\left(|0\rangle + e^{2\pi \mathrm{i} d/4}\,|1\rangle\right) \otimes |d_2\rangle\,. \tag{3.85}$$

Ao aplicar a porta H no segundo qubit e notando que $d/2 = d_1 \cdot 2^0 + d_2 \cdot 2^{-1}$, obtém-se o estado final

$$|\psi_f\rangle = (I \otimes H)\,|\psi_2\rangle \tag{3.86}$$
$$= 2^{-1/2}\left(|0\rangle + e^{2\pi \mathrm{i} d/4}\,|1\rangle\right) \otimes 2^{-1/2}\left(|0\rangle + e^{2\pi \mathrm{i} d_2/2}\,|1\rangle\right) \tag{3.87}$$
$$= 2^{-2/2}\left(|0\rangle + e^{2\pi \mathrm{i} d/4}\,|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi \mathrm{i} d_1} e^{2\pi \mathrm{i} d_2/2}\,|1\rangle\right). \tag{3.88}$$
$$= 2^{-2/2}\left(|0\rangle + e^{2\pi \mathrm{i} d/4}\,|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi \mathrm{i} d/2}\,|1\rangle\right). \tag{3.89}$$

A partir de $|\psi_f\rangle$, é possível obter um estado da base de Fourier após aplicar a operação swap.

$$\begin{aligned}
\mathrm{SWAP}\,|\psi_f\rangle &= 2^{-2/2}\left(|0\rangle + e^{2\pi \mathrm{i} d/2}\,|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi \mathrm{i} d/4}\,|1\rangle\right) && (3.90)\\
&= 2^{-2/2}\left(|00\rangle + e^{2\pi \mathrm{i} d/4}\,|01\rangle + e^{2\pi \mathrm{i} d\cdot 2/4}\,|10\rangle + e^{2\pi \mathrm{i} d\cdot 3/4}\,|11\rangle\right) && (3.91)\\
&= \frac{1}{2}\sum_{\ell=0}^{3} e^{2\pi \mathrm{i} d\ell/P}\,|\ell\rangle && (3.92)\\
&= |\mathcal{F}_4\,(d)\rangle\,. && (3.93)
\end{aligned}$$

Agora, deseja-se mostrar que é possível gerar os estados da base de Fourier para $p \geq 3$. Para isso, as seguintes definições serão necessárias.

Definição 3.4. Seja $p \geq 1$ e $d' \in \mathbb{N}$ cuja representação binária é $d_1 \ldots d_p$. Define-se a porta $\mathrm{QFT}_p^{\mathrm{rec}}$ como

$$\mathrm{QFT}_p^{\mathrm{rec}}\,|d'\rangle = 2^{-p/2}\bigotimes_{j=0}^{p-1}\left(|0\rangle + \exp\left(2\pi \mathrm{i} d'/2^{p-j}\right)|1\rangle\right). \tag{3.94}$$

—

Note que quando $p = 1$, obtém-se $\mathrm{QFT}_p^{\mathrm{rec}}\,|d'\rangle = H\,|d'\rangle$.

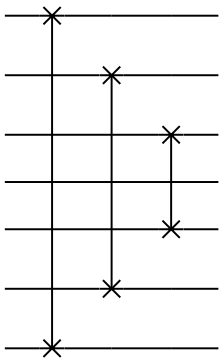
Definição 3.5. Seja p um inteiro maior ou igual a 2. Define-se SWAP'_p a sequência de operações SWAP que inverte a ordem de todos os qubits. Ou seja,

$$\mathrm{SWAP}'_p = \prod_{t=1}^{\lfloor p/2 \rfloor} \mathrm{SWAP}_{t,p-t}. \tag{3.95}$$

—

O circuito de SWAP'_7 está ilustrado na Fig. 28.

Figura 28 – Circuito que inverte a ordem de sete qubits.



Produzido pelo autor.

Em posse dessas definições, é possível descrever o circuito que implementa QFT_P para $p \geq 2$.

Teorema 3. *Sejam $p, P, d \in \mathbb{N}$ tais que $p \geq 2$, $P = 2^p$ e $0 \leq d < P$ cuja representação binária é $d_1 \dots d_p$. Então,*

$$\mathrm{QFT}_p^{\mathrm{rec}} = \left(I \otimes \mathrm{QFT}_{p-1}^{\mathrm{rec}}\right) \prod_{k=2}^{p} \mathcal{C}_{k,1}\left(R_k^{\mathcal{F}}\right)(H \otimes I) \tag{3.96}$$

e

$$\mathrm{SWAP}'_p \ \mathrm{QFT}_p^{\mathrm{rec}} |d\rangle = |\mathcal{F}_P(d)\rangle . \tag{3.97}$$

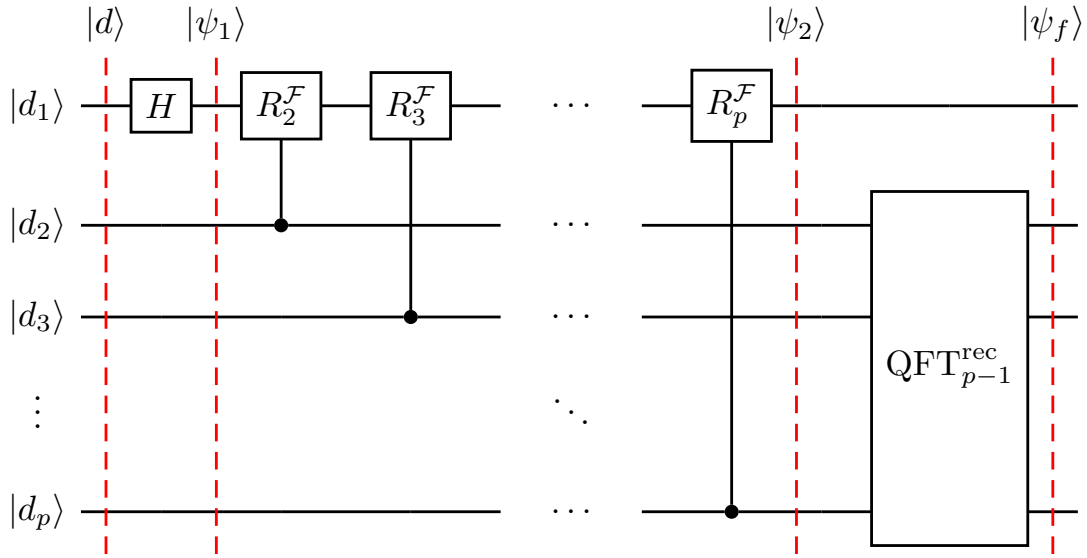
Ou seja, $\mathrm{SWAP}'_p \ \mathrm{QFT}_p^{\mathrm{rec}}$ *descreve o circuito que implementa* QFT_P. —

Demonstração. Prova-se a Eq. 3.96 por indução. Note que o caso base $p = 2$ já foi abordado da Eq. 3.82 à 3.89. Hipótese indutiva: suponha que

$$\mathrm{QFT}_{p'}^{\mathrm{rec}} = \left(I \otimes \mathrm{QFT}_{p'-1}^{\mathrm{rec}}\right) \prod_{k=2}^{p'} \mathcal{C}_{k,1}\left(R_k^{\mathcal{F}}\right)(H \otimes I) \tag{3.98}$$

é verdade para todos os valores $2 \leq p' \leq p-1$. Passo indutivo: demonstrar que a Eq. 3.96 é verdadeira para p. O circuito correspondente está desenhado na Fig. 29.

Figura 29 – Circuito de $\mathrm{QFT}_p^{\mathrm{rec}}$.



Fonte: Produzido pelo autor.

Primeiro aplica-se a porta $(H \otimes I)$ em $|d\rangle$, obtendo-se o estado

$$|\psi_1\rangle = (H \otimes I)|d_1\rangle |d_2 \dots d_p\rangle \tag{3.99}$$

$$= 2^{-1/2}\left(|0\rangle + \exp\left(2\pi \mathrm{i} d_1/2\right)|1\rangle\right) \otimes |d_2 \dots d_p\rangle . \tag{3.100}$$

Agora, aplica-se a sequência de portas controladas $\mathcal{C}_{k,1}\left(R_k^{\mathcal{F}}\right)$. Note que a ordem de aplicação dessas portas é irrelevante pois a ação de cada $R_k^{\mathcal{F}}$ é de multiplicar a fase de $|1\rangle$

por $\exp\left(2\pi\mathrm{i}/2^k\right)$. A aplicação ou não da porta $R_k^{\mathcal{F}}$ depende diretamente do valor d_k: a porta não atua caso $d_k = 0$ e atua caso $d_k = 1$, alterando o qubit alvo conforme

$$|1\rangle \to \exp\left(2\pi\mathrm{i}d_k/2^k\right)|1\rangle\,. \tag{3.101}$$

Note também que a divisão $d/2^p$ pode ser escrita como

$$\begin{aligned} d/2^p &= \left(d_1\cdot 2^{p-1} + \cdots + d_p\cdot 2^0\right)/2^p && (3.102)\\ &= \left(d_1/2^1 + \cdots + d_p/2^p\right) && (3.103)\\ &= \sum_{k=1}^{p} d_k/2^k. && (3.104)\end{aligned}$$

Juntado todos esses argumentos, a aplicação da sequência de $\mathcal{C}_{k,1}\left(R_k^{\mathcal{F}}\right)$ no estado $|\psi_1\rangle$ resulta em

$$\begin{aligned} |\psi_2\rangle &= \prod_{k=2}^{p}\mathcal{C}_{k,1}\left(R_k^{\mathcal{F}}\right)|\psi_1\rangle && (3.105)\\ &= 2^{-1/2}\left(|0\rangle + \prod_{k=1}^{p}\exp\left(2\pi\mathrm{i}d_k/2^k\right)|1\rangle\right)\otimes|d_2\ldots d_p\rangle && (3.106)\\ &= 2^{-1/2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}\sum_{k=1}^{p}d_k/2^k\right)|1\rangle\right)\otimes|d_2\ldots d_p\rangle && (3.107)\\ &= 2^{-1/2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d/2^p\right)|1\rangle\right)\otimes|d_2\ldots d_p\rangle\,. && (3.108)\end{aligned}$$

Por último, seja o número binário $d' = d_2\ldots d_p$. A aplicação de $I\otimes\mathrm{QFT}_{p-1}^{\mathrm{rec}}$ resulta em

$$\begin{aligned} |\psi_f\rangle &= \left(I\otimes\mathrm{QFT}_{p-1}^{\mathrm{rec}}\right)|\psi_2\rangle && (3.109)\\ &= 2^{-1/2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d/2^p\right)|1\rangle\right)\otimes\mathrm{QFT}_{p-1}^{\mathrm{rec}}|d_2\ldots d_{p-1}\rangle\,. && (3.110)\\ &= 2^{-p/2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d/2^p\right)|1\rangle\right)\left(\bigotimes_{j'=0}^{p-2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d'/2^{p-1-j'}\right)|1\rangle\right)\right), && (3.111)\end{aligned}$$

renomeando $j = j' + 1$,

$$\begin{aligned} |\psi_f\rangle &= 2^{-p/2}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d/2^p\right)|1\rangle\right)\bigotimes_{j=1}^{p-1}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d'/2^{p-j}\right)|1\rangle\right) && (3.112)\\ &= 2^{-p/2}\bigotimes_{j=0}^{p-1}\left(|0\rangle + \exp\left(2\pi\mathrm{i}d'/2^{p-j}\right)|1\rangle\right). && (3.113)\end{aligned}$$

Portanto, conclui-se que a Eq. 3.96 é verdadeira.

Resta demonstrar que a Eq. 3.97 realmente implementa QFT_P. Sabendo que SWAP'_p apenas inverte a ordem dos qubits, tomando ℓ um número inteiro $0 \le \ell < P$ com representação binária $\ell_1\ldots\ell_p$ e notando que

$$\ell/2^p = \sum_{k=1}^{p}\ell_k/2^k = \sum_{\ell_k=1}\ell_k/2^k, \tag{3.114}$$

obtém-se

$$\mathrm{SWAP}'_p\ \mathrm{QFT}_p^{\mathrm{rec}}\left|d\right\rangle = 2^{-p/2}\ \mathrm{SWAP}'_p \bigotimes_{j=0}^{p-1}\left(\left|0\right\rangle + \exp\left(2\pi \mathrm{i} d/2^{p-j}\right)\left|1\right\rangle\right) \tag{3.115}$$

$$= 2^{-p/2} \bigotimes_{k=1}^{p}\left(\left|0\right\rangle + \exp\left(2\pi \mathrm{i} d/2^{k}\right)\left|1\right\rangle\right) \tag{3.116}$$

$$= 2^{-p/2} \sum_{\ell=0}^{P-1} \exp\left(2\pi \mathrm{i} d\ell/2^{p}\right)\left|\ell\right\rangle \tag{3.117}$$

$$= \left|\mathcal{F}_P\left(d\right)\right\rangle, \tag{3.118}$$

conforme desejado. □

Convencendo-se que esse circuito implementa QFT_P num computador quântico, o circuito para QFT_P^{-1} é obtido facilmente ao fazer

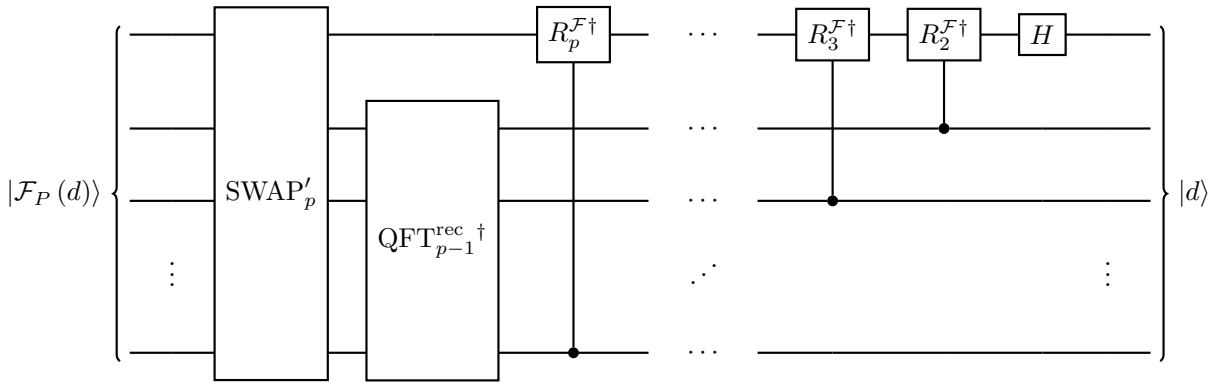
$$\mathrm{QFT}_P^{-1} = \mathrm{QFT}_p^{\dagger} \tag{3.119}$$

$$= \mathrm{QFT}_p^{\mathrm{rec}\dagger}\ \mathrm{SWAP}'_p \tag{3.120}$$

$$= \left(H \otimes I\right) \prod_{k=2}^{p} \mathcal{C}_{k,1}\left(R_k^{\mathcal{F}\dagger}\right)\left(I \otimes \mathrm{QFT}_{p-1}^{\mathrm{rec}\ \dagger}\right)\mathrm{SWAP}'_p. \tag{3.121}$$

originando o circuito da Fig. 30.

Figura 30 – Circuito para QFT_P^{-1}.



Fonte: Produzido pelo autor.

3.3 Estimativa de Fase

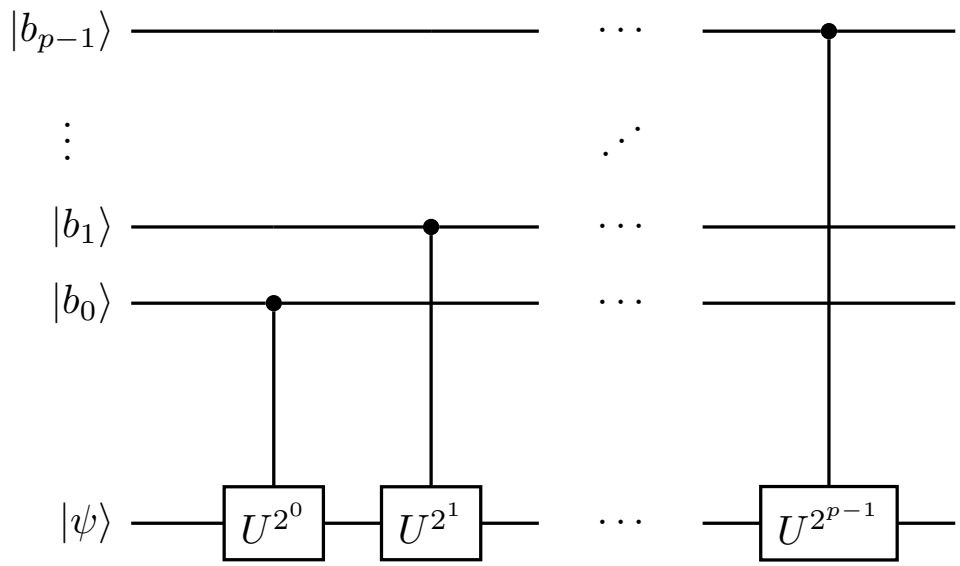
Seja $N \in \mathbb{N}$ tal que $N \geq 1$. Nessa seção será abordado o problema de estimar a fase $e^{2\pi \mathrm{i}\lambda}$ de um autovetor $\left|\lambda\right\rangle \in \mathcal{H}^N$ de uma matriz unitária U. A fase pode ser estimada a partir de uma estimativa do valor $0 \leq \lambda < 1$ no expoente do autovalor. Note que há uma similaridade na estrutura de $e^{2\pi \mathrm{i}\lambda}$ com os expoentes do estado $\left|\mathcal{F}_P\left(\lambda\right)\right\rangle$ (Def. 3.1). Essa similaridade levanta a possibilidade de utilizar a QFT e sua inversa para tentar estimar λ.

Antes de utilizar a QFT inversa, é necessário obter o estado $|\mathcal{F}_P(\lambda)\rangle$ de alguma forma; tópico abordado a seguir.

3.3.1 Elevação de Matriz Controlada

Seja $b \in \mathbb{N}$ cuja representação binária possui p dígitos: $b_{p-1}\ldots b_1 b_0$. Como usual na computação, bits menos significativos têm subíndices menores, possibilitando a representação $b = \sum_{j=0}^{p-1} b_j \cdot 2^j$. Sendo $|b\rangle = |b_{p-1}\rangle \otimes \cdots \otimes |b_0\rangle$ o estado correspondente ao número b.

Figura 31 – Parte do circuito do algoritmo de estimativa de fase.



Fonte: Produzido pelo autor.

Analisa-se o circuito da Fig. 31, que possui dois registradores. O primeiro registrador recebe $|b\rangle$ como entrada e o segundo registrador um vetor $|\psi\rangle \in \mathcal{H}^N$. Observe que o valor b_j é responsável por controlar a porta U^{2^j} que atua no segundo registrador. O segundo registrador não necessariamente é implementado com qubits, já que N não necessariamente é uma potência de 2 – *e.g.* pode ser um qudit (THEW et al., 2002). Notando que $U^{0\cdot 2^j} = I$ e $U^{1\cdot 2^j} = U^{2^j}$, a ação do circuito pode ser representada por

$$|b\rangle \otimes \prod_{j=0}^{p-1} U^{b_j \cdot 2^j} |\psi\rangle = |b\rangle \otimes U^{\sum_{j=0}^{p-1} b_j \cdot 2^j} |\psi\rangle \tag{3.122}$$

$$= |b\rangle \otimes U^b |\psi\rangle . \tag{3.123}$$

Ou seja, esse circuito aplica b vezes o operador U no vetor $|\psi\rangle$. Para simplificar a notação, faz-se a seguinte definição.

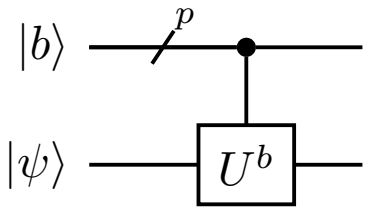
Definição 3.6. O operador $\mathcal{C}_{\text{pot}}(U)$ atua em $|b\rangle \otimes |\psi\rangle \in \mathcal{H}^P \otimes \mathcal{H}^N$ aplicando b potências de U em ψ.

$$\mathcal{C}_{\text{pot}}(U)\,|b\rangle \otimes |\psi\rangle = |b\rangle \otimes U^b\,|\psi\rangle\,. \tag{3.124}$$

—

O circuito de $\mathcal{C}_{\text{pot}}(U)$ no espaço reduzido é representado na Fig. 32.

Figura 32 – Representação do circuito $\mathcal{C}_{\text{pot}}(U)$ no espaço reduzido.



Fonte: Produzido pelo autor.

Sabendo do comportamento do circuito $\mathcal{C}_{\text{pot}}(U)$, faz-se a seguinte pergunta: "qual a saída do circuito se o vetor do segundo registrador for um autovetor de U?" Considerando o $e^{2\pi i\lambda}$-autovetor $|\lambda\rangle$ obtém-se

$$\begin{aligned}\mathcal{C}_{\text{pot}}(U)\,|b\rangle\,|\lambda\rangle &= |b\rangle \otimes U^b\,|\lambda\rangle &(3.125)\\ &= |b\rangle \otimes e^{b\cdot 2\pi i\lambda}\,|\lambda\rangle &(3.126)\\ &= e^{b\cdot 2\pi i\lambda}\,|b\rangle\,|\lambda\rangle\,. &(3.127)\end{aligned}$$

O fenômeno de *phase kickback* ocorrido é o que possibilita o funcionamento do algoritmo de estimativa de fase.

Uma pergunta análoga é: "o que ocorre se a entrada do segundo registrador for uma sobreposição não trivial da base ortonormal de autovetores, *i.e.* $|\psi\rangle = \sum_{j=1}^{N} \alpha_j\,|\lambda_j\rangle$?" Nesse caso,

$$\begin{aligned}\mathcal{C}_{\text{pot}}(U)\,|b\rangle\,|\psi\rangle &= |b\rangle \otimes U^b \sum_{j=1}^{N} \alpha_j\,|\lambda_j\rangle &(3.128)\\ &= |b\rangle \otimes \sum_{j=1}^{N} e^{b\cdot 2\pi i\lambda_j}\alpha_j\,|\lambda_j\rangle &(3.129)\\ &= \sum_{j=1}^{N} \left(e^{b\cdot 2\pi i\lambda_j}\alpha_j\,|b\rangle \otimes |\lambda_j\rangle\right). &(3.130)\end{aligned}$$

Observe que o fenômeno de *phase kickback* ainda ocorre, mas as amplitudes α_j provenientes da sobreposição também influenciam o primeiro registrador. Tal qual na sobreposição $|\psi\rangle$, as amplitudes α_j influenciam nas probabilidades de cada estado.

3.3.2 Circuito Completo

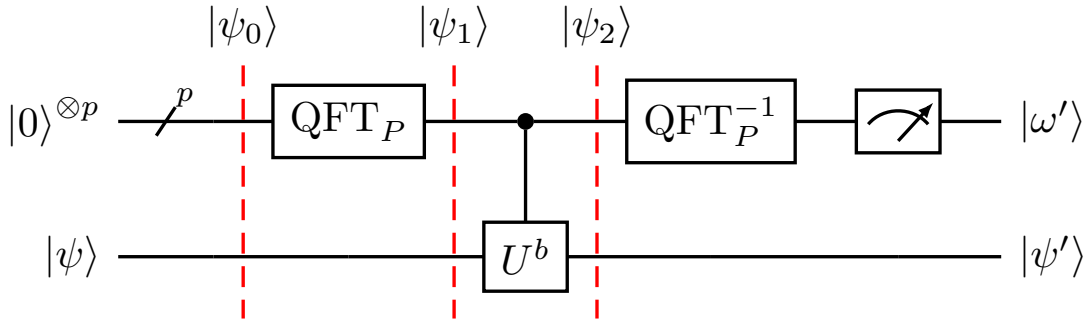
Com o conhecimento mais aprofundado sobre a ação do operador $\mathcal{C}_{\text{pot}}(U)$, é possível analisar o algoritmo de estimativa de fase (Alg. 2) cujo circuito está ilustrado na Fig. 33.

Algoritmo 2: Algoritmo de Estimativa de Fase – est_fase$(p, U, |\psi\rangle)$

Entrada: p: tamanho do primeiro registrador (precisão); U: operador alvo; $|\psi\rangle$: (sobreposição de) autovetor(es) de U.

1: $P \leftarrow 2^p$, e seja $|\psi_0\rangle = |0\rangle^{\otimes p} |\psi\rangle$ o estado inicial
2: Aplicar QFT_p no primeiro registrador
3: Realizar operação de potências de U controladas – operador $\mathcal{C}_{\text{pot}}(U)$
4: Aplicar QFT_p^{-1} no primeiro registrador
5: Seja $|\omega'\rangle$ o resultado da medição do primeiro registrador na base computacional
6: **retorna** ω'/P

Figura 33 – Circuito do algoritmo de estimativa de fase.



Fonte: Produzido pelo autor.

Analisando o algoritmo passo a passo, observa-se que a aplicação de QFT_P no primeiro registrador resulta na sobreposição uniforme de $|0\rangle, \ldots, |P-1\rangle$. Isso ocorre porque a entrada do primeiro registrador é fixada em $|0\rangle^{\otimes p}$. Sendo assim,

$$|\psi_1\rangle = (\text{QFT}_P \otimes I) |0\rangle |\psi\rangle \tag{3.131}$$

$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} |j\rangle |\psi\rangle . \tag{3.132}$$

Para simplificar a análise dos passos subsequentes, suponha que $|\psi\rangle$ é o $e^{2\pi i\lambda}$-autovetor $|\lambda\rangle$

de U. Após aplicar o operador de potências de U controladas obtém-se o estado

$$|\psi_2\rangle = \mathcal{C}_{\text{pot}}(U)\,|\psi_1\rangle \tag{3.133}$$

$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} |j\rangle \otimes U^j\,|\lambda\rangle \tag{3.134}$$

$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} e^{j\cdot 2\pi \mathrm{i}\lambda}\,|j\rangle\,|\lambda\rangle \tag{3.135}$$

$$= \frac{1}{\sqrt{P}} \sum_{j=0}^{P-1} \exp\left(2\pi \mathrm{i} j(P\lambda)/P\right)|j\rangle\,|\lambda\rangle \tag{3.136}$$

$$= |\mathcal{F}_P\,(P\lambda)\rangle\,|\lambda\rangle\,. \tag{3.137}$$

Agora, ignorando o segundo registrador, deseja-se aplicar a QFT_P^{-1} e realizar uma medição na base computacional para obter o resultado $|P\lambda\rangle$. Entretanto, isso não necessariamente é verdade. Recobre que $\lambda \in \mathbb{R}$ tal que $0 \leq \lambda < 1$. Logo, o valor λ pode ser representado como um número binário $0.\lambda_1^b\lambda_2^b\lambda_3^b\ldots$ não necessariamente finito. Então, analisa-se dois cenários possíveis.

No primeiro caso, suponha que λ possa ser representado *exatamente* com p dígitos binários – *i.e.* $\lambda = \lambda_1^b\lambda_2^b\ldots\lambda_{p-1}^b/2^p = 0.\lambda_1^b\lambda_2^b\ldots\lambda_{p-1}^b$ – conclui-se que $|\mathcal{F}_P\,(P\lambda)\rangle \in B_{\mathcal{F}}$. Logo, usando o Teorema 2,

$$|\omega'\rangle = |P\lambda\rangle \tag{3.138}$$

com probabilidade 1. Caso λ *não* possa ser representado com p dígitos binários, $P\lambda \notin \mathbb{N}$; mas deseja-se obter um resultado tão próximo quanto possível desse valor, *i.e.* ou $\lfloor P\lambda \rfloor$ ou $\lceil P\lambda \rceil$. Esse cenário já foi analisado no Teorema 2. Portanto,

$$|\omega'\rangle \in \{\,|\lfloor P\lambda \rfloor\rangle\,, |\lceil P\lambda \rceil\rangle\,\} \tag{3.139}$$

com probabilidade maior ou igual a $8/\pi^2$.

Resta ainda analisar o caso em que $|\psi\rangle$ é uma sobreposição $|\psi\rangle = \sum_l \alpha_l\,|\lambda_l\rangle$ de autovetores de U. Nesse caso,

$$|\psi_2\rangle = \frac{1}{\sqrt{P}} \sum_l \alpha_l \sum_{j=0}^{P-1} |j\rangle \otimes U^j\,|\lambda_l\rangle \tag{3.140}$$

$$= \frac{1}{\sqrt{P}} \sum_l \alpha_l \sum_{j=0}^{P-1} \exp\left(2\pi \mathrm{i} j(P\lambda_l)/P\right)|j\rangle \otimes |\lambda_l\rangle \tag{3.141}$$

$$= \sum_l \alpha_l\,|\mathcal{F}_P\,(P\lambda_l)\rangle \otimes |\lambda_l\rangle\,. \tag{3.142}$$

Deseja-se aplicar $(\text{QFT}_P^{-1} \otimes I)$ e fazer uma medição na base computacional no primeiro registrador. Por enquanto, o segundo registrador será mantido. Seja

$$|\hat{\omega}\rangle = \text{QFT}_P^{-1} \sum_{l=1}^{L} \alpha_l\,|\mathcal{F}_P\,(P\lambda_l)\rangle \otimes |\lambda_l\rangle\,. \tag{3.143}$$

Utilizando o conjunto de operadores de medida $\{ M_m \}$ onde

$$M_m = |m\rangle \langle m| \otimes I \tag{3.144}$$

com $m \in \mathbb{N}$ tal que $0 \leq m < P-1$; então, a probabilidade de medir m é

$$\begin{aligned}
\langle \hat{\omega}| M_m^\dagger M_m |\hat{\omega}\rangle = &\left(\sum_l \alpha_l^* \langle \mathcal{F}_P (P\lambda_l)| \langle \lambda_l| \right) \mathrm{QFT}_P |m\rangle \otimes I \\
&\langle m| \mathrm{QFT}_P^\dagger \otimes I \left(\sum_\ell \alpha_\ell |\mathcal{F}_P (P\lambda_\ell)\rangle |\lambda_\ell\rangle \right) && (3.145) \\
= &\left(\sum_l \alpha_l^* \langle \mathcal{F}_P (P\lambda_l) | \mathcal{F}_P (m)\rangle \right) \delta_{l,\ell} \\
&\left(\sum_\ell \alpha_\ell \langle \mathcal{F}_P (m) | \mathcal{F}_P (P\lambda_\ell)\rangle \right) && (3.146) \\
= &\sum_l |\alpha_l|^2 \ |\langle \mathcal{F}_P (P\lambda_l) | \mathcal{F}_P (m)\rangle|^2 . && (3.147)
\end{aligned}$$

Note a semelhança entre essa equação e o que foi obtido no início da demonstração do Teorema 2. Portanto, usando esse mesmo teorema, conclui-se que se $P\lambda_l \in \mathbb{N}$, o estado após a medida será $|P\lambda_l\rangle$ com probabilidade maior ou igual a $|\alpha_l|^2$ e caso $P\lambda_l \notin \mathbb{N}$, o estado após a medida será $|\lfloor P\lambda_l \rfloor\rangle$ ou $|\lceil P\lambda_l \rceil\rangle$ com probabilidade maior ou igual a $|\alpha_l|^2 \cdot 8/\pi^2$.

3.4 Algoritmo de Contagem

O algoritmo de contagem elegantemente une todas as seções desse capítulo. Relembre que o objetivo do algoritmo de busca (Alg. 1) é encontrar um elemento marcado pelo oráculo O_f. Toda a análise do algoritmo foi feita em torno do ângulo θ definido por $\sin\theta = \sqrt{k/N}$, onde k é a quantidade de elementos marcados por O_f e N a dimensão do espaço de Hilbert. Como a matriz U_G faz uma rotação de 2θ no hiperplano definido por $|x_0\rangle$ e $|x_1\rangle$, é possível analisar o algoritmo em torno dos autovetores

$$|\mp \mathrm{i}_x\rangle = \frac{|x_0\rangle \mp \mathrm{i}\,|x_1\rangle}{\sqrt{2}} \tag{3.148}$$

associados aos autovalores $e^{\pm 2\mathrm{i}\theta}$, respectivamente. A condição inicial do algoritmo de busca pode ser representada em termos desses autovetores:

$$\begin{aligned}
|\psi\rangle = &\cos\theta\,|x_0\rangle + \sin\theta\,|x_1\rangle && (3.149) \\
= &\langle -\mathrm{i}_x \,|\, \psi\rangle\, |-\mathrm{i}_x\rangle + \langle +\mathrm{i}_x \,|\, \psi\rangle\, |+\mathrm{i}_x\rangle && (3.150) \\
= &\frac{e^{\mathrm{i}\theta}}{\sqrt{2}} |-\mathrm{i}_x\rangle + \frac{e^{-\mathrm{i}\theta}}{\sqrt{2}} |+\mathrm{i}_x\rangle . && (3.151)
\end{aligned}$$

Agora, considere o problema de contar quantos elementos são marcados por O_f. Observe que há uma relação direta entre θ e a quantidade de elementos marcados k.

Portanto, uma boa estimativa de θ deve resultar numa boa estimativa de k; o que pode ser feito utilizando o algoritmo de estimativa de fase! O algoritmo de contagem está detalhado em Alg. 3.

Algoritmo 3: Algoritmo de Contagem

Entrada: O_f: Oráculo da função f; p: número de qubits do primeiro registrador do algoritmo de estimativa de fase; n: número de qubits do segundo registrador respeitando o domínio de f.

1: Construir operador $U_G = GO_f$
2: Preparar o estado $|\psi\rangle = H^{\otimes n}|0\rangle$
3: $\vartheta \leftarrow \text{est\_fase}(p, U_G, |\psi\rangle)$
4: $\theta' \leftarrow \vartheta\pi$
5: Se $\theta' > \pi/2$ então $\theta' \leftarrow \theta' - \pi/2$
6: **retorna** $k = \sin^2(\theta') \cdot N$

Executar o algoritmo de estimativa de fase com U_G como operador alvo resulta numa estimativa equiprovável de um dos autovalores $e^{\pm 2i\theta}$ – na realidade resulta num valor ϑ que é uma estimativa de $\pm\theta/\pi$. Obtém-se o ângulo estimado θ' ao computar $\theta' = \vartheta\pi$. Agora é necessário distinguir se θ' corresponde a uma estimativa de $+\theta$ ou de $-\theta$. Notando que

$$\sin\theta = \sqrt{\frac{k}{N}},\ \cos\theta = \sqrt{\frac{N-k}{N}} \implies 0 \leq \theta \leq \frac{\pi}{2}, \tag{3.152}$$

obtém-se a estimativa de $+\theta$ facilmente. Como $\sin\theta = \sqrt{k/N}$, calcular $\sin^2(\theta') \cdot N$ resulta numa estimativa da quantidade de elementos marcados. Resta analisar o quão precisa é essa estimativa.

3.4.1 Precisão do Algoritmo de Contagem

O foco da análise da precisão será no valor $\sin^2(\theta')$. A precisão da saída do algoritmo segue como um corolário simples. A precisão é dada pelo seguinte Teorema adaptado do Teorema 12 de BHMT (BRASSARD et al., 2002).

Teorema 4. *Sejam p a entrada do do algoritmo; $P = 2^p$; e θ' a estimativa do ângulo θ. Então $\sin^2\theta = 0 \implies \sin^2\theta' = 0$ e $\sin^2\theta = 1 \implies \sin^2\theta' = 1$ com certeza; caso contrário,*

$$\left|\sin^2\theta' - \sin^2\theta\right| \leq 2\pi\frac{\sin\theta\cos\theta}{P} + \frac{\pi^2}{P} \tag{3.153}$$

com probabilidade maior ou igual a $8/\pi^2$. Além disso, o algoritmo sempre realiza $P-1$ consultas ao oráculo. —

Demonstração. Caso $\sin^2\theta = 0$ ou $\sin^2\theta = 1$, temos $\theta = 0$ ou $\theta = \pi/2$, respectivamente. Logo, $\vartheta = 0$ e $\vartheta = 1/2$ precisam ser saídas exatas do algoritmo de estimativa de fase. Isso

acontece se for possível obter exatamente os estados $|\mathcal{F}_P(0)\rangle$ e $|\mathcal{F}_P(P/2)\rangle$ após a aplicação da porta $\mathcal{C}_{\text{pot}}(U_G)$; e já que P é par, isso de fato acontece.

Caso contrário, suponha que $\varepsilon \in \mathbb{R}$ tal que $\varepsilon \geq 0$ e $|\theta - \theta'| \leq \varepsilon$. Se $\theta' \geq \theta$,

$$\begin{aligned}
\sin^2(\theta+\varepsilon) - \sin^2\theta &= (\sin\theta\cos\varepsilon + \cos\theta\sin\varepsilon)^2 - \sin^2\theta && (3.154)\\
&= \sin^2\theta\cos^2\varepsilon - \sin^2\theta + \cos^2\theta\sin^2\varepsilon + 2\sin\varepsilon\cos\varepsilon\sin\theta\cos\theta && (3.155)\\
&= -\sin^2\theta\sin^2\varepsilon + (1-\sin^2\theta)\sin^2\varepsilon + \sin(2\varepsilon)\sin\theta\cos\theta && (3.156)\\
&\leq 2\varepsilon\sin\theta\cos\theta + \varepsilon^2. && (3.157)
\end{aligned}$$

Se $\theta' \leq \theta$,

$$\begin{aligned}
\sin^2\theta - \sin^2(\theta-\varepsilon) &= \sin^2\theta - \sin^2\theta\cos^2\varepsilon - \sin^2\varepsilon\cos^2\theta + 2\sin\varepsilon\cos\varepsilon\sin\theta\cos\theta && (3.158)\\
&= \sin^2\theta\sin^2\varepsilon - \sin^2\varepsilon\cos^2\theta + 2\varepsilon\sin\theta\cos\theta && (3.159)\\
&\leq 2\varepsilon\sin\theta\cos\theta + \varepsilon^2. && (3.160)
\end{aligned}$$

Logo,

$$|\theta - \theta'| \leq \varepsilon \implies |\sin^2\theta - \sin^2\theta'| \leq \sin(2\varepsilon)\sin\theta\cos\theta + \varepsilon^2. \quad (3.161)$$

O valor de ε depende do maior erro desejável no algoritmo de estimativa de fase, que é de $1/P$ (ou seja, idealmente apenas o dígito menos significativo está errado). Usando o Teorema 2, esse erro é obtido com probabilidade maior ou igual a $8/\pi^2$. E como a saída do algoritmo é multiplicada por π, deseja-se que $\varepsilon \leq \pi/P$. Logo,

$$|\sin^2\theta - \sin^2\theta'| \leq 2\pi\frac{\sin\theta\cos\theta}{P} + \frac{\pi^2}{P^2}. \quad (3.162)$$

Por último, o algoritmo sempre realiza $P-1$ consultas ao oráculo por conta da ação do operador $\mathcal{C}_{\text{pot}}(U_G)$ no algoritmo de estimativa de fase. □

Usando esse Teorema, é possível obter uma estimativa do erro do algoritmo de contagem; explicitada no seguinte corolário.

Corolário 1. *Sejam p a entrada do algoritmo; $P = 2^p$; θ' a estimativa do ângulo θ; k a quantidade de elementos marcados pelo oráculo O_f e k' sua estimativa dada pelo algoritmo de contagem. Então $k = 0 \implies k' = 0$ e $k = N \implies k' = N$ com certeza; caso contrário,*

$$|k' - k| \leq 2\pi\frac{\sqrt{k(N-k)}}{P} + \frac{\pi^2 N}{P^2}. \quad (3.163)$$

com probabilidade maior ou igual a $8/\pi^2$. Além disso, o algoritmo sempre realiza $P-1$ consultas ao oráculo. —

Demonstração. Maior parte das afirmações seguem trivialmente do Teorema 4. Mostra-se apenas como obter a eq. 3.163. Substituindo os valores de $\sin\theta$ e $\cos\theta$ e multiplicando ambos os lado por N:

$$N\left|\sin^2\theta' - \sin^2\theta\right| \leq 2\pi N\frac{\sqrt{k/N}\sqrt{(N-k)/N}}{P} + N\frac{\pi^2}{P^2} \tag{3.164}$$

$$\left|N\sin^2\theta' - N\sin^2\theta\right| \leq 2\pi\frac{\sqrt{k\,(N-k)}}{P} + \frac{\pi^2 N}{P^2}. \tag{3.165}$$

□

Analisa-se agora o significado do Corolário 1. Evidente que a precisão do algoritmo depende do tamanho do primeiro registrador do algoritmo de estimativa de fase. Sabe-se que o algoritmo de busca tem uma boa precisão com $O\left(\sqrt{N}\right)$ iterações para $k = O(1)$, e resultados similares são desejados para o algoritmo de contagem. Suponha que $P = \sqrt{N}$ e $k = 1$, então, pelo Corolário 1 o erro é menor ou igual a

$$2\pi\frac{\sqrt{1(N-1)}}{\sqrt{N}} + \frac{\pi^2 N}{N} \approx 2\pi + \pi^2 = O(1). \tag{3.166}$$

Já se $k \approx N$ – *e.g.* $k = N - 1$, obtém um erro da mesma ordem:

$$2\pi\frac{\sqrt{(N-1)1}}{\sqrt{N}} + \frac{\pi^2 N}{N} \approx 2\pi + \pi^2 = O(1). \tag{3.167}$$

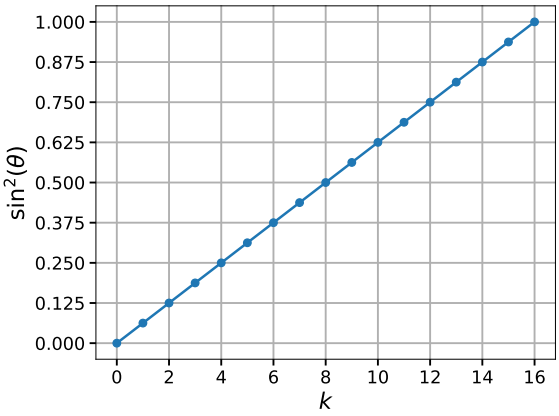
Porém, ao tomar $k \approx N/2$, a ordem do erro aumenta significativamente:

$$2\pi\frac{\sqrt{(N/2)(N-N/2)}}{\sqrt{N}} + \frac{\pi^2 N}{N} = \pi\sqrt{N} + \pi^2 = O(\sqrt{N}). \tag{3.168}$$

Esse comportamento é um pouco estranho para um algoritmo. Poucos elementos marcados ($k \approx 1$) e muitos elementos marcados ($k \approx N$) podem ser contados com precisão, mas quando essa quantia se aproxima da metade ($k \approx N/2$) a precisão diminui significativamente. Qual a razão desse comportamento? Primeiro leve em conta a simetria do problema. Se contar $k \approx 1$ pode ser feito com uma boa precisão, contar $k \approx N - 1$ também pode ser feito com boa precisão já que é equivalente a contar quantos elementos *não* estão marcados – *i.e.* contar $N - k \approx 1$. Mas ainda resta entender a razão para essa precisão diminuir quando $k \approx N/2$. A causa está no comportamento da função arcsin.

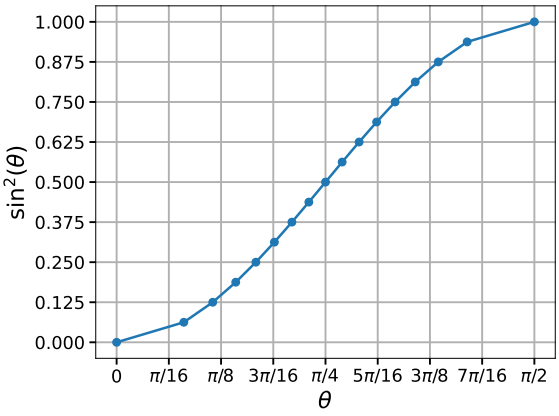
Note que $\sin^2\theta = k/N$ é linear em função de k (Fig. 34), mas não em função de θ (Fig. 35). Isso fica mais evidente ao compararmos k com $\theta = \arcsin\sqrt{k/N}$ (Fig 36); ou compararmos k com a diferença de um ângulo com seu anterior: $\Delta\theta(k) = \arcsin\sqrt{k/N} - \arcsin\sqrt{(k-1)/N}$; ilustrado na Fig. 37. Para gerar os gráficos das Figs. 34 a 37, utilizou-se $N = 16$.

Figura 34 – Gráfico da relação linear entre $\sin^2\theta$ e k.



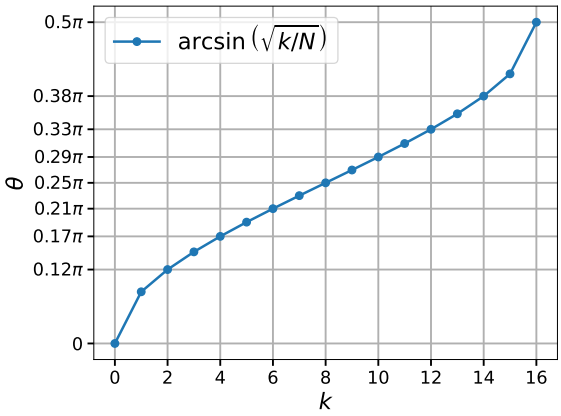
Fonte: Produzido pelo autor.

Figura 35 – Gráfico da relação não linear entre $\sin^2\theta$ e θ.



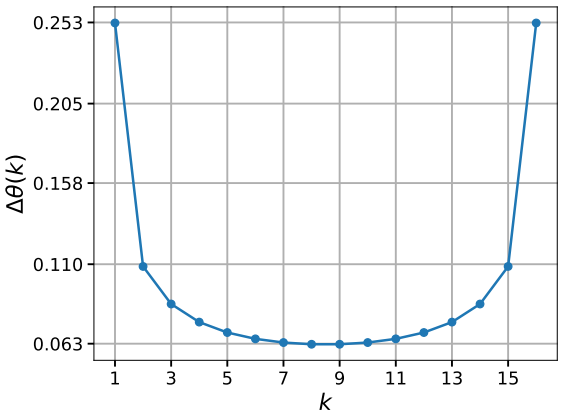
Fonte: Produzido pelo autor.

Figura 36 – Gráfico da relação não linear entre k e $\theta = \arcsin\left(\sqrt{k/N}\right)$.



Fonte: Produzido pelo autor.

Figura 37 – Gráfico das diferenças $\Delta\theta(k)$ com $N = 16$.

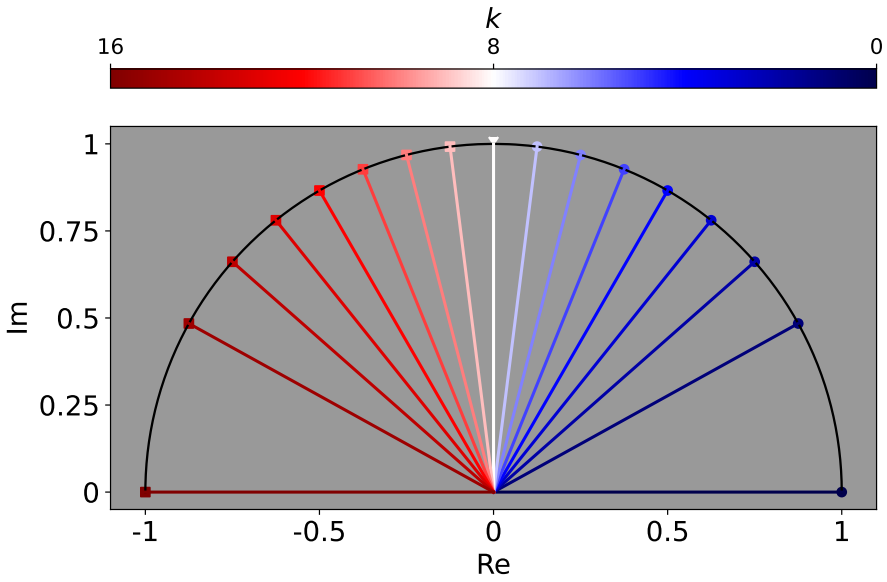


Fonte: Produzido pelo autor.

Analisa-se agora como essa relação entre k e θ influencia o comportamento do autovalor $e^{i2\theta}$. Fig. 38 ilustra como os ângulos 2θ variam no círculo unitário à medida que incrementa-se o valor de k. Na Fig. 38, usou-se $N = 16$. Os ângulos correspondentes à $k < N/2$ são representados por cores azuladas e o valor $e^{i2\theta}$ marcado com um círculo. Os ângulos correspondentes à $k > N/2$ são representados por cores avermelhadas e o valor $e^{i2\theta}$ marcado com um quadrado. O ângulo correspondente à $k = N/2$ é representado pela cor branca e o valor $e^{i2\theta}$ marcado por um triângulo. Os ângulos -2θ preencheriam a parte inferior do círculo unitário. Na Fig. 38, é possível perceber como os ângulos correspondentes a $k \approx N/2$ são mais próximos entre si do que os ângulos $k \approx 1$ e $k \approx N$ (vide Fig. 37); o que ajuda a explicar o comportamento do Corolário 1.

Um outro fator que influencia no erro do algoritmo de contagem é a Transformada

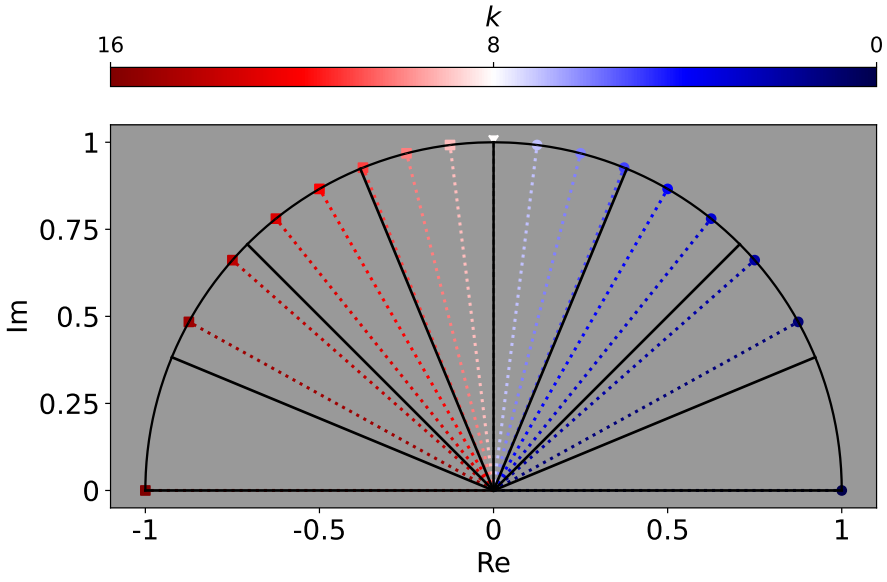
Figura 38 – Possíveis valores de 2θ e $e^{i2\theta}$ com $N = 16$.



Fonte: Produzido pelo autor.

de Fourier. Lembre-se que a Transformada de Fourier divide o círculo unitário em P partições igualmente espaçadas (os ângulos base). E como os ângulos representados na Fig. 38 não são igualmente espaçados, um valor de $P > N$ é necessário para distinguir exatamente entre todos os ângulos.

Figura 39 – Possíveis valores de 2θ e ângulos base de Fourier com $N = P = 16$.



Fonte: Produzido pelo autor.

A Fig 39 ilustra os ângulos da Fig. 38 em linhas pontilhadas. Os ângulos base de Fourier com $P = 16$ estão representados pela cor preta em linhas sólidas, sobrepondo os

ângulos 2θ.

É possível observar que mesmo um valor $P = O(N)$ engloba múltiplos valores possíveis para θ numa única partição. Ainda assim, utilizar $P = O\left(\sqrt{N}\right)$ permite distinguir valores $k \approx 1$ ou $k \approx N$ já que $\Delta\theta(k)$ é maior nesses casos (Fig. 37).

4 Algoritmo de Contagem no Grafo Bipartido Completo

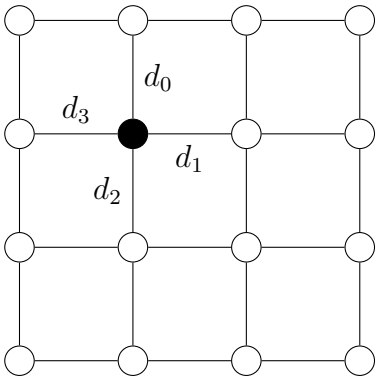
Nesse capítulo, entra-se em detalhes da aplicação do algoritmo de contagem no passeio quântico de um grafo bipartido completo. A Seção 4.1 descreve passeios quânticos em grafos regulares; Seção 4.2 entra em detalhes sobre o operador de evolução do passeio de busca no grafo bipartido completo; e a Seção 4.3 analisa os autovalores e autovetores de interesse, e seu impacto no algoritmo de contagem.

4.1 Passeios Quânticos em Grafos Regulares

Considere primeiramente o cenário clássico: um passeio aleatório. Um passeio aleatório ocorre num grafo simples $\Gamma(V, E)$. O grafo descreve possíveis posições onde um caminhante pode estar – *i.e.* vértices V de Γ –, e descreve caminhos que o caminhante pode tomar dependendo da sua posição – *i.e.* arestas E de Γ. O termo aleatório provém de que a escolha do caminho a ser tomado é feita de maneira aleatória e, normalmente, equiprovável.

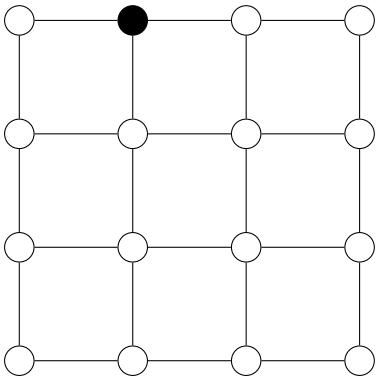
Considere o grafo apresentado na Fig. 40. Suponha que numa determinada etapa do passeio aleatório, o caminhante está no vértice de cor preta. Nessa situação, o caminhante pode ir para quatro direções possíveis: d_0, d_1, d_2 ou d_3. Então, joga-se uma *moeda* (4-dimensional, no caso) e o caminhante segue aquele caminho, *i.e.* sua próxima posição será o vértice adjacente ao atual. Por exemplo, se, na situação da Fig. 40, o resultado após jogar a moeda for d_0, o caminhante move-se "para cima" – sua próxima posição está ilustrada pelo vértice preto na Fig. 41.

Figura 40 – Etapa de um passeio aleatório.



Fonte: produzido pelo autor.

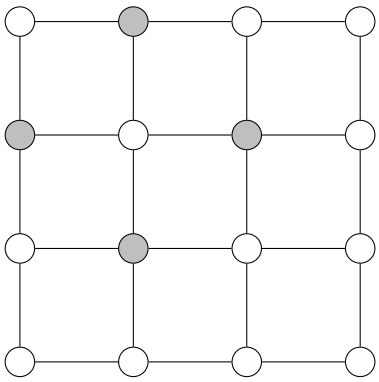
Figura 41 – Possível etapa seguinte.



Fonte: produzido pelo autor.

Como esperado de um algoritmo clássico, em cada etapa, o caminhante ocupa somente uma posição. Em contrapartida, num passeio quântico, deseja-se tirar proveito das propriedades da Mecânica Quântica; fazendo com que o caminhante esteja numa sobreposição de posições. Esse cenário é ilustrado na Fig. 42. Os vértices em cinza indicam uma possível sobreposição das posições do caminhante. Com essa intuição de como o passeio quântico funciona, formaliza-se o passeio quântico em grafos regulares.

Figura 42 – Sobreposição de posições.



Fonte: produzido pelo autor

Seja $\Gamma(V, E)$ um grafo d-regular com número par de vértices e com índice cromático d e $|V| = N$; então, é possível associar cada uma das d cores com uma direção (se o grafo tivesse um número ímpar de vértices, o índice cromático seria $d + 1$ e não seria possível associar cada cor a uma direção de modo geral). Logo, descreve-se passeio quântico no espaço de Hilbert $\mathcal{H}^N \otimes \mathcal{H}^d$, onde $\mathcal{H}^N$ é denomidado "espaço das posições" e $\mathcal{H}^d$ é denominado "espaço da moeda". Associa-se, bijetivamente, os vértices de Γ com os N vetores da base computacional. O *operador de evolução do passeio* U_w descreve a progressão do passeio é dado por

$$U_w = S\,(I \otimes C)\,, \tag{4.1}$$

onde S é o operador de *flip-flop shift* Nd-dimensional e C o operador da moeda d-dimensional. O operador S é responsável por fazer o caminhante andar, mudando sua posição de acordo com o caminho apontado pela moeda. Note que cada aplicação de U simula o comportamento descrito anteriormente: primeiro joga-se a moeda (C) para escolher a direção e posteriormente o caminhante se move naquela direção (S). Para definir o operador S formalmente, considere $v, u \in V$ e $e_c = vu \in E$ uma aresta cujo rótulo da coloração é $0 \leq c < d$, *i.e.* $\mathrm{c}\,(vu) = c$; a ação de e_c em v resulta num vértice adjacente a v e incidente a e_c, *i.e.* $e_c(v) = u$ se e somente se $e_c = vu$. Sendo assim, o operador S é dado por

$$S\,|v, c\rangle = |e_c(v), c\rangle = |u, c\rangle\,, \tag{4.2}$$

onde $|v,c\rangle = |v\rangle \otimes |c\rangle$ com $|v\rangle \in \mathcal{H}^N$ e $|c\rangle \in \mathcal{H}^d$. Esse operador é unitário já que $S = S^\dagger$,

$$S^2 |v,c\rangle = S |u,c\rangle = |e_c(u),c\rangle = |v,c\rangle . \tag{4.3}$$

4.1.1 Passeio com Moeda de Grover

Para esse passeio, será utilizado a moeda de Grover,

$$C = \frac{2}{d} \sum_{c,c'=0}^{d-1} |c\rangle \langle c'| - I. \tag{4.4}$$

Nesse caso, a ação do operador de evolução é

$$\begin{aligned} U_w |v,c\rangle &= S \left(|v\rangle \otimes \left(\frac{2}{d} \sum_{a,b=0}^{d-1} |a\rangle \langle b| - I \right) |c\rangle \right) && (4.5)\\ &= S \left(|v\rangle \otimes \left(\frac{2}{d} \sum_{a,b=0}^{d-1} |a\rangle \delta_{b,c} - |c\rangle \right) \right) && (4.6)\\ &= \left(\frac{2}{d} - 1 \right) S |v,c\rangle + \frac{2}{d} S \sum_{a \neq c} |v,a\rangle && (4.7)\\ &= \left(\frac{2}{d} - 1 \right) |e_c(v),c\rangle + \frac{2}{d} \sum_{a \neq c} |e_a(v),a\rangle && (4.8)\\ &= \left(\frac{2}{d} - 1 \right) |u, \mathrm{c}\,(vu)\rangle + \frac{2}{d} \sum_{u' \neq u} |u', \mathrm{c}\,(vu')\rangle && (4.9) \end{aligned}$$

Essa Equação será útil ao analisar o passeio quântico de busca.

4.2 Passeio de Busca no Grafo Bipartido Completo

Considere um grafo bipartido completo $\Gamma\,(V,E)$ de tal modo que $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$, $|V| = N$, $|V_1| = N_1$ e $|V_2| = N_2$. Sejam K_1 e K_2 os conjuntos de vértices marcados tais que $K_1 \subseteq V_1$, $K_2 \subseteq V_2$, $K = K_1 \cup K_2$, $|K_1| = k_1$, $|K_2| = k_2$, e $|K| = k$.

Este trabalho, entretanto, restringe-se ao subcaso em que $k_1 = k_2$ e $N_1 = N_2$. Esse grafo é N_1-regular e possui um número par de vértices. Ou seja, a quantidade de vértices em cada partição é a mesma. A Fig. 43 ilustra um grafo com essas restrições onde $N_1 = 5$ e $k_1 = 2$; os vértices marcados têm cor preta.

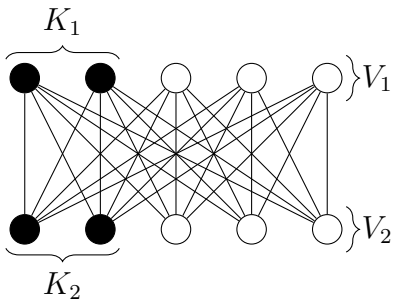
O operador de evolução de busca nesses grafos é dado por

$$U = U_w O_f, \tag{4.10}$$

onde U_w é dado pela Eq. 4.1; e O_f é o oráculo que inverte a amplitude dos elementos procurados,

$$O = \left(I - 2 \sum_{j \in K} |j\rangle \langle j| \right) \otimes I. \tag{4.11}$$

Figura 43 – Exemplo de grafo bipartido completo.



Fonte: produzido pelo autor.

Pode-se analisar a evolução do passeio num espaço reduzido. Note que algumas arestas ilustradas na Fig. 43 desempenham um papel em comum durante o passeio – *e.g.* arestas que vão de vértices não marcados em um conjunto para não marcados no outro conjunto. Antes de analisar a ação de U, considera-se apenas a ação de U_w – já que O_f simplesmente inverte o sinal em alguns casos.

Denote por $K_j^C = V_j \setminus K_j$ para $j \in \{1, 2\}$ e considere o estado

$$\left|K_1^C, K_2^C\right\rangle = \frac{1}{\sqrt{|K_1^C|}} \sum_{v \in K_1^C} |v\rangle \otimes \frac{1}{\sqrt{|K_2^C|}} \sum_{u \in K_2^C} |\mathrm{c}\,(vu)\rangle \tag{4.12}$$

a sobreposição uniforme dos vértices no conjunto K_1^C cuja moeda aponta para vértices no conjunto K_2^C. Esse estado é unitário já que

$$\begin{aligned}
\left\langle K_1^C, K_2^C \,\middle|\, K_1^C, K_2^C \right\rangle &= \frac{1}{|K_1^C|\,|K_2^C|} \sum_{v,v' \in K_1^C} \langle v \,|\, v' \rangle \sum_{u,u' \in K_2^C} \langle \mathrm{c}\,(vu) \,|\, \mathrm{c}\,(v'u') \rangle && (4.13)\\
&= \frac{1}{|K_1^C|\,|K_2^C|} \sum_{v \in K_1^C} \sum_{u,u' \in K_2^C} \langle \mathrm{c}\,(vu) \,|\, \mathrm{c}\,(vu') \rangle && (4.14)\\
&= \frac{1}{|K_1^C|\,|K_2^C|} \cdot \left|K_1^C\right| \cdot \left|K_2^C\right| && (4.15)\\
&= 1. && (4.16)
\end{aligned}$$

Aplicando U_w nesse estado e usando a Eq. 4.9,

$$\begin{aligned}
U_w \left|K_1^C, K_2^C\right\rangle &= \frac{1}{\sqrt{|K_1^C|\,|K_2^C|}} \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} U_w \,|v, \mathrm{c}\,(vu)\rangle && (4.17)\\
&= \frac{1}{\sqrt{|K_1^C|\,|K_2^C|}} \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} \left(\left(\frac{2}{d} - 1 \right) |u, \mathrm{c}\,(v,u)\rangle + \frac{2}{d} \sum_{u' \neq u} |u', \mathrm{c}\,(vu')\rangle \right) && (4.18)\\
&= \frac{1}{\sqrt{|K_1^C|\,|K_2^C|}} \left(|\varphi_1\rangle + |\varphi_2\rangle \right), && (4.19)
\end{aligned}$$

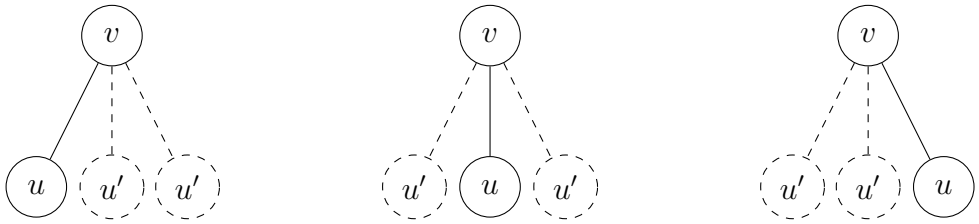
note que $u \in K_2^C$ e que $u' \in V_2$; logo, separou-se o somatório em dois casos: $|\varphi_1\rangle$ quando $u, u' \in K_2^C$, e $|\varphi_2\rangle$ quando $u' \in K_2$.

No primeiro caso, tem-se

$$|\varphi_1\rangle = \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} \left(\left(\frac{2}{d} - 1 \right) |u, \mathrm{c}\,(vu)\rangle + \frac{2}{d} \sum_{\substack{u' \neq u \\ u' \in K_2^C}} |u', \mathrm{c}\,(vu')\rangle \right). \tag{4.20}$$

Considere o grafo de exemplo apresentado na Fig. 43. Ao fixar $v \in K_1^C$, temos três possibilidades de u que contribuem no somatório mais externo; rotuladas e representadas por vértices com contornos sólidos na Fig. 44. Os vértices com cortornos tracejados indicam os valores de u' que contribuem no somatório mais interno dados v e u fixos. Observe que cada aresta vu é contabilizada outras $|K_2^C| - 1$ vezes pelo somatório mais interno.

Figura 44 – Alguns termos do somatório quando $u, u' \in K_2^C$.



Fonte: produzido pelo autor.

Logo,

$$|\varphi_1\rangle = \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} \left(\left(\frac{2}{d} - 1 \right) |u, \mathrm{c}\,(vu)\rangle + \frac{2}{d} \left(|K_2^C| - 1 \right) |u, \mathrm{c}\,(vu)\rangle \right) \tag{4.21}$$

$$= \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} \left(\frac{2}{d} |K_2^C| - 1 \right) |u, \mathrm{c}\,(vu)\rangle\,. \tag{4.22}$$

No segundo caso, é possível seguir um raciocínio análogo, obtendo

$$|\varphi_2\rangle = \frac{2}{d} \sum_{\substack{v \in K_1^C \\ u \in K_2^C}} \left(\sum_{u' \in K_2} |u', \mathrm{c}\,(v, u')\rangle \right) \tag{4.23}$$

$$= \frac{2}{d} \left| K_2^C \right| \sum_{v \in K_1^C} \sum_{u' \in K_2} |u', \mathrm{c}\,(v, u')\rangle\,. \tag{4.24}$$

Note que há uma similaridade entre os somatórios das Eqs. 4.22 e 4.24 com o somatório da Eq. 4.12. De fato, ao definir a sobreposição uniforme de vértices no K_2^C cuja moeda aponta para vértices em K_1^C

$$\left| K_2^C, K_1^C \right\rangle = \frac{1}{\sqrt{|K_2^C|}} \sum_{v \in K_2^C} |v\rangle \otimes \frac{1}{\sqrt{|K_1^C|}} \sum_{u \in K_1^C} |\mathrm{c}\,(vu)\rangle \tag{4.25}$$

e a sobreposição uniformee de vértices em K_2 cuja moeda aponta para vértices em K_1^C

$$\left|K_2, K_1^C\right\rangle = \frac{1}{\sqrt{|K_2|}} \sum_{v \in K_2} |v\rangle \otimes \frac{1}{\sqrt{|K_1^C|}} \sum_{u \in K_1^C} |\mathrm{c}\,(vu)\rangle\,, \tag{4.26}$$

obtém-se

$$U_w \left|K_1^C, K_2^C\right\rangle = \frac{1}{\sqrt{|K_1^C|\,|K_2^C|}} \left(\sum_{\substack{v \in K_2^C \\ u \in K_1^C}} \left(\frac{2}{d}|K_2^C| - 1\right) |v, \mathrm{c}\,(vu)\rangle + \frac{2}{d}\left|K_2^C\right| \sum_{\substack{v \in K_2 \\ u \in K_1^C}} |v, \mathrm{c}\,(vu)\rangle \right) \tag{4.27}$$

$$= \left(\frac{2}{d}|K_2^C| - 1\right) \left|K_2^C, K_1^C\right\rangle + \frac{2}{d}\sqrt{|K_2|\,|K_2^C|}\left|K_2, K_1^C\right\rangle. \tag{4.28}$$

Esse comportamento se repete para outros estados similares a $\left|K_1^C, K_2^C\right\rangle$. Considere a definição a seguir.

Definição 4.1. Denote por

$$|S_i, S_j\rangle = \frac{1}{\sqrt{|S_i|}} \sum_{v \in S_i} |v\rangle \otimes \frac{1}{\sqrt{|S_j|}} \sum_{u \in S_j} |\mathrm{c}\,(vu)\rangle \tag{4.29}$$

a sobreposição uniforme dos vértices em S_i cuja moeda aponta para vértices em S_j, onde $S_i \in \{\, K_i, K_i^C \,\}$ com $i, j \in \{\, 1, 2 \,\}$ de tal forma que $i \neq j$. —

Note que esses vetores formam uma base ortonormal B já que

$$\langle S_i, S_j \,|\, S_{i'}, S_{j'}\rangle = \frac{1}{\sqrt{|S_i|\,|S_{i'}|}} \sum_{\substack{v \in S_i \\ v' \in S_{i'}}} \langle v \,|\, v'\rangle \cdot \frac{1}{\sqrt{|S_j|\,|S_{j'}|}} \sum_{\substack{u \in S_j \\ u' \in S_{j'}}} \langle \mathrm{c}\,(vu) \,|\, \mathrm{c}\,(v'u')\rangle \tag{4.30}$$

$$= \frac{1}{\sqrt{|S_i|\,|S_{i'}|}} \delta_{i,i'}\,|S_i| \cdot \frac{1}{\sqrt{|S_j|\,|S_{j'}|}} \sum_{\substack{u \in S_j \\ u' \in S_{j'}}} \langle \mathrm{c}\,(vu) \,|\, \mathrm{c}\,(vu')\rangle \tag{4.31}$$

$$= \delta_{i,i'} \cdot \frac{1}{\sqrt{|S_j|\,|S_{j'}|}} \delta_{j,j'}\,|S_j| \tag{4.32}$$

$$= \delta_{i,i'}\delta_{j,j'}. \tag{4.33}$$

Além disso,

$$U_w\,|S_i, S_j\rangle = \left(\frac{2}{d}|S_j| - 1\right)|S_j, S_i\rangle + \frac{2}{d}\sqrt{\left|S_j^C\right|\,|S_j|}\left|S_j^C, S_i\right\rangle, \tag{4.34}$$

desde que $\left(K_j^C\right)^C = K_j$. Ou seja, se um estado $|\psi\rangle \in \mathrm{span}(B)$, então a ação de U_w fica restrita ao subespaço definido por B.

A partir da Eq. 4.34, a ação de U segue trivialmente. Se $S_i \in \{\, K_1, K_2 \,\}$, então $U\,|S_i, S_j\rangle = -U_w\,|S_i, S_j\rangle$ e, caso contrário, $U\,|S_i, S_j\rangle = U_w\,|S_i, S_j\rangle$. Com isso em mãos,

ordene B por $|K_1, K_2\rangle$, $\left|K_1, K_2^C\right\rangle$, $\left|K_1^C, K_2\right\rangle$, $\left|K_1^C, K_2^C\right\rangle$, $|K_2, K_1\rangle$, $\left|K_2, K_1^C\right\rangle$, $\left|K_2^C, K_1\right\rangle$ e $\left|K_2^C, K_1^C\right\rangle$. Dadas as restrições do problema, sabe-se também que a dimensão da moeda é $d = N_1$. Então, constrói-se o operador de evolução no subespaço span(B) como a matriz por blocos

$$U' = \begin{bmatrix} 0 & \mathcal{U}'(\theta_1) \\ \mathcal{U}'(\theta_2) & 0 \end{bmatrix}, \tag{4.35}$$

onde

$$\mathcal{U}'(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 & 0 \\ 0 & 0 & -\cos\theta & \sin\theta \\ -\sin\theta & -\cos\theta & 0 & 0 \\ 0 & 0 & \sin\theta & \cos\theta \end{bmatrix}, \tag{4.36}$$

e θ_j são ângulos tais que $\cos\theta_j = 1 - 2k_j/N_j$ e $\sin\theta_j = \frac{2}{N_j}\sqrt{k_j(N_j - k_j)}$ para $j \in \{1, 2\}$.

A motivação para utilizar N_2 e k_2 (ao invés de somente N_1 e k_1) é que a mesma matriz é obtida para qualquer grafo bipartido completo, mesmo sendo necessário alterar o espaço da moeda (RHODES; WONG, 2019). Portanto, decidiu-se manter a utilização de N_2 e k_2 para o cálculo de autovalores e autovetores.

4.2.1 Autovalores e Autovetores do Operador no Subespaço

A obtenção dos autovetores e autovalores é essencial para o algoritmo de contagem. Como a análise ficará restrita ao subespaço span(B), analisa-se os autovetores de U'. Os autovalores λ são as soluções para a equação

$$\det(U' - \lambda I) = 0. \tag{4.37}$$

Como

$$U' - \lambda I = \begin{bmatrix} \lambda I & \mathcal{U}'(\theta_1) \\ \mathcal{U}'(\theta_2) & \lambda I \end{bmatrix}, \tag{4.38}$$

e as duas matrizes por bloco debaixo comutam – *i.e.* $\lambda I\, \mathcal{U}'(\theta_2) = \mathcal{U}'(\theta_2)\, \lambda I$ –, o determinante é dado por (SILVESTER, 2000)

$$\det(U' - \lambda I) = \det\left(\lambda^2 I - \mathcal{U}'(\theta_1)\mathcal{U}'(\theta_2)\right) = 0. \tag{4.39}$$

Note que

$$\mathcal{U}'(\theta_1)\mathcal{U}'(\theta_2) = \begin{bmatrix} \cos\theta_1\cos\theta_2 & -\cos\theta_1\sin\theta_2 & \sin\theta_1\cos\theta_2 & -\sin\theta_1\sin\theta_2 \\ \cos\theta_1\sin\theta_2 & \cos\theta_1\cos\theta_2 & \sin\theta_1\sin\theta_2 & \sin\theta_1\cos\theta_2 \\ -\sin\theta_1\cos\theta_2 & \sin\theta_1\sin\theta_2 & \cos\theta_1\cos\theta_2 & -\cos\theta_1\sin\theta_2 \\ -\sin\theta_1\sin\theta_2 & \sin\theta_1\cos\theta_2 & \cos\theta_1\sin\theta_2 & \cos\theta_1\cos\theta_2 \end{bmatrix} \tag{4.40}$$

$$= \begin{bmatrix} \cos\theta_1 R(\theta_2) & \sin\theta_1 R(\theta_2) \\ -\sin\theta_1 R(\theta_2) & \cos\theta_1 R(\theta_2) \end{bmatrix} \tag{4.41}$$

$$= R(\theta_1)^T \otimes R(\theta_2), \tag{4.42}$$

onde

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{4.43}$$

Como visto anteriormente, $R(\theta)$ é uma matriz de rotação conhecida que possui autovalores $e^{\pm i\theta}$ associados aos autovetores $|\mp i\rangle = (|0\rangle \mp i\,|1\rangle)/\sqrt{2}$, respectivamente. Analogamente, $R(\theta)^T$ tem autovalores $e^{\pm i\theta}$ associados aos autovetores $|\pm i\rangle$. Juntando esses fatos com a Eq. 4.42 resulta que $\mathcal{U}'(\theta_1)\mathcal{U}'(\theta_2)$ tem autovalores $e^{i(\theta_1\pm\theta_2)}$ e seus complexos conjugados, e autovetores $|\pm i\rangle \otimes |\pm i\rangle$. Entretanto, esse resultado é a solução para a equação

$$\det\left(\lambda I - \mathcal{U}'(\theta_1)\mathcal{U}'(\theta_2)\right) = 0, \tag{4.44}$$

não para a Eq. 4.39. As soluções para a Eq. 4.39 são as raízes quadradas (positivas e negativas) dos valores obtidos – *i.e.* $e^{i(\theta_1\pm\theta_2)/2}$, $-e^{i(\theta_1\pm\theta_2)/2}$ e seus complexos conjugados.

Para calcular os autovetores, suponha que $|\lambda\rangle = |\lambda_1\rangle \oplus |\lambda_2\rangle$ é um λ-autovetor de U', onde $\oplus$ denota a soma direta. Então,

$$U'|\lambda\rangle = \begin{bmatrix} 0 & \mathcal{U}'(\theta_1) \\ \mathcal{U}'(\theta_2) & 0 \end{bmatrix} |\lambda_1\rangle \oplus |\lambda_2\rangle \tag{4.45}$$

$$= \mathcal{U}'(\theta_1)\,|\lambda_2\rangle \oplus \mathcal{U}'(\theta_2)\,|\lambda_1\rangle \tag{4.46}$$

implica que os autovetores obedecem o sistema de equações

$$\begin{cases} \mathcal{U}'(\theta_1)\,|\lambda_2\rangle &= \lambda\,|\lambda_1\rangle \\ \mathcal{U}'(\theta_2)\,|\lambda_1\rangle &= \lambda\,|\lambda_2\rangle \end{cases}. \tag{4.47}$$

Da primeira equação, tem-se que $|\lambda_1\rangle = \mathcal{U}'(\theta_1)\frac{1}{\lambda}\,|\lambda_2\rangle$. Substituindo isso na segunda equação obtém-se

$$\mathcal{U}'(\theta_2)\mathcal{U}'(\theta_1)\frac{1}{\lambda}\,|\lambda_2\rangle = \lambda\,|\lambda_2\rangle \tag{4.48}$$

$$R(\theta_2)^T \otimes R(\theta_1)\,|\lambda_2\rangle = \lambda^2\,|\lambda_2\rangle\,, \tag{4.49}$$

i.e. $|\lambda_2\rangle$ é um λ^2-autovetor de $R(\theta_2)^T \otimes R(\theta_1)$. Cálculos anteriores mostram que esses autovetores são $|\lambda_2\rangle = |s_2\mathrm{i}\rangle \otimes |s_1\mathrm{i}\rangle$ associados com os autovalores $\pm e^{\mathrm{i}(s_2\theta_2 - s_1\theta_1)}$ para $s_1, s_2 \in \{+1, -1\}$. Com $|\lambda_2\rangle$ e seu autovalor em mãos, é possível calcular

$$|\lambda_1\rangle = \frac{1}{\lambda}\mathcal{U}'(\theta_1)\,|\lambda_2\rangle \tag{4.50}$$

$$= \frac{1}{\lambda}\begin{bmatrix} \cos\theta_1 & -\sin\theta_1 & 0 & 0 \\ 0 & 0 & -\cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & -\cos\theta_1 & 0 & 0 \\ 0 & 0 & \sin\theta_1 & \cos\theta_1 \end{bmatrix} \frac{1}{2}\begin{bmatrix} 1 \\ s_1\mathrm{i} \\ s_2\mathrm{i} \\ -s_1 s_2 \end{bmatrix} \tag{4.51}$$

$$= \frac{1}{\lambda}\cdot\frac{1}{2}\begin{bmatrix} \cos\theta_1 - s_1\mathrm{i}\sin\theta_1 \\ -s_2\mathrm{i}\,(\cos\theta_1 - s_1\mathrm{i}\sin\theta_1) \\ -s_1\mathrm{i}\,(\cos\theta_1 - s_1\mathrm{i}\sin\theta_1) \\ -s_1 s_2\,(\cos\theta_1 - s_1\mathrm{i}\sin\theta_1) \end{bmatrix} \tag{4.52}$$

$$= \frac{e^{-s_1\mathrm{i}\ \theta_1}}{\lambda}\,|-s_1\mathrm{i}\rangle \otimes |-s_2\mathrm{i}\rangle\,. \tag{4.53}$$

Como $|\lambda_2\rangle$ é um λ^2-autovetor de $R(\theta_2)^T \otimes R(\theta_1)$, cada $|\lambda_2\rangle$ gera dois resultados possíveis para $|\lambda_1\rangle$. Por exemplo, tome $|\lambda_2\rangle = |+\mathrm{i}\rangle \otimes |-\mathrm{i}\rangle$, então $\lambda = \pm e^{\mathrm{i}(\theta_1+\theta_2)/2}$ e $|\lambda_1\rangle = \pm e^{\mathrm{i}(\theta_1-\theta_2)/2}\,|+\mathrm{i}\rangle \otimes |-\mathrm{i}\rangle$; consequentemente,

$$|\Sigma_\pm\rangle = \frac{1}{\sqrt{8}}\begin{bmatrix} \pm e^{\mathrm{i}\Delta} \\ \mp\mathrm{i}e^{\mathrm{i}\Delta} \\ \pm\mathrm{i}e^{\mathrm{i}\Delta} \\ \pm e^{\mathrm{i}\Delta} \\ 1 \\ -\mathrm{i} \\ \mathrm{i} \\ 1 \end{bmatrix} \tag{4.54}$$

é um $\pm e^{\mathrm{i}\Sigma}$-autovetor de U', onde $\Delta = (\theta_1 - \theta_2)/2$ e $\Sigma = (\theta_1 + \theta_2)/2$. Analogamente,

$$|\Delta_\pm\rangle = \frac{1}{\sqrt{8}}\begin{bmatrix} \pm e^{\mathrm{i}\Sigma} \\ \pm\mathrm{i}e^{\mathrm{i}\Sigma} \\ \pm\mathrm{i}e^{\mathrm{i}\Sigma} \\ \mp e^{\mathrm{i}\Sigma} \\ 1 \\ -\mathrm{i} \\ -\mathrm{i} \\ -1 \end{bmatrix}, \tag{4.55}$$

é um $\pm e^{\mathrm{i}\Delta}$-autovetor de U'.

Seguindo esse mesmo raciocínio, obtém-se todos os autovalores e autovetores de U': $|\Sigma_\pm\rangle$, $|\Delta_\pm\rangle$ e seus complexos conjugados – denotados respectivamente por $\left|\Sigma_\pm^*\right\rangle$ e

$\left|\Delta_{\pm}^{*}\right\rangle$. Esses autovetores estão respectivamente associados aos autovalores $\pm e^{\mathrm{i}\Sigma}$, $\pm e^{\mathrm{i}\Delta}$ e seus complexos conjugados.

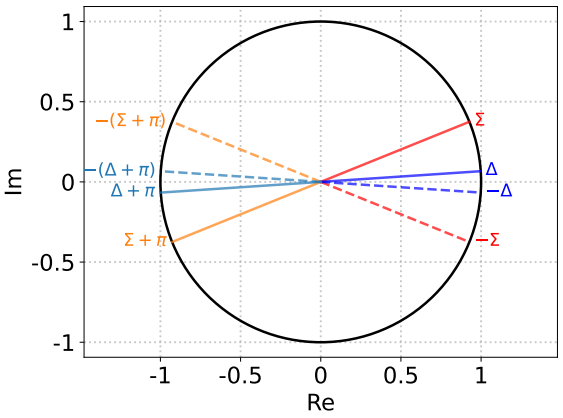
4.2.1.1 Comportamento dos Autovalores

Esta Seção dedica-se a analisar o comportamento dos autovalores. Uma intuição desse comportamento é útil para facilitar o entendimento dos resultados provenientes de usar U (Eq. 4.10) como entrada no algoritmo de estimativa de fase ou contagem.

Denomine os autovalores $\pm e^{\mathrm{i}\Sigma}$ e $\pm e^{-\mathrm{i}\Sigma}$ por Σ-autovalores. Analogamente, denote $\pm e^{\mathrm{i}\Delta}$ e $\pm e^{-\mathrm{i}\Delta}$ por Δ-autovalores. Note que $-e^{\pm\mathrm{i}\Sigma} = e^{\pm\mathrm{i}(\Sigma+\pi)}$ (análogo para os Δ-autovalores). Primeiro, nota-se que os valores de Σ e Δ dependem de θ_1 e θ_2, sendo que Σ se relaciona com a soma desses ângulos, enquanto Δ se relaciona com a diferença. Pelo modo como θ_j para $j \in \{1, 2\}$ foram definidos, tem-se que $-1 \leq \cos\theta_j \leq 1$ e $0 \leq \sin\theta_j \leq 1$; logo, $0 \leq \theta_j \leq \pi$. Consequentemente, $0 \leq \Sigma \leq \pi$ e $-\pi/2 \leq \Delta \leq \pi/2$.

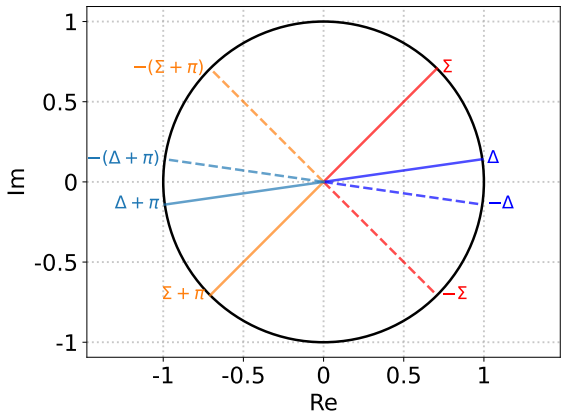
Figs. 45 e 46 ilustram os Σ e Δ-autovalores no círculo unitário com $N_1 = N_2 = 40$. Os Σ-autovalores são representados por cores vermelho-alaranjadas enquanto que os Δ-autovalores são representados por cores azuladas. Ângulos positivos são representados por linhas contínuas (*e.g.* Σ e $\Sigma + \pi$), enquanto que ângulos negativos são representados por linhas tracejadas (*e.g.* $-\Sigma$ e $-(\Sigma + \pi)$). Na Fig. 45, utilizou-se $k_1 = 2$ e $k_2 = 1$, enquanto que na Fig. 46, $k_1 = 8$ e $k_2 = 4$. Conforme esperado, $\Sigma > |\Delta|$. Também é possível notar que o ângulo Σ aumenta à medida que k_1 ou k_2 aumentam e que se k_1 for próximo a k_2, Δ é próximo de 0.

Figura 45 – Autovalores para $N_1 = N_2 = 40$, $k_1 = 2$ e $k_2 = 1$.



Fonte: Produzido pelo autor.

Figura 46 – Autovalores para $N_1 = N_2 = 40$, $k_1 = 8$ e $k_2 = 4$.



Fonte: Produzido pelo autor.

4.3 Contagem no Grafo Bipartido Completo

Relembre que o algoritmo de contagem original utiliza o operador de evolução de Grover como uma das entradas para o algoritmo de estimativa de fase; além de um autovetor dessa matriz (na realidade uma sobreposição de autovetores).

Analogamente ao Algoritmo de Grover, os autovalores de U (Eq. 4.10) no espaço reduzido possuem informações sobre a quantidade de elementos marcados. Essa informação pode ser obtida facilmente a partir dos ângulos θ_1 e θ_2. Sendo assim, deseja-se utilizar o algoritmo de estimativa de fase para obter estimativas de Σ e de Δ para então extrair a informação desejada. Para isso, entretanto, seria necessário preparar os autovetores $|\Sigma_+\rangle$ e $|\Delta_+\rangle$, que exigem conhecimento prévio dos valores de Σ e Δ. A solução é utilizar uma sobreposição de autovetores como entrada do segundo registrador.

Relembre que N_1 é a dimensão do espaço da moeda. Então, a sobreposição uniforme é dada por

$$|D\rangle = \frac{1}{\sqrt{N \cdot N_1}} \sum_{j=0}^{N-1} \sum_{c=0}^{N_1-1} |j, c\rangle \tag{4.56}$$

$$= \frac{1}{\sqrt{2N_1 N_2}} \sum_{\substack{S_i, S_j \\ i \neq j}} \sqrt{|S_i|\,|S_j|}\ \ |S_i, S_j\rangle\,. \tag{4.57}$$

Apesar do escopo desse trabalho estar reduzido a $N_1 = N_2$ e $k_1 = k_2$, trabalha-se com a expressão 4.57 para facilitar uma futura extensão dos resultados para o caso geral. Já que $|D\rangle$ pode ser escrito como uma combinação linear de B, tanto $|D\rangle$ quanto $U|D\rangle$ ficam restritos nesse subespaço. O algoritmo de contagem no grafo bipartido está descrito em 4. Note que é bastante similar ao algoritmo de contagem original, especialmente o pós-processamento clássico.

Algoritmo 4: Algoritmo de Contagem no Grafo Bipartido.

Entrada: O_f: Oráculo da função f; p: número de qubits do primeiro registrador do algoritmo de estimativa de fase; N: tamanho do segundo registrador respeitando o domínio de f; t: quantidade máxima de iterações.

1: Construir operador $U = U_w O_f$
2: Preparar o estado $|D\rangle$; $t' \leftarrow 0$
3: **enquanto** $t' < t$ **e** $\theta'_1 \in \{0, \pi\}$ **faça**
4: $\quad \vartheta \leftarrow \text{est\_fase}(p, U, |D\rangle)$
5: $\quad \theta'_1 \leftarrow 2\pi\vartheta$; $t' \leftarrow t' + 1$
6: **fim enquanto**
7: **se** $\theta'_1 \in \{0, \pi\}$ **então**
8: $\quad$ Se um elemento aleatório estiver marcado então $k' \leftarrow N$; senão $k' \leftarrow 0$
9: $\quad$ **retorna** k'
10: **fim se**
11: **retorna** $k' = \sin^2(\theta'_1/2) \cdot N$

Para prosseguir com a análise, é necessário representar $|D\rangle$ como uma sobreposição dos autovetores do subespaço de U. Essa análise é essencial pois influencia na probabilidade de obter uma determinada estimativa, conforme visto na Seção 3.3. Ou seja, deseja-se obter as amplitudes de

$$I\,|D\rangle = \sum_{\lambda} |\lambda\rangle\,\langle\lambda|\,D = \sum_{\lambda} \langle\lambda\,|\,D\rangle\,|\lambda\rangle\,, \tag{4.58}$$

onde λ e $|\lambda\rangle$ representam respectivamente os autovalores e autovetores apresentados na Seção 4.2.1.

Calculando-se a projeção de $|D\rangle$ em $|\Sigma_{\pm}\rangle$ obtém-se

$$\langle\Sigma_{\pm}\,|\,D\rangle = (\langle D\,|\,\Sigma_{\pm}\rangle)^{*} \tag{4.59}$$

$$= \frac{1}{4\sqrt{N_1 N_2}}\left(\pm e^{\mathrm{i}\Delta}\chi + \chi^{*}\right)^{*}, \tag{4.60}$$

onde

$$\chi = \sqrt{k_1 k_2} - \mathrm{i}\sqrt{k_1(N_2-k_2)} + \mathrm{i}\sqrt{(N_1-k_1)k_2} + \sqrt{(N_1-k_1)(N_2-k_2)} \tag{4.61}$$

$$= \left(\sqrt{k_1} + \mathrm{i}\sqrt{N_1-k_1}\right)\left(\sqrt{k_2} - \mathrm{i}\sqrt{N_2-k_2}\right). \tag{4.62}$$

Conforme visto na Seção 3.3, calcular $|\langle\Sigma_{\pm}\,|\,D\rangle|^2$ é necessário para obter a probabilidade de estimar os autovalores $\pm e^{\mathrm{i}\Sigma}$,

$$|\langle\Sigma_{\pm}\,|\,D\rangle|^2 = \frac{1}{16N_1N_2}\left(\pm e^{\mathrm{i}\Delta}\chi + \chi^{*}\right)\left(\pm e^{\mathrm{i}\Delta}\chi + \chi^{*}\right)^{*} \tag{4.63}$$

$$= \frac{1}{16N_1N_2}\left(2\chi\chi^{*} \pm 2\Re\left(e^{\mathrm{i}\Delta}\chi^2\right)\right) \tag{4.64}$$

$$= \frac{1}{8}\left(1 \pm \Re\left(\frac{e^{\mathrm{i}\Delta}\chi^2}{N_1N_2}\right)\right), \tag{4.65}$$

e usando

$$\frac{e^{\mathrm{i}\Delta}\chi^2}{N_1N_2} = e^{\mathrm{i}\Delta}\left(\frac{2k_1 - N_1 + 2\mathrm{i}\sqrt{N_1-k_1}}{N_1}\right)\left(\frac{2k_2 - N_2 - 2\mathrm{i}\sqrt{N_2-k_2}}{N_2}\right) \tag{4.66}$$

$$= e^{\mathrm{i}\Delta}\left(-\cos\theta_1 + \mathrm{i}\sin\theta_1\right)\left(-\cos\theta_2 - \mathrm{i}\sin\theta_2\right) \tag{4.67}$$

$$= e^{\mathrm{i}\Delta}e^{-\mathrm{i}\theta_1}e^{\mathrm{i}\theta_2} \tag{4.68}$$

$$= e^{-\mathrm{i}\Delta} \tag{4.69}$$

resulta em

$$|\langle\Sigma_{\pm}\,|\,D\rangle|^2 = \frac{1}{8}\left(1 \pm \cos\Delta\right). \tag{4.70}$$

Fazendo cálculos similares para os autovetores restantes e usando as identidades trigonométricas $1+\cos\theta = 2\cos^2(\theta/2)$, $1-\cos\theta = 2\sin^2(\theta/2)$; obtém-se a probabilidade de

de estimar os autovalores restantes (Apêndice B). Esse resultado relaciona-se diretamente com a estimativa do ângulo de um autovalor de U' e estão resumidos na Tabela 2. Então, a probabilidade de obter uma estimativa de algum ângulo do tipo Σ é

$$2 \cdot \frac{1}{4}\left(\cos^2\frac{\Delta}{2} + \sin^2\frac{\Delta}{2}\right) = \frac{1}{2}. \tag{4.71}$$

Análogo para os ângulos do tipo Δ.

Tabela 2 – Probabilidade de estimativa de cada ângulo dos autovalores de U'.

Ângulo estimado	Probabilidade de medida
$\pm\Sigma$	$\frac{1}{4}\cos^2(\Delta/2)$
$\pm(\Sigma+\pi)$	$\frac{1}{4}\sin^2(\Delta/2)$
$\pm\Delta$	$\frac{1}{4}\cos^2(\Sigma/2)$
$\pm(\Delta+\pi)$	$\frac{1}{4}\sin^2(\Sigma/2)$

Fonte: autor.

Analisando os dados da Tabela 2, percebe-se que a probabilidade de obter uma estimativa para um dado ângulo varia de acordo com a quantidade de elementos marcados. Por exemplo, se $k_1 \neq k_2$ então $\Delta \neq 0$ e a probabilidade de estimar tanto $\pm\Sigma$ quanto $\pm(\Sigma+\pi)$ é não nula. Além disso, considerando os ângulos apresentados nas Figs. 45 e 46, observa-se que no caso geral, pode ser necessário fazer a distinção entre os ângulos do tipo Σ e do tipo Δ; e fazer a distinção dos ângulos Σ e $-(\Sigma+\pi)$, já que eles sempre estão no intervalo $[0,\pi]$. Esses empecilhos motivaram a redução do escopo do problema para $k_1 = k_2$ e $N_1 = N_2$.

Uma consequência da redução do escopo é que $\Delta = 0$ e o valor de Σ varia. Logo, os ângulos $\pm\Sigma + \pi$ nunca serão estimados, e a probabilidade de estimar cada um dos ângulos tipo Δ varia. Porém, no caso de estimar um ângulo Δ, obtém-se os valores $\theta_1' = \{0,\pi\}$ exatamente, facilitando a identificação de um ângulos tipo Σ. Essa é a razão para o laço no passo 3.

Dois cenários podem fazer o algoritmo sair do laço: estimar um ângulo $\theta_1' \notin \{0,\pi\}$ ou após t iterações. No primeiro caso, garante-se que uma estimativa de $\pm\Sigma$ foi obtida. Por conta da redução de escopo, $\Sigma = (\theta_1+\theta_2)/2 = \theta_1$ e $k = 2k_1$. Então, a estimativa da quantidade de elementos marcados pode ser obtida a partir de $\cos(\pm\theta_1)$ – logo, independentemente do sinal de θ_1. Note que

$$\cos(\theta_1) = 1 - \frac{2k_1}{N_1} \tag{4.72}$$

$$k_1 = (1-\cos(\theta_1))\frac{N_1}{2} \tag{4.73}$$

$$k_1 = \sin^2(\theta_1/2)\cdot N_1 \tag{4.74}$$

$$\implies k = \sin^2(\theta_1/2)\cdot N. \tag{4.75}$$

Isso justifica o passo 11 do algoritmo. Ainda no contexto do primeiro caso, usar o Teorema 4 resulta numa estimativa do erro:

$$\left|\sin^2\frac{\theta_1'}{2} - \sin^2\frac{\theta_1}{2}\right| \geq 2\pi\frac{\sin\frac{\theta_1}{2}\cos\frac{\theta_1}{2}}{P} + \frac{\pi^2}{P} \tag{4.76}$$

$$= 2\pi\frac{\sin\left(\theta_1\right)/2}{P} + \frac{\pi^2}{P} \tag{4.77}$$

$$= 2\pi\frac{\frac{1}{N_1}\sqrt{k_1\left(N_1-k_1\right)}}{P} + \frac{\pi^2}{P} \tag{4.78}$$

$$\implies |k'-k| \leq 2\pi\frac{2\sqrt{k_1\left(N_1-k_1\right)}}{P} + \frac{\pi^2 N}{P} \tag{4.79}$$

$$= 2\pi\frac{\sqrt{k\left(N-k\right)}}{P} + \frac{\pi^2 N}{P} \tag{4.80}$$

com probabilidade maior ou igual a $8/\pi^2$.

O segundo caso é subdividido em outros dois cenários: (1) caso $k \in \{\,0, N\,\}$; (2) caso $k \notin \{\,0, N\,\}$ e t iterações foram executadas. No primeiro cenário, o ângulo θ_1 foi estimado corretamente, mas coincide com os valores possíveis de Δ. Uma consulta adicional ao oráculo é suficiente para definir se nenhum ou todos os elementos estão marcados. No segundo cenário, não estimou-se um ângulo Σ após t iterações, ocasionando um erro. A probabilidade disso acontecer é de $(1/2)^t$.

Juntando todos esses argumentos, conclui-se que o alg. 4 realiza $t(P-1)$ consultas ao oráculo; estima os casos $k = 0$ e $k = N$ exatamente com probabilidade de sucesso 1; e caso $0 < k < N$, o algoritmo retorna uma estimativa k' de k com erro

$$|k'-k| \leq 2\pi\frac{\sqrt{k\left(N-k\right)}}{P} + \frac{\pi^2 N}{P^2} \tag{4.81}$$

e com probabilidade de sucesso maior ou igual a $\left(1-\frac{1}{2^t}\right)\frac{8}{\pi^2}$. Portanto, os mesmos comentários feitos na Seção 3.4.1 sobre a ordem do erro dependendo do valor k estendem-se para o alg. 4.

5 Conclusão

O algoritmo de contagem original é utilizado para estimar a quantidade de entradas k que satisfazem uma busca num banco de dados não ordenado. Essa estimativa é obtida ao usar o operador de busca de Grover como entrada do algoritmo de estimativa de fase. Nesse trabalho, mostrou-se que é possível utilizar a mesma estratégia para estimar a quantidade k de elementos marcados num grafo; ou seja, utilizando o operador do passeio de busca como entrada do algoritmo de estimativa de fase. É necessário que os autovalores do operador dependam de k, cuja estimativa é obtida depois de um pós-processamento clássico.

Essa técnica foi aplicada utilizando o operador de evolução de busca do grafo bipartido completo (U', Eq. 4.35) no subcaso $k_1 = k_2$ e $N_1 = N_2$; onde k_1 e k_2 são as quantidades de vértices marcados dos conjuntos disjuntos V_1 e V_2 (respectivamente), e N_1 e N_2 são as cardinalidades de V_1 e V_2 (respectivamente). Obteve-se uma complexidade de $O\left(t\sqrt{N}\right)$ chamadas ao oráculo onde t é a quantidade máxima de vezes que o algoritmo de estimativa de fase é executado e $N = N_1 + N_2$; em comparação com $O\left(\sqrt{N}\right)$ do algoritmo de contagem original (BRASSARD et al., 2002). Obteve-se também um erro da ordem de $O\left(\sqrt{k}\right)$ – mais precisamente de $O\left(\sqrt{k\left(1-\frac{k}{N}\right)}\right)$ –, a mesma ordem de erro do algoritmo de contagem original; porém com uma probabilidade de sucesso maior ou igual a $(1-2^{-t})\,\frac{8}{\pi^2}$, enquanto a probabilidade de sucesso do algoritmo original é maior ou igual a $\frac{8}{\pi^2}$.

Uma consequência desse resultado foi a obtenção dos autovetores e autovalores exatos do operador U'. Previamente tinha-se apenas uma aproximação quando $k_1 = o(N_1)$ e $k_2 = o(N_2)$ (RHODES; WONG, 2019). Os autovalores e autovetores de U' também são os mesmos do operador de busca no caso geral (*e.g.* $N_1 \neq N_2$), desde que o espaço da moeda seja alterado adequadamente.

Para trabalhos futuros, ainda é necessário analisar outras situações no grafo bipartido completo. Particularmente, o caso em que $k_1 \neq k_2$ e $N_1 = N_2$ parece bem mais simples que o restante dos casos. Outras possibilidades abrangem a análise de como o algoritmo de contagem se comporta em outros grafos; por exemplo, o hipercubo e a malha. Também é interessante analisar como (e se) o algoritmo de contagem é influenciado por configurações excepcionais, *e.g.* a diagonal na malha.

Referências

ABAL, G. et al. Spatial search on a honeycomb network. *Mathematical Structures in Computer Science*, Cambridge University Press, v. 20, n. 6, p. 999–1009, 2010. Citado na página 15.

AHARONOV, Y.; DAVIDOVICH, L.; ZAGURY, N. Quantum random walks. *Physical Review A*, APS, v. 48, n. 2, p. 1687, 1993. Citado na página 14.

AMBAINIS, A.; KEMPE, J.; RIVOSH, A. Coins make quantum walks faster. *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, p. 1099–1108, 2005. Citado na página 15.

AMBAINIS, A.; RIVOSH, A. Quantum walks with multiple or moving marked locations. In: SPRINGER. *International Conference on Current Trends in Theory and Practice of Computer Science*. 2008. p. 485–496. Citado na página 15.

AXLER, S. *Linear algebra done right*. Springer, 2014. Citado 2 vezes nas páginas 17 e 26.

BERNSTEIN, E.; VAZIRANI, U. Quantum complexity theory. *SIAM Journal on computing*, SIAM, v. 26, n. 5, p. 1411–1473, 1997. Citado na página 14.

BEZERRA, G. A.; LUGÃO, P. H. G.; PORTUGAL, R. Quantum-walk-based search algorithms with multiple marked vertices. *Phys. Rev. A*, American Physical Society, v. 103, p. 062202, Jun 2021. Disponível em: <https://link.aps.org/doi/10.1103/PhysRevA.103.062202>. Citado na página 15.

BOYER, M. et al. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, Wiley Online Library, v. 46, n. 4-5, p. 493–505, 1998. Citado na página 15.

BRASSARD, G. et al. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, Providence, RI; American Mathematical Society; 1999, v. 305, p. 53–74, 2002. Citado 6 vezes nas páginas 15, 45, 53, 54, 67 e 87.

COPPERSMITH, D. An approximate fourier transform useful in quantum factoring. *arXiv preprint quant-ph/0201067*, 1994. Citado na página 50.

DEUTSCH, D. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, The Royal Society London, v. 400, n. 1818, p. 97–117, 1985. Citado na página 14.

DEUTSCH, D.; JOZSA, R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, The Royal Society London, v. 439, n. 1907, p. 553–558, 1992. Citado na página 14.

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

FEYNMAN, R. P. Simulating physics with computers. *International Journal of Theoretical Physics*, Springer, v. 21, p. 467–488, 1982. Citado na página 14.

GROVER, L. K. A fast quantum mechanical algorithm for database search. In: ACM INC. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996. p. 212–219. Citado 2 vezes nas páginas 14 e 45.

GROVER, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review letters*, APS, v. 79, n. 2, p. 325, 1997. Citado 2 vezes nas páginas 14 e 45.

KAYE, P. et al. *An introduction to quantum computing*. Oxford University Press on Demand, 2007. Citado na página 15.

LOVETT, N. B. et al. Universal quantum computation using the discrete-time quantum walk. *Physical Review A*, APS, v. 81, n. 4, p. 042330, 2010. Citado na página 14.

MACK, C. A. Fifty years of moore's law. *IEEE Transactions on semiconductor manufacturing*, IEEE, v. 24, n. 2, p. 202–207, 2011. Citado na página 14.

MOORE, G. E. et al. *Cramming more components onto integrated circuits*. McGraw-Hill New York, 1965. Citado na página 14.

NAHIMOVS, N.; RIVOSH, A. Exceptional configurations of quantum walks with grover's coin. In: SPRINGER. *International Doctoral Workshop on Mathematical and Engineering Methods in Computer Science*. 2015. p. 79–92. Citado na página 15.

NIELSEN, M. A.; CHUANG, I. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002. Citado 3 vezes nas páginas 14, 15 e 50.

PATT, Y. N. et al. One billion transistors, one uniprocessor, one chip. *Computer*, IEEE, v. 30, n. 9, p. 51–57, 1997. Citado na página 14.

PORTUGAL, R. *Quantum walks and search algorithms*. Springer, 2013. Citado 2 vezes nas páginas 14 e 15.

RHODES, M. L.; WONG, T. G. Quantum walk search on the complete bipartite graph. *Physical Review A*, APS, v. 99, n. 3, p. 032301, 2019. Citado 4 vezes nas páginas 15, 16, 79 e 87.

SHENVI, N.; KEMPE, J.; WHALEY, K. B. Quantum random-walk search algorithm. *Physical Review A*, APS, v. 67, n. 5, p. 052307, 2003. Citado na página 15.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: IEEE. *Proceedings 35th annual symposium on foundations of computer science*. 1994. p. 124–134. Citado na página 50.

SILVESTER, J. R. Determinants of block matrices. *The Mathematical Gazette*, Cambridge University Press, v. 84, n. 501, p. 460–467, 2000. Citado na página 79.

THEW, R. et al. Qudit quantum-state tomography. *Physical Review A*, APS, v. 66, n. 1, p. 012303, 2002. Citado 2 vezes nas páginas 38 e 62.

TULSI, A. Faster quantum-walk algorithm for the two-dimensional spatial search. *Physical Review A*, APS, v. 78, n. 1, p. 012310, 2008. Citado na página 15.

WEST, D. B. et al. *Introduction to graph theory*. Prentice Hall Upper Saddle River, 2001. v. 2. Citado na página 41.

WONG, T. G. Grover search with lackadaisical quantum walks. *Journal of Physics A: Mathematical and Theoretical*, IOP Publishing, v. 48, n. 43, p. 435304, 2015. Citado na página 15.

WONG, T. G.; SANTOS, R. A. Exceptional quantum walk search on the cycle. *Quantum Information Processing*, Springer, v. 16, n. 6, p. 154, 2017. Citado na página 15.

YU, B. et al. Finfet scaling to 10 nm gate length. In: IEEE. *Digest. International Electron Devices Meeting,*. 2002. p. 251–254. Citado na página 14.

Apêndices

APÊNDICE A – Mínimo da Equação 3.71

Deseja-se demonstrar que o ponto $w = 1/2$ é o único mínimo da função

$$f(w) = \frac{\sin^2(\pi w)}{P^2 \sin^2(\pi w/P)} + \frac{\sin^2(\pi(1-w))}{P^2 \sin^2(\pi(1-w)/P)}, \tag{A.1}$$

onde $0 < w < 1$ e $P \in \mathbb{N}^+$. Serão considerados dois casos particulares ($P = 1$ e $P = 2$) e então o caso geral será analisado.

A.1 P = 1

Nesse caso, $f(w)$ é constante:

$$f(w) = \frac{\sin^2(\pi w)}{\sin^2(\pi w)} + \frac{\sin^2(\pi(1-w))}{\sin^2(\pi(1-w))} \tag{A.2}$$

$$= 2. \tag{A.3}$$

Esse cenário é desconsiderado no Teorema 2 porque $P = 1$ implica um espaço de Hilbert unidimensional. Além disso, o círculo unitário é dividido em 1 uma única partição, ou seja, $f(w)$ contabiliza a probabilidade de obter w duas vezes.

A.2 P = 2

Usando a identidade trigonométrica $\sin^2(\theta/2) = \frac{1}{2}(1 - \cos\theta)$, obtém-se

$$\frac{\sin^2\theta}{\sin^2(\theta/2)} = \frac{(1+\cos\theta)(1-\cos\theta)}{\frac{1}{2}(1-\cos\theta)} \tag{A.4}$$

$$= 2 \cdot 2\cos^2\frac{\theta}{2}. \tag{A.5}$$

Usando esse resultado e a identidade trigonométrica para $\cos(\theta + \theta')$ calcula-se $f(w)$:

$$f(w) = \frac{\sin^2(\pi w)}{4\sin^2(\pi w/2)} + \frac{\sin^2(\pi(1-w))}{4\sin^2(\pi(1-w)/2)} \tag{A.6}$$

$$= \cos^2\frac{\pi w}{2} + \cos^2\frac{\pi(1-w)}{2} \tag{A.7}$$

$$= \cos^2\frac{\pi w}{2} + \left(\sin\frac{\pi}{2}\sin\frac{\pi w}{2} + \cos\frac{\pi}{2}\cos\frac{\pi w}{2}\right)^2 \tag{A.8}$$

$$= \cos^2\frac{\pi w}{2} + \sin^2\frac{\pi w}{2} \tag{A.9}$$

$$= 1. \tag{A.10}$$

Esse resultado é esperado porque divide-se o círculo unitário em duas partições, demarcadas pelos ângulos 0 e π. Evidentemente que ao fazer a medição, apenas um desses resultados será obtido, abrangendo todas as opções. Como $f(w)$ é constante nesse caso, qualquer ponto do domínio corresponde ao mínimo global.

A.3 Caso Geral

Analisa-se agora o caso de $P \geq 3$. Sendo $\varepsilon \in \mathbb{R}$ tal que $0 < \varepsilon < 1/2$, mostra-se que a função $f(w)$ é simétrica em torno do ponto $w = 1/2$.

$$f\left(\frac{1}{2}+\varepsilon\right) = \frac{\sin^2\left(\pi\left(\frac{1}{2}+\varepsilon\right)\right)}{P^2\sin^2\left(\frac{\pi}{P}\left(\frac{1}{2}+\varepsilon\right)\right)} + \frac{\sin^2\left(\pi\left(\frac{1}{2}-\varepsilon\right)\right)}{P^2\sin^2\left(\frac{\pi}{P}\left(\frac{1}{2}-\varepsilon\right)\right)} \tag{A.11}$$

$$= \frac{\sin^2\left(\pi\left(1-\left(\frac{1}{2}-\varepsilon\right)\right)\right)}{P^2\sin^2\left(\frac{\pi}{P}\left(1-\left(\frac{1}{2}-\varepsilon\right)\right)\right)} + \frac{\sin^2\left(\pi\left(\frac{1}{2}-\varepsilon\right)\right)}{P^2\sin^2\left(\frac{\pi}{P}\left(\frac{1}{2}-\varepsilon\right)\right)} \tag{A.12}$$

$$= f\left(\frac{1}{2}-\varepsilon\right). \tag{A.13}$$

Resta demonstrar que $f(1/2)$ é um mínimo global. A análise será feita em torno da função par $f_\pi(\theta)$ obtida a partir de $f(w)$ da seguinte maneira. Seja $w' = w - 1/2$, desloca-se a função $f(w)$ para a esquerda tomando $f_0(w') = f(w' + 1/2)$. Note que $f_0(w')$ é uma função par e que $-1/2 < w' < 1/2$. Para obter $f_\pi(\theta)$, faz-se uma outra conversão simples de domínio: $\theta = w'\pi$ e $f_\pi(\theta) = f_0(\theta/\pi)$. Assim, toda análise será feita em torno da função

$$f_\pi(\theta) = f\left(\frac{\theta}{\pi}+\frac{1}{2}\right) \tag{A.14}$$

$$= \frac{\sin^2\left(\pi\left(\frac{\theta}{\pi}+\frac{1}{2}\right)\right)}{\sin^2\left(\frac{\pi}{P}\left(\frac{\theta}{\pi}+\frac{1}{2}\right)\right)} + \frac{\sin^2\left(\pi(1-\left(\frac{\theta}{\pi}+\frac{1}{2}\right))\right)}{\sin^2\left(\frac{\pi}{P}\left(1-\left(\frac{\theta}{\pi}+\frac{1}{2}\right)\right)\right)} \tag{A.15}$$

$$= \frac{\sin^2\left(\theta+\frac{\pi}{2}\right)}{\sin^2\left(\frac{\theta}{P}+\frac{\pi}{2P}\right)} + \frac{\sin^2\left(\theta-\frac{\pi}{2}\right)}{\sin^2\left(-\frac{\theta}{P}+\frac{\pi}{2P}\right)} \tag{A.16}$$

$$= \cos^2(\theta)\left(\csc^2\left(\frac{\pi}{2P}+\frac{\theta}{P}\right)+\csc^2\left(\frac{\pi}{2P}-\frac{\theta}{P}\right)\right), \tag{A.17}$$

com domínio $\theta \in (-\pi/2, \pi/2)$. Como a função é par, restringe-se a análise para $0 \leq \theta < \pi/2$ e deseja-se provar que o ponto $f_\pi(0)$ é o mínimo global. Ou seja,

$$f_\pi(\theta) \geq f_\pi(0) \tag{A.18}$$

$$= \cos^2(0)\left(\csc^2\left(\frac{\pi}{2P}\right)+\csc^2\left(\frac{\pi}{2P}\right)\right) \tag{A.19}$$

$$= 2\csc^2\left(\frac{\pi}{2P}\right). \tag{A.20}$$

Divide-se a análise em dois casos: $P = 3$ e $P \geq 4$.

A.3.1 Caso 1 – P igual a 3

Para $P = 3$, usa-se as identidades

1. $\sin\left(\frac{\pi}{6} - x\right) = \cos\left(\frac{\pi}{3} + x\right)$;
2. $\sin(a \pm b) = \sin a \cos b \pm \cos a \sin b$;
3. $\cos(a \pm b) = \cos a \cos b \mp \sin a \sin b$;
4. $2\cos^2 x = \cos(2x) + 1$

Então,

$$f_\pi(\theta) = \cos^2(\theta)\left(\frac{1}{\sin^2\left(\frac{\pi}{6}+\frac{x}{3}\right)} + \frac{1}{\sin^2\left(\frac{\pi}{6}-\frac{x}{3}\right)}\right) \tag{A.21}$$

$$= \frac{\left(\cos\theta \sin\left(\frac{\pi}{6}+\frac{\theta}{3}\right)\right)^2 + \left(\cos\theta\cos\left(\frac{\pi}{3}+\frac{\theta}{3}\right)\right)^2}{\sin^2\left(\frac{\pi}{6}+\frac{\theta}{3}\right)\sin^2\left(\frac{\pi}{6}-\frac{\theta}{3}\right)} \tag{A.22}$$

$$= \frac{\frac{1}{4}\left(\sin\left(\frac{\pi}{6}+\frac{4\theta}{3}\right) + \sin\left(\frac{\pi}{6}-\frac{2\theta}{3}\right)\right)^2 + \frac{1}{4}\left(\cos\left(\frac{4\theta}{3}+\frac{\pi}{3}\right) + \cos\left(\frac{2\theta}{3}-\frac{\pi}{3}\right)\right)^2}{\frac{1}{4}\left(\cos\frac{2\theta}{3} - \cos\frac{\pi}{3}\right)^2} \tag{A.23}$$

$$= \frac{\gamma_+^2 + \gamma_-^2}{\left(\cos\frac{2\theta}{3} - \frac{1}{2}\right)^2} \tag{A.24}$$

$$= \frac{-\cos^2\frac{2\theta}{3} - \cos^2\frac{4\theta}{3} + 3 - \cos\frac{2\theta}{3} + 2\cos 2\theta}{\frac{1}{4}\left(2\cos\frac{2\theta}{3} - 1\right)^2} \tag{A.25}$$

$$= \frac{-\left(\cos\frac{2\theta}{3} + \cos\frac{4\theta}{3}\right)^2 + \left(\cos\left(\frac{2\theta}{3}\right) + \cos 2\theta\right) + 3 - \cos\frac{2\theta}{3} + 2\cos 2\theta}{\frac{1}{4}\left(2\cos\frac{2\theta}{3} - 1\right)^2} \tag{A.26}$$

$$= 4 \cdot \frac{-\left(\left(2\cos^2\frac{\theta}{3} - 1\right) + \left(8\cos^4\frac{\theta}{3} - 8\cos^2\frac{\theta}{3} + 1\right)\right)^2 + 3(1 + \cos 2\theta)}{\left(2\cos\frac{2\theta}{3} - 1\right)^2} \tag{A.27}$$

$$= 4 \cdot \frac{-4\cos^4\frac{\theta}{3}\left(4\cos^2\frac{\theta}{3} - 3\right)^2 + 6\left(2\cos\frac{\theta}{3}\cos\frac{2\theta}{3} - \cos\frac{\theta}{3}\right)^2}{\left(2\cos\frac{2\theta}{3} - 1\right)^2} \tag{A.28}$$

$$= \frac{-16\cos^4\frac{\theta}{3}\left(2\cos\frac{2\theta}{3} - 1\right)^2 + 24\cos^2\frac{\theta}{3}\left(2\cos\frac{2\theta}{3} - 1\right)^2}{\left(2\cos\frac{2\theta}{3} - 1\right)^2} \tag{A.29}$$

$$= -16\cos^4\frac{\theta}{3} + 24\cos^2\frac{\theta}{3} \tag{A.30}$$

$$= -16\left(\cos^2\frac{\theta}{3} - \frac{3}{4}\right)^2 + 9; \tag{A.31}$$

onde

$$\gamma_{\pm} = \gamma_1 \pm \gamma_2, \tag{A.32}$$

$$\gamma_1 = \frac{1}{2}\left(\cos\frac{2\theta}{3} + \cos\frac{4\theta}{3}\right), \quad \text{e} \tag{A.33}$$

$$\gamma_2 = \frac{\sqrt{3}}{2}\left(\cos\frac{4\theta}{3} - \cos\frac{2\theta}{3}\right). \tag{A.34}$$

Sabendo que $0 \leq \theta < \pi/2 \implies 1 \geq \cos^2\frac{\theta}{3} > 3/4$, e que $2\csc^2(\pi/6) = 8$, conclui-se que para $P = 3$,

$$f_\pi(\theta) \geq -16\left(\frac{1}{4}\right)^2 + 9 = 8 = 2\csc^2\frac{\pi}{6}. \tag{A.35}$$

A.3.2 Caso 2 – P maior ou igual a 4

Denote $\theta_\pm = \frac{\pi}{2P} \pm \frac{\theta}{P}$. Deseja-se demonstrar, para $P \geq 4$, que

$$f_\pi(\theta) = \cos^2(\theta) \cdot \frac{\sin^2(\theta_+) + \sin^2(\theta_-)}{\sin^2(\theta_+)\sin^2(\theta_-)} \geq 2\csc^2\left(\frac{\pi}{2P}\right). \tag{A.36}$$

Usando algumas identidades trigonométricas, é possível reescrever o numerador como

$$\begin{aligned}
\sin^2(\theta_+) + \sin^2(\theta_-) &= \left(\sin\frac{\pi}{2P}\cos\frac{\theta}{P} + \cos\frac{\pi}{2P}\sin\frac{\theta}{P}\right)^2 + \\
&\quad \left(\sin\frac{\pi}{2P}\cos\frac{\theta}{P} - \cos\frac{\pi}{2P}\sin\frac{\theta}{P}\right)^2 && \text{(A.37)}\\
&= 2\sin^2\frac{\pi}{2P}\cos^2\frac{\theta}{P} + 2\cos^2\frac{\pi}{2P}\sin^2\frac{\theta}{P} && \text{(A.38)}\\
&= 2\sin^2\frac{\pi}{2P}\left(1 - \sin^2\frac{\theta}{P}\right) + 2\cos^2\frac{\pi}{2P}\sin^2\frac{\theta}{P} && \text{(A.39)}\\
&= 2\sin^2\frac{\pi}{2P} + 2\sin^2\frac{\theta}{P}\left(\cos^2\frac{\pi}{2P} - \sin^2\frac{\theta}{P}\right) && \text{(A.40)}\\
&= 2\sin^2\frac{\pi}{2P} + 2\sin^2\frac{\theta}{P}\left(2\cos^2\frac{\pi}{2P} - 1\right) && \text{(A.41)}\\
&= 2\sin^2\frac{\pi}{2P} + 2\sin^2\frac{\theta}{P}\cos\frac{\pi}{P}. && \text{(A.42)}
\end{aligned}$$

Usando as mesmas identidades trigonométricas, é possível reescrever a raíz do denominador como

$$\begin{aligned}
\sin\left(\frac{\pi}{2P} + \frac{\theta}{P}\right)\sin\left(\frac{\pi}{2P} - \frac{\theta}{P}\right) &= \frac{1}{2}\left(\cos\frac{2\theta}{P} - \cos\frac{\pi}{P}\right) && \text{(A.43)}\\
&= \frac{1}{2}\left(\cos\frac{2\theta}{P} + 1 - 1 - \cos\frac{\pi}{P}\right) && \text{(A.44)}\\
&= \cos^2\frac{\theta}{P} - \cos^2\frac{\pi}{2P} && \text{(A.45)}\\
&= -\sin^2\frac{\theta}{P} + \sin^2\frac{\pi}{2P}. && \text{(A.46)}
\end{aligned}$$

Sendo assim, reescreve-se

$$f_\pi(\theta) = \frac{2\sin^2\frac{\pi}{2P} + 2\sin^2\frac{\theta}{P}\cos\frac{\pi}{P}}{\left(\sin^2\frac{\pi}{2P} - \sin^2\frac{\theta}{P}\right)^2}\cos^2\theta. \tag{A.47}$$

Para continuar a demonstração, será necessária a utilização das identidades auxiliares

$$\sin\frac{\theta}{P} \geq \frac{2\theta}{\pi}\sin\frac{\pi}{2P}, \tag{A.48}$$

e

$$\frac{2\sqrt{2}\pi^2\theta^2 + \pi^4}{\left(\pi^2 - 4\theta^2\right)^2}\cos^2\theta \geq 1, \tag{A.49}$$

demonstradas na seção A.3.3. Usando as identidades A.48 e A.49; e notando que $\sin\frac{\pi}{2P} \geq \sin\frac{\theta}{P}$ no domínio e $\cos\frac{\pi}{P} \geq \cos\frac{\pi}{4}$; obtém-se

$$f_\pi(\theta) \geq \frac{2\sin^2\frac{\pi}{2P} + 2\left(\frac{2\theta}{\pi}\sin\frac{\pi}{2P}\right)^2\cos\frac{\pi}{4}}{\left(\sin^2\frac{\pi}{2P} - \left(\frac{2\theta}{\pi}\sin\frac{\pi}{2P}\right)^2\right)^2}\cos^2\theta \tag{A.50}$$

$$= \frac{2\sin^2\frac{\pi}{2P}}{\sin^4\frac{\pi}{2P}} \cdot \frac{1 + 2\sqrt{2}\,\theta^2/\pi^2}{\left(1 - 4\theta^2/\pi^2\right)^2}\cos^2\theta \tag{A.51}$$

$$= 2\csc^2\frac{\pi}{2P} \cdot \frac{\pi^4 + 2\sqrt{2}\,\theta^2\pi^2}{\left(\pi^2 - 4\theta^2\right)^2}\cos^2\theta \tag{A.52}$$

$$\geq 2\csc^2\frac{\pi}{2P}. \tag{A.53}$$

A.3.3 Identidades Auxiliares

Essa Seção dedica-se à demonstração das identidades descritas pelas Eqs. A.48 e A.49.

A.3.3.1 Identidade A.48

A identidade

$$\sin\frac{\theta}{P} \geq \frac{2\theta}{\pi}\sin\frac{\pi}{2P} \tag{A.54}$$

ilustra o limite inferior dado por uma reta que passa por baixo de $\sin\frac{\theta}{P}$ coincidindo nos pontos $\theta = 0$ e $\theta = \pi/2$:

$$\sin\frac{0}{P} - \frac{0}{\pi}\sin\frac{\pi}{2P} = \sin\frac{\pi}{2P} - 1\cdot\sin\frac{\pi}{2P} = 0. \tag{A.55}$$

O restante da demonstração segue da derivada segunda, já que

$$\frac{\partial^2}{\partial\theta^2}\left(\sin\frac{\theta}{P} - \frac{2}{\pi}\theta\sin\frac{\pi}{2P}\right) = -\frac{1}{P^2}\sin\frac{\theta}{P} < 0 \tag{A.56}$$

no domínio $0 \leq \theta < \pi/2$. Logo, a identidade A.48 possui concavidade para baixo no domínio e

$$\sin\frac{\theta}{P} - \frac{2\theta}{\pi}\sin\frac{\pi}{2P} > 0 \tag{A.57}$$

quando $0 < \theta < \pi/2$, concluindo a demonstração.

A.3.3.2 Identidade A.49

Deseja-se demonstrar que a identidade

$$\frac{2\sqrt{2}\pi^2\theta^2 + \pi^4}{\left(\pi^2 - 4\theta^2\right)^2}\cos^2\theta \geq 1 \tag{A.58}$$

é verdadeira no domínio $0 \leq \theta < \pi/2$. Note que a expressão é igual a 1 quando $\theta = 0$. Para o restante da demonstração, utiliza-se a identidade.

$$\cos\theta \geq 1 - \frac{\theta^2}{2} + \frac{\theta^4\left(2\pi^2 - 16\right)}{\pi^4}, \tag{A.59}$$

demonstrada a seguir.

Considere o domínio $\theta \in [0, \pi/3]$. Expandindo $\cos\theta$ em Série de Taylor em torno de $\theta = 0$,

$$\cos\theta = 1 - \frac{\theta^2}{2} + \frac{\theta^4}{24} - \frac{\theta^6}{720} + \frac{\theta^8}{40320} + O\left(\theta^{10}\right). \tag{A.60}$$

Como o termo de oitava ordem é positivo, o somatório até o termo de sexta ordem resulta num limite inferior de $\cos\theta$:

$$\cos\theta \geq 1 - \frac{\theta^2}{2} + \frac{\theta^4}{24} - \frac{\theta^6}{720}. \tag{A.61}$$

Usando esse limite inferior e denotando o lado direito de Eq. A.59 por γ_θ,

$$\cos\theta - \gamma_\theta \geq \frac{\theta^4}{24} - \frac{\theta^6}{720} - \frac{\theta^4\left(2\pi^2 - 16\right)}{\pi^4} \tag{A.62}$$

$$= 2\theta^4\left(-\frac{x^2}{1440} - \frac{1}{\pi^2} + \frac{1}{48} + \frac{8}{\pi^4}\right). \tag{A.63}$$

Por conta do termo $2\theta^4$, conclui-se que essa expressão tem raíz em $\theta = 0$. Já o termo entre parênteses possui raíz no domínio em $\theta \approx 1.537 > \pi/3$. Avaliando a expressão entre parênteses para $\theta = 0$, obtém-se um valor positivo $\approx 3.3 \cdot 10^{-3}$. Logo, a expressão entre parênteses possui concavidade para baixo e a Eq. A.59 é verdadeira para $\theta \in [0, \pi/3]$.

Considere o domínio $\theta \in (\pi/3, \pi/2)$. Expandindo $\cos\theta$ em Série de Taylor em torno de $\theta = \pi/2$,

$$\cos\theta = -\left(\theta - \frac{\pi}{2}\right) + \frac{1}{6}\left(\theta - \frac{\pi}{2}\right)^3 - \frac{1}{120}\left(\theta - \frac{\pi}{2}\right)^5 + O\left(\left(\theta - \frac{\pi}{2}\right)^7\right). \tag{A.64}$$

Note que para $\theta < \pi/2$, o termo de terceira ordem é negativo, enquanto o termo de quinta ordem é positivo. Sendo assim, considere o limite inferior dado por

$$\cos\theta \geq -\theta + \frac{\pi}{2} + \frac{1}{6}\left(\theta - \frac{\pi}{2}\right)^3. \tag{A.65}$$

Usando esse limite inferior e denotando o lado direito de Eq. A.59 por γ_θ,

$$\cos\theta - \gamma_\theta \geq -\frac{x^4(2\pi^2-16)}{\pi^4} + \frac{\left(x-\frac{\pi}{2}\right)^3}{6}) + \frac{x^2}{2} - x - 1 + \frac{\pi}{2}. \tag{A.66}$$

Essa expressão tem raízes reais nos pontos $\theta \approx 0.88 < \pi/3$ e $\theta = \pi/2$. Avaliando a expressão no ponto $\pi/3$ obtém-se um valor positivo $\approx 1.8 \cdot 10^{-2} > 0$. Logo, a Eq. A.59 é verdadeira no domínio $\theta \in [0, \pi/2)$.

Para demonstrar a Eq. A.49, basta mostrar, utilizando a Eq. A.59 que

$$\frac{2\sqrt{2}\pi^2\theta^2 + \pi^4}{\left(\pi^2 - 4\theta^2\right)^2}\left(1 - \frac{\theta^2}{2} + \frac{\theta^4\left(2\pi^2-16\right)}{\pi^4}\right)^2 - 1 \geq 0 \tag{A.67}$$

no domínio. Usando a propriedade distributiva, obtém-se

$$\frac{x^2}{\pi^6}\left(c_4x^4 + c_2x^2 + c_0\right), \tag{A.68}$$

onde

$$c_4 = 8\sqrt{2}\left(4 - \pi^2\right) + \frac{\pi^4}{\sqrt{2}}, \tag{A.69}$$

$$c_2 = 2\pi^2\left(8 - \pi^2\sqrt{2}\right)\left(1 + \sqrt{2}\right) + \frac{\pi^6}{4}, \quad \text{e} \tag{A.70}$$

$$c_0 = \pi^4\left(8 + 2\sqrt{2} - \pi^2\right). \tag{A.71}$$

A expressão A.68 é igual a 0 quando $\theta = 0$. Resta saber se ela é positiva no restante do domínio – $0 < \theta < \pi/2$. Considere apenas o termo entre parênteses. Esse termo possui raízes nos pontos $\theta \approx \pm 1.58$ e $\theta \approx \pm 3.89$. Como $\pi/2 < 1.58$, resta saber se o termo entre parênteses é positivo quando $-\pi/2 < \theta < \pi/2$. Avaliando para $\theta = 0$, obtém-se um valor positivo ≈ 93.4. Portanto, a identidade da Eq. A.49 é verdadeira.

APÊNDICE B – Projeção da Sobreposição Uniforme das Arestas nos Autovetores

Resta calcular os valores de $\left\langle \Sigma_{\pm}^{*} \,\middle|\, D \right\rangle$, $\langle \Delta_{\pm} \,|\, D \rangle$ e $\left\langle \Delta_{\pm}^{*} \,\middle|\, D \right\rangle$. Relembre que $|D\rangle$ é dado pela Eq. 4.57, os autovetores são dados pelas Eqs. 4.54 e 4.55 e seus complexos conjugados. Então,

- Para $\left\langle \Sigma_{\pm}^{*} \,\middle|\, D \right\rangle$, tem-se que

$$\left\langle \Sigma_{\pm}^{*} \,\middle|\, D \right\rangle = \left(\left\langle D \,\middle|\, \Sigma_{\pm}^{*} \right\rangle \right)^{*} = \langle D \,|\, \Sigma_{\pm} \rangle \,. \tag{B.1}$$

Logo,

$$\left| \left\langle \Sigma_{\pm}^{*} \,\middle|\, D \right\rangle \right|^{2} = |\langle \Sigma_{\pm} \,|\, D \rangle|^{2} \,. \tag{B.2}$$

- Para $\langle \Delta_{\pm} \,|\, D \rangle$, tem-se que

$$\langle \Delta_{\pm} \,|\, D \rangle = (\langle D \,|\, \Delta_{\pm} \rangle)^{*} \tag{B.3}$$

$$= \frac{1}{4\sqrt{N_1 N_2}} \left(\pm e^{\mathrm{i}\Sigma} \xi + \xi^{*} \right)^{*} , \tag{B.4}$$

onde

$$\xi = \sqrt{k_1 k_2} + \mathrm{i}\sqrt{k_1 (N_2 - k_2)} + \mathrm{i}\sqrt{(N_1 - k_1) k_2} - \sqrt{(N_1 - k_1)(N_2 - k_2)} \tag{B.5}$$

$$= \left(\sqrt{k_1} + \mathrm{i}\sqrt{N_1 - k_1} \right) \left(\sqrt{k_2} + \mathrm{i}\sqrt{N_2 - k_2} \right) . \tag{B.6}$$

Logo,

$$|\langle \Delta_{\pm} \,|\, E \rangle|^{2} = \frac{1}{16 N_1 N_2} \left(\pm e^{\mathrm{i}\Sigma} \xi + \xi^{*} \right) \left(\pm e^{\mathrm{i}\Sigma} \xi + \xi^{*} \right)^{*} \tag{B.7}$$

$$= \frac{1}{16 N_1 N_2} \left(2\xi\xi^{*} \pm 2\Re \left(e^{\mathrm{i}\Sigma} \xi^{2} \right) \right) \tag{B.8}$$

$$= \frac{1}{8} \left(1 \pm \Re \left(\frac{e^{\mathrm{i}\Sigma} \xi^{2}}{N_1 N_2} \right) \right) , \tag{B.9}$$

e usando

$$\frac{e^{\mathrm{i}\Sigma} \xi^{2}}{N_1 N_2} = e^{\mathrm{i}\Sigma} \left(\frac{2k_1 - N_1 + 2\mathrm{i}\sqrt{N_1 - k_1}}{N_1} \right) \left(\frac{2k_2 - N_2 + 2\mathrm{i}\sqrt{N_2 - k_2}}{N_2} \right) \tag{B.10}$$

$$= e^{\mathrm{i}\Sigma} \left(-\cos\theta_1 + \mathrm{i}\sin\theta_1 \right) \left(-\cos\theta_2 + \mathrm{i}\sin\theta_2 \right) \tag{B.11}$$

$$= e^{\mathrm{i}\Sigma} e^{-\mathrm{i}\theta_1} e^{-\mathrm{i}\theta_2} \tag{B.12}$$

$$= e^{-\mathrm{i}\Sigma} \tag{B.13}$$

resulta em

$$|\langle \Delta_{\pm} \,|\, D \rangle|^{2} = \frac{1}{8} \left(1 \pm \cos\Sigma \right) . \tag{B.14}$$

- Para $\left\langle \Delta_{\pm}^{*} \,\middle|\, E \right\rangle$, tem-se que

$$\left\langle \Delta_{\pm}^{*} \,\middle|\, D \right\rangle = \left(\left\langle D \,\middle|\, \Delta_{\pm}^{*} \right\rangle \right)^{*} = \langle E \,|\, \Delta_{\pm} \rangle \,. \tag{B.15}$$

  Logo,

$$\left| \left\langle \Delta_{\pm}^{*} \,\middle|\, D \right\rangle \right|^{2} = |\langle \Delta_{\pm} \,|\, D \rangle|^{2} \,. \tag{B.16}$$

Juntando todos esses resultados e usando as identidades trigonométricas $1 + \cos\theta = 2\cos^2(\theta/2)$ e $1 - \cos\theta = 2\sin^2(\theta/2)$, obtém-se a Tabela 2.