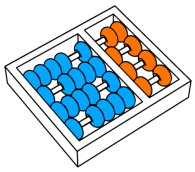
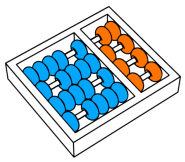


Alex Bredariol Grilo

"Computação Quântica e Teoria da Computação"

CAMPINAS
2014



Universidade Estadual de Campinas
Instituto de Computação

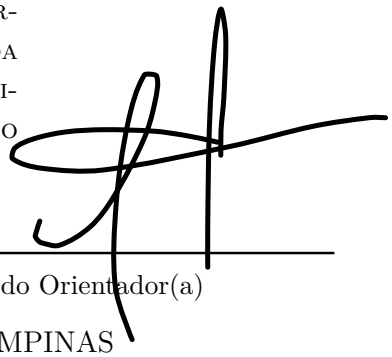
Alex Bredariol Grilo

"Computação Quântica e Teoria da Computação"

Orientador(a): **Prof. Dr. Arnaldo Vieira Moura**

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Computação da Universidade Estadual de Campinas para obtenção do título de Mestre em Ciência da Computação.

Este exemplar corresponde à versão final da Dissertação defendida por Alex Bredariol Grilo, sob orientação de Prof. Dr. Arnaldo Vieira Moura.



Assinatura do Orientador(a)

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

G879c

Grilo, Alex Bredariol, 1987-
Computação quântica e teoria de computação / Alex Bredariol Grilo. – Campinas, SP : [s.n.], 2014.

Orientador: Arnaldo Vieira Moura.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Computação.

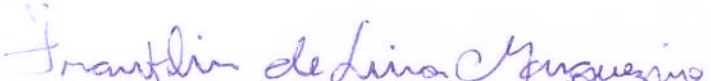
1. Computação quântica. 2. Complexidade computacional. 3. Teoria dos autômatos. 4. Algoritmos. I. Moura, Arnaldo Vieira,1950-. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Informações para Biblioteca Digital

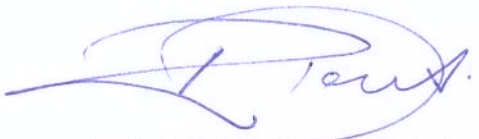
Título em outro idioma: Quantum computing and theoretical computer science
Palavras-chave em inglês:
Quantum computing
Computational complexity
Machine theory
Algorithms
Área de concentração: Ciência da Computação
Titulação: Mestre em Ciência da Computação
Banca examinadora:
Arnaldo Vieira Moura [Orientador]
Franklin de Lima Marquezino
Ricardo Dahab
Data de defesa: 11-04-2014
Programa de Pós-Graduação: Ciência da Computação

TERMO DE APROVAÇÃO

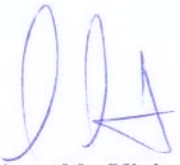
Defesa de Dissertação de Mestrado em Ciência da Computação, apresentada pelo(a) Mestrando(a) **Alex Bredariol Grilo**, aprovado(a) em **11 de abril de 2014**, pela Banca examinadora composta pelos Professores Doutores:



Prof(a). Dr(a). Franklin de Lima Marquezino
Titular



Prof(a). Dr(a). Ricardo Dahab
Titular



Prof(a). Dr(a). Arnaldo Vieira Moura
Presidente

Instituto de Computação
Universidade Estadual de Campinas

Computação Quântica e Teoria da Computação

Alex Bredariol Grilo[1]

11 de abril de 2014

Banca Examinadora:

- Prof. Dr. Arnaldo Vieira Moura (Supervisor/*Orientador*)
- Prof. Dr. Ricardo Dahab
  IC/Unicamp
- Prof. Dr. Franklin de Lima Marquezino
  PESC/COPPE/UFRJ
- Profa. Dra. Chistiane Neme Campos
  IC/Unicamp
- Prof. Dr. Arnaldo Mandel
  IME/USP

[1]Financiado parcialmente pelo projeto CNPq 132192/2012-8, pelos projetos FAPESP 2012/06648-0 e 2012/22478-7

Resumo

A Computação Quântica é um tópico relativamente recente e pouco conhecido, principalmente no meio da Computação. Seu estudo surgiu na tentativa de físicos simularem sistemas regidos pela Mecânica Quântica por computadores clássicos, o que se conjecturou inviável. Portanto, um novo modelo computacional que utiliza a estrutura quântica da matéria para computar foi teorizado para suprir estas deficiências.

Este trabalho tem como objetivo principal estudar as influências da Computação Quântica na Teoria da Computação. Para atingir tal objetivo, primeiramente são expostos os conhecimentos básicos da Mecânica Quântica através de uma linguagem voltada para Teóricos de Computação sem conhecimento prévio na área, de forma a remover a barreira inicial sobre o tema.

Em seguida, serão apresentadas inovações na área da Teoria de Computação oriundas da Computação Quântica. Começaremos com os principais Algoritmos Quânticos desenvolvidos até hoje, que foram os primeiros passos para demonstrar a possível superioridade computacional do novo modelo. Dentre estes algoritmos, apresentaremos o famoso Algoritmo de Shor, que fatora números em tempo polinomial.

Adicionalmente, neste trabalho foram estudados tópicos mais avançados e atuais em Computabilidade e Complexidade Quânticas. Sobre Autômatos Quânticos, foram estudados aspectos de um modelo que mistura estados clássicos e quânticos, focando na comparação do poder computacional em relação aos Autômatos Finitos Clássicos. Do ponto de vista de Classes de Complexidade, será abordada a questão se em linguagens da classe QMA, o análogo quântico da classe NP, consegue-se atingir probabilidade de erro nulo na aceitação de instâncias positivas.

Abstract

Quantum Computing is a relatively new area and it is not well known, mainly among Computer Scientists. It has emerged while physicists tried to simulate Quantum Systems with classical computers efficiently, which has been conjectured impossible. Then, a new computational model that uses the quantum structure of matter to perform computations has been theorized in order to perform these operations.

We intend in this work to study the influences of Quantum Computing in Theoretical Computer Science. In order to achieve this goal, we start by presenting the basics of Quantum Computing to Theoretical Computer Science readers with no previous knowledge in this area, removing any initial barriers for a clean understanding of the topic.

We will then follow by showing innovations in Theoretical Computer Science introduced by Quantum Computation. We start by showing the main Quantum Algorithms, that exemplify advantages of the new computational model. Among these algorithms, we will present the Shor Algorithm that factors numbers in polynomial time.

We follow with more advanced topics in Quantum Computability and Complexity. We study Quantum Finite Automata Models that work with quantum and classical states, focusing on comparing their computational power with Deterministic Finite Automata. In Complexity Theory, we study the question if for languages in QMA, the quantum analogue of NP, zero probability error can be achieved in yes-instances.

Ao vô Armando, que me ensinou a viver sorrindo

Agradecimentos

Primeiramente agradeço a minha família, especialmente a meu pai e minha mãe, pelo apoio incondicional em todas as etapas da minha vida, indispensáveis para chegar até onde cheguei.

Agradeço ao meu orientador Arnaldo pois ele também teve um papel fundamental durante este mestrado. Às vezes chegava para a reunião achando que tudo ia dar errado, e magicamente no final havia uma luz no fim do túnel.

Agradeço ao CNPq e principalmente à FAPESP pelo suporte financeiro durante o mestrado e o estágio no exterior.

Agradeço a todos os professores que foram importantíssimos em minha formação para que hoje eu tenha conhecimento técnico, e mais importante que isso, senso crítico, para realizar meu trabalho. Destaco o agradecimento ao professor Zanoni que serviu de tutor para mim durante toda a minha graduação.

Agradeço ao Iordanis e Jamie por me acolherem no LIAFA durante seis bons meses.

Agradeço a todos os funcionários do Instituto de Computação por, dos bastidores, darem suporte às atividades realizadas no mestrado.

Agradeço aos amigos do Contra, do COTUCA, CC07, do CACo, do LOCo, da Unicamp, de meus trabalhos, do vôlei, da Espanha, da França e da vida, que me acompanharam e fizeram a jornada valer muito mais a pena. Os meios justificam os fins.

Finalmente, agradeço à minha banca, os professores Ricardo Dahab e Franklin Marquezino, pelos comentários e sugestões a fim de melhorar o meu trabalho.

Sumário

Lista de Figuras

Capítulo 1

Introdução

Na história da Computação, sabemos que os primeiros algoritmos foram criados mais de dois mil anos antes de máquinas que automatizassem em larga escala suas operações, acelerando cálculos e evitando erros humanos. Tais algoritmos buscavam sistematizar métodos para solucionar manualmente problemas matemáticos, sendo também precursores de qualquer formalização dos conceitos de Algoritmo e Computação.

No início do século XX, com a concepção do conceito de Algoritmo, começou-se a indagar sobre quais os problemas poderiam ou não ser resolvidos computacionalmente, resultando na criação da área de Computabilidade. Posteriormente, com a construção de computadores de propósito geral capazes de realizar operações simples mais rapidamente do que qualquer ser humano, começou a preocupação, então, com a eficiência dos algoritmos, para que estes pudessem ser, de fato, utilizados na resolução de problemas do dia-a-dia.

Paralelamente, no final do século XIX, físicos perceberam que o conhecimento dos fenômenos da natureza então disponíveis eram insuficientes para explicar resultados de experimentos tratando de partículas subatômicas e, progressivamente, formulou-se uma nova teoria que hoje conhecemos como Mecânica Quântica.

Após a consolidação desta nova teoria, já na década de 80,, Richard Feynman, um dos pesquisadores que ajudou a formulá-la, questionou sobre a eficiência de computadores na simulação do comportamento quântico da matéria, conjecturando que tal tarefa não poderia ser realizada de forma eficiente. Como resposta, Feynman idealizou um novo modelo de computador, baseado no funcionamento da própria Mecânica Quântica, que poderia, então, realizar essa simulação de forma eficiente.

Hoje, este é considerado o nascimento da Computação Quântica.

De caráter multidisciplinar, a Computação Quântica teve desde então avanços importantes sob a perspectiva de diversas áreas de conhecimento, como Física Experimental, Teoria da Informação e Teoria da Computação. Neste trabalho, serão focados os aspectos que dizem respeito a esta última área, especialmente nas novidades relacionadas às áreas de Computabilidade e Complexidade Computacional.

Mesmo com todo esforço já dispendido, ainda hoje não existem Computadores Quânticos de propósito geral e escaláveis para utilização. Surge então a pergunta:

Por que estudar Computação Quântica?

Assumindo que computadores quânticos serão, um dia, construídos, ao estudar e propor Algoritmos Quânticos, o estudo dos recursos necessários para sua execução servem: (*i*) de motivação para a construção de computadores que possam executá-los; (*ii*) para termos consciência das implicações que tal modelo poderá trazer ao ser amplamente utilizado; e (*iii*) para a validação de dispositivos que reivindicam possuir poder computacional quântico.

Além destes fatos, existem motivações que justificam o estudo de Computação Quântica, independentemente da construção de computadores quânticos.

Primeiramente, temos que alguns resultados da Teoria de Computação Quântica possuem uma relação estreita com conceitos da Física. O estudo de tais problemas a partir de uma perspectiva diferente pode permitir o melhor entendimento de fundamentos da Mecânica Quântica.

Além disso, temos que o estudo da Computação Quântica sob as lentes da Teoria da Computação pode trazer novos resultados para a própria Teoria de Computação clássica. O estudo de um problema sob o ponto de vista de um novo modelo computacional pode trazer novas ideias para solucioná-lo sem tais recursos. Encontramos hoje algoritmos clássicos inspirados em algoritmos quânticos, além de provas de teoremas envolvendo somente elementos clássicos, utilizando argumentos inspirados no modelo quântico.

Dentro deste contexto, o objetivo deste trabalho é entender alguns pontos em que o advento da Computação Quântica influencia a área de Teoria da Computação. Desta forma, pretende-se (*i*) estudar as bases da Computação Quântica e elaborar um texto que introduza o tema de forma didática para pessoas de Teoria de Computação; e (*ii*) aprofundar o estudo em alguns tópicos mais atuais, de forma a entender e

avançar o estado da arte nestes pontos.

O Capítulo 2 apresenta os conceitos necessários da Mecânica Quântica para a compreensão da Computação Quântica, bem como o modelo computacional que será amplamente utilizados na descrição de algoritmos quânticos. No Capítulo 3 são apresentados os principais algoritmos e classes de complexidade quânticos. Estes dois capítulos compõe a parte da dissertação relativa ao estudo básico da área de Computação Quântica. Ressaltamos que, para leitores familiarizados com a área de Computação Quântica, estes capítulos não são necessários para o entendimento dos capítulos que os seguem.

No Capítulo 4 estudamos a influência da Mecânica Quântica no poder computacional de dispositivos mais simples, apresentando um modelo de Autômato Finito Quântico, bem como propriedades do modelo e linguagens reconhecidas por ele. Já no Capítulo 5, será apresentado mais a fundo um problema atual da Complexidade Computacional Quântica. Estes dois capítulos constituem a parte da dissertação envolvendo o estudo mais aprofundado de tópicos atuais da área.

Terminaremos esta seção indicando as contribuições deste trabalho. Em seguida apresentaremos brevemente a evolução histórica da área de Computação Quântica e finalizaremos o capítulo com a bibliografia básica da área.

Contribuições do trabalho

Primeiramente, temos que a parte inicial deste trabalho, formada pelo Capítulo 2 e Capítulo 3, se apresenta como uma alternativa aos poucos textos introdutórios sobre Computação Quântica em língua portuguesa voltados para cientistas da Computação [29][76][85].

O Capítulo 4 contém uma revisão geral de um dos modelos de autômatos quânticos, unificando a literatura sobre o tópico. Ressaltamos que este capítulo também contém resultados originais obtidos durante o mestrado do candidato que resultaram em publicações. O estudo das linguagens reconhecidas pelo modelos 2QCFA [1] categorizando segundo a hierarquia clássica de linguagens foi apresentado no *IV Workshop-Escola de Computação e Informação Quântica* e publicado em seus anais [48]. Foi apresentado na escola *Computer Science days in Ekaterinburg (CSEdays)* um trabalho sobre as características e propriedades do modelo 2QCFA e um resumo estendido do trabalho foi publicado em seus anais [49], e o artigo correspondente foi publicado no

[1] O modelo 2QCFA será formalmente apresentado no Capítulo 4.

Siberian Electronic Mathematical Reports [50].

O Capítulo 5 contém um estudo, em português, de um resultado parcial relativamente recente sobre uma questão em aberto em Complexidade Computacional Quântica. No mesmo capítulo apresentamos também um variação original do resultado da literatura, obtida pelo candidato durante seu estágio no *Laboratoire d'Informatique Algorithmique: Fondements et Applications, CNRS, Université Paris VII*, sob supervisão de Iordanis Kerenidis e Jamie Sikora.

1.1 Breve História da Computação Quântica

Nesta seção, faremos uma breve revisão histórica da Computação Quântica, apontando seus principais marcos, de modo a entender o contexto em que a área se encontra hoje.

Na década de 80, Richard Feynman sugeriu que os computadores clássicos só conseguiriam simular o funcionamento de sistemas quânticos com um custo exponencial em termos de tempo computacional [42]. Então, propôs um computador que extrairia da estrutura quântica da matéria seu poder computacional.

Desde então, paralelamente à evolução do estudo sobre como implementar na prática um computador quântico, físicos, matemáticos e cientistas da computação passaram a pesquisar o ganho que computadores quânticos poderiam trazer se fossem implementados na prática. No final da década de 80, Deutsch apresentou os dois modelos computacionais quânticos mais importantes, as Máquinas de Turing Quânticas [34] e Circuitos Quânticos [35], que permitiram o desenvolvimento de algoritmos quânticos compatíveis com concretizações futuras de computadores quânticos. Posteriormente, Yao demonstrou que esses dois modelos são equivalentes [94]. No final da década de 90, Bernstein e Vazirani descreveram como construir uma Máquina de Turing Quântica Universal [25], uma Máquina de Turing Quântica capaz de simular qualquer Máquina de Turing Quântica.

Na início da década de 90, foram desenvolvidos os algoritmos quânticos de Deutsch [34] e de Deutsch-Josza [36], os quais permitem descobrir características de funções através de oráculos de forma mais eficiente quando comparados com algoritmos determinísticos clássicos, no segundo caso com ganho exponencial na complexidade em tempo.

A grande notoriedade da Computação Quântica, entretanto, ocorreu em 1994,

quando Shor apresentou algoritmos quânticos eficientes para o problema de fatoração em números primos e o problema do logaritmo discreto [82]. Esses dois problemas são muito importantes pois alguns dos métodos criptográficos mais utilizados atualmente assumem que não há uma forma eficiente de resolvê-los. Portanto, existindo um computador quântico, estes métodos criptográficos seriam facilmente quebrados.

Outro algoritmo importante para computação quântica foi o algoritmo de buscas apresentado por Grover [51]. Procurar um elemento em uma base de dados não ordenada de n elementos necessita tempo $\Omega(n)$ no pior caso, no caso clássico. Grover apresentou um algoritmo quântico que realiza tal busca em tempo $O(\sqrt{n})$. Tal ganho não é exponencial, porém a aplicabilidade do resultado é muito importante, pois pode-se conseguir uma aceleração quadrática, portanto substancial, na solução de problemas da classe NP.

Nos anos 2000, novos algoritmos quânticos foram desenvolvidos, alguns utilizando os algoritmos anteriores como submódulos [39] [10] [54] [14] [87] [86], outros utilizando novas técnicas [13]. Foram descobertos também novos métodos para se encontrar limitantes quânticos para vários problemas [24] [20] [12], que mostram, por exemplo, que o Algoritmo de Grover é ótimo assintoticamente.

Na área de Complexidade Computacional, foram estendidos o estudo de diversos tópicos para o novo modelo, criando análogos quânticos para as principais classes de complexidade, desde as classes mais simples referentes a Algoritmos Quânticos [25], bem como às classes envolvendo o conceito de certificados e provas [6][88], complexidade de comunicação [33] ou de importância criptográfica [89] [91].

Paralelamente, outros modelos de computação mais simples foram estendidos para o modelo quântico, e hoje encontramos variantes de Autômatos Finitos Quânticos e Autômatos de Pilha Quânticos [73] [66] [11], e vários estudos sobre seu poder computacional e propriedades de linguagens aceitas por tais modelos [69] [80].

Mais recentemente, uma área de estudo que vem se desenvolvendo é utilizar argumentos quânticos na prova de teoremas puramente clássicos [62] [61] [43] [38]. Entretanto, ainda se busca um meio de generalizar essas técnicas, a fim de se criar um *framework* para que elas possam ser aplicadas a outros problemas de forma mais direta, criando um análogo quântico ao método probabilístico proposto por Erdös [8].

1.2 Revisão Bibliográfica

Iremos, nesta seção, descrever a bibliografia básica para uma introdução à Computação Quântica. As referências para os temas mais avançados desta dissertação serão apresentados nos capítulos correspondentes.

O livro de Yanofsky [93] é ideal como uma introdução do tema para cientistas da computação, pois utiliza uma linguagem bem voltada para esse meio, com recursos didáticos como exemplos e gráficos, para tópicos mais específicos de Matemática e Física. Entretanto, este livro aborda os temas de forma mais superficial.

Os livros de Kaye, Laflamme e Mosca [59], Mermin [71] e Hirvensalo [53] são mais concisos e focam na apresentação da Computação Quântica de uma maneira mais formal, porém ainda com um foco para cientistas de computação.

O livro de Nielsen e Chuang [74] é o livro mais completo sobre Computação Quântica, apresentando o tema sobre diversas perspectivas e é considerado em geral a bibliografia principal para a área.

Na língua portuguesa, encontramos os trabalhos de de Vignatti, Netto e Bittencourt [85] e Portugal, Lavor, Carvalho e Maculan [76] que apresentam uma introdução a Computação Quântica focando em Algoritmos Quânticos. O trabalho de Cardonha, Silva e Fernandes [29] além de apresentar os conteúdos básicos, também avança em alguns pontos de Computabilidade e Complexidade quânticas.

Capítulo 2

Fundamentos

Dado que a Computação Quântica é uma área multidisciplinar, são necessários conceitos de diferentes áreas para entender, mesmo que basicamente, como funcionam as engrenagens dos algoritmos quânticos, e para se ter uma ideia de como eles seriam implementados. Dado que este trabalho é endereçado a pessoas com conhecimento em Ciência da Computação, este capítulo tem como objetivo inicial introduzir os conceitos básicos de Mecânica Quântica e aplicá-los na apresentação do modelo computacional de Circuitos Quânticos.

Começaremos o capítulo mostrando um exemplo de experimento que demonstra a fragilidade da Física Clássica em explicar seu resultado, demonstrando a necessidade da criação de um novo modelo que pudesse prever corretamente os resultados de tais experimentos. Faremos, então, uma breve exposição da Notação de Dirac, o padrão adotado em Mecânica Quântica para representação de estados.

Seguiremos expondo e explicando os quatro postulados da Mecânica Quântica, sobre os quais estão baseados todos os conceitos de Computação Quântica. Iremos então, apresentar propriedades adicionais dos estados quânticos que possuem consequências diretas na sua utilização em processos computacionais.

Finalizaremos o capítulo apresentando o modelo de Circuitos Quânticos, que será utilizado largamente ao longo deste trabalho.

Assume-se aqui um conhecimento básico prévio de Álgebra Linear, que pode ser visto de modo mais detalhado no livro de Anton e Rorres [15], ou revisado de forma mais focada para o tema na Seção 2.1 de Nielsen e Chuang [74].

2.1 A insuficiência da Física Clássica

Como mencionado previamente, a Física Clássica se mostrou insuficiente para prever fenômenos verificados em laboratórios fazendo com que pesquisadores passassem a repensar seus princípios fundamentais. Iremos nesta seção apresentar um de tais experimentos.

O experimento em questão foi idealizado de forma independente pelos físicos Ludwig Mach [68] e Ludwig Zehnder [97], e é conhecido hoje como o Interferômetro de Mach-Zehnder.

Neste experimento são utilizados semi-espelhos, que estão representados na Figura 2.1. Nesta imagem, temos uma fonte emissora de fótons EF alinhada ao semi-espelho SE e dois detectores de fótons DF1 e DF2. O que se verifica na prática é que, em média, metade dos fótons emitidos é detectada por DF1 e a outra metade é detectada por DF2.

Mach e Zehnder, então, elaboraram um experimento cuja esquematização pode ser vista na Figura 2.2. Nele, no lugar dos detectores de fótons do experimento anterior, são acoplados os espelhos E1 e E2, que refletem totalmente em 90 graus os fótons que chegam até eles. No ponto em que os feixes de fótons se encontrariam, colocamos um segundo semi-espelho SE2 e só então são instalados os detectores de fótons DF1 e DF2.

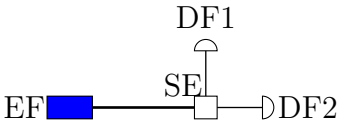


Figura 2.1: Funcionamento de um semi-espelho.

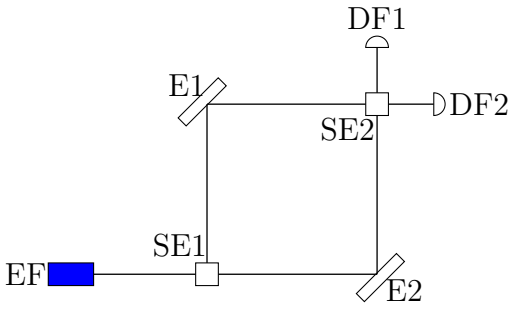


Figura 2.2: Experimento proposto por Mach e Zehnder

Aplicando os conceitos da Física Clássica a partir do funcionamento de um semi-espelho, o resultado esperado do experimento é mostrado na Figura 2.3a, onde as

larguras das linhas representam a intensidade dos feixes de elétrons. Nela, vemos que cada um dos feixes de fótons que chegam em SE2, se dividiria pela metade e ambos gerariam os feixes F3 e F4, cada um com em média metade dos fótons emitidos originalmente. Portanto, cada um dos detectores DF1 e DF2 captaria, em média, metade dos fótons emitidos por EF.

Entretanto, ao executar este experimento na prática, observou-se que todos os fótons emitidos por EF são detectados por DF2, como ilustrado na Figura 2.3b, contradizendo qualquer intuição sobre o resultado.

(a) Resultado esperado do experimento proposto por Mach e Zehnder

(b) Resultado verificado na prática do experimento proposto por Mach e Zehnder

Figura 2.3: Experimento do Inteferômetro de Mach-Zehnder

2.2 Postulados da Mecânica Quântica

Iremos nesta seção apresentar os postulados que regem a Mecânica Quântica, exemplificando seu funcionamento com os elementos da Computação Quântica.

Porém, antes de estudarmos os postulados em si, apresentaremos a Notação de Dirac, que é o meio mais comum em Mecânica Quântica para expressar os vetores que representam os estados de sistemas quânticos. Esta notação foi adotada também no estudo de Computação Quântica dadas as facilidades que ela incorpora.

Dado um espaço de Hilbert complexo $\mathcal{H}$ n-dimensional, representamos um vetor vetor em $\mathcal{H}$ como $|v\rangle$. Dado um vetor $|v\rangle = \begin{pmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{pmatrix}$ em $\mathcal{H}$, com $\alpha_i \in \mathbb{C}$, temos que seu dual é $|v\rangle^\dagger = \langle v| = \begin{pmatrix} \alpha_1^* & \cdots & \alpha_n^* \end{pmatrix}$, onde α_i^* é o conjugado complexo de α_i e $\dagger$ é a operação de transpor a matriz e conjugar seus elementos.

Neste mesmo contexto, denotamos o produto interno entre $|v_1\rangle = \begin{pmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{pmatrix}$ e $|v_2\rangle =$

$\begin{pmatrix} \beta_1 \\ \cdots \\ \beta_n \end{pmatrix}$ como

$$\langle v_1|v_2\rangle = \begin{pmatrix} \alpha_1^* & \cdots & \alpha_n^* \end{pmatrix} \begin{pmatrix} \beta_1 \\ \cdots \\ \beta_n \end{pmatrix} = \sum_{i=1}^{n} \alpha_i^* \beta_i.$$

Também aparecerá frequentemente, quando falamos de medições, a notação

$$|v_1\rangle\langle v_2| = \begin{pmatrix} \alpha_1 \\ \cdots \\ \alpha_n \end{pmatrix} \begin{pmatrix} \beta_1^* & \cdots & \beta_n^* \end{pmatrix} = \begin{pmatrix} \alpha_1\beta_1^* & \alpha_1\beta_2^* & \ldots & \alpha_1\beta_n \\ \alpha_2\beta_1^* & \alpha_2\beta_2^* & \ldots & \alpha_2\beta_n \\ & & \ldots & \\ \alpha_{n-1}\beta_1^* & \alpha_{n-1}\beta_2^* & \ldots & \alpha_{n-1}\beta_n \\ \alpha_n\beta_1^* & \alpha_n\beta_2^* & \ldots & \alpha_n\beta_n \end{pmatrix},$$

que consiste do produto matricial dos vetores $|v_1\rangle$ e $\langle v_2|$ resultando em uma matriz $n \times n$.

2.2.1 Princípio da sobreposição

Começamos o estudo da Mecânica Quântica enunciando seu primeiro postulado, que descreve a configuração dos estados de sistemas quânticos.

Postulado 1. *O estado de um sistema quântico é descrito por um vetor unitário em um espaço de Hilbert complexo $\mathcal{H}$.*

A Postulado 1 estabelece que ao trabalhar com um sistema quântico, estamos abstratamente trabalhando com vetores em um espaço vetorial. Neste trabalho, cometeremos o abuso de notação de referenciar um estado quântico pela sua representação vetorial no espaço de Hilbert correspondente de forma indistinta.

Iremos trabalhar somente com estados em sistemas finitos, e agora evidenciaremos algumas implicações diretas deste fato aliado ao Postulado 1. Dados um espaço de Hilbert complexo $\mathcal{H}$ de dimensão finita n e uma base ortonormal $\{|b_0\rangle, |b_1\rangle, ..., |b_{n-1}\rangle\}$ de $\mathcal{H}$, temos que um estado $|\psi\rangle$ neste espaço de Hilbert pode ser descrito por uma combinação linear dos elementos da base

$$|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |b_i\rangle.$$

Além disso, como pelo Postulado 1, $|\psi\rangle$ é unitário, temos que

$$\sum_{i=0}^{n-1} |\alpha_i|^2 = 1,$$

onde o valor α_i é conhecido como a *amplitude* referente ao estado $|b_i\rangle$.

Qubits

Estudaremos agora o principal sistema quântico utilizado na Computação Quântica, os *qubits*. Um *qubit* é um estado de um sistema quântico 2-dimensional, sendo descrito como um vetor unitário no espaço de Hilbert complexo 2-dimensional $\mathcal{B}$. Usualmente, ao descrever um estado em $\mathcal{B}$, utilizamos a base formada pelos vetores $|0\rangle \equiv \binom{1}{0}$ e $|1\rangle \equiv \binom{0}{1}$, sendo esta base conhecida como *base computacional*.

Pelo Postulado 1, o estado $|\psi\rangle$ de um *qubit* é uma superposição unitária de $|0\rangle$ e $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \text{onde } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1.$$

Uma consequência direta desta definição é que um *qubit* pode assumir um número infinito de estados, quando α e β variam.

2.2.2 Evolução dos estados

Dado que sabemos já, pelo primeiro postulado, como os sistemas quânticos se caracterizam, iremos ver agora como tais sistemas evoluem.

Postulado 2. *A evolução temporal dos estados de um sistema quântico fechado é descrita por um operador linear unitário.*

Em outras palavras, a Postulado 2 estabelece que para qualquer evolução de um sistema fechado que leva o estado quântico inicial $|\psi_1\rangle$ ao estado final $|\psi_2\rangle$, existe um operador linear unitário U tal que

$$|\psi_2\rangle = U|\psi_1\rangle.$$

Esta operação pode ser representada por uma matriz, e como a operação é unitária temos que

$$U^\dagger U = UU^\dagger = I$$

onde $U^\dagger$ é a matriz conjugada e transposta de U. Esta propriedade possui duas consequências importantes. Primeiramente, após aplicarmos um operador unitário sobre um vetor, sua norma se mantém. Portanto, o estado final também possuirá norma unitária como definido pelo Postulado 1. Além disso, todo operador unitário quântico é inversível, o que implica que as operações quânticas são reversíveis.

Iremos agora exemplificar um operador sobre *qubits*.

Exemplo Seja $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ um operador no espaço $\mathcal{B}$. H é um operador quântico válido, pois é linear, dado que é representado por uma matriz, e unitário, pois $H = H^\dagger$ e $HH = I$.

O funcionamento de H sobre os elementos da base computacional é

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

Este operador é conhecido como operador de Hadamard e funciona como uma moeda quântica, partindo de um estado base para uma superposição equiprovável dos dois elementos da base.

Ressaltamos que o funcionamento do semi-espelho do Interferômetro de Mach-Zehnder descrito na Seção 2.1 pode ser descrito como uma porta de Hadamard. ■

2.2.3 Medições

Em sistemas clássicos, pode-se, a qualquer momento, observar uma propriedade de um objeto, sem que isso tenha um efeito colateral. Entretanto, veremos agora que em sistemas quânticos o mesmo não ocorre.

Postulado 3. *Medições quânticas são descritas por um conjunto de operadores de medição $\{M_m\}$, que atuam no espaço do sistema sendo medido. Assumimos que o índice m é o resultado da medição.*

Se temos um sistema quântico no estado $|\psi\rangle$ e fazemos uma medição em relação a $\{M_m\}$, a probabilidade do resultado ser i é:

$$p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle,$$

e o estado do sistema quântico após a medição será

$$\frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}.$$

Além disso, o conjunto de operadores tem que satisfazer a equação de completude:

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

que garante que a soma das probabilidades seja 1*:*

$$\sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\left(\sum_m M_m^\dagger M_m\right)|\psi\rangle = 1.$$

Portanto, pelo Postulado 3, após realizar a medição, o estado quântico colapsa em um novo estado, alterando o sistema. Veremos agora um exemplo de medição sobre *qubits*.

Exemplo Dizemos que medimos um *qubit* na base computacional quando aplicamos a medição utilizando os operadores

$$M_0 = |0\rangle\langle 0| = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \text{ e } M_1 = |1\rangle\langle 1| = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Portanto, ao realizarmos a medição na base computacional de um *qubit*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ onde } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1,$$

temos como resultado o valor 0 com probabilidade $|\alpha|^2$, e o estado colapsa para $|0\rangle$, e o valor 1 com probabilidade $|\beta|^2$, e o estado colapsa para $|1\rangle$. ■

Podemos generalizar o conceito de medição usando uma base arbitrária de um sistema quântico n-dimensional $\{|b_0\rangle, ..., |b_{n-1}\rangle\}$, utilizando para isso os operadores de medição $\{|b_0\rangle\langle b_0|, ..., |b_{n-1}\rangle\langle b_{n-1}|\}$.

Outras formas de medição

Utilizamos, no Postulado 3 o que chamamos de medições gerais. Existem, entretanto, outras formas alternativas e equivalentes de definir as medições, que facilitam a visualização de algumas propriedades dependendo do contexto em que são utilizadas.

Medição Projetiva Uma medição projetiva é descrita por um observável, que é um operador Hermitiano[1] que opera no espaço vetorial do sistema a ser observado. Um resultado de Teoria de Matrizes é que se uma matriz é Hermitiana, então seus autovalores são reais.

[1]Um operador linear A é Hermitiano quando seu conjugado transposto é igual ao próprio A, ou seja $A = A^\dagger$.

Seja n o posto da matriz Hermitiana M que representa o operador, seus autovalores $\lambda_1, ..., \lambda_n$ e respectivos autovetores $|\phi_1\rangle, ..., |\phi_n\rangle$. Temos então que $M = \sum_{i=1}^{n} \lambda_i |\phi_i\rangle\langle\phi_i|$.

Se realizamos a medição do estado quântico $|\psi\rangle$ com respeito a M, temos como resultado o autovalor λ_i com probabilidade $p_i = \langle\psi|\phi_i\rangle\langle\phi_i|\psi\rangle$ e após a medição o sistema colapsa para o estado $\frac{|\phi_i\rangle\langle\phi_i||\psi\rangle}{\sqrt{p_i}}$.

Intuitivamente, se escrevermos $|\psi\rangle$ utilizando como base os autovetores de M, $|\psi\rangle = \alpha_1|\phi_1\rangle + ... + \alpha_n|\phi_n\rangle$, a probabilidade do resultado ser λ_i é $|\alpha_i|^2$.

Alternativamente, podemos cometer um abuso de notação e descrever medições projetivas através conjunto de projetores.

POVMs POVMs (*Positive Operator-Valued Measure*) são amplamente utilizados quando não há interesse no estado do sistema após a medição, mas somente no resultado da medição e sua respectiva distribuição de probabilidade.

Neste tipo de medição, existe um conjunto de elementos POVM $\{E_m\}$, sendo que as únicas restrições sobre eles são que os operadores devem ser positivos[2] e que $\sum_m E_m = I$. Neste caso, a probabilidade do resultado de uma medição sobre o estado quântico $|\psi\rangle$ ser i é $\langle\psi|E_i|\psi\rangle$.

Distinguindo estados

Veremos agora um resultado que implica que, apesar de um sistema quântico possuir um número infinito de estados, não é possível distinguir dois estados quaisquer com um número finito de medições.

Teorema 2.2.1. *Dados dois estados quânticos $|\psi_1\rangle$ e $|\psi_2\rangle$, distintos e não ortogonais, não é possível distigui-los com erro* 0*.*

Demonstração. Iremos efetuar a prova deste teorema por contradição. Suponhamos então que tal medição exista com os operadores de medição M_1 e M_2 tal que

$$\langle\psi_1|M_1^\dagger M_1|\psi_1\rangle = 1 \text{ e } \langle\psi_2|M_2^\dagger M_2|\psi_2\rangle = 1.$$

Como $\sum_{i\in\{1,2\}} M_i^\dagger M_i = I$, temos que

$$\sum_{i\in\{1,2\}} \langle\psi_1|M_i^\dagger M_i|\psi_1\rangle = 1 = \langle\psi_1|M_1^\dagger M_1|\psi_1\rangle = 1,$$

[2]Um operador é dito positivo quando todos seus autovalores são positivos

e, portanto $\langle\psi_1|M_2^\dagger M_2|\psi_1\rangle = 0$.

Vamos agora decompor $|\psi_2\rangle$ em relação $|\psi_1\rangle$ e $|\psi_1^\perp\rangle$, onde $|\psi_1^\perp\rangle$ é algum vetor unitário ortogonal a $|\psi_1\rangle$ tal que

$$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_1^\perp\rangle, \text{ para } \alpha, \beta \in \mathbb{C}, |\alpha|, |\beta| > 0 \text{ e } |\alpha|^2 + |\beta|^2 = 1.$$

Temos então que

$$\begin{aligned}
&\langle\psi_2|M_2^\dagger M_2|\psi_2\rangle \\
&= |\alpha|^2\langle\psi_1|M_2^\dagger M_2|\psi_1\rangle + |\beta|^2\langle\psi_1^\perp|M_2^\dagger M_2|\psi_1^\perp\rangle \\
&= |\beta|^2\langle\psi_1^\perp|M_2^\dagger M_2|\psi_1^\perp\rangle \\
&\leq |\beta^2| < 1,
\end{aligned}$$

o que é uma contradição. □

Fase global

Sejam dois estados quânticos $|\psi\rangle$ e $e^{i\theta}|\psi\rangle$. Dizemos que $|\psi\rangle$ é igual $e^{i\theta}|\psi\rangle$ em relação a uma fase global $e^{i\theta}$. Apesar de serem distintos, sob ponto de vista dos resultados da medição e suas respectivas probabilidades, temos que estes dois estados quânticos possuem a mesma distribuição estatística. Isso decorre do fato de que

$$\langle\psi|e^{-i\theta}M_m^* M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^* M_m|\psi\rangle.$$

2.2.4 Sistemas compostos

Veremos agora o último postulado da Mecânica Quântica, que descreve o comportamento da combinação de dois sistemas quânticos. Porém, antes de apresentarmos o postulado em si, iremos revisar o conceito de produto tensorial, ou produto de Kronecker, entre dois espaços vetoriais e entre duas matrizes.

Definição 2.2.2. *Sejam $\mathcal{H}_1$ um espaço vetorial n-dimensional e $\mathcal{H}_2$ um espaço vetorial m-dimensional. O produto tensorial $\mathcal{H}_1 \otimes \mathcal{H}_2$ é um espaço vetorial mn-dimensional.*

Definição 2.2.3. *Sejam*

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \dots & \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ & \dots & \\ b_{m1} & \dots & b_{mm} \end{pmatrix}$$

duas matrizes. Temos que o produto tensorial $A \otimes B$ entre elas é

$$A \otimes B = \begin{pmatrix} a_{11}B & ... & a_{1n}B \\ & ... & \\ a_{n1}B & ... & a_{nn}B \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & ... & a_{11}b_{1m} & a_{12}b_{11} & ... & a_{1n}b_{1m} \\ a_{11}b_{21} & a_{11}b_{22} & ... & a_{11}b_{2m} & a_{12}b_{21} & ... & a_{1n}b_{2m} \\ & & & ... & & & \\ a_{11}b_{m1} & a_{11}b_{m2} & ... & a_{11}b_{mm} & a_{12}b_{m1} & ... & a_{1n}b_{mm} \\ a_{21}b_{11} & a_{21}b_{12} & ... & a_{21}b_{1m} & a_{22}b_{11} & ... & a_{2n}b_{1m} \\ & & & ... & & & \\ a_{n1}b_{m1} & a_{n1}b_{m2} & ... & a_{n1}b_{mm} & a_{n2}b_{m1} & ... & a_{nn}b_{mm} \end{pmatrix}$$

Iremos agora, apresentar o quarto postulado da Mecânica Quântica.

Postulado 4. *Sejam dois sistemas quânticos independentes, representados pelos espaços de Hilbert $\mathcal{H}_1$ e $\mathcal{H}_2$. O estado de sistema quântico obtido na combinação desses dois sistemas é um vetor unitário no espaço de Hilbert formado pelo produto tensorial $\mathcal{H}_1 \otimes \mathcal{H}_2$. Se o primeiro sistema está no estado $|\psi_1\rangle$ e o segundo no estado $|\psi_2\rangle$, o estado do sistema composto será $|\psi_1\rangle \otimes |\psi_2\rangle$.*

Na representação de estados quânticos, as notações $|\psi_1\rangle \otimes |\psi_2\rangle$, $|\psi_1\rangle|\psi_2\rangle$, $|\psi_1, \psi_2\rangle$ e $|\psi_1\psi_2\rangle$ são utilizadas indistintamente, conforme o contexto mais apropriado.

O produto tensorial entre n cópias do espaço de Hilbert $\mathcal{H}$ é denotado $\mathcal{H}^{\otimes n}$ e o estado neste espaço correspondente a n cópias do estado $|\psi\rangle$ é denotado $|\psi\rangle^{\otimes n}$.

É importante ressaltar também que operadores unitários para sistemas compostos podem ser descritos também a partir dos operadores unitários dos subsistemas que o compõe.

Lema 2.2.4. *Seja um operador unitário A no espaço de Hilbert $\mathcal{H}_1$ n-dimensional e um operador unitário B no espaço de Hilbert $\mathcal{H}_2$ m-dimensional. Então $A \otimes B$ é um operador no espaço de Hilbert $\mathcal{H}_1 \otimes \mathcal{H}_2$, mn-dimensional.*

Demonstração. Pela definição do produto tensorial, temos que $A \otimes B$ é mn-dimensional. Agora basta provar que a matriz conjugada transposta de $A \otimes B$ é unitária.

Pela Definição 2.2.3, temos que

$$A \otimes B = \begin{pmatrix} a_{11}B & ... & a_{1n}B \\ & ... & \\ a_{n1}B & ... & a_{nn}B \end{pmatrix} \text{ e } (A \otimes B)^\dagger = \begin{pmatrix} a_{11}^* aB^\dagger & ... & a_{n1}^* B^\dagger \\ & ... & \\ a_{1n}^* B^\dagger & ... & a_{nn}^* B^\dagger \end{pmatrix}.$$

Portanto, temos que

$$\begin{aligned}(A \otimes B)(A \otimes B)^\dagger &= \begin{pmatrix} \sum_{i=1}^n a_{1i}a_{i1}^* BB^\dagger & ... & \sum_{i=1}^n a_{1i}a_{in}^* BB^\dagger \\ & ... & \\ \sum_{i=1}^n a_{ni}a_{i1}^* BB^\dagger & ... & \sum_{i=1}^n a_{ni}a_{in}^* BB^\dagger \end{pmatrix} \\ &= \begin{pmatrix} 1I & ... & 0I \\ & ... & \\ 0I & ... & 1I \end{pmatrix} \\ &= I_{nm},\end{aligned}$$

dado que $AA^\dagger = I_n$ e $BB^\dagger = I_m$.

A prova de que $(A \otimes B)^\dagger(A \otimes B) = I$ é simétrica ao caso anterior. □

Registradores quântico

Inspirado no Postulado 4, podemos fazer a composição de n *qubits*, obtendo um registrador quântico, que é representado por um vetor no espaço de *Hilbert* 2^n-dimensional $\mathcal{B}^{\otimes n}$. A base computacional para tal registrador possui 2^n elementos, representadas por

$$|00....00\rangle = \begin{pmatrix} 1 \\ 0 \\ ... \\ 0 \\ 0 \end{pmatrix}, |00...01\rangle = \begin{pmatrix} 0 \\ 1 \\ ... \\ 0 \\ 0 \end{pmatrix}, ..., |11...10\rangle = \begin{pmatrix} 0 \\ 0 \\ ... \\ 1 \\ 0 \end{pmatrix} \text{ e } |11...11\rangle = \begin{pmatrix} 0 \\ 0 \\ ... \\ 0 \\ 1 \end{pmatrix}.$$

Utilizaremos indistintamente a notação $|i\rangle$ para $i \in \{0,1\}^n$, uma cadeia binária com n bits, e $|i\rangle$ para $i \in \mathbb{N}$, e neste caso consideramos a representação binária de i com o número de bits correspondente ao contexto utilizado.

Os estados de um registrador quântico são formados por superposições dos 2^n estados da base e, da mesma forma que no caso de um único *qubit*, cada elemento da base computacional possui uma amplitude complexa, sendo que a norma do vetor deverá ser unitária. Podemos resumir essas informações em

$$|\psi\rangle = \sum_{i \in \{0,1\}^n} a_i |i\rangle, \quad \text{onde } a_i \in \mathbb{C}, i \in \{0,1\}^n, \text{ e } \sum_{i \in \{0,1\}^n} |a_i|^2 = 1.$$

Podemos observar que numa abordagem mais direta para simular um sistema quântico classicamente, seria necessário armazenar o valor da amplitude de cada elemento da base. Com isso, a quantidade de memória necessária cresce exponencialmente em relação ao número de *qubits* no sistema. Por esse motivo, suspeita-se que sistemas quânticos não podem ser representados em computadores clássicos sem incorrer em um custo computacional exponencial [42].

Sistemas emaranhados

Verificamos, pelo Postulado 4, que podemos formar sistemas quânticos a partir da composição de outros dois sistemas quânticos menores. Veremos agora que dado um estado quântico maior, nem sempre conseguimos fatorá-lo em estados menores independentes. Tais estados são chamados de estados emaranhados.

Exemplo Seja um sistema quântico composto por dois *qubits*. Ele pode ser definido genericamente como $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle, \alpha_i \in \mathbb{C}, \sum |\alpha_i|^2 = 1$. Para fatorar esse sistema em dois *qubits* independentes $|\gamma\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ e $|\gamma'\rangle = \beta'_0|0\rangle + \beta'_1|1\rangle$, temos que encontrar os valores de $\beta_0, \beta_1, \beta'_0$ e β'_1, respeitando

$$\begin{cases} \beta_0\beta'_0 = \alpha_0 \\ \beta_0\beta'_1 = \alpha_1 \\ \beta_1\beta'_0 = \alpha_2 \\ \beta_1\beta'_1 = \alpha_3 \end{cases}$$

Entretanto, ao tentar fatorar $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, temos que resolver o seguinte sistema

$$\begin{cases} \beta_0\beta'_0 = 1 \\ \beta_0\beta'_1 = 0 \\ \beta_1\beta'_0 = 0 \\ \beta_1\beta'_1 = 1 \end{cases}$$

o que não é possível, pois todos os valores deverão ser não nulos para garantir a primeira e última equações, entretanto para que a segunda e terceira equações sejam satisfeitas, pelo menos dois dos valores terão que ser nulos ■

Iremos agora definir uma das bases para sistemas quânticos com 2 *qubits* mais utilizadas após a base computacional: a base de Bell.

Definição 2.2.5 (Base de Bell)**.** *A Base de Bell para o espaço $\mathcal{B}^{\otimes 2}$ é formada pelos quatro elementos:*

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

.

Cada estado da Base de Bell pode ser chamado de um estado de Bell e um par de *qubits* em um estado de Bell é chamado de um par EPR[3].

2.3 Estados mistos

O conceito que vimos até agora de estados quânticos é perfeitamente adequado enquanto estudamos um sistema quântico isolado como um todo. Estes estados, que satisfazem o Postulado 1 completamente, são chamados de estados puros. Veremos agora que quando lidamos parcialmente com um sistema quântico ou com uma distribuição probabilística de estados quânticos, surgem os chamados estados mistos.

Definição 2.3.1. *Um estado misto é o resultado de uma distribuição probabilística de estados puros*

$$\{(p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), ..., (p_k, |\psi_k\rangle)\},$$

com $\sum_i p_i = 1$. Neste caso, o estado do sistema é $|\psi_i\rangle$ com probabilidade p_i.

Teremos, entretanto, que fazer adaptações nos conceitos estudados até agora para operarmos com esse outro tipo de estados. Começaremos apresentando a ferramenta matemática necessária para representá-los e, em seguida, revisaremos os conceitos de operadores unitários e medições para estes estados. Terminaremos a seção mostrando estados reduzidos e sua purificação.

[3]O nome EPR vem de seus idealizadores Albert Einstein, Boris Podolsky e Nathan Rosen que o propuseram [40] como um suposto paradoxo da Mecânica Quântica.

2.3.1 Matriz de densidade

A representação de Dirac é muito útil quando estamos lidando com estados puros. Porém, ao estudarmos estados mistos, esta notação não consegue capturar toda a informação do sistema. Iremos estudar agora uma forma alternativa de representar estados quânticos, que será primordial para o estudo de estados mistos.

Definição 2.3.2. *Dado um estado quântico puro $|\psi\rangle$, temos que sua matriz de densidade é $\rho = |\psi\rangle\langle\psi|$.*

Exemplo Vamos agora calcular a matriz de densidade do estado de Bell $|\Psi^+\rangle$:

$$\begin{aligned}
|\Psi^+\rangle\langle\Psi^+| &= \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)\left(\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|\right) \\
&= \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
&= \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix}
\end{aligned}$$

■

Agora, estenderemos a definição para os estados mistos.

Definição 2.3.3. *Dado um estado quântico misto*

$$\{(p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), ..., (p_k, |\psi_k\rangle)\},$$

sua matriz de densidade ρ é

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Para finalizar, iremos caracterizar as matrizes de densidades válidas, i.e., as matrizes de densidade que representam um estado quântico misto válido.

Teorema 2.3.4. *Uma matriz de densidade ρ corresponde a um estado misto se e somente se $Tr(\rho) = 1$ [4] e ρ é um operador positivo [5].*

[4] *O operador de traço Tr, da álgebra linear, corresponde à soma dos elementos da diagonal principal da matriz.*

[5] *Operadores são chamados positivos se e somente se todos seus autovalores forem positivos.*

Demonstração. Se $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ para algum conjunto $\{(p_i, |\psi_i\rangle)\}$, temos que

$$Tr(\rho) = Tr\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i Tr(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1,$$

e para todo vetor $|\phi\rangle$ no espaço vetorial, temos

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0.$$

Seja agora ρ um operador positivo tal que $Tr(\rho) = 1$. Seja $\rho = \sum_i \lambda_i |\phi_i\rangle$ a decomposição espectral de ρ. Como ρ é um operador positivo, seus autovalores λ_i são todos positivos, e seus autovetores $|\phi_i\rangle$ estão normalizados. Como ρ tem traço unitário, temos que $\sum_i \lambda_i = 1$. Portanto, a distribuição $\{(\lambda_i, |\phi_i\rangle)\}$ representa um estado quântico misto válido e sua matriz de densidade é ρ. □

2.3.2 Transformações unitárias, medições e estados compostos

Veremos agora como transformações unitárias, medições e composição de estados atuam sobre as matrizes de densidades dos estados mistos.

Calculemos a matriz de densidade do estado misto resultante da aplicação do operador unitário U sobre o estado misto $\{(p_i, |\psi_i\rangle)\}$, cuja matriz de densidade é ρ. Teremos como resultado um estado misto cuja distribuição probabilística de estados é $\{(p_i, U|\psi_i\rangle)\}$:

$$\sum_i p_i U^\dagger |\psi\rangle\langle\psi| U = U^\dagger \left(\sum_i p_i |\psi\rangle\langle\psi|\right) U = U^\dagger \rho U.$$

Para a medição de um estado misto com matriz de densidade ρ considerando os operadores de medição $\{M_m\}$, temos que a probabilidade do resultado da medição ser o valor i é de

$$Tr(M_i^\dagger M_i \rho),$$

e neste caso o estado do sistema após a medição colapsa para

$$\frac{M_i \rho M_i^\dagger}{Tr(M_i^\dagger M_i \rho)}.$$

Para a composição de dois estados mistos ρ_1 e ρ_2, o estado misto resultante terá matriz de densidade $\rho_1 \otimes \rho_2$.

2.3.3 Traço parcial e estado reduzido

Veremos agora que estados mistos aparecem mesmo em contextos nos quais o sistema como um todo é um estado puro. Em particular, quando consideramos somente uma parte de um estado emaranhado, o estado parcial é um estado misto.

Definição 2.3.5. *Seja ρ^{AB} a matriz de densidade de um estado no espaço formado pela composição sistemas quânticos A e B. O estado reduzido de ρ^{AB} em relação à A é o componente do estado original referente somente ao sistema A.*

Para calcular o valor deste sistema reduzido, utilizaremos o conceito matemático de traço parcial.

Definição 2.3.6. *Dados os sistemas quânticos A e B e os estado $|a_0\rangle, |a_1\rangle \in A$ e $|b_0\rangle, |b_1\rangle \in B$, temos que o traço parcial é definido como*

$$Tr_B(|a_0\rangle\langle a_1| \otimes |b_0\rangle\langle b_1|) = |a_0\rangle\langle a_1||Tr(|b_0\rangle\langle b_1|)|.$$

Exemplo Sejam B_1 e B_2 os sistemas referentes ao primeiro e segundo *qubit*, respectivamente, do estado $|\Psi^+\rangle$. Vamos agora calcular o estado reduzido do primeiro *qubit* desse sistema quântico.

$$\begin{aligned}
&Tr_{B_1}(|\Psi^+\rangle\langle\Psi^+|) \\
&= Tr_{B_1}\left(\frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)\right) \\
&= \frac{1}{2}\left(|0\rangle\langle 0|Tr(|0\rangle\langle 0|) + |0\rangle\langle 1|Tr(|0\rangle\langle 1|) + |1\rangle\langle 0|Tr(|1\rangle\langle 0|) + |1\rangle\langle 1|Tr(|1\rangle\langle 1|)\right) \\
&= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\
&= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \\
&= \frac{1}{2}I.
\end{aligned}$$

Este estado é chamado de estado totalmente misto ou estado completamente misto. ■

Purificação

Provaremos agora um resultado que mostra que para todo sistema quântico A no estado misto ρ^A, existe um sistema de referência R tal que o estado global do sistema ρ^{AR} é puro. Dizemos que, neste caso, ρ^{AR} é a purificação de ρ^A.

Teorema 2.3.7. *Seja $\rho^A = \sum_i p_i |i^A\rangle\langle i^A|$, para uma base $\{|i^A\rangle\}$ de um sistema quântico A. Então existem um sistema de referência R e um estado puro ρ^{AR} no sistema AR tal que $tr_R(\rho^{AR}) = \rho^A$.*

Demonstração. Seja o sistema de referência R igual ao sistema A, com uma base ortonormal $\{|i^R\rangle\}$, e seja

$$\rho^{AR} = \sum_i \sqrt{p_i}|i^A\rangle|i^R\rangle.$$

Vamos agora calcular o estado parcial do subsistema A em ρ^{AR}:

$$\begin{aligned} Tr_R(|\rho^{AR}\rangle\langle\rho^{AR}|) &= \sum_{i,j} \sqrt{p_i p_j}|i^A\rangle\langle j^A|Tr(|i^R\rangle\langle j^R|) \\ &= \sum_{i=j} \sqrt{p_i p_j}|i^A\rangle\langle j^A| \\ &= \sum_i p_i |i^A\rangle\langle i^A| \\ &= \rho^A, \end{aligned}$$

e a segunda igualdade vem do fato que $Tr(|i\rangle\langle i|) = 1$ e $Tr(|i\rangle\langle j|) = 0$ para $|i\rangle$ e $|j\rangle$ ortogonais. □

Provamos então que é possível assumir que toda matriz de densidade é o estado parcial de um sistema quântico puro.

2.4 Teorema da não clonagem

Outra característica muito comum no modelo clássico é a clonagem (ou cópia) em que, dado um estado em um sistema S é possível reproduzi-lo em um sistema equivalente S'. Mostraremos nesta seção que no modelo quântico é impossível que haja uma operação que, dado um estado quântico, o copie.

Teorema 2.4.1. *Seja $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ um estado quântico de um qubit, desconhecido. Não existe uma operação unitária U tal que $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ para todo $|\psi\rangle$.*

Demonstração. Vamos provar por contradição que tal operação unitária U não existe. Suponhamos então que U exista e sejam $|\phi\rangle$ e $|\psi\rangle$ dois estados ortogonais em $\mathcal{B}$ e

$$|x\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle).$$

Segue-se, pela definição de U que

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \text{ e } U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle.$$

Temos que

$$\begin{aligned} U|x\rangle|0\rangle &= |x\rangle|x\rangle \\ &= \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle) \otimes \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle) \\ &= \frac{1}{2}(|\phi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle + |\psi\rangle|\psi\rangle). \end{aligned}$$

Por outro lado temos que

$$\begin{aligned} U|x\rangle|0\rangle &= U(\frac{1}{\sqrt{2}}(|\phi\rangle|0\rangle + |\psi\rangle|0\rangle)) \\ &= \frac{1}{\sqrt{2}}(U|\phi\rangle|0\rangle + U|\psi\rangle|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|\phi\rangle|\phi\rangle + |\psi\rangle|\psi\rangle). \end{aligned}$$

Como $|\psi\rangle$ e $|\phi\rangle$ são ortogonais, os vetores $|\phi\rangle|\phi\rangle$, $|\phi\rangle|\psi\rangle$, $|\psi\rangle|\phi\rangle$ e $|\psi\rangle|\psi\rangle$ formam uma base desse espaço vetorial e o estado $U|x\rangle|0\rangle$ foi escrito de duas formas distintas como combinação linear dessa base, o que gera uma contradição. □

Este fato tem consequências diretas na Computação e Informação Quânticas, dado que muitos resultados clássicos dependem de copiar o conteúdo de um valor para alterá-lo, o que, no caso quântico, se torna impossível.

2.5 Circuitos quânticos

Será apresentado nesta seção, o modelo que utilizaremos para descrever Algoritmos Quânticos, os Circuitos Quânticos.

O primeiro modelo de máquina quântica definido foi o modelo de Máquinas de Turing Quânticas, proposto inicialmente por Deutsch[34]. Bernstein e Vazirani ampliaram o estudo, demonstrando a existência de uma Máquina de Turing Quântica Universal eficiente capaz de simular qualquer outra Máquina de Turing Quântica [25].

Paralelamente aos estudos deste modelo, Deutsch propôs também o modelo de Circuitos Quânticos, baseado no modelo de circuitos booleanos [35]. Yao promoveu avanços estudando a complexidade de tais circuitos [95] e posteriormente provou o que o modelo de Circuitos Quânticos e Máquinas de Turing Quânticas são equivalentes [94].

Como o modelo de Máquinas de Turing Quânticas é demasiadamente teórico e não-intuitivo, quase todo o trabalho envolvendo algoritmos e complexidade quânticos são desenvolvidos sobre o modelos de circuitos, e portanto, será este modelo que iremos apresentar.

Uma introdução sobre o modelo de Máquinas de Turing Quânticas pode ser encontrada no artigo original de Bernstein e Vazirani [25] ou no trabalho de Cardonha, Silva e Fernandes [29], este último em português.

Começaremos e estudo estudando as principais portas quânticas que iremos utilizar nos Algoritmos e Autômatos Quânticos. Finalmente apresentamos a notação utilizada para representar graficamente os Circuitos Quânticos e apresentaremos dois circuitos que serão utilizados nas provas de alguns resultados.

2.5.1 Portas quânticas

Vimos no Postulado 2 da Mecânica Quântica que estados quânticos evoluem através de operações unitárias. Entretanto, ao definir um modelo computacional quântico, devemos restringir quais são as operações que servirão como base para construção de outras. Caso contrário, encontraremos casos patológicos de transformações unitárias que resolvem problemas complexos de forma não factível.

Em Circuitos Clássicos, são utilizadas portas lógicas para manipular n bits de entrada e computar uma saída de m bits, como por exemplo as portas **AND** e **OR**. Porém, como as operações quânticas são reversíveis, a entrada e saída de uma porta

quântica devem ter o mesmo número de *qubits*.

A reversibilidade das portas quânticas pode parecer, em um primeiro momento, restritiva, dado que portas lógicas usuais, como as portas lógicas **AND** e **OR**, não são reversíveis [6]. Porém sabe-se que operações irreversíveis podem ser simuladas em portas quânticas, utilizando uma quantidade polinomial de *qubits* adicionais [23] [67].

Serão mostradas agora algumas portas quânticas importantes e de uso recorrente em Computação Quântica.

Operadores de Pauli. Três portas de 1 *qubit* muito comuns em circuitos quânticos são os operadores de Pauli:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ e } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

A porta **I** é a operação identidade, que não altera a configuração do estado quântico. A porta **X** é o *bit flip* quântico, invertendo as amplitudes dos elementos da base computacional $|0\rangle$ e $|1\rangle$. As portas **Y** e **Z** possuem usos mais específicos e aplicam uma fase relativa entre os elementos da base computacional.

Porta de Hadamard. Como visto no Exemplo 2.2.2, a porta de Hadamard é uma porta de um *qubit* e pode ser representada pela seguinte matriz unitária:

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

Para registradores quânticos com mais *qubits*, pode-se aplicar a porta de Hadamard a cada um dos bits individualmente. Isto produz o mesmo efeito que a porta de Walsh-Hadamard, representada pela matriz W_n, onde o valor da linha i e coluna j é:

$$W_n(i,j) = (-1)^{i \cdot j} \frac{1}{\sqrt{2^n}}.$$

onde $i \cdot j$ denota o produto interno das representações binárias de i e j, modulo 2: *i.e.* $i \cdot j = i_0 j_0 \oplus i_1 j_1 \oplus ... \oplus i_{n-2} j_{n-2} \oplus i_{n-1} j_{n-1}$. Portanto, com a porta de Walsh-Hadamard, é possível gerar uma sobreposição equiprovável de todos os elementos

[6] Basta reparar que se a saída de uma porta **AND** for 0, não é possível identificar os valores de entrada.

da base computacional, ou seja, todas as amplitudes terão a mesma norma. Como veremos no próximo capítulo, esta superposição é muito útil para, por exemplo, computar o valor de uma função em todos os pontos da base computacional de forma balanceada.

Swap. A porta *Swap*, representada por **S**, opera sobre dois registradores quânticos de mesmo tamanho, invertendo seu conteúdo:

$$S|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle.$$

Portas controladas. Uma porta U-controlada é uma porta quântica que tem como entrada x bits controladores e y bits alvos. Se algum bit controlador for $|0\rangle$, os valores dos bits alvos permanecem inalterados. Caso o valor de todos os bits controladores sejam $|1\rangle$, a porta quântica U atua sobre os bits alvos.

Exemplo Seja $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ uma transformação unitária sobre um *qubit*. Podemos criar uma porta controlada $c(U)$ com um *qubits* de controle, que aplica U no *qubit* alvo quando o bit controlador for $|1\rangle$. Podemos representar $c(U)$ com:

$$c(U) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}.$$

■

Porta de Toffoli. A Porta de Toffoli ou a porta **CCNOT** é uma porta controlada de 3 *qubits* sendo os 2 primeiros os *qubits* controladores. Quando ambos tiverem o valor $|1\rangle$, o valor do terceiro *qubit* é invertido.

A Porta de Toffoli pode ser representada pelo mapeamento

$$|a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|b\rangle|c \oplus ab\rangle.$$

A Porta de Toffoli é universal na computação clássica, ou seja, qualquer circuito clássico pode ser implementado utilizando somente portas de Toffoli [44]. Como a

porta de Toffoli também é quântica, sabemos que todos os circuitos clássicos podem ser simulados em computadores quânticos.

Oráculos Oráculos, também conhecidos como "caixas-pretas", são operadores lineares unitários que calculam uma função característica arbitrária, porém desconhecida.

Dada uma função $f(x) : \{0,1\}^n \to \{0,1\}$, o oráculo U_f possui o seguinte comportamento:

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle,$$

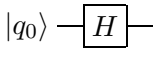
onde x é um registrador de n *qubits* e y é um único *qubit*.

Oráculos são amplamente utilizados em algoritmos quânticos voltados para problemas de busca ou problemas de se extrair informações de funções desconhecidas, além de serem a base da teoria de Complexidade de Consulta e Teste de Propriedades.

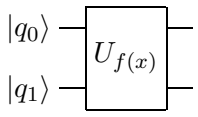
2.5.2 Circuitos quânticos

Finalmente, descreveremos a notação gráfica que reúne os elementos estudados até agora a fim de descrever processos computacionais capazes de resolver problemas. Ressaltamos que, quando conveniente, um circuito quântico será descrito em pseudocódigo.

A maioria das portas quânticas são representadas por retângulos com seu símbolo no interior. Veja o exemplo da porta de Hadamard na Figura 2.4a e um oráculo para a função f na Figura 2.4b



(a) Circuito quântico com um *qubit*, no qual é aplicado a porta de Hadamard.



(b) Circuito quântico com dois *qubits*, sobre o qual é aplicada uma consulta ao oráculo $U_f(x)$.

Figura 2.4: Exemplo de portas

Algumas portas específicas possuem uma representação simplificada. Por exemplo, a porta **CNOT** é normalmente representada como na Figura 2.5 e portas controladas são representadas como na Figura 2.6

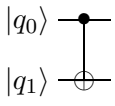


Figura 2.5: Porta **CNOT**, sendo o $|q_0\rangle$ o *qubit* controlador.

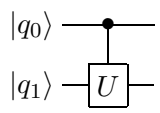
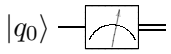
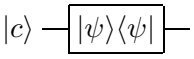


Figura 2.6: Porta controlada.

Finalmente, medições são representadas como na Figura 2.7. Na Figura 2.7a não especificamos os operadores de medições ou projetores. Na Figura 2.7b especificamos um projetor que define o subespaço de aceitação do circuito.



(a) Medição sobre um *qubit*.



(b) Medição sobre um *qubit* utilizando o projetor de aceitação $|\psi\rangle\langle\psi|$.

Figura 2.7: Representações de medições

2.5.3 Transformada Quântica de Fourier

Apresentaremos agora a porta quântica para a Transformada Quântica de Fourier (TQF). Esta porta quântica está destacada das outras devido a sua enorme importância, sendo fundamental nos principais algoritmos quânticos que apresentam ganhos exponenciais de complexidade. Iniciaremos discutindo o funcionamento desta porta quântica. Em seguida, apresentaremos o circuito que a implementa e finalizaremos com algumas de suas propriedades.

Funcionamento

Intuitivamente, a Transformada Discreta de Fourier (TDF) converte uma amostra de n valores $x_1, ..., x_n$ de um domínio original, em geral temporal, para um domínio de frequências. A TDF possui diversas aplicações nas mais variadas áreas de estudo,

sendo algumas delas análise de sinais, compressão de dados e até no projeto de algoritmos. Classicamente, é possível calcular a TDF em tempo $O(n \log n)$ utilizando o algoritmo da Transformada Rápida de Fourier.

A Transformada Quântica de Fourier efetua a mesma transformação que a transformada discreta, mas é aplicada sobre estados quânticos, alterando a amplitude dos mesmos. Podemos definir a Transformada Quântica de Fourier sobre uma base ortonormal $|0\rangle, ..., |N-1\rangle$ como

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle. \tag{2.1}$$

De forma distinta da TDF, os valores após aplicar a TQF não são acessíveis, dado que estão codificados nas amplitudes dos elementos das bases, e portanto não é possível obtê-los através de medições. Com isso, as aplicação da TQF são distintas da TDF, e veremos algumas delas em algoritmos quânticos no próximo capítulo.

Circuito

Seja $N = 2^n$. Podemos reescrever a transformação da Equação 2.1 através da seguinte notação matricial:

$$QFT_N = \begin{bmatrix} 1 & 1 & 1 & ... & 1 & 1 \\ 1 & \omega & \omega^2 & ... & \omega^{N-2} & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & ... & \omega^{2(N-2)} & \omega^{2(N-1)} \\ & & & ... & & \\ 1 & \omega^j & \omega^2 j & ... & \omega^{j(N-2)} & \omega^{j(N-1)} \\ & & & ... & & \\ 1 & \omega^{(N-1)} & \omega^{2(N-1)} & ... & \omega^{(N-1)(N-2)} & \omega^{(N-1)^2} \end{bmatrix},$$

onde ω é a N-ésima raiz complexa da unidade[7]. Pode-se facilmente verificar que a matriz conjugada transposta de $\mathbf{QFT}_N$ é também sua inversa, resultando que $\mathbf{QFT}_N$ é unitária, e portanto uma porta quântica válida. Entretanto, mostraremos aqui que é possível realizar esta transformação utilizando portas quânticas mais simples. Iniciaremos essa demonstração, fatorando a Equação 2.1:

[7] A N-ésima raiz completa da unidade é o valor $\omega = e^{\frac{2\pi i}{N}}$.

$$
\begin{aligned}
&\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_{n-1}=0}^{1} \sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} \frac{k_l}{2^l}} |k_1 k_2 ... k_{n-1} k_n\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_{n-1}=0}^{1} \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{\frac{2\pi i j k_l}{2^l}} |k_l\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{\frac{2\pi i j k_l}{2^l}} |k_l\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} (|0\rangle + e^{2\pi i j \frac{1}{2^l}} |1\rangle).
\end{aligned}
$$

Como podemos ver acima, a operação da TQF pode ser fatorada como o produto tensorial de outras portas quânticas mais simples que, aplicadas em estados da base computacional, resulta em uma superposição de todos os estados da base computacional com uma fase relativa sobre o estado $|1\rangle$.

Propriedades

Veremos agora algumas propriedades que serão úteis na prova de resultados no próximo capítulo. Essas propriedades mostram o comportamento da TQF sobre superposições periódicas.

Teorema 2.5.1. *Seja* $|\phi\rangle = \sum_{j=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} |jr\rangle$ *um estado quântico periódico com um período* r*, divisor de* N*. Temos que* $\boldsymbol{QFT}_N |\phi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |j\frac{N}{r}\rangle$*.*

Demonstração. Para um valor de $0 \leq j \leq r-1$, inteiro, temos que a amplitude referente a $|j\frac{N}{r}\rangle$ é

$$
\frac{1}{\sqrt{N}} \frac{\sqrt{r}}{\sqrt{N}} \sum_{k=1}^{\frac{N}{r}-1} \omega^{(kr)\left(\frac{jN}{r}\right)} = \frac{\sqrt{r}}{N} \sum_{k=1}^{\frac{N}{r}-1} 1 = \frac{1}{\sqrt{r}},
$$

onde a primeira igualdade vem do fato de que a N-ésima raiz complexa da unidade elevada a um múltiplo de N é igual a 1.

Como os r elementos da base computacional na forma $|j\frac{N}{r}\rangle$ possuem amplitude $\frac{1}{\sqrt{r}}$ e o estado tem norma 1, temos que todos os outros elementos da base possuem amplitude 0. □

Iremos provar agora um resultado mais geral, envolvendo as superposições periódicas com um deslocamento.

Teorema 2.5.2. *Seja* $|\phi\rangle = \sum_{j=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}}|c + jr\rangle$ *um estado quântico periódico com um período* r *divisor de* N*, e deslocamento* $c < r$*. Segue então que* $\boldsymbol{QFT}_N|\phi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \omega^{\frac{cjN}{k}} |j\frac{N}{r}\rangle$.

Demonstração. De forma análoga à primeira prova, faremos a análise da amplitude de um estado $|j\frac{N}{r}\rangle$ para um valor de $0 \leq j \leq r-1$ inteiro:

$$\frac{1}{\sqrt{N}} \frac{\sqrt{r}}{\sqrt{N}} \sum_{k=1}^{\frac{N}{r}-1} \omega^{(c+kr)\left(\frac{jN}{r}\right)} = \frac{\sqrt{r}}{N} \sum_{k=1}^{\frac{N}{r}-1} \omega^{\frac{cjN}{r}} = \frac{1}{\sqrt{r}} \omega^{\frac{cjN}{r}}.$$

Os r elementos da base computacional na forma $|j\frac{N}{r}\rangle$ possuem amplitude com norma $\frac{1}{\sqrt{r}}$ e o estado final é unitário. Então segue que os outros elementos da base possuem amplitude 0. □

Nota 2.5.3. *Os Teoremas 2.5.1 e 2.5.2 são facilmente adaptados para o operador inverso da TQF, dado que, neste caso, basta a inversão do sinal do expoente de* ω*.*

2.5.4 *Swap test*

Apresentaremos nesta seção o *Swap test*, um teste que permite comparar os valores de dois registradores quânticos, quando temos a garantia que estes não estão emaranhados. Dois estados quânticos puros e não emaranhados passarão no teste quando forem iguais, e falharão no teste com probabilidade $\frac{1}{2}$ quando forem ortogonais.

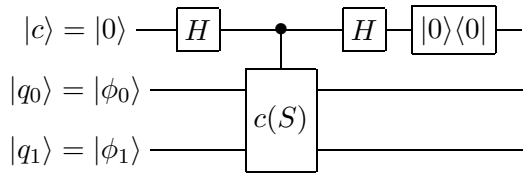


Figura 2.8: *Swap test*

Teorema 2.5.4. *Sejam* $|\phi_0\rangle$ *e* $|\phi_1\rangle$ *dois estados quânticos não-emaranhados. O Swap test, descrito na Figura 2.8, aceita com probabilidade* $\frac{1}{2} + \frac{1}{2}|\langle\phi_0|\phi_1\rangle|^2$.

Demonstração. Executando o procedimento sobre os estados $|\phi_0\rangle$ e $|\phi_1\rangle$, antes da medição o estado do sistema será:

$$\begin{aligned}
&(H \otimes I \otimes I)c(S)(H \otimes I \otimes I)|0\rangle|\phi_0\rangle|\phi_1\rangle \\
&= (H \otimes I \otimes I)c(S)\left(\frac{1}{\sqrt{2}}|0\rangle|\phi_0\rangle|\phi_1\rangle + \frac{1}{\sqrt{2}}|1\rangle|\phi_0\rangle|\phi_1\rangle\right) \\
&= (H \otimes I \otimes I)\left(\frac{1}{\sqrt{2}}|0\rangle|\phi_0\rangle|\phi_1\rangle + \frac{1}{\sqrt{2}}|1\rangle|\phi_1\rangle|\phi_0\rangle\right) \\
&= \frac{1}{2}|0\rangle(|\phi_0\rangle|\phi_1\rangle + |\phi_1\rangle|\phi_0\rangle) + \frac{1}{2}|1\rangle(|\phi_0\rangle|\phi_1\rangle - |\phi_1\rangle|\phi_0\rangle).
\end{aligned}$$

Se escrevermos $|\phi_1\rangle = \alpha|\phi_0\rangle + \beta|\psi\rangle$, para algum $|\psi\rangle \perp |\phi_0\rangle$ e $\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$, temos

$$\begin{aligned}
&\frac{1}{2}|0\rangle(|\phi_0\rangle|\phi_1\rangle + |\phi_1\rangle|\phi_0\rangle) + \frac{1}{2}|1\rangle(|\phi_0\rangle|\phi_1\rangle - |\phi_1\rangle|\phi_0\rangle) \\
&= \frac{1}{2}|0\rangle(\alpha|\phi_0\rangle|\phi_0\rangle + \beta|\phi_0\rangle|\psi\rangle + \alpha|\phi_0\rangle|\phi_0\rangle + \beta|\psi\rangle|\phi_0\rangle) \\
&+ \frac{1}{2}|1\rangle(\alpha|\phi_0\rangle|\phi_0\rangle + \beta|\phi_0\rangle|\psi\rangle - \alpha|\phi_0\rangle|\phi_0\rangle - \beta|\psi\rangle|\phi_0\rangle) \\
&= \frac{1}{2}|0\rangle(2\alpha|\phi_0\rangle|\phi_0\rangle + \beta|\phi_0\rangle|\psi\rangle + \beta|\psi\rangle|\phi_0\rangle) + \frac{1}{2}|1\rangle(\beta|\phi_0\rangle|\psi\rangle - \alpha|\phi_0\rangle|\phi_0\rangle).
\end{aligned}$$

Temos que a probabilidade de medir $|0\rangle$, o que significa que os estados passaram o *Swap test*, é

$$\begin{aligned}
&\alpha^2 + \frac{1}{4}\beta^2 + \frac{1}{4}\beta^2 \\
&= (\frac{1}{2}\alpha^2 + \frac{1}{2}\beta^2) + \frac{1}{2}\alpha^2 \\
&= \frac{1}{2} + \frac{1}{2}\alpha^2 \\
&= \frac{1}{2} + \frac{1}{2}|\langle\phi_0|\phi_1\rangle|^2.
\end{aligned}$$

□

Nota 2.5.5. *Pode-se facilmente estender a análise anterior para os estados mistos não emaranhados $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ e $\sigma = \sum_j q_i|\phi_j\rangle\langle\phi_j|$, sendo que a probabilidade de aceitação será*

$$\sum_{ij} p_i q_j \left(\frac{1}{2} - \frac{|\langle\psi_i|\phi_j\rangle|^2}{2}\right) = \frac{1}{2} - \frac{1}{2}\sum_{ij} p_i q_j |\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{2} - \frac{Tr(\rho\sigma)}{2}.$$

Mostraremos agora a probabilidade de rejeição de um estado misto arbitrário que está ϵ-distante de todos estados puros.

Teorema 2.5.6 (Extraído de [2])**.** *Seja ρ um estado misto. Se $\langle\psi|\rho|\psi\rangle \leq 1-\epsilon$ para todos os estados puros $|\psi\rangle$, então o Swap test entre ρ e qualquer outro estado quântico é rejeitado com probabilidade pelo menos $\frac{\epsilon}{2}$.*

Demonstração. Seja uma base que diagonaliza ρ. Temos então que, nesta base, a matriz de densidade de ρ é a matriz que contém seus autovalores λ_i na sua diagonal.

Como assumimos que $\lambda_j < 1-\epsilon$, para qualquer estado misto σ, o *Swap test* entre ρ e σ aceita com probabilidade

$$\frac{1}{2} + \frac{Tr(\rho\sigma)}{2} = \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{N} \lambda_i \sigma_{ii} < \frac{1}{2} + \frac{1-\epsilon}{2}\sum_{i=1}^{N} \sigma_{ii} \leq 1 - \frac{\epsilon}{2}.$$

□

Capítulo 3

Algoritmos e Classes de Complexidade Quânticos

Iremos estudar, neste capítulo, exemplos de como o modelo computacional quântico pode ser usado para resolver alguns problemas de forma mais eficiente. Apresentaremos também as principais Classes de Complexidade Quânticas e iremos compará-las com as Classes de Complexidade Clássicas.

3.1 Introdução

Existem hoje, na literatura, uma gama variada de algoritmos quânticos que resolvem desde problemas abstratos, como descobrir propriedades de funções [34], até problemas mais práticos como fluxo em redes [14] e fatoração de números [82]. Entretanto, grande parte destes algoritmos utilizam como base os primeiros algoritmos quânticos propostos e iremos, nesta seção, apresentá-los. A complexidade em tempo dos algoritmos será analisada considerando o número de portas utilizadas e o número de consultas a oráculos.

Começaremos apresentando o Algoritmo de Deutsch [34] que resolve um problema simples, e em seguida mostraremos sua extensão, o Algoritmo de Deutsch-Josza [36]. Em seguida, mostraremos os dois Algoritmos Quânticos mais relevantes até hoje, o Algoritmo de Shor [82] para fatoração de números e o Algoritmo de Grover [51] para buscas em vetores desordenados.

Na Seção 3.3, apresentaremos as principais Classes de Complexidade Quânticas,

em geral, análogas às principais Classes de Complexidade Clássicas. Tal estudo permite comparar o poder computacional quântico e clássico em relação aos recursos utilizados.

3.2 Algoritmos Quânticos

Nesta seção iremos apresentar os principais algoritmos quânticos encontrados na literatura. Estes até hoje servem como base para o desenvolvimento de novos algoritmos, seja modificando-se os algoritmos originais, seja utilizando-os como sub-rotinas.

Começaremos apresentando o algoritmo de Deutsch, que demonstra de maneira mais simplificada como podemos obter vantagem com o paralelismo quântico, e em seguida será apresentada sua extensão, o Algoritmo de Deutsch-Josza, que extrai do paralelismo quântico um ganho exponencial em relação a algoritmos clássicos para a a solução de um problema.

Seguiremos com os dois algoritmos quânticos mais notáveis por suas aplicações. Primeiramente veremos o Algoritmo de Shor, que resolve o problema da fatoração em tempo polinomial. Por último veremos o Algoritmo de Grover, que realiza buscas em um banco de dados desordenado com aceleração quadrática em relação a algoritmos clássicos para solução do problema.

3.2.1 Algoritmo de Deutsch

Começaremos expondo o problema de promessa que mostraremos que o Algoritmo de Deutsch irá resolver.

Problema 1. *Dado um oráculo U_f para uma função $f : \{0,1\} \to \{0,1\}$ deseja-se descobrir se f é constante $(f(0) = f(1))$ ou balanceada $(f(0) \neq f(1))$.*

O melhor algoritmo clássico para resolver o Problema 1 faz duas consultas à função f, uma para o valor 0 e outra para o valor 1, e compara os dois resultados. Deutsch demonstrou em 1985 que quanticamente, pode-se descobrir se $f(0) = f(1)$ com somente uma consulta a U_f [34].

Antes de estudarmos o Algoritmo de Deutsch em si, estudaremos um fenômeno chamado *phase quick back*. Como visto na Seção 2.5.1, o oráculo U_f tem o funcionamento descrito por

$$|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

Vamos estudar o caso em que aplicamos uma consulta ao oráculo com $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Se $f(x) = 0$, temos então que

$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

enquanto que se $f(x) = 1$, temos

$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |x\rangle\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Podemos generalizar esses dois casos:

$$U_f|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Chamamos esse efeito de *phase quick back*, dado que a fase resultante da consulta ao oráculo foi propagado para o primeiro *qubit*.

O algoritmo proposto por Deutsch está descrito na Figura 3.1 e iremos agora provar sua corretude.

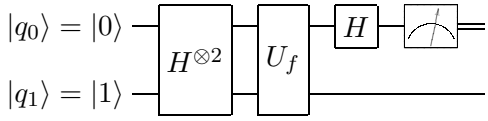


Figura 3.1: Algoritmo de Deutsch

Teorema 3.2.1. *Dado um oráculo U_f para uma função $f : \{0,1\}^2 \to \{0,1\}$, se o resultado da medição do circuito proposto na Figura 3.1 é $|0\rangle$ a função f é constante, e caso o resultado da medição seja $|1\rangle$ f é balanceada.*

Demonstração. Após a primeira aplicação da porta de Hadamard nos dois *qubits*, temos que seu estado é

$$H^{\otimes 2}|0\rangle|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle).$$

e após fazer uma consulta a U_f, o valor dos dois *qubits* passa a ser:

$$U_f\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle).$$

Como os dois *qubits* não estão emaranhados, podemos considerar somente ao primeiro *qubit*, sem perda de generalidade. Aplicando-se a operação de Hadamard sobre esse *qubit*, temos:

$$H\left(\frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)\right) = \\ \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)})|1\rangle.$$

Temos então que se $f(0) = f(1)$ a função é constante e o resultado da medição é $|0\rangle$ dado que $(-1)^{f(0)}$ e $-(-1)^{f(1)}$ se anulam. Já se $f(0) \neq f(1)$, a função é balanceada e o resultado da medição é $|1\rangle$, dado que $(-1)^{f(0)}$ e $(-1)^{f(1)}$ se anulam. □

Temos então que, no modelo quântico, conseguimos diminuir o número de consultas ao oráculos em de 2 para 1. Entretanto, esta diminuição não é significativa em termos assintóticos. Veremos agora uma extensão do problema que resultará em um ganho exponencial no modelo quântico.

3.2.2 Algoritmo de Deutsch-Josza

Vamos agora propor uma generalização do Problema 1 e veremos um algoritmo quântico para este novo problema.

Problema 2. *Dado um oráculo U_f para uma função $f : \{0,1\}^n \to \{0,1\}$ tal que a distribuição da imagem de f é de dois tipos:*

1. *a função f é constante, ou seja, o valor de $f(x)$ é igual para todo $x \in \{0,1\}^n$; ou*

2. *a função f é balanceada, ou seja, para metade dos elementos do domínio, a imagem é 0 e para a outra metade a imagem é 1.*

Deseja-se, então, descobrir em qual dos casos f se encontra.

Um algoritmo determinístico para resolver o Problema 2 precisa de $O(2^{n-1})$ consultas ao oráculo, dado que necessita avaliar mais do que a metade dos elementos do domínio. Iremos mostrar o algoritmo quântico proposto por Deutsch e Josza em 1992, e que permite resolver este problema com somente uma consulta ao oráculo U_f [36].

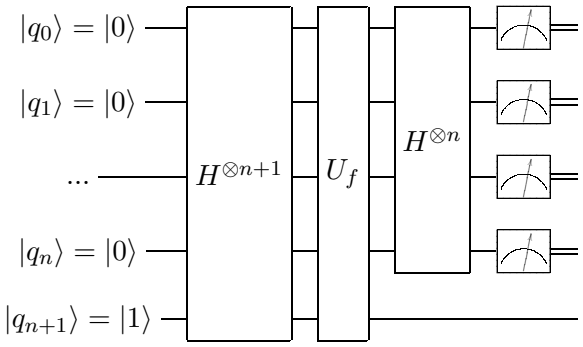


Figura 3.2: Algoritmo de Deutsch-Josza

Teorema 3.2.2. *Dado um oráculo U_f para uma função $f : \{0,1\}^n \to \{0,1\}$, se o resultado da medição do circuito proposto na Figura 3.2 é $|0...0\rangle$ a função f é constante, caso contrário, f é balanceada.*

Demonstração. Após a aplicação da porta de Hadamard em cada um dos *qubits*, o estado do registrador quântico é

$$H^{\otimes n+1}|00...00\rangle|1\rangle = \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

para $N = 2^n$.

Após a consulta a U_f, temos que estado passa a ser

$$U_f \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} (-1)^{f(i)}|i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Como os primeiros n *qubits* não estão emaranhados com o último, iremos ignorar este em nossos cálculos, sem perda de generalidade. Ao aplicar a porta de Hadamard sobre os n primeiros *qubits*, temos

$$\begin{aligned} H^{\otimes n} \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} (-1)^{f(i)}|i\rangle &= \frac{1}{N} \sum_{i\in\{0,1\}^n} (-1)^{f(i)} \sum_{j\in\{0,1\}^n} (-1)^{i\cdot j}|j\rangle \\ &= \frac{1}{N} \sum_{i\in\{0,1\}^n} \sum_{j\in\{0,1\}^n} (-1)^{f(i)}(-1)^{i\cdot j}|j\rangle \\ &= \frac{1}{N} \sum_{j\in\{0,1\}^n} \sum_{i\in\{0,1\}^n} (-1)^{f(i)}(-1)^{i\cdot j}|j\rangle. \end{aligned}$$

Vamos então analisar o valor da amplitude α_0 associada ao elemento $|0..0\rangle$ na equação anterior:

$$\alpha_0 = \frac{1}{N} \sum_{i \in \{0,1\}^n} (-1)^{f(i)} (-1)^0 |j\rangle = \frac{1}{N} \sum_{i \in \{0,1\}^n} (-1)^{f(i)} |j\rangle.$$

Se a função for balanceada, temos que para metade dos valores em $\{0,1\}^n$ a função f tem valor 0 e na outra metade tem valor 1. Neste caso, as somas dos valores de $(-1)^{f(i)}$ se cancelarão e $\alpha_0 = 0$. Já no caso em que a função é constante, temos que $f(i)$ possui o mesmo valor para qualquer elemento de $\{0,1\}^n$, logo, $\alpha_0 = \pm 1$. Portanto a função é constante se e somente se o resultado da medição for $|0..0\rangle$. □

Com este resultado, temos que, dado um oráculo U_f, conseguimos uma separação exponencial entre os modelos computacionais determinístico e quântico.

3.2.3 Algoritmo de Shor e a fatoração em números primos

O estudo sobre números primos e suas propriedades está presente na história da humanidade há mais de dois milênios, datando desta época, por exemplo, um dos métodos mais simples para descobrir se um número é primo ou não, o Crivo de Erastótenes. Entretanto este método é computacionalmente ineficiente e por muito tempo somente algoritmos probabilísticos [72][78] eram conhecidos para este problema e questionava-se se ele poderia ser resolvido deterministicamente. Em 2002, Agrawal, Kayal e Saxena resolveram este problema, apresentando um algoritmo capaz de decidir se um número é primo ou não em tempo polinomial [4].

Um problema relacionado ao problema dos números primos é o problema da fatoração: dado um número maior que 1, deseja-se saber a sequência única de números primos que, multiplicados, resultam no número desejado. Existem métodos para resolver este problema classicamente, porém todos possuem complexidade de tempo exponencial e é um problema aberto até hoje se existe um algoritmo polinomial clássico para resolver este problema. Conjectura-se que este problema é difícil classicamente, e sobre esta conjectura está baseado um dos principais métodos criptográficos utilizados na atualidade.

Em 1992, Peter Shor apresentou um surpreendente algoritmo quântico capaz de resolver o problema da fatoração em tempo polinomial [82], sendo este o principal resultado que temos até hoje da superioridade de computadores quânticos sobre computadores clássicos.

Iremos, nesta seção, apresentar o algoritmo proposto por Shor, que encontra, na verdade, uma fator não trivial do número desejado. Porém, a partir disto pode-se encontrar a fatoração do número dado, utilizando-se este algoritmo como uma sub-rotina um número polinomial de vezes em relação ao tamanho da entrada.

Inicialmente mostraremos como reduzir o problema de encontrar um fator não trivial de um número para o problema de encontrar o período de uma função periódica. Em seguida, será apresentado o algoritmo quântico que resolve o problema de encontrar o período de uma função periódica em tempo polinomial. Ressaltamos que, pelo procedimento descrito por Shor, o gargalo clássico para resolver o problema da fatoração classicamente é encontrar o período.

Assumiremos que o número que desejamos fatorar é um número composto [1] ímpar [2] e que não é uma potência de um número primo [3]. Iremos então utilizar a seguinte notação durante toda esta seção: n é o número que desejamos fatorar e teremos $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, onde $k \geq 2$, os p_i são números primos distintos e $e_i \geq 1$ para $1 \leq i \leq k$. Denotaremos também $n_i = p_i^{e_i}$.

Nesta seção, serão necessários alguns conceitos básicos de Teoria dos Números que são revisados no Apêndice A.

Encontrando fatores de um número

Nesta seção, mostraremos como resolver o problema de encontrar um fator não trivial de um número, assumindo que sabemos encontrar o período de uma função periódica de forma eficiente. Veremos, a seguir, que o método para encontrar um período apresenta um erro exponencialmente pequeno de não encontrá-lo, e por simplicidade este erro será ignorado neste ponto.

Definição 3.2.3. *Uma função $f : \mathbb{Z}_n \to \mathbb{Z}_n$ é periódica se existe um valor r, chamado período, tal que $f(x) = f(x + r \mod n)$.*

O algoritmo para resolver tal problema se encontra na Figura 3.3, porém, antes de provar sua corretude, iremos enunciar um lema auxiliar, cuja prova se encontra no Apêndice B.

[1] Para descobrir se um número é primo ou não, basta utilizar o Algoritmo AKS [4]

[2] Todo número par possui trivialmente o fator 2

[3] Podemos verificar em tempo $\log n$ se n é uma potência de primo, verificando a i-ésima raiz de n, para $2 \leq i \leq \log n$ e se for um número natural, verificar se é primo

Lema 3.2.4. *Seja $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ a decomposição em fatores primos de um número ímpar composto n. A probabilidade de a ordem de a em $\mathbb{Z}_n$, $r = ord_n(a)$, ser par e $a^{\frac{r}{2}} \not\equiv -1 \mod n$ é pelo menos $\frac{9}{16}$.*

```
1  Sorteie um número aleatório a entre 2 e N;
2  if mdc(a, N) > 1 then
3  |  Retorne mdc(a, N);
4  end
5  Encontre o período r da função f_{a,n}(x) = a^x mod n;
6  if r é ímpar or x^{r/2} ≡ ±1 then
7  |  Retorne ERRO;
8  else
9  |  Retorne max{mdc(N, x + 1), mdc(N, x − 1)};
10 end
```

Figura 3.3: Algoritmo de Shor

Teorema 3.2.5. *O Algoritmo de Shor, mostrado na Figura 3.3, retorna, com probabilidade pelo menos $\frac{9}{16}$, um fator não trivial de n.*

Demonstração. Seja a o número sorteado no passo 1. Se $d = mdc(a, n) > 1$, então d é um fator não trivial de n, que será retornado pelo procedimento, que neste caso reponde corretamente com probabilidade 1.

Vamos, então, assumir que $d = 1$ e verificar o comportamento do resto do algoritmo. Seja r a ordem de a em $\mathbb{Z}_n$ e vamos assumir que r é par e $a^{\frac{r}{2}} \not\equiv -1 \mod n$, e pelo Lema 3.2.4, isto ocorre com probabilidade pelo menos $\frac{9}{16}$.

Como r é a ordem de a em $\mathbb{Z}_n$, por definição temos que $a^r \equiv 1 \mod n$, o que implica por resultados de aritmética modular que $a^r - 1 \equiv 0 \mod n$, ou seja, n divide $a^r - 1$. Como assumimos r par, segue que $a^r - 1 = (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$ e $(a^{\frac{r}{2}} + 1)$ e $(a^{\frac{r}{2}} - 1)$ são inteiros. Portanto n possui pelo menos um fator em comum com $(a^{\frac{r}{2}} + 1)$ ou $(a^{\frac{r}{2}} - 1)$ e esse fator pode ser facilmente encontrado calculando-se o máximo divisor comum entre esses números. Porém, esse máximo divisor comum pode ser igual a n, o que resultaria em um fator trivial do número.

Se considerarmos o caso em que n divide $a^{\frac{r}{2}} - 1$, tem-se que $a^{\frac{r}{2}} \equiv 1 \mod n$, e temos uma contradição, pois neste caso r não seria a ordem de a em $\mathbb{Z}_n$. Se

considerarmos o caso em que n divide $a^{\frac{n}{2}} + 1$, teríamos $a^{\frac{r}{2}} \equiv -1 \mod n$, o que, assumimos anteriormente não ser o caso.

Portanto temos que, dada a ordem de a em $\mathbb{Z}_n$, podemos encontrar um fator não trivial de n com probabilidade $\frac{9}{16}$. □

Temos que a função $f_{a,n}(k) = a^k \mod n$ é periódica e seu período é justamente a ordem r dado que $a^r \equiv a^0 \mod n \equiv 1 \mod n$. Portanto, se conseguirmos encontrar o período da função $f_{a,n}$ de forma eficiente, resolvemos o problema da fatoração. Veremos agora justamente um algoritmo quântico para o problema de encontrar o período da função $f_{a,n}$.

Encontrando a ordem

Agora apresentaremos um algoritmo quântico para encontrar o período da função $f_{a,n}(k) = a^k \mod n$ através de um oráculo $U_{f_{a,n}}$ para essa função, onde

$$U_{f_{a,n}}|x\rangle|y\rangle \to |k\rangle|y \oplus (a^k \mod n)\rangle.$$

Seja $m = \lceil 5 \log n \rceil$ e $M = 2^m$. Iremos assumir aqui que r divide M, o que é uma restrição forte e não necessariamente acontece na prática, porém simplificará alguns elementos técnicos da prova, mantendo ainda as ideias principais usadas na demonstração. Indicamos os livros de Nielsen e Chuang [74] ou Hirvensalo [53] para a prova do caso mais geral.

1 Prepare os registradores quânticos $|0^n\rangle|0^{\lceil m \rceil}\rangle$;
2 Aplique a porta $H^{\otimes m}$ no primeiro registrador ;
3 Aplique a operação $|x\rangle|y\rangle \to |k\rangle|y \oplus (a^k \mod n)\rangle$;
4 Efetue uma medição no segundo registrador quântico ;
5 Aplique a inversa da Transformada Quântica de Fourier no primeiro registrador quântico ;
6 Efetue uma medição no primeiro registrador quântico e seja c o resultado desta medição ;
7 Encontre a fração reduzida $\frac{r}{s}$ de $\frac{c}{M}$;

Figura 3.4: Algoritmo para encontrar a ordem

Teorema 3.2.6. *Seja $r = ord_n(a)$, e assumimos que r divide M, onde $m = \lceil 5 \log n \rceil$ e $M = 2^m$. O Algoritmo para encontrar a ordem, descrito na Figura 3.4 retorna r com probabilidade pelo menos $\frac{1}{\log n}$.*

Demonstração. Temos que após a aplicação da porta de Hadamard no primeiro registrador, o estado dos dois registradores é

$$\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle|0\rangle.$$

Após a consulta ao oráculo da função $f_{a,n}$ no passo 3, temos que o estado dos registradores quânticos é

$$\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle|a^k \mod n\rangle = \frac{1}{\sqrt{M}} \sum_{l=0}^{r-1} \sum_{q=0}^{s_l} |qr+l\rangle|a^l \mod n\rangle,$$

onde a segunda igualdade resulta do fato que a função $f_{a,n}$ é periódica, e seu período r é a ordem de a em relação a n.

A medição no segundo registrador quântico fixa um deslocamento $0 \leq l^* \leq r-1$, sorteado uniformemente, resultando em

$$\sqrt{\frac{r}{M}} \sum_{q=0}^{s_l} |qr+l^*\rangle|a^{l^*} \mod n\rangle.$$

Como temos uma função periódica no intervalo de 0 a M, com período r e deslocamento l^*, a inversa da Transformada Quântica de Fourier irá resultar em

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{2\pi i l^* k}{r}} |k\frac{M}{r}\rangle,$$

como vimos no Teorema 2.5.2 e Nota 2.5.3.

Quando efetuamos uma medição no primeiro registrador quântico, teremos o valor

$$k\frac{M}{r},$$

em que k é escolhido aleatoriamente para algum valor em $\{0, ..., r-1\}$. Como sabemos o valor de M, podemos encontrar a fração reduzida de $\frac{k\frac{M}{r}}{M} = \frac{p}{q}$ e, se k e r forem primos entre si, esta fração reduzida encontra justamente os valores $p = k$ e $q = r$.

Temos, por um resultado de Teoria dos Números, que existem $\Omega(\frac{r}{\log r})$ números primos menores que r e que r possui no máximo $\log r$ números primos como divisores. Segue-se, então que existem pelo menos $\Omega(\frac{r}{\log r} - \log r) = \Omega(\frac{r}{\log r})$ números menores que r que são coprimos com r. Portanto, temos que, ao sortear um número uniformemente entre $\{0, ..., r-1\}$, teremos probabilidade $\Omega(\frac{1}{\log r})$, ou seja $\Omega(\frac{1}{\log n})$ de sortear um número coprimo com r. □

Utilizando o limitante de Chernoff para limitar a probabilidade de que múltiplas execuções falhem, temos o seguinte corolário, que nos indica um algoritmo que retorna r com alta probabilidade.

Corolário 3.2.7. *Ao repetir o Algoritmo para encontrar a ordem, descrito na Figura 3.4, um número* $O(\log n)$ *vezes, temos que em pelo menos uma das iterações encontramos* r *com probabilidade exponencialmente perto de* 1*.*

3.2.4 Problemas de busca e o algoritmo de Grover

Um problema muito comum em computação é a busca de um elemento específico em uma base de dados desordenada. Neste problema, é computacionalmente fácil verificar se um dado elemento é aquele procurado, entretanto a dificuldade consiste em encontrar esse elemento dentre todos os outros.

Este problema é tão geral que todos os problemas em NP se encaixam nele, pois temos um algoritmo verificador que reconhece um certificado e o espaço de busca são todos os possíveis certificados para ele.

Denotaremos como $N = 2^n$ o número de elementos na base de dados. Classicamente, temos o limitante inferior de $\Omega(N)$ para este problema, dado que mesmo probabilisticamente temos que verificar uma fração constante do número de elementos.

Nesta seção, descreveremos o algoritmo quântico para resolver este problema em tempo $O(\sqrt{N})$ proposto por Grover em 1996 [51], resultando em uma aceleração quadrática comparada com o modelo clássico.

Por simplicidade, iremos provar o funcionamento do algoritmo quando, na base dados, existe exatamente um elemento buscado. As provas de casos mais gerais para o Algoritmo de Grover são pequenas alterações nesta prova e podem ser encontradas em referências como Nielsen e Chuang [74] ou Hirvensalo [53].

Iniciaremos agora definindo formalmente o problema. Em seguida, apresentaremos as operações que formam a componente básica do Algoritmo de Grover.

Problema 3. *Seja* $f : \{0,1\}^n \to \{0,1\}$ *uma função, sendo que existe um elemento desconhecido* $x_0 \in \{0,1\}^n$ *tal que*

$$f(x) = \begin{cases} 0, & \text{se } x \neq x_0 \\ 1, & \text{se } x = x_0 \end{cases}$$

Deseja-se encontrar o valor de x_0*.*

Iteração de Grover

A ideia do Algoritmo de Grover é aplicar sucessivamente um certo número de vezes o operador de Grover, que aumentará a probabilidade de $|x_0\rangle$ ser medido a cada iteração. O operador de Grover consiste em duas operações que iremos apresentar agora: reflexão pela média e inversão de fase.

Denotaremos a superposição normalizada de todos os elementos da base computacional ortogonais a $|x_0\rangle$ por

$$|x_0^\perp\rangle = \sum_{i \neq x_0} \frac{1}{\sqrt{N-1}} |i\rangle.$$

Inversão de fase. A operação de inversão de fase irá atuar marcando o elemento procurado $|x_0\rangle$, e invertendo o sinal de sua fase. Como não se conhece o elemento procurado, utilizaremos uma consulta a U_f utilizando o mesmo artifício usado na Seção 3.2.1: o *qubit* que irá receber a resposta da consulta ao oráculo será preparado no estado $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, resultando em que a operação de U_f sobre um estado da base $|i\rangle$ será

$$\frac{1}{\sqrt{2}} U_f |i\rangle(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} |i\rangle(|0 \oplus f(i)\rangle - |1 \oplus f(i)\rangle) = (-1)^{f(i)} \frac{1}{\sqrt{2}} |i\rangle(|0\rangle - |1\rangle).$$

Para não carregar a notação, assumiremos então que a consulta a U_f tem como entrada somente o registrador $|x\rangle = \sum_i \alpha_i |i\rangle$ e tem como resultado $\sum_i (-1)^{f(x)} \alpha_i |i\rangle$, marcando o elemento cujo resultado da função é 1.

Se a consulta a U_f for aplicada em um estado no espaço gerado pelos vetores $|x_0\rangle$ e $|x_0^\perp\rangle$, a inversão de fase é uma reflexão em torno de $|x_0^\perp\rangle$. Tal interpretação pode ser vista na Figura 3.5.

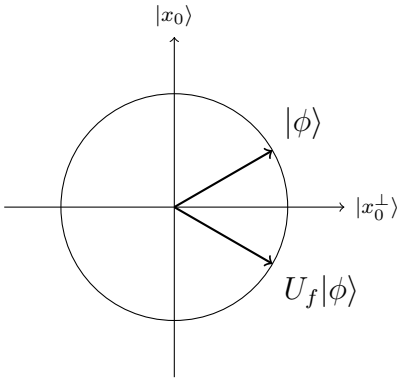


Figura 3.5: Interpretação geométrica da inversão de fase

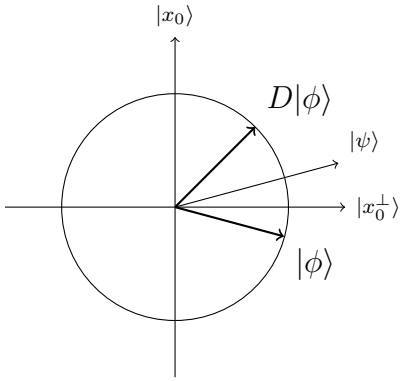


Figura 3.6: Interpretação geométrica da inversão pela média

Reflexão pela média. Dado um estado $|\phi\rangle = \sum_{i\in\{0,1\}^n} \alpha_i|i\rangle$, seja

$$\mu = \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} \alpha_i$$

a média das amplitudes de todos os elementos da base computacional. A operação reflexão pela média tem como objetivo realizar a transformação

$$\alpha_i|i\rangle \to (\mu + (\mu - \alpha_i))|i\rangle. \tag{3.1}$$

Em um primeiro momento, não é imediato perceber se esta operação é unitária. Então iremos justamente provar que este é o caso, mostrando que esta operação é equivalente à operação

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n},$$

que, em termos gerais, consiste em aplicar a porta de Hadamard, inverter a fase de todos os elementos da base computacional ortogonais a $|0\rangle$ e aplicar a porta de Hadamard novamente.

Seja $|\psi\rangle = H^{\otimes n}|0\rangle$. Analizaremos agora o funcionamento de D:

$$
\begin{aligned}
D &= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} \\
&= 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - H^{\otimes n} I H^{\otimes n} \\
&= 2|\psi\rangle\langle\psi| - I \qquad (3.2) \\
&= \frac{1}{2^{n-1}} \begin{pmatrix} 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \\ & & ... & & \\ 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ & & ... & & \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix} \qquad (3.3) \\
&= \frac{1}{2^{n-1}} \begin{pmatrix} 1-2^{n-1} & 1 & ... & 1 & 1 \\ 1 & 1-2^{n-1} & ... & 1 & 1 \\ & & ... & & \\ 1 & 1 & ... & 1-2^{n-1} & 1 \\ 1 & 1 & ... & 1 & 1-2^{n-1} \end{pmatrix}. \qquad (3.4)
\end{aligned}
$$

Podemos ver da Equação 3.2 que uma outra interpretação para D é inverter a fase para os elementos do subespaço ortogonal a $|\psi\rangle$. Para ver isso, basta verificar que

$$D|\psi\rangle = 2|\psi\rangle\langle\psi||\psi\rangle - I|\psi\rangle = |\psi\rangle,$$

e que para um vetor $|\chi\rangle \perp |\psi\rangle$ temos

$$D|\chi\rangle = 2|\psi\rangle\langle\psi||\chi\rangle - I|\chi\rangle = -|\chi\rangle.$$

Geometricamente o efeito do operador D é realizar o espelhamento referente a $|\psi\rangle$. A Figura 3.6 mostra o funcionamento de D no plano gerado pelos vetores $|x_0\rangle$ e $|x_0^{\perp}\rangle$. Vemos também da Equação 3.4 que D possui somente valores reais e além disso é simétrico, resultando em $D = D^{\dagger}$. Segue então que

$$
\begin{aligned}
DD^{\dagger} = D^{\dagger}D &= DD \\
&= (2|\psi\rangle\langle\psi| - I)(2|\psi\rangle\langle\psi| - I) \\
&= 4|\psi\rangle\langle\psi||\psi\rangle\langle\psi| - 2|\psi\rangle\langle\psi| - 2|\psi\rangle\langle\psi| + I \\
&= 4|\psi\rangle\langle\psi| - 4|\psi\rangle\langle\psi| + I \\
&= I
\end{aligned}
$$

implicando que D é unitária.

Sabemos agora que que D é uma operação quântica válida, veremos seu funcionamento sobre um vetor $|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, utilizando a Equação 3.3 para representar D:

$$
\begin{aligned}
D|\phi\rangle &= \left(\frac{1}{2^{n-1}} \begin{pmatrix} 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \\ & & ... & & \\ 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ & & ... & & \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix} \right) \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} \\
&= \frac{1}{2^{n-1}} \begin{pmatrix} 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \\ & & ... & & \\ 1 & 1 & ... & 1 & 1 \\ 1 & 1 & ... & 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} - \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ & & ... & & \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} \\
&= \begin{pmatrix} 2\frac{\sum_{i=0}^{2^n-1} \alpha_i}{2^n} \\ 2\frac{\sum_{i=0}^{2^n-1} \alpha_i}{2^n} \\ ... \\ 2\frac{\sum_{i=0}^{2^n-1} \alpha_i}{2^n} \\ 2\frac{\sum_{i=0}^{2^n-1} \alpha_i}{2^n} \end{pmatrix} - \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} \\
&= \begin{pmatrix} 2\mu \\ 2\mu \\ ... \\ 2\mu \\ 2\mu \end{pmatrix} - \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ ... \\ \alpha_{n-1} \\ \alpha_n \end{pmatrix} \\
&= \sum_{i=0}^{2^n-1} (\mu + (\mu - \alpha_i))|i\rangle,
\end{aligned}
$$

que é justamente o operador descrito na Equação 3.1.

Algoritmo de Grover

Tendo visto seus componentes básicos, iremos agora estudar o comportamento do Algoritmo de Grover, que consiste em iniciar com a superposição de todos os elementos da base computacional e aplicar, sucessivamente, a consulta ao oráculo e a

inversão pela média.

1 Prepare um registrador quântico com o estado $\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle$;
2 **for** *i de* 1 *a* $\frac{\pi}{4}\sqrt{N}$ **do**
3 | Aplique uma consulta ao oráculo U_f;
4 | Aplique o operador de inversão pela média D;
5 **end**
6 Meça e retorne o resultado;

Figura 3.7: Algoritmo de Grover

Teorema 3.2.8. *O Algoritmo de Grover, descrito na Figura 3.7 retorna o valor procurado com probabilidade* $1 - O(\frac{1}{N})$.

Demonstração. A superposição criada inicialmente pode ser reescrita como

$$\frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|x_0^\perp\rangle.$$

Como visto anteriormente, a inversão pela média será, na verdade uma reflexão em torno de $|\psi\rangle$. Podemos verificar, então, que ao aplicar sucessivamente U_f e D, o estado resultante ficará sempre no subespaço 2-dimensional gerado por $|x_0\rangle$ e $|x_0^\perp\rangle$. Para analizar o funcionamento do algoritmo, iremos utilizar duas bases deste espaço, indistintamente: a base gerada por $|x_0\rangle$ e $|x_0^\perp\rangle$ e a base gerada por $|\psi\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|x_0^\perp\rangle$ e $|\bar{\psi}\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|x_0\rangle - \frac{1}{\sqrt{N}}|x_0^\perp\rangle$. Para a converter vetores de uma base para outra,

$$\begin{aligned}
|\psi\rangle &= \sin\theta|x_0\rangle + \cos\theta|x_0^\perp\rangle, \\
|\bar{\psi}\rangle &= \cos\theta|x_0\rangle - \sin\theta|x_0^\perp\rangle, \\
|x_0\rangle &= \sin\theta|\psi\rangle + \cos\theta|\bar{\psi}\rangle \text{ e} \\
|x_0^\perp\rangle &= \cos\theta|\psi\rangle - \sin\theta|\bar{\psi}\rangle,
\end{aligned}$$

onde $\sin\theta = \frac{1}{\sqrt{N}}$ e $\cos\theta = \frac{\sqrt{N-1}}{\sqrt{N}}$.

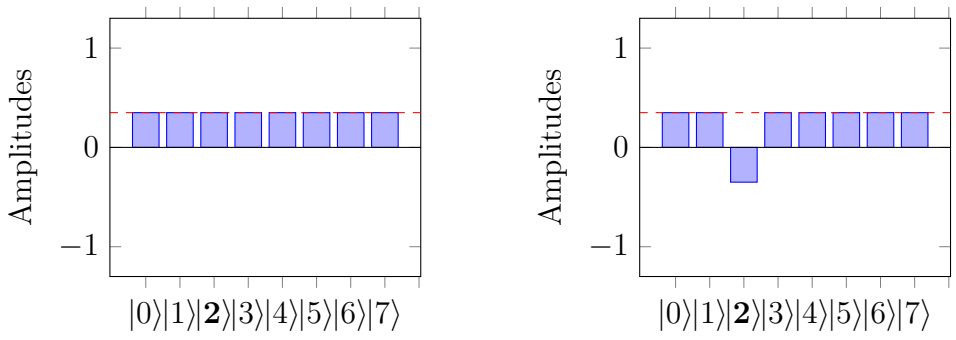
Após a primeira aplicação da operação de inversão de fase, teremos

$$U_f|\psi\rangle = -\sin\theta|x_0\rangle + \cos\theta|x_0^\perp\rangle = \cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle.$$

Em seguida, a operação de inversão pela média resultará em

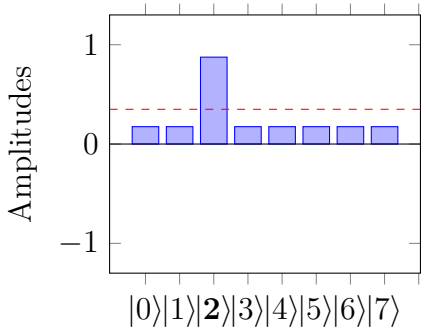
$$D(\cos 2\theta|\psi\rangle - \sin 2\theta|\bar{\psi}\rangle) = \cos 2\theta|\psi\rangle + \sin 2\theta|\bar{\psi}\rangle = \sin 3\theta|x_0\rangle + \cos 3\theta|x_0^{\perp}\rangle.$$

É ilustrado, na Figura 3.8 o comportamento das amplitudes dos elementos da base computacional em uma iteração de Grover com $N = 8$ e onde o elemento marcado é o $|2\rangle$.



(a) Sobreposição oringinal

(b) Inversão da fase



(c) Inversão pela média

Figura 3.8: Exemplo de uma iteração de Grover, com $N = 8$ e o elemento marcado é $|2\rangle$.

É fácil verificar, por indução, que após k iterações de Grover, temos

$$(DU_f)^k|\psi\rangle = \cos 2k\theta|\psi\rangle + \sin 2k\theta|\bar{\psi}\rangle = \sin(2k+1)\theta|x_0\rangle + \cos(2k+1)\theta|x_0^{\perp}\rangle,$$

e nosso objetivo é aproximar $(2k+1)\theta$ de $\frac{\pi}{2}$, de forma que resultado da medição esteja próximo de $|x_0\rangle$. Portanto, buscamos o valor inteiro k mais próximo de $\frac{\pi}{4\theta} - \frac{1}{2}$.

Como para valores de N grandes o suficiente, podemos aproximar $\theta = \sin\theta = \frac{1}{\sqrt{N}}$, temos $k = \lfloor \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \rfloor$, e segue-se então que $(2k+1)\theta = \frac{\pi}{2} + \epsilon$, com $|\epsilon| \in O(\frac{1}{\sqrt{N}})$ e, portanto mediremos $|x_0\rangle$ com probabilidade

$$\sin^2\left(\frac{\pi}{2} + \epsilon\right) = \cos^2\epsilon \geq 1 - \frac{\epsilon^2}{2} = 1 - O\left(\frac{1}{N}\right),$$

provando o resultado. □

3.3 Classes de complexidade quânticas

Nesta subseção descreveremos as Classes de Complexidade Quânticas mais importantes e iremos relacioná-las às Classes de Complexidade Clássicas. Assumimos um conhecimento básico em Teoria de Complexidade, e revisamos as Classes de Complexidade Clássicas referenciadas aqui no Apêndice C.

3.3.1 Classe BQP

Nesta subseção, iremos apresentar a Classe de Complexidade que contém os problemas considerados tratáveis no modelo computacional quântico. Esta classe foi proposta por Bernstein e Vazirani [25], em seu trabalho sobre Máquinas de Turing Quânticas. Iremos agora definir formalmente a classe BQP.

Definição 3.3.1. *Dizemos que uma linguagem L está na classe BQP, se existe uma um algoritmo quântico A que, dado uma cadeia $x \in \Sigma^*$, A aceita x com probabilidade pelo menos $\frac{2}{3}$ quando $x \in L$ e A rejeita x com probabilidade pelo menos $\frac{2}{3}$ quando $x \notin L$.*[4]

Em outras palavras, a classe BQP contém os problemas que podem ser resolvidos de forma eficiente no modelo computacional quântico com uma probabilidade pequena de erro.

Como limitantes inferiores, temos que P $\subseteq$ BQP, dado que circuitos clássicos podem ser simulados por circuitos quânticos com as Portas de Toffoli, e também que BPP $\subseteq$ BQP, dado que os bits aleatórios podem ser gerados com Portas de

[4] *A probabilidade $\frac{2}{3}$ é arbitrária, e pode ser amplificada para $1 - 2^{-poly(|x|)}$ em tempo polinomial.*

Hadamard, seguidas de medições. Ressaltamos que o Algoritmo de Deutsch-Josza demonstrado anteriormente não prova que P $\neq$ BQP, dado que a separação do algoritmo é relativizada, i.e., dependente de um oráculo usado como caixa-preta.

Bernstein e Vazirani provaram que BQP $\subseteq$ $P^{\#P}$ [25], implicando que BQP está em PSPACE. Posteriormente, Adleman, Demarrais e Huang melhoraram o limitante para a classe PP [3].

Relação entre BQP e NP

Vimos, na Seção 3.2.4 que podemos fazer a busca de um elemento em uma base de dados desordenada de tamanho N em tempo $O(\sqrt{N})$. Para resolver um problema em NP, podemos estender esta base de dados como todos os possíveis certificados do tamanho esperado $n = p(|x|)$ e o oráculo como o circuito do algoritmo verificador. Entretanto, esta alternativa tem complexidade de tempo $O(2^{\frac{n}{2}})$, apresentando uma aceleração quadrática em relação ao modelo clássico, porém mantendo ainda complexidade exponencial.

Pode-se perguntar, então, se é possível fazer melhor tendo acesso ao algoritmo verificador somente como caixa-preta. Em 1997, Bennet, Bernstein Brassard e Vazirani resolveram esta questão negativamente [24]. Eles provaram que ao realizar a busca relativa a um oráculo, temos um limitante inferior $\Omega(\sqrt{N})$ de consultas ao oráculo, e, portanto, não existe um algoritmo mais eficiente assintoticamente que o Algoritmo de Grover.

Entretanto, ainda está em aberto se é possível criar um Algoritmo Quântico para algum problema NP-completo em que é utilizada a estrutura do problema para sua solução, permitindo uma complexidade de tempo polinomial.

3.3.2 Classe QMA

Apesar de a classe NP possuir várias definições equivalentes, essas definições não são facilmente transportadas para o modelo quântico. A abordagem mais utilizada e mais útil hoje em dia é a extensão a partir de conceitos de certificado e algoritmos verificadores.

Definição 3.3.2. *Uma linguagem L está na classe* QMA(C, S)*, se existe um algoritmo quântico verificador V de tempo polinomial, e que satisfaz os seguintes critérios:*

- *(Completude) Para todo $x \in L$, existe um estado quântico $|\psi\rangle$ de tamanho polinomial em relação a entrada e tal que V aceita $|x\rangle|\psi\rangle$ com probabilidade pelo menos C;*
- *(Robustez) Para todo $x \notin L$ e para todos os estados quânticos $|\psi\rangle$ de tamanho polinomial em relação à entrada, V aceita $|x\rangle|\psi\rangle$ com probabilidade no máximo S.*

Segue então a definição canônica de QMA.

Definição 3.3.3. $\mathrm{QMA} = \mathrm{QMA}(\frac{2}{3}, \frac{1}{3})$.

Assim como para a classe BQP, ressaltamos que a escolha das constante $\frac{2}{3}$ e $\frac{1}{3}$ é arbitrária pois pelo Teorema da Repetição Paralela [90], podemos amplificar a completude e a robustez de qualquer constante para $1 - 2^{-poly(|x|)}$ e $2^{-poly(|x|)}$, respectivamente.

Do fato de que $\mathrm{P} \subseteq \mathrm{BQP}$, temos que $\mathrm{NP} \subseteq \mathrm{QMA}$ dado que o algoritmo verificador clássico pode ser usado na versão quântica, bastando que meça o certificado antes de utilizá-lo na computação. O menor limitante superior conhecido até hoje para QMA é a classe PP, e está inclusão foi provada por Watrous e Marriot utilizando resultados de classes de contagem [70].

Hoje, muita pesquisa envolvendo a classe QMA busca generalizar resultados para a classe NP em um contexto quântico. Entretanto, concretamente, não existem tantos resultados. O mais notável destes resultados é a generalização do Teorema de Cook-Levin, onde Kitaev provou que o problema de Hamiltonianos Locais (uma generalização do SAT) é QMA-completo [6]. Hoje, um dos principais problemas em aberto acerca QMA-completude e o problema dos Hamiltonianos Locais, é a busca da generalização do Teorema PCP [17] [18] [37], que provaria que existe uma constante para a qual não existe um algoritmo de aproximação para o problema de Hamiltonianos Locais [5].

Iremos agora estudar algumas variações da classe QMA encontradas na literatura.

$\mathbf{QMA}_1$

Apesar de conseguirmos amplificar a probabilidade de aceitação para $1 - 2^{-poly(|x|)}$, podemos estar interessados no caso em que para instâncias positivas, o algoritmo verificador sempre responderá corretamente.

Definição 3.3.4. *A classe* QMA *com completude perfeita é* $\mathrm{QMA}_1 = \mathrm{QMA}(1, \frac{1}{3})$.

Uma pergunta com origens no contexto clássico em que $\mathrm{MA} = \mathrm{MA}_1$, é se toda linguagem em QMA também está em QMA_1. Esta pergunta ainda está em aberto e discutiremos alguns resultados parciais no Capítulo 5.

QCMA

A classe QCMA é uma classe intermediária entre NP e QMA. Neste caso, o algoritmo verificador é quântico, mas o certificado é ainda clássico. Como todo circuito clássico pode ser transformado em um circuito quântico com aumento de tamanho somente polinomial, temos ainda que $\mathrm{NP} \subseteq \mathrm{QCMA}$. Além disso, temos que um protocolo QMA pode realizar a medição na base computacional e após isso executar o algoritmo verificador QCMA, resultando em $\mathrm{QCMA} \subseteq \mathrm{QMA}$.

Conjectura-se que $\mathrm{NP} \neq \mathrm{QCMA}$ e $\mathrm{QCMA} \neq \mathrm{QMA}$, porém nenhum destes resultados foram provados.

QMA(2)

Uma outra generalização da definição da classe QMA é quando são fornecidas ao Verificador múltiplos certificados por Provadores distintos e não-emaranhados. Para as classes NP e MA, a existência de múltiplos provadores não afeta o poder computacional do modelo, dado que um Provador único consegue simular os múltiplos provadores e vice-versa. Já no modelo quântico, não se espera o mesmo poder computacional.

Seja $\mathrm{QMA}(k)$ a extensão da classe QMA com k provadores. É simples verificar que $\mathrm{QMA} \subseteq \mathrm{QMA}(k)$, pois basta o Verificador ignorar $k-1$ mensagens e utilizar o mesmo algoritmo verificador da classe QMA. Entretanto não se sabe como um Verificador de QMA conseguiria simular um algoritmo verificador de $\mathrm{QMA}(k)$, dado que neste último caso, o algoritmo verificador sabe que as k provas estão não-emaranhadas, e esse fato pode ajudar na rejeição de cadeias que não estão em uma linguagem em $\mathrm{QMA}(k)$.

Por outro lado, sabe-se que $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ [52], para $k \in poly(n)$. A ideia é que os 2 provadores fornecem as k provas, e o verificador utilizará o *Swap test* para verificar se cada uma das supostas provas é um estado puro não-emaranhado.

Além disso, sabe-se que NP está na classe QMA(2) com certificados limitados no tamanho $\log n$ [26, 22, 45], dando evidência de que a classe QMA(2) é uma Classe de Complexidade extensa.

Para limitantes superiores desta classe, o problema ainda está em aberto pois só se sabe que a classe QMA(2) está contida, trivialmente, em NEXP.

NQP

A classe NQP não é exatamente uma variação da classe QMA, mas foi a primeira proposição de um análogo quântico da classe NP, porém baseada na definição envolvendo algoritmos não-determinísticos.

Esta classe consiste das linguagens para as quais existe um algoritmo quântico que aceita uma cadeia com probabilidade não nula se e somente se esta cadeia está na linguagem.

Não se sabe ao certo qual a relação entre as classes NQP e QMA. Entretanto Kobayashi, Matsumoto e Yamakami [65] provaram que

$$\mathrm{NQP} = \bigcup_{f:\mathbb{Z}\to(0,1]} \mathrm{QMA}(f, 0),$$

onde $\mathrm{QMA}(f, 0)$, para f constante, é a classe QMA com robustez perfeita.

3.3.3 Sistemas Interativos de Provas Quânticos

Sistemas Interativos de Provas Quânticos, QIP, são generalizações dos Sistemas Interativos de Prova, descritos no Apêndice C.8, onde o Provador e Verificador possuem poder computacional quântico. A ideia geral é que um Verificador, que possui poder computacional quântico, porém limitado, troca mensagens quânticas com um Provador de poder computacional ilimitado, a fim de reconhecer uma linguagem. O Provador irá ajudar o Verificador a provar que cadeias estão na linguagem, porém o Verificador deverá ser robusto de forma a não ser enganado por um Provador desonesto.

Um dos resultados mais importante neste modelo computacional é que podemos reduzir alguns recursos do modelo, mantendo o mesmo poder computacional. Kitaev e Watrous provaram que é possível cobrir toda a classe QIP com apenas 3 mensagens e completude perfeita [63]. Ressaltamos que, além do artigo original, este resultado

pode ser encontrado de uma forma mais didática e em português, na dissertação de Cardonha [28].

Como PSPACE = IP $\subseteq$ QIP, ficou ainda aberta a questão se esta continência era estrita. Recentemente, Jain, Ji, Upadhyay e Watrous provaram que QIP $\subseteq$ PSPACE, provando a igualdade entre estas classes [56].

Capítulo 4

Autômatos quânticos

Além dos modelos computacionais mais importantes no quesito de computabilidade como Máquinas de Turing e Circuitos booleanos, outros modelos foram também estendidos tendo como base o novo paradigma da Mecânica Quântica, de forma a estudar a influência direta desta nova teoria em processo computacionais. Neste capítulo estudaremos um destes modelos, os Autômatos Finitos Quânticos. Iniciaremos o estudo apresentando rapidamente os primeiros modelos computacionais deste tipo desenvolvidos. Em seguida, apresentaremos o nosso objeto principal de estudo neste capítulo, os Autômatos Finitos Bidirecionais com Estados Quânticos e Clássicos (2QCFA do inglês *Two-Way Finite Automata with Quantum and Classical States*). Estudaremos propriedades deste modelo, seu poder computacional e finalizaremos com um estudo parcial dos limites deste modelo.

Este capítulo é baseado em um trabalho apresentado na escola *Computer Science days in Ekaterinburg (CSEdays)* [49] e publicado *Siberian Electronic Mathematical Reports* [50], abordando o modelo 2QCFA e apresentando propriedades e linguagens reconhecidas pelo modelo. A Seção 4.5, que apresenta as linguagens reconhecidas por 2QCFAs de uma forma hierarquizada, é baseada no trabalho apresentado no *IV Workshop-Escola de Computação e Informação Quântica* [48].

4.1 Introdução

Vimos que os principais modelos computacionais quânticos, Máquinas de Turing Quânticas e Circuitos Quânticos, são extensões diretas de modelos similares da Teo-

ria de Computação Clássica, adicionando comportamentos oriundos da Mecânica Quântica.

Considerando que a Computação Quântica tem como um dos objetivos estudar a influência da Mecânica Quântica em processos computacionais, podemos estender outros modelos computacionais mais simples de forma a verificar o comportamento dos novos modelos em relação a seus análogos clássicos.

Além disso, experimentalmente, hoje não se consegue construir um sistema computacional estável com muitos *qubits*. Portanto, estudar modelos computacionais em que estes recursos são limitados nos ajuda a entender situações em que os modelos quânticos teriam aplicações com ganhos substanciais em relação a modelos computacionais clássicos.

Iremos, inicialmente, definir modelos de Autômatos Finitos Quânticos que iniciaram o estudo na área, entretanto nosso principal objeto de estudo serão os Autômatos Finitos Bidirecionais com Estados Clássicos e Quânticos (2QCFA). Neste modelo, os estados clássicos controlam a cabeça de leitura, bem como a aceitação e rejeição da cadeia de entrada, enquanto os estados quânticos são utilizados como uma memória auxiliar. Este modelo surgiu para resolver alguns problemas apontados nos modelos de Autômatos Finitos puramente Quânticos propostos anteriormente a ele.

Neste modelo, conseguimos simular tanto Autômatos Finitos Determinísticos quanto comportamento randômico [1]. Portanto, estamos particularmente interessados nos resultados em que os 2QCFAs demonstram um poder computacional maior que Autômatos Finitos Determinísticos e Probabilísticos. Com este objetivo, estudaremos algumas linguagens reconhecidas pelo modelo, estabelecendo um paralelo com a hierarquia clássica de linguagens formais. Destacamos que esta hierarquização foi feita de maneira inédita durante o mestrado do candidato [48].

Finalmente, estudaremos os limites do modelo, deixando em aberto uma conjectura sobre linguagens decidíveis que não são reconhecidas pelo modelo. Mostraremos um resultado parcial já provado no trabalho de Yakaryilmaz e Say [92], entretanto apresentamos uma nova prova, mais direta e contendo elementos mais simples do que a prova original, sendo também resultado do trabalho de mestrado do candidato [49][50].

[1] Como vimos na Seção 2.5.1, podemos simular uma moeda aplicando sobre $|0\rangle$ o operador de Hadamard e realizar a medição logo em seguida

4.2 Trabalhos relacionados

Inicialmente, foram propostas duas definições independentes de Autômatos Quânticos Finitos. Moore e Crutchfield [73] propuseram o Autômato Finito Quântico Unidirecional de Medida-Única (MO-1QFA do inglês *Measure-Once One-way Quantum Finite Automata*). Neste modelo, temos que a configuração de um MO-1QFA é a superposição unitária de estados quânticos cuja função de transição, dependente do símbolo sob a cabeça de leitura, deve ser unitária de modo a respeitar os fundamentos da Mecânica Quântica. Veremos agora de forma um pouco mais detalhada o funcionamento deste modelo.

Definição 4.2.1. *Um MO-1QFA* $M = (\mathcal{Q}, \Sigma, |q_0\rangle, \{U_\sigma\}, \mathcal{Q}_a)$ *é uma 5-tupla onde*

- $\mathcal{Q}$ *é um espaço de Hilbert complexo finito;*
- Σ *é um alfabeto finito de símbolos;*
- $|q_0\rangle \in \mathcal{Q}$ *é o estado inicial de* M*;*
- $\{U_\sigma\}$*, para* $\sigma \in \Sigma$*, é um conjunto de matrizes unitárias de transição associadas a cada símbolo do alfabeto;*
- $\mathcal{Q}_a \subseteq \mathcal{Q}$ *é o subespaço de aceitação, sendo que o projetor* P_a *está associado a ele.*

Ao computar sobre uma cadeia $w = w_1...w_n$, o MO-1QFA começa no estado inicial $|q_0\rangle$ e com a cabeça de leitura sobre o símbolo w_1. Em seguida, aplica a operação associada a cada símbolo w_i e move a cabeça de leitura para a próxima posição. Após computar sobre toda a cadeia, é realizada uma medição em relação aos projetores $\{P_a, I - P_a\}$, e se o resultado estiver em $\mathcal{Q}_a$ consideramos que M aceita a cadeia, rejeitando caso contrário. A probabilidade de aceitação de w, é então

$$p_a(w) = ||P_a U_{w_n} ....U_{w_1}|q_0\rangle||^2.$$

e, neste caso, podemos estabelecer critérios de reconhecimento de linguagens $L \subseteq \Sigma^*$ tais como

- para todo $w \in L$, $p_a(w) \geq \lambda_a$, e
- para todo $w \notin L$, $p_a(w) \leq \lambda_r$,

para $\lambda_a, \lambda_r \in [0,1]$ fixos, $\lambda_a > \lambda_r$.

Moore e Crutchfield provaram alguns fechos para as linguagens reconhecidas pelo modelo, um lema do bombeamento e também que o conjunto de linguagens reconhecida por MO-1QFAs é um subconjunto estrito das linguagens regulares.

Kondacs e Watrous [66], de forma independente de Moore e Crutchfield, propuseram uma outra variante de Autômatos Finitos Quânticos na qual a cada passo, é realizada uma medida. Este novo modelo é conhecido como os Autômatos Quânticos Finitos de Várias-Medidas, e foram estudadas suas versões unidirecionais (MM-1QFA do inglês *Many-Measure one-way quantum finite automata*) e bidirecionais (MM-2QFA do inglês *Many-Measure two-way quantum finite automata*).

A principal diferença deste modelo quando comparado ao proposto por Moore e Crutchfield é que são definidos subespaços de aceitação, rejeição e continuação. A cada passo, é feita a medição pelos projetores correspondentes a esses subespaços, e, se o resultado da medição estiver no subespaço de aceitação ou rejeição, o MM-QFA para. Vamos agora definir mais formalmente o modelo.

Definição 4.2.2. *Um MM-QFA* $M = (\mathcal{Q}, \Sigma, |q_0\rangle, \delta, \mathcal{Q}_a, \mathcal{Q}_r)$ *é uma 6-tupla onde*

- $\mathcal{Q}$ *é um espaço de Hilbert complexo finito*
- Σ *é um alfabeto finito de símbolos*
- $|q_0\rangle \in \mathcal{Q}$ *é o estado inicial de* M
- δ *é a função de transição dos estados quânticos*
- $\mathcal{Q}_a \subseteq \mathcal{Q}$ *é o subespaço de aceitação, sendo que o projetor* P_a *está associado a ele.*
- $\mathcal{Q}_r \subseteq \mathcal{Q}$ *é o subespaço de rejeição, ortogonal a* $\mathcal{Q}_a$*, sendo que o projetor* P_r *está associado a ele.*

Para os MM-1QFA, a função de transição δ é igual a do modelo MO-1QFA. Neste caso a computação é diferente pois, após aplicar δ, é feita a medição em relação a $\{P_a, P_r, I - P_a - P_r\}$, e se o resultado da medição estiver em $\mathcal{Q}_a$ ou $\mathcal{Q}_r$, o autômato irá parar, aceitando ou rejeitando. O reconhecimento de linguagens também está associado à probabilidade com a qual as cadeias de entrada são aceitas. Kondacs

e Watrous provaram que o conjunto de linguagens reconhecidos por este modelo também é um subconjunto estrito das linguagens regulares.

Para a variante bidirecional (MM-2QFA), existem algumas diferenças. Primeiramente, para demarcar a cadeia de entrada, assumimos que existem dois marcadores, um à esquerda da cadeia na posição 0 da fita (†) e um à direita na posição $|w|+1$ da fita (‡), com $\dagger, \ddagger \notin \Sigma$. Denotamos $\Gamma = \Sigma \cup \{\dagger, \ddagger\}$ como o alfabeto da fita. A função de transição δ também é diferente, dado que deve definir a posição para a qual a cabeça de leitura vai se movimentar. Definimos então a função de transição

$$\delta : \mathcal{Q} \times \Gamma \times \mathcal{Q} \times \{-1, 0, 1\} \to \mathbb{C},$$

ou seja, estando a cabeça de leitura sob o símbolo $\sigma \in \Gamma$ no estado $|q_1\rangle \in \mathcal{Q}$, o MM-2QFA faz a transição para o estado $|q_2\rangle \in \mathcal{Q}$ e altera a posição da cabeça de leitura para posição $d \in \{-1, 0, 1\}$ com amplitude $\delta(|q_1\rangle, \sigma, |q_2\rangle, d)$. Assumimos que quando está em um marcador, a função de transição nunca move a cabeça de leitura para fora da fita. Outra característica de δ também é ser reversível e unitária, para obedecer os postulados da Mecânica Quântica.

A computação de um MM-2QFA, então, será começar no estado $|q_0\rangle$, na posição 0 da fita e aplicar sucessivamente a função de transição δ e realizar uma medição segundo os projetores $\{P_a, P_r, I - P_a - P_r\}$. Se após a medição, o estado resultante estiver em $\mathcal{Q}_a$ ou $\mathcal{Q}_r$, o autômato para, aceitando ou rejeitando. Kondacs e Watrous provaram que o conjunto de linguagens reconhecidas por MM-2QFAs são um superconjunto das linguagens regulares.

No modelo MM-2QFA, uma configuração da computação é uma superposição de estados e posição na fita, permitindo a cabeça de leitura estar em diferente posições ao mesmo tempo. Isso implica, em termos práticos, que o modelo só seria implementável com uma memória de pelo menos $\log |w|$ bits de informação, o que contradiz seu tamanho finito.

Para resolver este problema, Ambainis e Watrous [11] propuseram uma nova variante quântica para autômatos finitos chamada Autômato Finito Bidirecional com Estados Clássicos e Quânticos (2QCFA do inglês *Two-Way Finite Automata with Quantum and Classical States*). Este modelo será estudado em profundidade neste trabalho e daremos sua definição formal na próxima seção. A ideia geral é que um conjunto de estados clássicos que controla a cabeça de leitura e a aceitação ou rejeição da cadeia de entrada. Este conjunto clássico de estados define também as operações que serão realizadas em um número constante de estados quânticos.

Com essa variação, teremos em todo momento uma configuração clássica e quântica, ambas de tamanho constante. No trabalho original sobre este modelo, Ambainis e Watrous [11] mostraram linguagens não-regulares que são reconhecidas pelo modelo 2QCFA.

Macko [69] estudou propriedades de fecho para vários modelos de autômatos finitos quânticos. Para as linguagens reconhecidas por 2QCFAs, foi provado que o fecho por homomorfismo é igual ao conjunto das linguagens recursivamente enumeráveis.

Posteriormente, Qiu [77] provou para o conjunto de linguagens reconhecidos com erro unilateral por 2QCFAs fechos por união, intersecção, reversão e concatenação com algumas restrições. Utilizando estes resultados de fecho, Qiu também mostrou outras linguagens não-regulares reconhecidas pelo modelo.

Zheng, Liu e Li [80][81] estudaram famílias de linguagens que podem ser reconhecidas por 2QCFAs com um número de estados assintoticamente inferior ao necessário por autômatos não-determinísticos e probabilísticos.

4.3 O modelo 2QCFA

Como vimos na seção anterior, dadas a crítica ao tamanho dos estados no modelo MM-2QFA, Ambainis e Watrous [11] propuseram o modelo de Autômatos Finitos Bidirecionais com Estados Quânticos e Clássicos (2QCFA). Neste modelo, a cabeça de leitura pode se mover para a direita, esquerda ou permanecer na mesma posição, assim como nos MM-2QFAs. Entretanto este movimento será determinado pelos estados clássicos, implicando que a cabeça de leitura estará somente em uma posição em qualquer momento da computação do autômato. Os estados quânticos servirão como uma "memória" durante a computação. Vamos agora definir formalmente este modelo.

Definição 4.3.1. *Um 2QCFA é uma* 9*-tupla* $M = (\mathcal{Q}, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_a, S_r)$, *onde*

- $\mathcal{Q}$ *é o conjunto de estados quânticos;*
- S *é o conjunto de estados clássicos;*
- Σ *é o alfabeto de entrada;*
- Θ *é o operador de evolução quântico;*

- δ *é a função de transição clássica;*
- $|q_0\rangle \in \mathcal{Q}$ *é o estado inicial quântico;*
- $s_0 \in S$ *é o estado inicial clássico;*
- $S_a \subseteq S$ *é o conjunto de estados de aceitação;*
- $S_r \subseteq S$ *é o conjunto de estados de rejeição, sendo* $S_a \cap S_r = \emptyset$.

Assim como no MM-2QFA, assumimos que, além da cadeia de uma entrada w, a fita contém um marcador à esquerda † na posição 0 da fita e um marcador à direita ‡ na posição $|w| + 1$. O alfabeto de fita é $\Gamma = \Sigma \cup \{\dagger, \ddagger\}$.

Definição 4.3.2. *O conjunto de estados finais é* $S_f = S_a \cup S_r$ *e o conjunto de estados não finais* $S_{nf} = S \backslash S_f$.

Como estabelecido na teoria da Mecânica Quântica, operadores sobre sistemas quânticos assumem dois tipos: transformações lineares unitárias e medições. Neste modelo a operação sobre o estado quântico é definida a partir da configuração clássica do autômato. Portanto, a função de evolução dos estados quânticos Θ é dada por $\Theta : S_{nf} \times \Gamma \to \mathcal{U}(\mathcal{Q}) \cup \mathcal{M}(\mathcal{Q})$, onde $\mathcal{U}(\mathcal{Q})$ é o conjunto de operadores lineares unitários sobre o espaço de Hilbert $\mathcal{Q}$ e $\mathcal{M}(\mathcal{Q})$ é o conjunto de medições projetivas sobre $\mathcal{Q}$. Denotaremos como $P \in \mathcal{M}(\mathcal{Q})$ como um conjunto de projetores $\{\Pi_1, ..., \Pi_m\}$, para $m \leq dim(\mathcal{Q})$ [2]. Dado o estado quântico $|\psi\rangle \in \mathcal{Q}$, se consideramos a medição referente a P, temos que o resultado será i com probabilidade $||\Pi_i|\psi\rangle||^2$ e, neste caso, o estado quântico colapsa para $\frac{\Pi_i|\psi\rangle}{||\Pi_i|\psi\rangle||^2}$, com $1 \leq i \leq m$.

A função de transição δ depende, como no caso clássico, do estado clássico atual e do símbolo sob a cabeça de leitura, e depende também de Θ. Caso $\Theta(s, \sigma) \in \mathcal{U}(\mathcal{Q})$, $\delta : S_{nf} \times \Gamma \to S \times \{-1, 0, 1\}$ irá mapear a configuração clássica atual para um novo estado clássico e definirá a direção de movimento da cabeça de leitura. Caso $\Theta(s, \sigma) = P \in \mathcal{M}(\mathcal{Q})$, seja R o conjunto dos possíveis resultados da medição. Neste caso δ também poderá utilizar este resultado para realizar a transição, sendo $\delta : S_{nf} \times \Gamma \times R \to S \times \{-1, 0, 1\}$.

Assumimos que quando o símbolo sob a cabeça de leitura é um marcador, a transição correspondente sob δ manterá a cabeça de leitura nas posições válidas da fita.

[2] Veja a Seção 2.2.3 sobre projeções projetivas.

A computação de um 2QCFA M consiste na aplicação sucessiva das funções de transição Θ e δ até que o estado clássico seja um estado de aceitação ou rejeição. Neste caso, M para, aceitando ou rejeitando a cadeia de entrada.

Como a função de transição clássica δ pode depender do resultado de medições, que são intrinsecamente probabilísticas, os estados clássicos também possuem uma natureza probabilística. Isso resulta que, como nos outros modelos vistos na Seção 4.2, podemos atribuir uma probabilidade $p_a(w)$ de aceitação da cadeia de entrada w. Da mesma forma, podemos definir a probabilidade de rejeição de w como $p_r(w)$. Se assumimos que os 2QCFAs sempre param, temos que $p_a(w) + p_r(w) = 1$.

Considerando as probabilidades com que cadeias são aceitas ou rejeitadas por 2QCFAs, podemos definir classes de linguagens decididas pelo modelo. A primeira delas é definida como as linguagens que conseguem ser reconhecidas de modo exato por algum 2QCFA.

Definição 4.3.3. *Um autômato quântico M reconhece uma linguagem L com erro zero se para todo $w \in L$, temos $p_a(w) = 1$ e para todo $w \notin L$, temos $p_r(w) = 1$.*

Podemos, entretanto, relaxar a restrição e exigir que o autômato sempre responda corretamente para cadeias que estão na linguagem, caso contrário, aceitamos um erro ϵ definido previamente.

Definição 4.3.4. *Um autômato quântico M reconhece uma linguagem L com erro unilateral ϵ se para todo $w \in L$, temos $p_a(w) = 1$, e para todo $w \notin L$, temos $p_r(w) > 1 - \epsilon$.*

4.4 Fechos

Iremos, nesta seção, apresentar alguns resultados de fecho para o conjunto de linguagens reconhecidas por 2QCFAs com erro unilateral limitado.

Grande parte das provas apresentadas nesta seção são variações das provas apresentadas por Qiu [77] e a prova do fecho por homomorfismo inverso foi inspirada por resultados provados por Macko [69].

4.4.1 Intersecção

Nesta seção iremos provar que as linguagens aceitas por 2QCFAs com erro unilateral são fechadas pela operação de intersecção.

A ideia da prova é construir um 2QCFA M que simula o funcionamento de dois outros 2QCFA M_1 e M_2 em série, rejeitando uma cadeia quando M_1 rejeitaria e, caso M_1 fosse aceitá-la, M finaliza simulando o funcionamento de M_2. Iniciaremos mostrando a probabilidade com que M aceita e rejeita, baseado nas probabilidades de aceitação de M_1 e M_2. O fecho por intersecção segue diretamente.

Teorema 4.4.1 (Variação do Teorema 1 de Qiu [77])**.** *Para $i \in \{1, 2\}$, seja M_i um 2QCFA tal que M_i para ao computar sobre $w \in \Sigma^*$ em tempo esperado $O(t_i(|w|))$ e a probabilidade de aceitação e rejeição são, respectivamente, $p_{a_i}(w)$ e $p_{r_i}(w)$. Então existe um 2QCFA M tal que, ao computar sobre uma cadeia $w \in \Sigma^*$, M aceita com probabilidade $p_{a_1}(w)p_{a_2}(w)$ e rejeita com probabilidade $p_{r_1}(w) + p_{a_1}(w)p_{r_2}(w)$, sendo que M para sobre w em tempo esperado $O(t_1(|w|) + t_2(|w|) + |w|)$.*

Demonstração. Sejam

$$M_1 = (\mathcal{Q}_1, S_1, \Sigma, \Theta_1, \delta_1, |q_{0_1}\rangle, s_{0_1}, S_{a_1}, S_{r_1}) \text{ e}$$
$$M_2 = (\mathcal{Q}_2, S_2, \Sigma, \Theta_2, \delta_2, |q_{0_2}\rangle, s_{0_2}, S_{a_2}, S_{r_2})$$

os 2QCFAs do enunciado e $S_{n_i} = S \backslash (S_{a_i} \cup S_{r_i})$ o conjunto de estados não-finais de M_i.

Iremos agora construir um 2QCFA $M = (\mathcal{Q}, S, \Sigma, \Theta, \delta, |q_0\rangle, s_0, S_a, S_r)$ com as propriedades desejadas e, para isso, sejam

$$\begin{aligned}
\mathcal{Q} &= \mathcal{Q}_1 \otimes \mathcal{Q}_2, \\
S &= S_1 \cup S_2 \\
|q_0\rangle &= |q_{0_1}\rangle |q_{0_2}\rangle, \\
s_0 &= s_{0_1}, \\
S_a &= S_{a_2} \text{ e} \\
S_r &= S_{r_1} \cup S_{r_2}.
\end{aligned}$$

Antes de estudar o funcionamento do operador de evolução quântica Θ, vamos definir o conjunto de projetores que serão utilizados no novo 2QCFA. Para um conjunto de projetores $P_1 = \{\Pi_1, ..., \Pi_m\}$ sobre o espaço $\mathcal{Q}_1$, iremos definir o conjunto de projetores $P_1' = \{\Pi_1', ...\Pi_m'\}$ tal que $\Pi_i' = \Pi_i \otimes I_{\mathcal{Q}_2}$. Da mesma forma, para um conjunto de projetores $P_2 = \{\Psi_1, ..., \Psi_m\}$ sobre o espaço $\mathcal{Q}_2$, iremos definir o conjunto de projetores $P_2'' = \{\Psi_1', ...\Psi_m'\}$ tal que $\Psi_i' = I_{\mathcal{Q}_1} \otimes \Psi_i$.

A função Θ será definida como

$$\Theta(s,\sigma) = \begin{cases} \text{aplicar } V_1 \otimes I_{\mathcal{Q}_2}, & \text{se } s \in S_{n_1} \text{ e } \Theta_1(s,\sigma) = V_1 \in \mathcal{U}(\mathcal{Q}_1) \\ \text{medir com } P_1', & \text{se } s \in S_{n_1} \text{ e } \Theta_1(s,\sigma) = P_1 \in \mathcal{M}(\mathcal{Q}_1) \\ \text{aplicar } I_{\mathcal{Q}_1} \otimes I_{\mathcal{Q}_2}, & \text{se } s \in S_{a_1} \\ \text{aplicar } I_{\mathcal{Q}_1} \otimes V_2, & \text{se } s \in S_{n_2} \text{ e } \Theta_2(s,\sigma) = V_2 \in \mathcal{U}(\mathcal{Q}_2) \\ \text{medir com } P_2'', & \text{se } s \in S_{n_2} \text{ e } \Theta_2(s,\sigma) = P_2 \in \mathcal{M}(\mathcal{Q}_2) \end{cases}.$$

Como, por construção, o estado inicial é o produto tensorial entre os estados inicias dos 2QCFAs M_1 e M_2 e as operações unitárias são realizadas não-trivialmente somente em um dos subespaços relativo a $\mathcal{Q}_1$ ou $\mathcal{Q}_2$, realizar a medição considerando $P_1 \in \mathcal{M}(\mathcal{Q}_1)$ sobre um estado $|\psi\rangle \in \mathcal{Q}$ é equivalente a realizar a medição $P_1' \in \mathcal{M}(\mathcal{Q}_1 \otimes \mathcal{Q}_2)$ sobre $|\psi\rangle \otimes |\phi\rangle \in \mathcal{Q}_1 \otimes \mathcal{Q}_2$, dado que a medição terá como resultado i com a mesma probabilidade e, neste segundo caso, teremos que o estado colapsa para $\Pi_i|\psi\rangle \otimes |\phi\rangle$, não alterando o estado relativo a $\mathcal{Q}_2$. Pelo mesmo argumento, é equivalente aplicar $P_2 \in \mathcal{M}(\mathcal{Q}_2)$ e aplicar $P_2'' \in \mathcal{M}(\mathcal{Q}_1 \otimes \mathcal{Q}_2)$, em nosso caso.

A função de transição clássica δ deverá ser definida após medições e após operações unitárias. Após medições, a função de transição clássica deverá se comportar como as funções originais:

$$\delta(s,\sigma,i) = \begin{cases} \delta_1(s,\sigma,i), & \text{se } s \in S_1 \\ \delta_2(s,\sigma,i), & \text{se } s \in S_2 \end{cases}.$$

Após a aplicação de uma operação unitária, δ será:

$$\delta(s,\sigma) = \begin{cases} \delta_1(s,\sigma), & \text{se } s \in S_{n_1} \\ \delta_2(s,\sigma), & \text{se } s \in S_{n_2} \\ (s,-1), & \text{se } s \in S_{a_1} \text{ e } \sigma \in \Sigma \cup \{\ddagger\} \\ (s_{0_2},0), & \text{se } s \in S_{a_1} \text{ e } \sigma = \dagger \end{cases}.$$

Por construção, M irá simular o funcionamento de M_1 até que o estado clássico s esteja em $S_{a_1} \cup S_{r_1}$. Devemos notar que o funcionamento de M nesta primeira fase equivale ao funcionamento de M_1 dado que a configuração clássica é a igual a de M_1, o estado quântico inicial não está emaranhado com nenhum outro sistema e o subespaço referente à simulação de M_2 não é alterado nem medido. Neste caso,

se $s \in S_{r_1}$, M rejeita a cadeia de entrada. Caso a configuração clássica de M entre em algum estado de S_{a_1}, pela construção de δ, a cabeça de leitura voltará a primeira posição da fita de entrada e M começará a simular M_2. Para a cadeia de entrada $w \in \Sigma^*$, a probabilidade de rejeição nesta primeira fase é de $p_{r_1}(w)$ e a probabilidade com que M irá começar a simular M_2 é de $p_{a_1}(w)$.

A simulação de M_2 não será afetada pela simulação prévia de M_1, dado que a configuração clássica inicial será a mesma que M_2 espera e, como dito anteriormente, o estado quântico referente a $\mathcal{Q}_2$ não foi alterado. Portanto, ao começar, M simulará M_2 sem nenhuma diferença de comportamento. Neste caso, as probabilidades de aceitação e rejeição da cadeia de entrada w, na simulação de M_2 será $p_{a_2}(w)$ e $p_{r_2}(w)$, respectivamente. Como a probabilidade de entrar na segunda fase é de $p_{a_1}(w)$, temos que a probabilidade de aceitação e rejeição durante a simulação de M_2 é $p_{a_1}(w)p_{a_2}(w)$ e $p_{a_1}(w)p_{r_1}(w)$, respectivamente.

Logo, a probabilidade de aceitação de w na computação por M é de $p_{a_1}(w)p_{a_2}(w)$ e a probabilidade de rejeição é $p_{r_1}(w) + p_{a_1}(w)p_{r_2}(w)$.

O tempo esperado da computação da primeira fase sobre a entrada w é igual ao tempo esperado $O(t_1(|w|))$ de M_1, e o tempo esperado da segunda fase é igual ao tempo esperado de computação da entrada w por M_2, $O(t_2(|w|))$. Como para passar da primeira fase para a segunda a cabeça de leitura deve voltar para a primeira posição, existe o custo computacional de no máximo $|w|$ passos entre as fases. Portanto, M para ao computar w em tempo $O(t_1(|w|) + t_2(|w|) + |w|)$. □

Considerando os 2QCFA M_1 e M_2 que reconhecem as linguagens L_1 e L_2 com erro unilateral ϵ, temos que $p_{a_i}(w) = 1$ para $w \in L_i$ e $p_{r_i}(w) \geq 1 - \epsilon$ para $w \notin L_i$. Com isso, o fecho por intersecção passa a ser um caso especial do Teorema 4.4.1.

Corolário 4.4.2. *Sejam $L_1, L_2 \subset \Sigma^*$ duas linguagens decidíveis pelo modelo 2QCFAs com erro unilateral ϵ em tempo esperado $O(t_1(|w|))$ e $O(t_2(|w|)$, respectivamente. Então $L_1 \cap L_2$ é decidível por um 2QCFA com erro unilateral $2\epsilon - \epsilon^2$ em tempo esperado $O(t_1(|w|) + t_2(|w|) + |w|)$.*

4.4.2 União

Nesta seção provaremos o fecho por união das linguagens reconhecidas por 2QCFAs com erro unilateral, de uma forma bem semelhante àquela utilizada na Seção 4.4.1.

A intuição acerca do 2QCFA construído nesta seção é bem semelhante ao da seção anterior, sendo a única diferença a condição em que será iniciada a simulação do segundo 2QCFA. Começaremos, do mesmo modo, provando um teorema mais genérico antes de provar o o resultado de fecho.

Teorema 4.4.3 (Variação do Teorema 2 de Qiu [77])**.** *Para $i \in \{1, 2\}$, seja M_i um 2QCFA tal que M_i para sobre $w \in \Sigma^*$ em tempo esperado $O(t_i(|w|))$ e a probabilidade de aceitação e rejeição são, respectivamente, $p_{a_i}(w)$ e $p_{r_i}(w)$. Então existe um 2QCFA M tal que, para uma cadeia $w \in \Sigma^*$, M a aceita com probabilidade $p_{a_1}(w) + p_{r_1}(w)p_{a_2}(w)$ e a rejeita com probabilidade $p_{r_1}(w)p_{r_2}(w)$, sendo que M para sobre w em tempo $O(t_1(|w|) + t_2(|w|) + |w|)$.*

Ideia da prova. No Teorema 4.4.1, o 2QCFA M foi construído de forma a simular inicialmente M_1 e ao chegar em um estado final de aceitação, M começaria a simular M_2; se fosse de rejeição, M rejeitaria a cadeia de entrada.

Para este teorema, M deve ser construído de forma análoga, mas ao chegar em um estado final de M_1, se for um estado de aceitação M aceitará e, se for um estado de rejeição M começará a simular M_2.

Utilizando os mesmos elementos do Teorema 4.4.1, é fácil perceber que a probabilidade total de aceitação é $p_{a_1}(w) + p_{r_1}(w)p_{a_2}(w)$ e a probabilidade de rejeição é $p_{r_1}(w)p_{r_2}(w)$, e que o tempo esperado para que M pare é $O(t_1(|w|) + t_2(|w|) + |w|)$. □

Considerando os 2QCFAs M_1 e M_2 que reconhecem as linguagens L_1 e L_2 com erro unilateral ϵ, temos que $p_{a_i}(w) = 1$ para $w \in L_i$ e $p_{r_i}(w) \geq 1 - \epsilon$ para $w \notin L_i$. Com isso, temos que o fecho por intersecção é um caso especial do Teorema 4.4.3.

Corolário 4.4.4. *Sejam $L_1, L_2 \subset \Sigma^*$ duas linguagens decidíveis pelo modelo 2QCFAs com erro unilateral ϵ em tempo esperado $O(t_1(|w|))$ e $O(t_2(|w|)$, respectivamente. Então $L_1 \cup L_2$ é decidível por um 2QCFA com erro unilateral $2\epsilon - \epsilon^2$ em tempo esperado $O(t_1(|w|) + t_2(|w|) + |w|)$.*

4.4.3 Concatenação

Veremos agora a prova de que a concatenação de duas linguagens reconhecidas com erro unilateral por 2QCFAs cujos alfabetos são disjuntos também é reconhecida por 2QCFAs com erro unilateral.

A ideia, novamente, é simular os dois 2QCFAs em série, e, como os alfabetos são disjuntos, consideramos os símbolos de um alfabeto como marcadores de fim de cadeia para o 2QCFA da outra linguagem.

Teorema 4.4.5 (Variação do Teorema 5 de Qiu [77])**.** *Para $i \in \{1, 2\}$, sejam Σ_i um alfabeto e M_i um 2QCFA tal que M_i para ao computar sobre $w \in \Sigma_i^*$ em tempo esperado $O(t_i(|w|))$ e cujas probabilidades de aceitação e rejeição são, respectivamente, $p_{a_i}(w)$ e $p_{r_i}(w)$, para $\Sigma_1 \cap \Sigma_2 = \emptyset$. Então existe um 2QCFA M tal que, para uma cadeia $w = uv$, tal que $u \in \Sigma_1^*$ e $v \in \Sigma_2^*$, M aceita com probabilidade $p_{a_1}(u)p_{a_2}(v)$ e rejeita com probabilidade $p_{r_1}(u) + p_{a_1}(u)p_{r_2}(v)$, sendo que M para ao computar sobre w em tempo $O(t_1(|u|) + t_2(|v|) + |w|)$. Caso w não esteja na forma uv descrita, a cadeia é rejeitada com probabilidade* 1*.*

Ideia da prova. A ideia da prova é primeiramente verificar se a cadeia de entrada w está no formato uv, $u \in \Sigma_1^*$ e $v \in \Sigma_2^*$, rejeitando se não estiver. Como veremos posteriormente, isto pode ser feito com erro zero e em tempo linear no tamanho da entrada dado que estamos tratando de uma linguagem regular. Veja o Teorema 4.5.1.

Então, o 2QCFA M irá simular M_1 na primeira parte da entrada, tratando os símbolos em Σ_2 da mesma forma que o marcador direito ‡. Se M_1 fosse aceitar a cadeia, M vai para o primeiro símbolo da cadeia que esteja no conjunto $\Sigma_2 \cup \{‡\}$, e então começará a simular M_2 na segunda parte da cadeia, tratando elementos de Σ_1 como o marcador esquerdo †.

Utilizando os mesmos elementos do Teorema 4.4.1, é fácil perceber que, quando a cadeia está no formato explicitado no enunciado, a probabilidade total de aceitação é $p_{a_1}(u)p_{a_2}(v)$ e a probabilidade de rejeição é $p_{r_1}(u) + p_{a_1}(v)p_{r_2}(v)$, e o tempo esperado para que M pare é de $O(t_1(|u|) + t_2(|v|) + |w|)$. □

Segue, direto do Teorema 4.4.5, o corolário da concatenação de linguagens reconhecidas com erro unilateral ϵ cujos alfabetos são disjuntos.

Corolário 4.4.6. *Sejam $L_1 \subseteq \Sigma_1^*$ e $L_2 \subseteq \Sigma_2^*$, $\Sigma_1 \cap \Sigma_2 = \emptyset$, duas linguagens decidíveis pelo modelo 2QCFAs com erro unilateral ϵ em tempo esperado $O(t_1(|w|))$ e $O(t_2(|w|))$, respectivamente. Então $L_1 \cdot L_2$ é decidível por um 2QCFA com erro unilateral $2\epsilon - \epsilon^2$ em tempo esperado $O(t_1(|w|) + t_2(|w|) + |w|)$.*

4.4.4 Reversão

Iremos mostrar nesta seção que o conjunto de linguagens reconhecidas por 2QCFAs com erro unilateral também é fechado por reversão. A ideia da prova é simples pois, como a cabeça de leitura é bidirecional, basta realizar a computação "de trás para frente".

Teorema 4.4.7 (Variação do Teorema 4 de Qiu [77])**.** *Seja M um 2QCFA tal que M para ao computar sobre $w \in \Sigma^*$ em tempo esperado $O(t(|w|))$ e cujas probabilidades de aceitação e rejeição são, respectivamente, $p_a(w)$ e $p_r(w)$. Então existe um 2QCFA M^R tal que, para uma cadeia $w \in \Sigma^*$, M a aceita com probabilidade $p_a(w^R)$ e a rejeita com probabilidade $p_r(w^R)$, sendo que M^R para ao computar sobre w em tempo esperado $O(t(|w|) + |w|)$.*

Demonstração. Seja $M = (Q, S, \Sigma, \Theta, \delta, q_0, s_0, S_a, S_r)$ o 2QCFA do enunciado. Vamos agora construir o 2QCFA $M^R = (Q, S^R, \Sigma, \Theta^R, \delta^R, q_0, s_0^R, S_a, S_r)$.

O conjunto de estados clássicos será igual a S acrescido do elemento $s_0^R \notin S$, ou seja $S^R = S \cup \{s_0^R\}$.

A função de transição Θ^R é definida como

$$\Theta^R(s,\sigma) = \begin{cases} \Theta(s,\sigma), & \text{se } s \in S \\ I, & \text{se } s = s_0^R \end{cases}.$$

A função de transição clássica δ^R, para os estados em S e símbolos em Σ é exatamente como δ, apenas invertendo-se a direção para qual a cabeça de leitura se move. Para as transições do novo estado, s_0^R, a função clássica irá se mover para a direita até chegar ao final da fita, quando a transição levará ao estado inicial clássico de M, s_0. Resumindo, após operações unitárias, temos

$$\delta^R(s,\sigma) = \begin{cases} (s_0^R, +1), & \text{se } s = s_0^R \text{ e } \sigma \neq \ddagger \\ (s_0, 0), & \text{se } s = s_0^R \text{ e } \sigma = \ddagger \\ (s', -p), & \text{se } s \in S,\ \sigma \in \Sigma \text{ e } \delta(s,\sigma) = (s', p) \\ (s', -p), & \text{se } s \in S,\ \sigma = \dagger \text{ e } \delta(s,\ddagger) = (s', p) \\ (s', -p), & \text{se } s \in S,\ \sigma = \ddagger \text{ e } \delta(s,\dagger) = (s', p) \end{cases}.$$

Podemos verificar que, como s_0^R é o estado inicial do novo 2QCFA, com as funções de transição δ^R e Θ^R, o autômato M^R irá se mover até chegar no marcador direito

sem alterar os estados quânticos. Ao chegar no marcador, a transição será feita para o estado inicial do 2QCFA original s_0.

Então, pela definição de δ^R e Θ^R, o funcionamento de M^R será o mesmo de M com duas alterações:

1. M^R irá tratar o marcador direito como M trata o marcador esquerdo, e vice-versa

2. M^R se moverá na direção contrária àquela em que M se moveria, segundo sua função de transição clássica.

É fácil perceber que, a partir do momento em que a transição para s_0 for feita, o 2QCFA M^R irá simular M na cadeia w^R. Portanto, a probabilidade de aceitação será igual a da cadeia w^R quando M computa, ou seja $p_a(w^R)$.

Temos também que o tempo de execução esperado de M^R compreende o mo movimento para chegar até a última posição e, em seguida, os movimentos simular o 2QCFA original, ou seja, $O(|w| + t(|w|))$. □

Corolário 4.4.8. *Se $L \subseteq \Sigma^*$ é uma linguagem decidível pelo modelo 2QCFAs com erro unilateral ϵ em tempo esperado $O(t(|w|))$, então L^R é decidível por um 2QCFA com erro unilateral ϵ em tempo esperado $O(t(|w|) + |w|)$.*

4.4.5 Homomorfismo inverso

Iremos, agora, apresentar a prova de que o conjunto de linguagens reconhecidas por 2QCFAs é fechada por homomorfismo inverso. Esta prova é baseada nas provas de que as linguagens regulares são fechadas por homomorfismo inverso, bem como na prova de Macko [69], o qual mostra que o conjunto das linguagens reconhecidas por MM-1,5QFAs[3] também o são.

A ideia geral da prova é que ao computar sobre um símbolo σ, computaremos, na verdade sobre $h(\sigma)$. Como o autômato em questão é bidirecional, teremos que guardar o símbolo específico de $h(\sigma)$ que está sendo computado na configuração atual do 2QCFA. Porém como $|h(\sigma)| = c$, para uma constante c, poderemos fazer isso utilizando os estados clássicos.

[3]MM-1,5QFA é um modelo intermediário entre MM-1QFA e MM-2QFA.

Teorema 4.4.9. *Sejam $h : \Sigma_1 \to \Sigma_2$ um homomorfismo, M um 2QCFA tal que M para ao computar $w \in \Sigma_2^*$ em tempo esperado $O(t(|w|))$ e cujas probabilidades de aceitação e rejeição são, respectivamente, $p_a(w)$ e $p_r(w)$. Então existe um 2QCFA M' tal que, para uma cadeia $w \in \Sigma^*$, M aceita com probabilidade $p_a(h(w))$ e rejeita com probabilidade $p_r(h(w))$, sendo que M para ao computar w em tempo $O(|w| + t(|h(w)|))$.*

Demonstração. Seja $M = (Q, S, \Sigma_2, \Theta, \delta, q_0, s_0, S_a, S_r)$ o 2QCFA do enunciado. Vamos agora construir o 2QCFA $M' = (Q, S', \Sigma_1, \Theta', \delta', q_0', s_{0_e}, S_a', S_r')$ com as propriedades desejadas.

Mostraremos, inicialmente, o conjunto de estados clássicos do novo 2QCFA. Teremos mais estados, pois serão eles que irão simular o movimento da cabeça de leitura quando $|h(a)| > 1$. Sejam os conjunto $S_1' = \bigcup_{s \in S}\{s_e, s_d\}$ e $S_2' = \{s_i | s \in S \text{ e } 1 \leq i \leq max_{\sigma \in \Sigma_1}|h(\sigma)|\}$. Definimos

$$S' = S_1' \cup S_2'.$$

A ideia dos estados em S_1' é manter o histórico da direção original da cabeça de leitura em uma transição. Esta informação é importante quando $|h(\sigma)| = 0$, pois deveremos ignorar σ neste caso, passando para o próximo elemento mantendo a mesma direção da transição original.

Já os estados de S_2' são os estados que irão auxiliar a guardar a informação de qual símbolo $h(\sigma)$ estaria sendo computado pelo 2QCFA original M.

Veremos agora o funcionamento da função de transição quântica Θ'. Quando a cabeça de leitura estiver sobre o marcador esquerdo (direito) e o estado clássico for s_e (s_d) a função de transição quântica será igual à de M no mesmo marcador e com estado clássico s. Para estados clássicos em S_2' e $\sigma \in \Sigma$, a informação codificada nos estados irá definir seu funcionamento, simulando a função de transição quântica original. Nos outros casos, a função de transição quântica Θ' será a identidade. Sintetizando, teremos

$$\Theta(s, \sigma) = \begin{cases} \Theta(s', \dagger), & \text{se } s = s_e' \in S_1' \text{ e } \sigma = \dagger \\ \Theta(s', \ddagger), & \text{se } s = s_d' \in S_1' \text{ e } \sigma = \ddagger \\ \Theta(s', h(\sigma)_i), & \text{se } s = s_i' \in S_2', i \leq |h(\sigma)| \text{ e } \sigma \in \Sigma \\ I, & \text{caso contrário} \end{cases},$$

onde $h(\sigma)_i$ é a i-ésima posição na cadeia $h(\sigma)$.

Vamos apresentar agora a função de transição clássica. Para facilitar a exposição dividiremos a função considerando cada um dos conjuntos de estados S'_1 e S'_2.

Para os estados $s_p \in S'_1$, teremos

$$\delta'(s_p,\sigma) = \begin{cases} (s_1,0), & \text{se } \sigma \in \Sigma_1,\ p = d \text{ e } |h(\sigma)| > 0 \\ (s_{|h(\sigma)|},0), & \text{se } \sigma \in \Sigma_1,\ p = e \text{ e } |h(\sigma)| > 0 \\ (s_d,+1), & \text{se } \sigma \in \Sigma_1,\ p = d \text{ e } |h(\sigma)| = 0 \\ (s_e,-1), & \text{se } \sigma \in \Sigma_1,\ p = e \text{ e } |h(\sigma)| = 0 \\ (s'_d,+1), & \text{se } \sigma = \dagger \text{ e } \delta(s,\dagger) = (s',+1) \\ (s'_e,-1), & \text{se } \sigma = \ddagger \text{ e } \delta(s,\ddagger) = (s',-1) \\ (s'_e,0), & \text{se } \sigma = \dagger \text{ e } \delta(s,\dagger) = (s',0) \\ (s'_d,0), & \text{se } \sigma = \ddagger \text{ e } \delta(s,\ddagger) = (s',0) \end{cases}.$$

Intuitivamente, as duas primeiras cláusulas são para $|h(\sigma)| \geq 1$. A diferença entre as duas registra quando se chega pela esquerda ou pela direita no símbolo σ. A terceira e a quarta cláusulas são relativas aos casos em que $|h(\sigma)| = 0$, e neste caso, M' deve ignorar este símbolo. As quatro últimas cláusulas cobrem os casos em que se chegou em um marcador, e, neste caso, a transição é feita sem o auxílio dos estados de S'_2.

Para os estados $s_i \in S'_2$, teremos

$$\delta'(s_i,\sigma) = \begin{cases} (s'_i,0), & \text{se } \delta(s,\sigma) = (s',0) \\ (s'_{i+1},0), & \text{se } \delta(s,\sigma) = (s',+1) \text{ e } |h(\sigma)| \geq i+1 \\ (s'_d,+1), & \text{se } \delta(s,\sigma) = (s',+1) \text{ e } |h(\sigma)| < i+1 \\ (s'_{i-1},0), & \text{se } \delta(s,\sigma) = (s',-1) \text{ e } i > 1 \\ (s'_e,-1), & \text{se } \delta(s,\sigma) = (s',-1) \text{ e } i = 1 \end{cases}.$$

Intuitivamente, neste caso, o símbolo da fita da configuração clássica de M é criado com as informações do símbolo da fita lido por M' e o índice do estado clássico de M'. Com isso, consegue-se fazer as transições entre os símbolos de $h(\sigma)$, e, quando se chegou a uma das extremidades desta cadeia, passa-se para o próximo símbolo da cadeia original.

A definição de δ' para os valores não definidos anteriormente poderá ser arbitrária, dado que, por construção, os estados clássicos nunca chegarão em tal configuração.

Por construção, temos que M' estará na configuração formada pelo estado clássico s_j, estado quântico $|\psi\rangle$ sobre a i-ésima posição da fita ao computador sobre w com

a mesma probabilidade de que M está na posição $|h(w_1, ..., w_{i-1})| + j$ da fita, no estado s e estado quântico $|\psi\rangle$. Temos também que M' estará sobre o marcador esquerdo (direito) no estado clássico s_e (s_d) e o estado quântico é $|\psi\rangle$ com a mesma probabilidade com que M está no marcador esquerdo (direito), no estado clássico s e estado quântico $|\psi\rangle$. Isso se dá pois as transições simulam o funcionamento de M sobre $h(w)$, ignorando os símbolos σ tal que $|h(\sigma)| = 0$, e realizando a transição entre os símbolos de $h(\sigma)$, para $|h(\sigma)| \geq 0$, através dos índices nos estados de S_2'. Portanto, para uma cadeia $w \in \Sigma_1^*$, a probabilidade de aceitação é $p_a(h(w))$.

Temos um caso patológico em que a cadeia de entrada é formada somente por símbolos em que $|h(\sigma)| = 0$, e, neste caso, o maior custo da computação é encontrar um elemento em que isso não ocorre, com complexidade $O(|w|)$. Se este não for o caso, a complexidade de tempo é igual à de M computando sobre $h(w)$. Temos então que a complexidade da computação de w por M' é $O(|w| + t(|h(w)|))$.

□

4.5 Computabilidade

Iremos, nesta seção, apresentar de uma forma estruturada algumas linguagens reconhecidas pelo modelo 2QCFA. A organização da apresentação dividirá as linguagens segundo a hierarquia clássica. Ressaltamos que este estudo é original na literatura.

Iniciamos apresentando a relação das linguagens regulares e das linguagens reconhecidas por 2QCFAs. Seguimos na Seção 4.5.2 apresentando linguagens de diversos graus de dificuldade dentre as linguagens livres de contexto que são reconhecidas por 2QCFAs. Finalmente na Seção 4.5.3 apresentamos 2QCFAs que reconhecem linguagens não livre de contexto. Assumiremos um conhecimento básico prévio em linguagens formais e autômatos, sendo referências para tais assuntos os livros de Hopcroft e Ullman [55] e Sipser [83].

4.5.1 Linguagens regulares

Nesta seção, iremos provar um teorema simples mostrando que todas as linguagens regulares podem ser reconhecidas por um 2QCFA com erro nulo em tempo linear. A ideia da prova é simular o autômato determinístico que decide a linguagem, ignorando os estados quânticos.

Teorema 4.5.1. *Se F é uma linguagem regular, então existe um 2QCFA M que decide L com erro nulo em tempo linear.*

Demonstração. Seja $D = (S_1, \Sigma, \delta_1, s_0, F)$ um autômato determinístico que decide L. Seja $M = (\mathcal{Q}, S, \Sigma, \Theta, \delta, |0\rangle, s_0, S_{acc}, S_{rej})$ um 2QCFA, tal que $\mathcal{Q}$ é um espaço de Hilbert bidimensional e

$$\begin{aligned} S &= S_1 \cup \{s_{acc}, s_{rej}\}, \\ S_{acc} &= \{s_{acc}\} \text{ e} \\ S_{rej} &= \{s_{rej}\}. \end{aligned}$$

Para todos estados clássicos e símbolos do alfabeto da fita, o operador de evolução quântico Θ irá aplicar a identidade. Portanto, o operador de evolução clássico δ não precisará ser definido após medições . Após a aplicação de operações unitárias, δ se comportará da seguinte forma:

$$\delta(s,\sigma) = \begin{cases} (s, +1), & \text{se } \sigma = \dagger \\ (\delta_1(s,\sigma), +1), & \text{se } \sigma \in \Sigma \\ (s_{acc}, 0), & \text{se } \sigma = \ddagger \text{ e } s \in F \\ (s_{rej}, 0), & \text{se } \sigma = \ddagger \text{ e } s \notin F. \end{cases}$$

Por construção, os estados quânticos não interferem na computação de uma cadeia por M. Pode ser demonstrado facilmente que D estará sobre a i-ésima posição da cadeia de entrada no estado s se e somente se M estiver sobre a célula de posição i e no mesmo estado clássico.

No final da computação, se D aceita a entrada, M irá atingir $\ddagger$ em um estado clássico de F. Neste caso, δ irá transitar para um estado de aceitação. Caso contrário, M irá atingir $\ddagger$ em um estado que não pertence a F e δ transitará para um estado de rejeição. Portanto M aceita a entrada se e somente se D também a aceitar.

Como podemos ver, as transições que não movem a cabeça de leitura para a direita são aquelas que fazem uma transição para o estado de parada. Portanto, necessitam de $|w| + 2$ passos para M aceitar ou rejeitar a entrada. □

4.5.2 Linguagens livre de contexto

Nesta seção, serão estudados 2QCFAs que reconhecem Linguagens Livres de Contexto (LLCs) de distintas dificuldades. Começaremos apresentando uma LLC determinística que é reconhecida com erro unilateral pelo modelo 2QCFA em tempo polinomial. Seguimos mostrando duas LLCs não-determinísticas e não-ambíguas que são reconhecidas pelo modelo. Na última seção, mostramos um 2QCFA que reconhece uma LLC ambígua.

2QCFAs e Linguagens Livres de Contexto Determinísticas

São exemplos destas linguagens a linguagem de cadeias em que o número de símbolos a é igual ao número de símbolos b, a linguagem xcy, tal que $x, y \in \{a, b\}^*$ e $|x| = |y|$ [80], dentre outras. Entretanto, a técnica utilizada em tais provas é a técnica originalmente proposta por Ambainis e Watrous [11] para demostrar que a LLC determinística $L_= = \{a^n b^n | n \geq 0\}$ é reconhecida pelo modelo 2QCFA com erro unilateral arbitrário. Iremos agora apresentar tal 2QCFA.

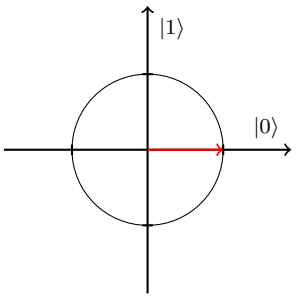
A ideia geral do 2QCFA é, primeiramente, verificar se a cadeia de entrada está na forma a^*b^*. Após isso, faz-se uma varredura pela cadeia, efetuando rotações em um *qubit* para cada símbolo da entrada. Para cada a, faz-se a rotação de $\sqrt{2}\pi$ e, para cada b, faz-se a rotação de $-\sqrt{2}\pi$. A Figura 4.1 ilustra essas rotações.

É fácil perceber que para cadeias na linguagem, ao final da varredura o *qubit* estará no estado original. Pode-se também limitar a amplitude do estado final para cadeias que não estão na linguagem. Entretanto essa probabilidade pode ser pequena e, por isso, será necessário um procedimento para amplificá-la.

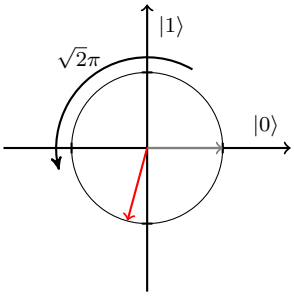
Começaremos provando a probabilidade que o Procedimento de Aceitação descrito na Figura 4.2 decide pela aceitação, terminando assim a execução do autômato. Então, provaremos o Teorema 4.5.5, mostrando a corretude do 2QCFA apresentado na Figura 4.3 para decidir a linguagem $L_=$.

Lema 4.5.2. *O procedimento descrito na Figura 4.2 retorna* 1 *com probabilidade* $\frac{1}{2^k(n+1)^2}$.

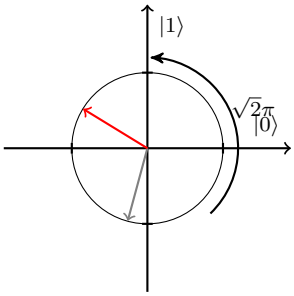
Demonstração. A primeira parte do Laço em questão nada mais é do que uma instância do Problema do Jogador [41] onde um dos jogadores começa com 1 moeda e o outro jogador começa com $n = i + j$ moedas. Por resultados clássicos de Processos Estocásticos [41], temos que a probabilidade de chegar em † é de $\frac{n}{n+1}$ e a



(a) Estado inicial do sistema

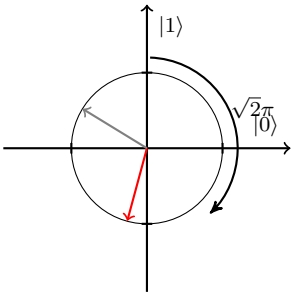


(b) Estado quântico após computar “a”



-

(c) Estado quântico após computar “aa”



-

(d) Estado quântico após computar “aab”

Figura 4.1: Exemplo da evolução de estados quânticos ao computar a cadeia “aab”

probabilidade de chegar em ‡ é de $\frac{1}{n+1}$. Como o processo é repetido duas vezes, a probabilidade de terminar as duas vezes em ‡ é de $\frac{1}{(n+1)^2}$.

Já na segunda parte do laço, a probabilidade de que nenhuma moeda resulte em "cara" é de $\frac{1}{2^k}$. Portanto, este procedimento retorna 1 com probabilidade $\frac{1}{2^k(n+1)^2}$. □

```
   Input: Entrada w = a^i b^j e k > 0
 1 repeat
 2 |  Mova a cabeça de leitura para o primeiro a ;
 3 |  while símbolo atual da fita não for † ou ‡ do
 4 |  |  Jogue uma moeda ;
 5 |  |  if resultado da moeda for "cara" then
 6 |  |  |  Mova a cabeça de leitura para a direita ;
 7 |  |  else
 8 |  |  |  Mova a cabeça de leitura para a esquerda;
 9 |  |  end
10 |  end
11 until duas vezes;
12 if nas duas vezes ‡ foi atingido then
13 |  Jogue k moedas ;
14 |  if nenhuma moeda for "cara" then return 1
15 end
16 return 0;
```

Figura 4.2: Procedimento de Aceitação para reconhecer $L_=$

Antes de provar o principal teorema, iremos provar um lema auxiliar envolvendo algumas identidades trigonométricas.

Lema 4.5.3 (Adaptado de Lema 6 de Ambainis e Watrous [11])**.** *Para $i, j \in \mathbb{N}$, $i \neq j$, temos que*

$$\sin^2 \sqrt{2}(i-j)\pi \geq \frac{1}{2(i-j)^2}.$$

Demonstração. Seja k o valor inteiro mais próximo de $\sqrt{2}(i-j)$, e vamos assumir $k < \sqrt{2}(i-j)$, sendo o outro caso simétrico. Temos que $k^2 < 2(i-j)^2$, e como k e $2(i-j)$ são números inteiros, segue que

$$k^2 + 1 \leq 2(i-j)^2, \text{ ou seja } k \leq \sqrt{2(i-j)^2 - 1}.$$

Input: Entrada w e erro $0 < \epsilon < \frac{1}{2}$
Prepare o estado quântico $|q\rangle$ no estado $|0\rangle$;
$k \leftarrow 1 - \lfloor \log \epsilon \rfloor$;
$U_a \leftarrow R_{\sqrt{2}\pi}$;
$U_b \leftarrow R_{-\sqrt{2}\pi}$;
Verifique classicamente se $w \in a^*b^*$ e rejeite se não for ;
while *verdadeiro* **do**
    Mova a cabeça de entrada para o primeiro a ;
    while *símbolo atual* σ *não é* ‡ **do**
        Aplique a operação U_σ no estado quântico ;
        Mova a cabeça de leitura para a direita ;
    end
    Meça o estado quântico ;
    if *resultado for* $|1\rangle$ **then** Rejeite ;
    if *Procedimento de Aceitação retornar* 1 **then** Aceite ;
end

Figura 4.3: 2QCFA M que reconhece $L_=$

Dado que

$$(\sqrt{2}(i-j)-\sqrt{2(i-j)^2-1})(\sqrt{2}(i-j)+\sqrt{2(i-j)^2-1}) = 2(i-j)^2-2(i-j)^2+1 = 1,$$

temos

$$\sqrt{2}(i-j)-k \geq \sqrt{2}(i-j)-\sqrt{2(i-j)^2-1} = \frac{1}{\sqrt{2}(i-j)+\sqrt{2(i-j)^2+1}} > \frac{1}{2\sqrt{2}(i-j)}.$$

Como k é o inteiro mais próximo de $\sqrt{2}(i-j)$, temos que $k \in [0, \frac{1}{2}]$, e, neste intervalo, $\sin \pi x \geq 2x$. Portanto

$$\begin{aligned}
\sin^2 \sqrt{2}(i-j)\pi &= \sin^2 (\sqrt{2}(i-j)-k)\pi \\
&\geq (2(\sqrt{2}(i-j)-k))^2 \\
&\geq \left(\frac{2}{2\sqrt{2}(i-j)}\right)^2 \\
&\geq \frac{1}{2(i-j)^2}.
\end{aligned}$$

□

Agora, iremos provar que a linguagem $L_=$ pode ser reconhecida por um 2QCFA com erro unilateral ϵ e tempo polinomial.

Definição 4.5.4. *Seja R_α o operador unitário* $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$.

Teorema 4.5.5 (Lemas 6 e 7 de Ambainis e Watrous [11])**.** *O 2QCFA M descrito na Figura 4.3 reconhece a linguagem $L_= = \{a^n b^n | n \geq 0\}$ com erro unilateral ϵ, $0 < \epsilon < \frac{1}{2}$, em tempo $O(|w|^4)$, onde w é a cadeia de entrada.*

Demonstração. Como a linguagem $\{a^*b^*\}$ é uma linguagem regular, pelo Teorema 4.5.1, temos que o passo 5 pode ser implementado por um 2QCFA com erro nulo e tempo linear. Portanto, se a cadeia não tiver o formato $a^i b^j$, a cadeia é rejeitada. Podemos, então, assumir que a cadeia de entrada possui tal formato.

Para cadeias $w \in L_=$, é fácil verificar que a composição das operações unitárias do passo 9 é equivalente à aplicação do operador identidade, dado que para cada rotação de $\sqrt{2}\pi$, haverá uma rotação de $-\sqrt{2}\pi$ para compensá-la. Neste caso, a medição realizada no passo 12 nunca resultará em $|1\rangle$, logo a entrada nunca será rejeitada. Pelo Lema 4.5.2, o procedimento de aceitação no passo 14 retorna 1 com probabilidade $\frac{1}{2^k(n+1)^2}$, portanto o número de execuções esperados do laço principal é de $O(|w|^2)$.

Agora iremos verificar o resultado para cadeias $w \notin L_=$. Após executar um número i de rotações por $\sqrt{2}\pi$ e j rotações por $\sqrt{2}\pi$, o estado quântico ao final da varredura é

$$\cos\sqrt{2}(i-j)\pi|0\rangle + \sin\sqrt{2}(i-j)\pi|1\rangle,$$

sendo a probabilidade de rejeição no passo 13 de $\sin^2\sqrt{2}(i-j)\pi$. Pelo Lema 4.5.3, temos que essa probabilidade é de pelo menos $\frac{1}{2(i-j)^2}$.

Portanto, a cada iteração, para $i \neq j$, a entrada é rejeitada na linha 12 com probabilidade $p_r > \frac{1}{2(i-j)^2}$ e, pelo Lema 4.5.2, a entrada é aceita no passo 14 com probabilidade $p_a = \frac{1}{2^k(n+1)^2} \leq \frac{\epsilon}{2(i+j+1)^2}$.

Ao repetir indefinidamente, temos que a probabilidade de rejeição é:

$$\sum_{k\geq 0}(1-p_r)^k(1-p_a)^k p_r = \frac{p_r}{p_a+p_r-p_a p_r} > \frac{p_r}{p_a+p_r} > \frac{\frac{1}{2}}{\frac{1}{2}+\frac{\epsilon}{2}} = \frac{1}{1+\epsilon} > 1-\epsilon.$$

Além disso, temos que o o número esperado de iterações no laço principal tem como limitante superior o número de execuções até que a cadeia seja aceita, que é $O(|w|^2)$, como visto anteriormente.

Como, o tempo de execução do Procedimento de Aceitação é $O(|w|^2)$, temos que o 2QCFA para em tempo esperado $O(|w|^4)$. □

Nota 4.5.6. *É fácil perceber que se alterarmos $U_a = R_{\sqrt{2}\pi}$ e $U_b = R_{k\sqrt{2}\pi}$, pode-se provar com os mesmos argumentos que a linguagem $L_=^k = \{a^{kn}b^n | n \geq 0\}$, para um $k \in \mathbb{N}$ fixo, é decidível pelo modelo 2QCFA.*

Nota 4.5.7. *Usando os Teoremas 4.4.5 e 4.5.5, pode-se provar facilmente que as linguagens $\{a^n b^n c^* | n \geq 0\}$ e $\{a^* b^n c^n | n \geq 0\}$ são decidíveis por algum 2QCFA.*

2QCFAs e Linguagens Livres de Contexto não-determinística e não-ambíguas

Nesta seção, iremos mostrar dois resultados envolvendo LLCs não-determinísticas e não-ambíguas que são reconhecidas pelo modelo 2QCFA com erro unilateral. Mostraremos primeiramente que a linguagem $\{a^n b^n | n \geq 0\} \cup \{a^{2n} b^n | n \geq 0\}$ é decidida em tempo polinomial e em seguida que a linguagem dos palíndromos sobre o alfabeto $\{a, b\}$ é reconhecida em tempo exponencial.

A linguagem $\{a^n b^n | n \geq 0\} \cup \{a^{2n} b^n | n \geq 0\}$

Usando o resultado da seção anterior, juntamente como Corolário 4.4.4, vamos provar que a linguagem $L = \{a^n b^n | n \geq 0\} \cup \{a^{2n} b^n | n \geq 0\}$ é reconhecida por um 2QCFA com erro unilateral arbitrário em tempo polinomial [4].

Teorema 4.5.8. *A linguagem $\{a^n b^n | n \geq 1\} \cup \{a^{2n} b^n | n \geq 1\}$ pode ser reconhecida pelo modelo 2QCFA com erro unilateral δ em tempo polinomial, para algum $0 < \delta < \frac{1}{2}$ arbitrário.*

Demonstração. Seja $\epsilon = 1 - \sqrt{1 - \delta}$. Pelo Teorema 4.5.5 e Nota 4.5.6, temos que existem os 2QCFAs M_1 e M_2 que reconhecem as linguagens $\{a^n b^n | n \geq 0\}$ e $\{a^{2n} b^n | n \geq 0\}$, respectivamente, em tempo polinomial e com erro unilateral ϵ.

Portanto, a partir de M_1 e M_2 e pelo Lema 4.4.3, temos que existe um 2QCFA que reconhece a linguagem $\{a^n b^n | n \geq 0\} \cup \{a^{2n} b^n | n \geq 0\}$ em tempo polinomial e com erro unilateral $2\epsilon - \epsilon^2 = \delta$. □

[4] O exemplo 4.11 de Reghizzi [79] mostra que $\{a^n b^n | n \geq 0\} \cup \{a^{2n} b^n | n \geq 0\}$ é uma LLC não-determinística e não-ambígua.

Palíndromos

Seja $L_{pal} = \{x | x \in \{a,b\}^* \text{ e } x = x^R\}$ a linguagem dos palíndromos sobre o alfabeto $\{a,b\}$[5].

Apresentaremos agora o resultado de Ambainis e Watrous [11] que mostra que L_{pal} é reconhecida por um 2QCFA em tempo exponencial. Iniciaremos definindo duas matrizes que farão parte do 2QCFA para reconhecer L_{pal}.

Definição 4.5.9. *Sejam*

$$A = \begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} \text{ e } B = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & 4 \end{pmatrix}.$$

Enunciaremos um lema proposto por Ambainis e Watrous [11], envolvendo a multiplicação das matrizes da Definição 4.5.9. A prova deste lema será apresentada no Apêndice D.

Lema 4.5.10. *Seja* $u = Y_1^{-1}...Y_n^{-1}X_n...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, *tal que* $X_i, Y_i \in \{A, B\}$. *Se* $X_j \neq Y_j$ *para algum valor de* j, *então* $u_2^2 + u_3^2 > 25^{-n}$.

Input: Entrada w e $k > 0$
1 $f \leftarrow 0$;
2 **while** *símbolo atual* $\sigma \neq \dagger$ **do**
3 | Simule k jogadas de moeda **if** *alguma moeda for "cara"* **then** $f \leftarrow 1$;
4 | Mova a cabeça de leitura para a esquerda ;
5 **end**
6 **return** f ;

Figura 4.4: Procedimento de aceitação para palíndromos

Iremos agora mostrar a probabilidade de aceitação resultante do procedimento demonstrado na Figura 4.4.

Lema 4.5.11. *O procedimento de aceitação descrito na Figura 4.4 retorna* 0 *com probabilidade* $2^{-k(n+1)}$.

[5] O exemplo 4.12 de Reghizzi [79] mostra que L_{pal} é uma LLC não-determinística e não-ambígua.

Demonstração. O procedimento de aceitação retorna 0 quando as k moedas jogadas de todos símbolos da entrada resultam em "cara", o que ocorre com probabilidade $2^{-k(n+1)}$. □

Input: Entrada w e erro $0 < \epsilon < \frac{1}{2}$
Prepare um estado quântico em $\mathbb{C}^3$ em $|0\rangle$;
$U_a \leftarrow \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} & 0 \\ \frac{3}{5} & \frac{4}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix}$;
$U_b \leftarrow \begin{pmatrix} \frac{4}{5} & 0 & -\frac{3}{5} \\ 0 & 1 & 0 \\ \frac{3}{5} & 0 & \frac{4}{5} \end{pmatrix}$;
$k \leftarrow \max\{\log 25, -\log \epsilon\}$;
while *verdadeiro* **do**
    while *símbolo atual* $\sigma \neq \ddagger$ **do**
        Aplique U_σ no estado quântico ;
        Mova a cabeça de leitura para a direita ;
    end
    Mova a cabeça de leitura para o primeiro símbolo da cadeia de entrada;
    while *símbolo atual* $\sigma \neq \ddagger$ **do**
        Aplique U_σ^{-1} no estado quântico ;
        Mova a cabeça de leitura para a direita ;
    end
    Meça o estado quântico e rejeite se for $|1\rangle$ ou $|2\rangle$;
    Se Procedimento de aceitação retornar 1, aceite;
end

Figura 4.5: 2QCFA para decidir L_{pal}

Finalmente mostraremos o 2QCFA que aceita L_{pal}.

Teorema 4.5.12. *O 2QCFA mostrado na Figura 4.5 reconhece a linguagem L_{pal} com erro unilateral $0 < \epsilon < \frac{1}{2}$ arbitrário, e para após tempo esperado exponencial em relação ao tamanho da entrada.*

Demonstração. Para cadeias $w \in L_{pal}$, a aplicação dos operadores unitários nas

linhas 7 e 12 resulta em

$$\begin{aligned}
&U_{w_1}...U_{w_n}U_{w_1}^{-1}...U_{w_n}^{-1}|0\rangle \\
&= U_{w_1}...U_{w_n}U_{w_n}^{-1}...U_{w_1}^{-1}|0\rangle \\
&= U_{w_1}...U_{w_{n+1}}IU_{w_{n+1}}^{-1}...U_{w_1}^{-1}|0\rangle \\
&= U_{w_1}...U_{w_{n+1}}U_{w_{n+1}}^{-1}...U_{w_1}^{-1}|0\rangle \\
&... \\
&= U_{w_1}U_{w_1}^{-1}|0\rangle \\
&= I|0\rangle \\
&= |0\rangle
\end{aligned}$$

onde a primeira igualdade vem do fato de que por ser palíndromo, $w_i = w_{n-i+1}$.

Pelo Lema 4.5.11, a probabilidade de aceitação em cada iteração será de $2^{-k(n+1)}$, portanto o número esperado de iterações é de $2^{k(n+1)}$.

Para instâncias negativas, pelo Lema 4.5.10, temos que a sequência de operações resultando em $U_{w_1}...U_{w_n}U_{w_1}^{-1}...U_{w_n}^{-1}|0\rangle$ resultará em um estado $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$, com $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ e $\alpha_1^2 + \alpha_2^2 \geq 25^{-n}$. Portanto, a probabilidade p_r com que o passo 15 rejeita é de pelo menos 25^{-n}. Pelo Lema 4.5.11, o procedimento de aceitação no passo 16 irá aceitar com probabilidade $p_a = 2^{-k(n+1)}$. Portanto, a probabilidade com que a cadeia será rejeitada, tomando $k \geq \max\{\log 25, -\log \epsilon\}$, é de

$$\sum_{j\geq 0}(1-p_r)^j(1-p_a)^j p_r = \frac{p_r}{p_r + p_a - p_a p_r} \geq 1 - \epsilon.$$

Temos que o número esperado de iterações do laço principal será no máximo

$$\min\{25^n, 2^{k(n+1)}\} = 25^n,$$

dado que é esperado que após esse número de passos, a cadeia de entrada seja rejeitada. □

2QCFAs e Linguagens Livres de Contexto inerentemente ambíguas

Nesta subseção, mostraremos que o modelos 2QCFA reconhece também algumas LLC inerentemente ambíguas, uma das classes de LLCs mais difíceis de reconhecer. Mostraremos que a linguagem $L_{ijk} = \{a^i b^j c^k | i = j \text{ ou } j = k\}$ pode ser reconhecida em tempo polinomial e com erro unilateral arbitrário [6].

[6] Em Sipser [83] podemos ver que a linguagem L_{ijk} é uma LLC inerentemente ambígua.

Teorema 4.5.13. *A linguagem L_{ijk} é reconhecida por um 2QCFA com erro unilateral δ em tempo $O(|w|^4)$, onde w é a cadeia de entrada e $0 < \delta < \frac{1}{2}$.*

Demonstração. Como descrito na Nota 4.5.7 as linguagens $L_1 = \{a^n b^n c^* | n \geq 0\}$ e $L_2 = \{a^* b^n c^n | n \geq 0\}$ podem ser reconhecidas com erro unilateral $\epsilon = 1 - \sqrt{1-\delta}$ pelo modelo 2QCFA em tempo esperado $O(|w|^4)$. Dado que $L_{ijk} = L_1 \cup L_2$, pelo Teorema 4.4.3, temos que L_{ijk} é reconhecida por um 2QCFA com erro unilateral δ, em tempo esperado $O(|w|^4)$. □

4.5.3 Linguagens não livres de contexto

Iremos mostrar agora duas linguagens não livres de contexto (LNLC) que são reconhecidas por 2QCFAs. Iniciaremos apresentando o 2QCFA para a linguagem $\{a^n b^n c^n | n \geq 0\}$ que é reconhecida em tempo polinomial e erro unilateral e, em seguida mostraremos que a linguagem $L_{wcw} = \{wcw | w \in a, b^*\}$ pode ser reconhecida com erro unilateral e tempo exponencial.

A linguagem $a^n b^n c^n$

Mostraremos nesta seção, um 2QCFA que reconhece a LNLC $L_n = \{a^n b^n c^n | n \geq 0\}$[7].

Teorema 4.5.14. *A linguagem L_n é reconhecida por um 2QCFA com erro unilateral δ em tempo $O(|w|^4)$, onde w é a cadeia de entrada e $0 < \delta < \frac{1}{2}$.*

Demonstração. Como descrito na Nota 4.5.7, as linguagens $L_1 = \{a^n b^n c^* | n \geq 0\}$ e $L_2 = \{a^* b^n c^n | n \geq 0\}$ são decidíveis pelo modelo 2QCFA com erro unilateral $\epsilon = 1 - \sqrt{1-\delta}$ e em tempo $O(|w|^4)$. Dado que $L_n = L_1 \cap L_2$, pelo Teorema 4.4.1, sabemos que L_n é reconhecida por um 2QCFA com erro unilateral δ em tempo esperado $O(|w|^4)$. □

A linguagem wcw

Iremos agora mostrar um 2QCFA que reconhece com erro unilateral a linguagem não LLC $L_{wcw} = \{wcw | w \in \{a, b\}^*\}$ em tempo exponencial. A ideia geral do 2QCFA é similar à do 2QCFA apresentado para reconhecer a linguagem dos palíndromos, descrito na Figura 4.5.

[7] O exemplo 6.1 de Hopcroft e Ullman [55] mostra que L_n não é livre de contexto.

Teorema 4.5.15 (Seção 4 de Zheng, Qiu e Li [81]). *Existe um 2QCFA M que reconhece a linguagem L_{wcw} com erro unilateral ϵ, $0 < \epsilon < \frac{1}{2}$, e com número esperado de passos exponencial no tamanho da entrada.*

Ideia da prova. Primeiramente M irá rejeitar se a cadeia de entrada não estiver na forma xcy, $x, y \in \{a, b\}^*$, o que pode ser feito em tempo linear e com erro nulo pelo Teorema 4.5.1.

Se a cadeia de entrada não for rejeitada na primeira etapa, M percorrerá a cadeia x aplicando a transformação U_σ sobre um estado quântico inicial $|0\rangle$, e então percorrerá y na direção inversa aplicando U_σ^{-1} para cada símbolo σ, sendo $U_a = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} & 0 \\ \frac{3}{5} & \frac{4}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ e $U_b = \begin{pmatrix} \frac{4}{5} & 0 & -\frac{3}{5} \\ 0 & 1 & 0 \\ \frac{3}{5} & 0 & \frac{4}{5} \end{pmatrix}$, como definido na Figura 4.5.

Como visto no Teorema 4.5.12, se $x = y$ após percorrer x e y o estado quântico estará sempre em $|0\rangle$ e, se $x \neq y$, o estado quântico não estará em $|0\rangle$ com probabilidade pelo menos 25^{-n}. Portanto uma medição é feita e se for $|1\rangle$ ou $|2\rangle$, a cadeia é rejeitada. Senão, o procedimento para aceitação descrito na Figura 4.4 é executado e se não retornar 1, recomeça-se o processo. □

4.6 Linguagens não reconhecidas por 2QCFAs

Um dos aspectos em que o estudo de 2QCFAs ainda encontra-se mais primitivo é a caracterização de linguagens que não podem ser reconhecidas por tais modelos. Nos modelos unidirecionais, Moore e Crutchfield [73] apresentaram um Lema do Bombeamento para MO-1QFAs e Kondacs e Watrous [66] mostraram uma linguagem regular que não pode ser reconhecida por MM-1QFAs.

Entretanto, existem algumas linguagens sobre as quais conjectura-se que não possam ser reconhecidas pelo modelo com erro unilateral, tal como a linguagem $L_< = \{a^i b^j | i < j\}$ e algumas de suas variações[8]. Outro exemplo de linguagem que acredita-se não poder ser reconhecida é a linguagem de parênteses balanceados.

Nesta seção iremos apresentar a prova de um resultado parcial envolvendo o

[8]Se $L_<$ fosse reconhecida, então as linguagens $L_> = \{a^i b^j | i > j\}$ e $L_\neq = \{a^i b^j | i \neq j\}$ também o seriam.

reconhecimento da linguagem $L_<$ por um 1QCFA [9] com erro unilateral ϵ. Este resultado foi provado originalmente por Yakaryilmaz e Say[92], porém em uma forma indireta. Aqui, apresentaremos uma nova prova, original, que usa apenas conceitos do modelo em que estamos trabalhando.

Primeiramente, iremos provar um lema sobre matrizes unitárias.

Lema 4.6.1. *Para todas as matrizes unitárias U e qualquer valor de $\epsilon > 0$, existe um valor k e uma matriz J, tal que $U^k = I + \epsilon J$ e os autovalores de J tem norma no máximo* 1.

Demonstração. Seja m a dimensão do espaço em que a operação linear U opera. Como U é uma matriz unitária, ela pode ser diagonalizada. Sejam P e D as matrizes que diagonalizam U, ou seja $U = PDP^{-1}$. Temos que P é uma matriz cujas colunas são autovetores normalizados de U e D é uma matriz diagonal onde $D_{jj} = e^{\omega_j i}$ é o autovalor de norma 1 associado ao j-ésimo autovetor de U, para $1 \leq j \leq m$. Temos também que $U^s = PD^sP^{-1}$.

Vamos procurar um k tal que $|e^{k\omega_j i} - 1| < \epsilon$. Para isso, vamos particionar o plano complexo em $N = \lceil \frac{2\pi}{\epsilon} \rceil$ partes. Sejam $w_l = \{e^{\frac{2\pi t i}{N}} | t \in \mathbb{R}, l \leq t < l + 1\}$ as partições, $0 \leq l < N$. Seja p_k^j o número da partição na qual o valor $e^{k\omega_j i}$ está, para $0 \leq j < m$. Dado que o número de configurações possíveis para $(p_k^1, ..., p_k^m)$ é no máximo N^m, existem valores distintos de k_1 e k_2, $1 \leq k_1 < k_2 \leq N^m$, para os quais $p_{k_1}^j = p_{k_2}^j$ para todo $0 \leq j < m$. Neste caso, para $k = k_2 - k_1$, temos que $e^{k\omega_j i} \in \{e^{\frac{2\pi t i}{N}} | t \in (-1, 1)\}$. Dado que a corda entre dois pontos é menor que o arco correspondente, temos que $|e^{k\omega_j i} - 1| < \frac{2\pi}{N} = \epsilon$.

Seja então $J' = \frac{1}{\epsilon}(D^k - I)$. Os autovalores de J são

$$\lambda'_j = \frac{1}{\epsilon}(e^{k\omega_j i} - 1),$$

cujas normas são menores que 1. Como temos que $D^k = I + \epsilon J'$, temos $U^k = I + \epsilon J$, para $J = PJ'P^{-1}$. Além disso, temos que os autovalores de J e J' são iguais. □

Agora, provaremos um lema que auxiliará nos casos mais gerais que veremos a seguir.

[9] O modelo 1QCFA difere do 2QCFA por ser unidirecional, permitindo que a cabeça de leitura se movimente somente para a direita

Lema 4.6.2. *Se $\Theta(q_1, \sigma) = \Theta(q_2, \sigma) \in \mathcal{U}(\mathcal{Q})$, para todo $\sigma \in \Sigma$ e todo $q_1, q_2 \in Q$, então o modelo 1QCFA não pode reconhecer a linguagem $L_< = \{a^i b^j | i < j\}$ com erro unilateral ϵ.*

Demonstração. Assumindo que Θ é independente do estado clássico, sejam A e B as transformações unitárias quando a e b estão sob a cabeça de leitura, respectivamente. Se $w = a^i b^j$, o estado quântico após computar toda a cadeira será $B^j A^i |0....0\rangle$.

Temos, pelo Lema 4.6.1, existe um valor de k e uma matriz J tal que o maior autovalor de J tem norma no máximo 1 e $B^k = I + \delta J$, para $\delta = \frac{\epsilon}{3}$. Vamos agora examinar as cadeias $w_i = a^l b^{l+ik}, i \geq 0,\ l \geq 0$. Para $i > 0$, a cadeia w_i deve ser aceita com probabilidade 1, e para $i = 0$ a cadeia deve ser aceita com probabilidade no máximo $1 - \epsilon$.

Sendo Π_a o projetor do subespaço de aceitação, temos que a probabilidade da cadeia w_0 ser aceita é

$$||\Pi_a U^l A^l |q_0\rangle||^2 \leq 1 - \epsilon,$$

e, portanto

$$||\Pi_a U^l A^l |q_0\rangle|| < 1.$$

Por outro lado, a probabilidade de que w_1 ser aceita é

$$\begin{aligned}
&||\Pi_a U^k U^l A^l |q_0\rangle||^2 \\
&= \left|\left|\Pi_a (I + \delta J) U^l A^l |q_0\rangle\right|\right|^2 \\
&= \left|\left|\Pi_a U^l A^l |q_0\rangle + \delta \Pi_a J U^l A^l |q_0\rangle\right|\right|^2 \\
&\leq \left|\left|\Pi_a U^l A^l |q_0\rangle\right|\right|^2 + 2 \left|\left|\Pi_a U^l A^l |q_0\rangle\right|\right| \left|\left|\delta \Pi_a J U^l A^l |q_0\rangle\right|\right| + \left|\left|\delta \Pi_a J U^l A^l |q_0\rangle\right|\right|^2 \\
&\leq 1 - \epsilon + 2 \left|\left|\delta \Pi_a J U^l A^l |q_0\rangle\right|\right| + \left|\left|\delta \Pi_a J U^l A^l |q_0\rangle\right|\right|^2 \\
&\leq 1 - \epsilon + 2\delta + \delta \\
&= 1 - \epsilon + \frac{2\epsilon}{3} + \frac{\epsilon^2}{9} \\
&< 1,
\end{aligned}$$

contradizendo o fato que a cadeia w_1 é aceita com probabilidade 1. □

Então se o 1QCFA não fizer nenhuma medição até que chegue ao marcador da direita, ele não conseguirá reconhecer a linguagem.

Lema 4.6.3. *Se $\Theta(q,\sigma) \in \mathcal{U}(\mathcal{Q})$, para todo $\sigma \in \Sigma$ e todo $q \in Q$, então nenhum 1QCFA consegue reconhecer a linguagem $L_< = \{a^i b^j | i < j\}$ com erro unilateral ϵ.*

Demonstração. Se nenhuma medição é feita até que a cabeça de leitura chegue no marcador da direita, como o número de estados clássicos é finito, para uma cadeia de entrada grande o suficiente, haverá um ciclo de operadores quânticos aplicados com período r, após s passos inciais. Usando o mesmo argumento do Lema 4.6.2, não há possibilidade de que cadeias $w_i = \{a^s b^{s+ikr} |\ i \geq 0\}$ para algum k associado ao erro ϵ, sejam aceitas ou rejeitadas com a probabilidade correta. □

Agora, mostraremos que a realização das medições não ajuda a reconhecer a linguagem $L_<$.

Lema 4.6.4. *Se um 1QCFA faz uma medição antes de processar toda a entrada, ele não consegue reconhecer a linguagem $L_<$ com erro unilateral ϵ.*

Demonstração. Se mais de uma medição é feita durante a computação da cadeia de entrada, é fácil verificar que a sub-cadeia entre as medições é ignorada na computação, sendo impossível distinguir cadeias em $L_<$ de cadeias que não estão na linguagem.

Se somente uma medição é feita, toda computação após essa medição é descartada, dado que o modelo agirá como um autômato finito determinístico. Pelo Lema 4.6.3 e o fato de que $L_<$ não é regular, concluímos que um 1QCFA com essas características não conseguirá reconhecer a linguagem. □

Finalmente, destes lemas auxiliares, temos o resultado geral.

Teorema 4.6.5. *Nenhum 1QCFA reconhece a linguagem $L_< = \{a^i b^j | i < j\}$.*

Demonstração. Diretos dos Lemas 4.6.2, 4.6.3 e 4.6.4. □

4.7 Conclusões

Neste capítulo, procuramos apresentar os resultados mais notáveis envolvendo o modelo 2QCFA. Acreditamos que este modelo tenha uma importante característica, dada sua implementação ser mais viável, pois os estados clássicos possuem ainda um papel relevante dentro da computação, além do fato de que a maioria dos 2QCFAs vistos utilizam poucos *qubits* para guardar os estados quânticos necessários.

As linguagens reconhecidas por 2QCFAs são fechadas pela maioria das principais operações com conjuntos, sendo isso importante para a composição entre 2QCFAs levando ao reconhecimento de novas linguagens, como nos Teoremas 4.5.13 e 4.5.14. Acreditamos que problemas em aberto importantes com relação a este modelo é saber se o conjunto das linguagens reconhecidas com erro unilateral limitado é fechado por complemento e para o caso mais geral de concatenação, sem restrição nos alfabetos das linguagens.

Sobre as linguagens reconhecíveis pelo modelo de 2QCFA com erro unilateral, foram mostrados 2QCFAs que aceitam linguagens das principais subclasses das linguagens decidíveis.

Entretanto, ainda está em aberto a relação exata entre essas classes de linguagens. O resultado parcial mostrado na Seção 4.6 não é definitivo para mostrar que o conjunto das LLCs não está contido nas linguagens reconhecidas por 2QCFAs. Mas é um passo importante, dado que exclui uma técnica utilizada por outros autômatos, que consiste em repetir várias vezes o movimento de um 1QCFA, através de uma varredura, para amplificar a probabilidade de acerto. A Figura 4.6 esquematiza a relação esperada entre as classes de linguagens aqui abordadas.

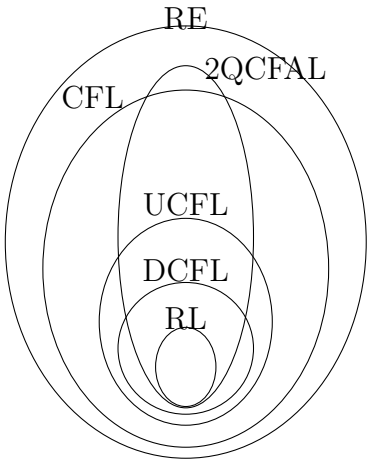


Figura 4.6: Hierarquia esperada das linguagens reconhecidas por erro unilateral por 2QCFAs

Um outro tópico importante que não foi abordado neste capítulo é sobre a decidibilidade de problemas relacionados a 2QCFAs. Por exemplo dado um 2QCFA, é decidível se a linguagem reconhecida por ele é vazia? Alguns autores estudaram tais

problemas para outros modelos. Amano e Iwama [9] mostraram que é indecidível se um MM-1,5QFA [10] aceita alguma cadeia, sendo este resultado extensível para o modelo de 2QCFA. Blondel, Jeandel, Koiran e Portier [27] também estudaram estes problemas para outros modelos de autômatos quânticos com probabilidade de aceitação fixa. Entretanto, ainda estão em aberto outros problemas para esta classe, tais como a igualdade do conjunto de linguagens reconhecidos por dois 2QCFAs distintos.

[10] O modelo MM-1,5QFA é um modelo intermediário entre MM-1QFA e MM-2QFA

Capítulo 5

QMA e Completude Perfeita

Dado o caráter probabilístico da Mecânica Quântica, a definição da classe QMA permite com que o algoritmo verificador responda incorretamente com uma pequena probabilidade. Baseando-se em resultados clássicos, como a do análogo probabilístico MA, pode-se perguntar se podemos atingir a completude perfeita para a classe QMA, isto é, se é possível que o algoritmo verificador possua um erro unilateral, respondendo corretamente para instâncias positivas.

Neste capítulo, apresentaremos dois resultados parciais envolvendo a questão QMA vs. QMA_1. O primeiro mostra que relativizando, isto é, fornecendo um oráculo $\mathcal{U}$, temos $\mathrm{QMA}_1^{\mathcal{U}} \subsetneq \mathrm{QMA}^{\mathcal{U}}$. O segundo resultado mostra que, dados recursos adicionais para o algoritmo verificador, conseguimos computar todas as linguagens em QMA com completude perfeita. Como veremos, apesar desses recursos adicionais serem de tamanho constante, a constante é muito grande, sendo a utilidade do resultado apenas teórica.

5.1 Introdução

Vimos, no Capítulo 3, que na Teoria de Complexidade Quântica, as classes NP e MA foram generalizadas para o novo modelo computacional quântico, resultando na classe QMA. Como as classes MA e QMA apresentam resultados inerentemente probabilísticos, suas definições permitem uma margem de erro para o algoritmo verificador, usualmente $\frac{1}{3}$. Porém, basta uma repetição paralela do protocolo um número polinomial de vezes para reduzir o erro exponencialmente, em ambos os casos. Deseja-se,

então, saber se é possível atingir erro 0 sem perder o poder computacional.

Para o caso da robustez 0, isto é, o algoritmo verificador nunca falha para instâncias negativas, sabe-se que a classe MA pode ser reduzida para a classe NP. Entretanto, suspeita-se que todo algoritmo probabilístico pode ser desaleatorizado, resultando em MA = NP, neste caso a classe MA estaria trivialmente fechada para esta propriedade.

Já para a classe QMA, Kobayashi, Matsumoto e Yamakami [65] provaram uma outra caracterização da classe NQP, qual seja

$$\mathrm{NQP} = \bigcup_{f:\mathbb{Z}\to(0,1]} \mathrm{QMA}(f,1),$$

relacionando as duas versão da classe NP através da robustez 0.

Já para completude perfeita, temos classicamente que $\mathrm{MA} = \mathrm{MA}_1$ [96] [46]. Esta prova depende do caráter clássico do algoritmo verificador probabilístico, possibilitando argumentos combinatórios. Para classes de complexidade quânticas, inicialmente foi provado que a classe QIP é fechada por completude perfeita, sendo uma das implicações do Teorema de Kitaev-Watrous [63]. O passo principal para atingir a completude perfeita é adicionar uma rodada de comunicação em que o Verificador envia seus *qubits* para o Provador, que poderá, então, aplicar operações que convençam o Verificador a aceitar instâncias positivas.

Mais recentemente, também foi provado que a classe QCMA é fechada sob a completude perfeita [58]. Neste caso, uma base universal selecionada para os circuitos quânticos, aliada com o fato de que o certificado é clássico, implica que a probabilidade de aceitação é racional e tem descrição polinomial em relação ao tamanho da entrada. Neste caso, o Provador consegue enviar de maneira eficiente este valor para o Verificador, que é utilizado para atingir a completude perfeita.

Entretanto, para a classe QMA, o fato de ser ou não fechada pela completude perfeita ainda é um problema em aberto. Apresentaremos, neste capítulo, dois resultados parciais acerca deste tema.

Primeiramente, apresentaremos o resultado de que, relativizando por um conjunto de oráculos $\mathcal{U}$, $\mathrm{QMA}^{\mathcal{U}} \neq \mathrm{QMA}_1^{\mathcal{U}}$. Este resultado foi provado por Aaronson [1] e implica que qualquer método que almeje $\mathrm{QMA} = \mathrm{QMA}_1$, deve ultrapassar a barreira da relativização.

Em seguida, apresentaremos um resultado que mostra que dados alguns recursos adicionais, consegue-se decidir todas as linguagens em QMA com a característica da

completude perfeita. Começaremos com o resultado provado por Kobayashi, Le Gall e Nishimura (KLGN) [64] de que se o Provador e Verificador compartilharem um número constante de pares EPR *a priori*, é possível atingir a completude perfeita com um novo protocolo baseado no primeiro. Em seguida, mostraremos uma alteração do protocolo de KLGN em que, ao invés de termos um número constante de pares EPR, temos uma rodada de tamanho constante de mensagens clássicas. Este último resultado foi desenvolvido pelo candidato durante seu estágio no *Laboratoire d'Informatique Algorithmique: Fondements et Applications, CNRS, Université Paris VII*, sob supervisão de Iordanis Kerenidis e Jamie Sikora.

5.2 Separação por oráculo

Iremos, nesta seção apresentar o resultado de Aaronson que prova a existência de um oráculo $\mathcal{U}$, tal que $\mathrm{QMA}^{\mathcal{U}} \neq \mathrm{QMA}_1^{\mathcal{U}}$ [1].

A demonstração deste fato utiliza alguns resultados de cálculo analítico, que serão expostos inicialmente. Segue, então, a demonstração do teorema que prova a separação relativizada.

5.2.1 Funções analíticas

Iremos agora definir os conceitos necessários para a prova de que existe um oráculo que separa QMA e QMA_1, bem como enunciaremos alguns resultados que serão úteis mais tarde. As provas destes resultados fogem do escopo deste trabalho.

Começaremos com a definição de expansões de Taylor.

Definição 5.2.1. *A expansão de Taylor de uma função infinitamente diferenciável $f(x)$ e definida no intervalo aberto $(a-r, a+r)$, ao redor do ponto a, é*

$$\sum_{n\geq 0} \frac{f^{(n)}(a)}{n!}(x-a)^n,$$

onde $f^{(n)}(a)$ é a n-ésima derivada da função f no ponto a.

Vamos agora definir o conceito de funções analítica reais. Intuitivamente, estas são as funções que podem ser localmente expandidas em séries de Taylor.

Definição 5.2.2. *Uma função $f : \mathbb{R} \to \mathbb{R}$ é chamada de analítica real se para todo $x_0 \in \mathbb{R}$, a expansão de Taylor sobre x_0 converge e é igual a $f(x)$ numa vizinhança de x_0.*

Exemplos de funções analíticas reais são polinômios e funções trigonométricas. Além disso, sabe-se que a soma, multiplicação e composição de funções analíticas reais resultam também em funções analíticas reais.

Agora será apresentado um Teorema de Alekseevsky, Kriegl, Losik e Michor (AKLM) [7] referente a polinômios cujos coeficientes são dados por funções analíticas reais e suas raízes.

Teorema 5.2.3 (Teorema 5.1 de AKLM [7])**.** *Seja o polinômio*

$$p_\theta(x) = b_0(\theta) + b_1(\theta)x + b_2(\theta)x^2 + ...b(\theta)_N x^N,$$

com o parâmetro $\theta \in \mathbb{R}$ e com todas as raízes reais. Se todos os coeficiente $b_i(\theta)$, $0 \leq i \leq N$, forem funções analíticas reais de θ, então existem funções analíticas reais $\lambda_i : \mathbb{R} \to \mathbb{R}$, $0 \leq i \leq N$, tais que $\lambda_i(\theta)$ é o conjunto de raízes de $p_\theta(x)$, para todo $\theta \in \mathbb{R}$.

Finalmente, apresentaremos um teorema que caracteriza funções analíticas reais constantes.

Teorema 5.2.4. *Seja $f : \mathbb{R} \to \mathbb{R}$ uma função analítica real. Se existe um intervalo aberto $(x, y) \subset \mathbb{R}$ no qual f é constante, então f é constante.*

5.2.2 $\mathbf{QMA}^{\mathcal{U}} \neq \mathbf{QMA}_1^{\mathcal{U}}$

Iremos nesta seção apresentar a prova de que existe um oráculo $\mathcal{U}$ tal que $\mathrm{QMA}^{\mathcal{U}} \neq \mathrm{QMA}_1^{\mathcal{U}}$. A ideia geral da prova envolve oráculos da forma $U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, tal que $\theta = 0$ ou $1 \leq \theta \leq 2$. O problema, então, será decidir em qual caso nos encontramos, sendo $1 \leq \theta \leq 2$ o caso positivo.

Mostraremos que, permitindo erro bilateral, é possível responder corretamente com alta probabilidade. Basta realizar as consultas e realizar medições, aceitando caso alguma das medições resulte em $|1\rangle$. Entretanto, se $1 \leq \theta \leq 2$, com uma pequena probabilidade, podemos ter como resultado da medição somente $|0\rangle$, e neste caso, não é possível diferenciar do caso $\theta = 0$.

Começaremos com um fato relacionando a complexidade de consulta, probabilidade máxima de aceitação e autovalores.

Lema 5.2.5. *Seja V um algoritmo verificador quântico que tem como entrada um certificado $|\psi\rangle$ e faz T consultas a um oráculo quântico descrito por uma matriz unitária U. Seja $a(U)$ a probabilidade máxima em que V^U aceita a cadeia de entrada, dentre todos os possíveis certificados. Então existe uma matriz complexa $E(U)$ de dimensão $2^Q \times 2^Q$ tal que*

1. *Cada elemento de $E(U)$ é um polinômio sobre os elementos de U de grau no máximo $2T$;*
2. *$E(U)$ é Hermitiana para todo U;*
3. *$a(U)$ é igual ao maior autovalor de $E(U)$, para todo U.*

Demonstração. Seja $a(U, |\psi\rangle)$ a probabilidade de aceitação do verificador V com o oráculo U e certificado $|\psi\rangle$. Sejam os vetores $\{|v_i\rangle|\ 0 \leq i \leq 2^Q\}$, não necessariamente normalizados, considerando o oráculo U e tal que

$$a(U, |\psi\rangle) = \sum_i |\langle v_i|\psi\rangle|^2.$$

Por resultados de limitantes inferiores na complexidade de consulta quântica [21], cada elemento de $|v_i\rangle$ deve que ser um polinômio sobre os elementos de U, de grau no máximo T, dado que, inicialmente, temos um polinômio de grau 0 e a cada consulta ao oráculo, o grau deste polinômio aumenta em no máximo 1.

Seja $E = \sum_i |v_i\rangle\langle v_i|$. Temos então que E é uma matriz $2^Q \times 2^Q$, hermitiana e seus elementos são polinômios de grau no máximo $2T$. Temos também que $a(U, |\psi\rangle) = \langle\psi|E|\psi\rangle$, o que implica em

$$a(U) = \max_{|\psi\rangle} a(U, |\psi\rangle) = \max_{|\psi\rangle} \langle\psi|E|\psi\rangle,$$

que é justamente o maior autovalor de E. □

Passamos agora para a prova do teorema principal.

Teorema 5.2.6. *Existe um oráculo $\mathcal{U}$ tal que* $\mathrm{QMA}_1^{\mathcal{U}} \neq \mathrm{QMA}^{\mathcal{U}}$.

Demonstração. Seja θ um valor real e seja $U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Vamos assumir que nos é prometido $\theta = 0$ ou $1 \leq \theta \leq 2$, e, permitido o acesso a um oráculo U_θ, queremos descobrir qual dos casos se apresenta, dado que $1 \leq \theta \leq 2$ é a instância positiva.

Primeiramente, podemos ver que este problema está em BQP^{U_θ}, dado que um algoritmo quântico, sem nenhuma ajuda do certificado, pode-se fazer acesso ao oráculo dando como entrada o estado $|0\rangle$ e realizar a medição após o oráculo várias vezes. Se em alguma das medições o resultado foi $|1\rangle$, significa que $1 \leq \theta \leq 2$. Caso contrário, com alta probabilidade, $\theta = 0$. Como $\mathrm{BQP} \subseteq \mathrm{QMA}$, temos que o problema também está em QMA^{U_θ}.

Seja V o circuito do algoritmo verificador, T o número de consultas que V faz ao oráculo U_θ, Q o tamanho do certificado e $a(\theta)$ o valor máximo de aceitação dentre todos os possíveis certificados. Pelo Lema 5.2.5, existe uma matriz complexa $E(\theta)$ de dimensão $N \times N$, para $N = 2^Q$, tal que

1. Cada elemento de $E(\theta)$ é um polinômio de grau no máximo $2T$ sobre $\cos\theta$ e $\sin\theta$;

2. $E(\theta)$ é Hermitiana para todo $\theta \in \mathbb{R}$;

3. $a(\theta)$ é igual ao maior autovalor de $E(\theta)$, para todo $\theta \in \mathbb{R}$.

Sejam $\lambda_i(\theta)$, $1 \leq i \leq N$, os autovalores de $E(\theta)$. Então os valores de $\lambda_i(\theta)$ são as raízes do polinômio característico de $E(\theta)$, parametrizado por θ, de grau N:

$$p_\theta(x) = b_0(\theta) + b_1(\theta)x + ... + b_n(\theta)x^N.$$

Cada coeficiente $b_i(\theta)$ é um polinômio sobre os elementos de $E(\theta)$ de grau no máximo N, e portanto pelo item (1), cada coeficiente é um polinômio sobre $\cos\theta$ e $\sin\theta$ de grau no máximo $2TN$. Pelo item (2), todos os valores de $\lambda_i(\theta)$ são reais e portanto todos os $b_i(\theta)$ também o são. Juntando esses dois itens, temos que cada $b_i(\theta)$ é uma função analítica real de θ, e, pelo Teorema 5.2.3 temos que $\lambda_i(\theta)$ também são funções analíticas reais, para $0 \leq i \leq N$.

Pelo item (3), a probabilidade de aceitação $a(\theta)$ de V, maximizada por todos os possíveis certificados, é igual ao maior autovalor $\lambda_i(\theta)$. Se V for um circuito verificador em QMA_1, temos $a(0) \leq \frac{1}{3}$ e $a(\theta) = 1$, para todo $1 \leq \theta \leq 2$. Como N é finito, isso implica que existe um $i \in \{1, ..., 2^Q\}$ tal que $\lambda_i(0) \leq \frac{1}{2}$ mas $\lambda_i(\theta) = 1$ para todo $\theta \in (1, 2)$. Entretanto, pelo Teorema 5.2.4, isto contradiz o fato de que $\lambda_i(\theta)$ é analítica real, dado que se $\lambda_i(\theta)$ é constante para um intervalo aberto, a função deveria ser constante. Portanto existe uma escolha de θ tal que V não resolve o problema corretamente, dado $U = U(\theta)$ como oráculo. □

5.3 QMA e pares EPR

Nesta seção, será apresentado um resultado de Kobayashi, Le Gall e Nishimura (KLGN) [64] em que é mostrado que, se o Provador e o Verificador compartilharem pares EPR antes do início do protocolo, é possível atingir a completude perfeita.

Definição 5.3.1. *A classe* $\mathrm{QMA}^{k\text{-}EPR}$ *é formada pelas linguagens para as quais existe um protocolo* QMA *em que o Provador e o Verificador compartilharam k pares EPR antes da execução do protocolo.*

Iniciaremos apresentando uma representação alternativa de canais quânticos, chamadas de representação de Choi-Jamiołkowski, que permitirá a simulação de tais canais. Seguiremos apresentando alguns procedimentos básicos que serão utilizados na prova do teorema principal, que em seguida será demonstrado.

Ressaltamos que os resultados desta seção são baseados nos lemas do artigo original de KLGN [64].

5.3.1 Simulando canais quânticos com estados

Mostraremos agora resultados independentes de Choi [30] e Jamiołkowski [57], que descrevem uma das várias formas de representação de canais quânticos, os quais são generalizações dos operadores quânticos unitários. Esta representação utilizará estados quânticos, e será útil pois permitirá a simulação de um operador quântico arbitrário a partir seu estado de Choi-Jamiołkowski.

Em nosso caso, precisaremos simular uma família bem específica de operações unitárias

$$W_p = \begin{bmatrix} \sqrt{1-p} & \sqrt{p} \\ \sqrt{p} & -\sqrt{1-p} \end{bmatrix},$$

onde $p \in \mathbb{R}$ e $p \in [0,1]$. Estamos especificamente interessados nos casos em que p não é eficientemente computável pois, neste caso, aplicar W_p diretamente é uma tarefa computacionalmente difícil. Neste caso, temos que o estado de Choi-Jamiołkowski relativo a W_p, $|J(W_p)\rangle$, é

$$|J(W_p)\rangle = \sqrt{1-p}|\Phi^-\rangle + \sqrt{p}|\Psi^+\rangle,$$

onde $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ e $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ são os estados de Bell apresentados na Definição 2.2.5.

Mostraremos agora como simular a aplicação de W_p a partir de uma cópia de $|J(W_p)\rangle$, permitindo uma probabilidade constante de falha.

Lema 5.3.2. *A simulação de W_q por $J(W_q)$, descrita na Figura 5.1, resulta no estado $W_p|q_1\rangle$ com probabilidade $\frac{1}{4}$ ou falha com probabilidade $\frac{3}{4}$.*

Demonstração. Antes da medição, o estado do sistema é

$$\begin{aligned}
&(a|0\rangle + b|1\rangle)(\sqrt{1-p}|\Phi^-\rangle + \sqrt{p}|\Psi^+\rangle) \\
&= \frac{1}{2}(|\Phi^+\rangle(a\sqrt{1-p}|0\rangle + a\sqrt{p}|1\rangle + b\sqrt{p}|0\rangle - b\sqrt{1-p}|1\rangle) \\
&\quad + |\Phi^-\rangle(a\sqrt{1-p}|0\rangle + a\sqrt{p}|1\rangle - b\sqrt{p}|0\rangle + b\sqrt{1-p}|1\rangle) \\
&\quad + |\Psi^+\rangle(a\sqrt{p}|0\rangle - a\sqrt{1-p}|1\rangle + b\sqrt{1-p}|0\rangle + b\sqrt{p}|1\rangle) \\
&\quad + |\Psi^-\rangle(a\sqrt{p}|0\rangle - a\sqrt{1-p}|1\rangle - b\sqrt{1-p}|0\rangle - b\sqrt{p}|1\rangle)).
\end{aligned}$$

Se aplicarmos uma medição na base de Bell sobre os dois primeiros qubits, o resultado será $|\Phi^+\rangle$ com probabilidade $\frac{1}{4}$, e neste caso o valor do terceiro qubit será

$$(a\sqrt{1-p} + b\sqrt{p})|0\rangle + (a\sqrt{p} - b\sqrt{1-p})|1\rangle = \begin{bmatrix} \sqrt{1-p} & \sqrt{p} \\ \sqrt{p} & -\sqrt{1-p} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = W_p|q_1\rangle.$$

Com probabilidade $\frac{3}{4}$ temos como resultado da medição $|\Phi^-\rangle$, $|\Psi^+\rangle$ ou $|\Psi^-\rangle$, resultando uma falha na simulação. □

Simulando sobre o estado $|0\rangle$

O resultado apresentado no Lema 5.3.2 mostra como simular W_p sobre um qubit em um estado arbitrário. Mostraremos agora como melhorar o resultado quando o qubit está no estado $|0\rangle$, obtendo probabilidade de sucesso 1.

Lema 5.3.3. *A simulação de W_q a partir de $J(W_q)$ sobre $|0\rangle$, apresentada na Figura 5.2, retorna o valor $W_p|0\rangle$.*

Demonstração. Após aplicar a transformação T sobre $|J(W_p)\rangle$, o sistema estará no estado:

$$T|J(W_q)\rangle = \sqrt{1-p}|00\rangle + \sqrt{p}|10\rangle = (\sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle) \otimes |0\rangle,$$

Input: qubits $|q_1\rangle, |q_2\rangle, |q_3\rangle$, tal que:

$$|q_1\rangle = a|0\rangle + b|1\rangle \text{ e } |q2\rangle|q3\rangle = |J(W_p)\rangle = \sqrt{1-p}|\Phi^-\rangle + \sqrt{p}|\Psi^+\rangle,$$

onde $p \in [0,1]$ e $a, b \in \mathbb{C}$

1 Meça $|q_1\rangle|q_2\rangle$ na base de Bell ;
2 **if** *resultado é* $|\Phi^+\rangle$ **then**
3 | Retorne $|q_3\rangle$
4 **else**
5 | Retorne "falha"
6 **end**

Figura 5.1: Procedimento para simular W_p a partir de $|J(W_p)\rangle$

e descartando o segundo qubit, temos

$$\sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle = W_p|0\rangle.$$

□

Input:

$$|J(W_q)\rangle = \sqrt{1-p}|\Phi^-\rangle + \sqrt{p}|\Psi^+\rangle,$$

com $p \in [0,1]$

1 Aplique a operação

$$T : |\Phi^-\rangle \to |00\rangle, |\Psi^-\rangle \to |01\rangle, |\Psi^+\rangle \to |10\rangle, |\Phi^+\rangle \to |11\rangle$$

sobre $|J(W_q)\rangle$;
2 Retorne o primeiro qubit ;

Figura 5.2: Simulando W_p com $|J(W_p)\rangle$ sobre $|0\rangle$

5.3.2 Procedimentos básicos

Nesta subseção, serão descritos os componentes básicos utilizados para provar que a classe QMA está contida em $\text{QMA}_1^{\text{k·EPR}}$. Primeiramente, será apresentado o Procedimento de Reflexão, que irá amplificar a probabilidade de aceitação das cadeias da

linguagem dadas algumas premissas, atingindo completude perfeita. Iremos demonstrar também como simular o funcionamento do Procedimento de Reflexão, dado que executá-lo de maneira exata é computacionalmente difícil para o Verificador.

Procedimento de Reflexão

Nesta subseção, iremos considerar protocolos QMA que possuem a propriedade de que todas as cadeias da linguagem são aceitas com probabilidade máxima exatamente $\frac{1}{2}$ e que cadeias que não estão na linguagem são aceitas com probabilidade no máximo $2^{-poly(|x|)}$. Para esses protocolos será possível amplificar a probabilidade de aceitação para instâncias positivas, atingindo completude perfeita.

A ideia principal do Procedimento de Reflexão foi proposta por Watrous [91] no contexto de Sistemas Interativos de Prova Quânticos de Conhecimento Zero. Kempe, Kobayashi, Matsumoto e Vidick [60] foram os primeiros a utilizar esta ideia de modo a atingir completude perfeita em Sistemas Interativos de Prova Quânticos com Múltiplos Provadores. Finalmente, KLGN utilizaram a estratégia para atingir completude perfeita na simulação de protocolos QMA em $\mathrm{QMA}^{\mathrm{k\cdot EPR}}$ [64].

Considerando o protocolo QMA original, denotamos por Π_{init} o operador de projeção para o subespaço correspondente a seus estados iniciais válidos, ou seja, um certificado $|\psi\rangle$ e *qubits* auxiliares $|0\rangle$; denotamos por V_x seu circuito verificador e por Π_{acc} o operador de projeção para o subespaço de aceitação do protocolo original.

Como provado por Marriott e Watrous[70], todos os autovetores $|\phi_j\rangle$ de

$$M_x = \Pi_{init} V_x^\dagger \Pi_{acc} V_x \Pi_{init}$$

associados aos autovalores λ_j são estados iniciais válidos para o protocolo QMA que tem V_x como verificador, pois

$$\Pi_{init}|\phi_j\rangle = \frac{1}{\lambda_j}\Pi_{init} M_x |\phi_j\rangle = \frac{1}{\lambda_j} M_x |\phi_j\rangle = |\phi_j\rangle.$$

Além disso, temos que o autovalor λ_j é exatamente a probabilidade de aceitação do protocolo quando o estado inicial é $|\phi_j\rangle$:

$$\lambda_j = \langle\phi_j|M_x|\phi_j\rangle = ||\Pi_{acc} V_x \Pi_{init}|\phi_j\rangle||^2.$$

Iremos agora demonstrar como o Procedimento de Reflexão atua sobre essa família especial de protocolos QMA.

Input: Estado quântico $|\phi\rangle$
1 Verifique se estado está em Π_{init} e rejeitar se não estiver ;
2 Aplique V_x ;
3 Aplique a operação $I - 2\Pi_{acc}$;
4 Aplique $V_x^\dagger$;
5 Rejeite se estado estiver em Π_{init} ;

Figura 5.3: Procedimento de Reflexão

Lema 5.3.4. *Seja $|\phi_j\rangle$ um autovetor de M_x correspondente ao autovalor λ_j. Se utilizamos $|\phi_j\rangle$ como entrada para o Procedimento de Reflexão, descrito na Figura 5.3, este irá rejeitar com probabilidade $(1-2\lambda_j)^2$.*

Demonstração. A projeção do sistema após o passo 4 sobre o subespaço das configurações iniciais válidas é

$$\begin{aligned}\Pi_{init}V_x^\dagger(I-2\Pi_{acc})V_x|\phi_j\rangle &= \Pi_{init}V_x^\dagger(I-2\Pi_{acc})V_x\Pi_{init}|\phi_j\rangle \\ &= |\phi_j\rangle - 2\Pi_{init}V_x^\dagger\Pi_{acc}V_x\Pi_{init}|\phi_j\rangle \\ &= |\phi_j\rangle - 2M_x|\phi_j\rangle \\ &= |\phi_j\rangle - 2\lambda_j|\phi_j\rangle \\ &= (1-2\lambda_j)|\phi_j\rangle.\end{aligned}$$

Portanto, a probabilidade de rejeição após a medição no passo 5 é de $(1-2\lambda_j)^2$. □

Corolário 5.3.5. *Sejam x uma instância positiva e $|\phi^*\rangle$ o autovetor de M_x correspondente ao maior autovalor $\lambda^* = \frac{1}{2}$. Se utilizarmos $|\phi^*\rangle$ como entrada do Procedimento de Reflexão, o procedimento irá aceitar com probabilidade* 1.

Lema 5.3.6. *Se x for uma instância negativa, então o Procedimento de Reflexão irá aceitar com probabilidade no máximo $2^{-poly(|x|)}$.*

Demonstração. Seja $|\psi\rangle$ uma entrada para o Procedimento de Reflexão e $|\psi\rangle = \sum_{j=1}^{d}\alpha_j|\phi_j\rangle$ sua decomposição espectral em relação aos autovetores de M_x. Temos que a projeção do sistema após o passo 4 sobre o subespaço de configurações iniciais válidas é

$$\begin{aligned}
&\Pi_{init} V_x^\dagger (I - 2\Pi_{acc}) V_x |\psi\rangle \\
&= \sum_j \alpha_j \Pi_{init} V_x^\dagger (I - 2\Pi_{acc}) V_x |\phi_j\rangle \\
&= \sum_j \alpha_j (1 - 2\lambda_j) |\phi_j\rangle,
\end{aligned}$$

onde a última igualdade vem do Lema 5.3.4.

Usando o fato de que x é uma instância negativa, sabemos que o maior autovalor de M_x é no máximo $2^{-poly(|x|)}$. Portanto, a probabilidade de rejeição no passo 5 é no mínimo

$$\begin{aligned}
\sum_j |\alpha_j|^2 (1 - 2\lambda_j)^2 &\geq (1 - 2^{-poly(|x|)+1})^2 \sum_{j=1}^{d} |\alpha_j|^2 \\
&= (1 - 2^{-poly(|x|)+1})^2 \\
&\geq 1 - 2^{-poly(|x|)+2} \\
&= 1 - 2^{-poly(|x|)},
\end{aligned}$$

onde λ_j são os autovalores associados aos autovetores $|\phi_j\rangle$. □

Simulação do Procedimento de Reflexão

Na seção anterior, descrevemos o Procedimento de Reflexão para protocolos com a propriedade muito restrita de que todas as instâncias positivas possuem probabilidade de aceitação máxima exatamente igual a $\frac{1}{2}$. Nesta seção, iremos apresentar como obter esta propriedade com auxílio de informação extra fornecida pelo Provador.

Apresentamos também um procedimento que, dado o certificado original do protocolo QMA, gera um novo *qubit* não-emaranhado com o sistema e cujas amplitudes estão relacionadas à probabilidade de aceitação do protocolo original.

Terminamos apresentando a simulação do Procedimento de Reflexão usando os dois elementos anteriores.

Probabilidade de aceitação máxima $\frac{1}{2}$ para instâncias positivas Iremos, nesta seção, descrever um método que demonstra como obter, com auxilio do Provador, probabilidade máxima de aceitação exatamente $\frac{1}{2}$ para instâncias positivas.

Se conseguíssemos computar de modo eficiente a probabilidade de aceitação máxima p_x para cada instância positiva x, seria possível jogar uma moeda com proba-

bilidade $q_x = \frac{1}{2p_x}$ de se obter $|1\rangle$ e o Verificador aceitaria se e somente se o protocolo original aceitasse e o resultado da moeda fosse $|1\rangle$. Neste caso, é fácil notar que a probabilidade de aceitação máxima para instâncias positivas seria exatamente $p_x q_x = \frac{1}{2}$ e a robustez não aumentaria.

Porém, na maioria dos casos, computar p_x é inviável. É neste contexto que podemos utilizar os estados de Choi-Jamiołkowski para simular a operação da moeda

$$W_{q_x} = \begin{bmatrix} \sqrt{1-q_x} & \sqrt{q_x} \\ \sqrt{q_x} & -\sqrt{1-q_x} \end{bmatrix},$$

através do método descrito na Figura 5.1.

Ao realizarmos a simulação da moeda em paralelo ao protocolo original, pelo Lema 5.3.2, temos a probabilidade de sucesso $\frac{1}{4}$ e, neste caso, a operação do Verificador é equivalente a $V'_x = V_x \otimes W_{q_x}$ e com projeção $\Pi'_{acc} = \Pi_{acc} \otimes |1\rangle\langle 1|$. Segue-se, então, que a probabilidade de aceitação máxima para instâncias positivas é exatamente $\frac{1}{2}$, condicionada no sucesso na simulação.

Procedimento de Destilação Para provar robustez do protocolo $\mathrm{QMA}_1^{\mathrm{k\cdot EPR}}$, será necessário que a prova original do protocolo QMA não esteja emaranhada com os registradores que contém as cópias do estado de Choi-Jamiołkowski utilizados na simulação de W_{q_x}. Entretanto, um Provador desonesto pode enviar esses registradores emaranhados. Para resolver esse problema, KLGN[64] utilizou um procedimento baseado em resultados de Marriott e Watrous[70], chamado Procedimento de Destilação. No final deste procedimento, teremos, com uma determinada probabilidade de sucesso, um *qubit* não-emaranhado cujas amplitudes codificam a probabilidade de aceitação no protocolo original, e este *qubit* será utilizado no Procedimento de Reflexão no lugar do certificado original e do circuito V_x.

Definição 5.3.7. *Sejam $p_x \in [0,1]$ e $p = \frac{p_x^2}{\sqrt{2p_x^2 - 2p_x + 1}}$. O estado $|\chi_p\rangle$ é definido como*

$$|\chi_p\rangle = \frac{1}{\sqrt{2p_x^2 - 2p_x + 1}}((1-p_x)|0\rangle + p_x|1\rangle) = \sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle.$$

Nota 5.3.8. *Pode-se ver facilmente que ao aplicarmos T^{-1} sobre o estado $|\chi_p\rangle|0\rangle$, onde T é a função definida na Figura 5.2, obtemos $|J(W_p)\rangle$.*

Input: Registrador E
1 Crie um qubit R no estado $|0\rangle$;
2 Aplique V_x sobre E ;
3 Aplique $\Pi_{rej} \otimes I + \Pi_{acc} \otimes X$ sobre (E, R) ;
4 Aplique $V_x^\dagger$ sobre E ;
5 **if** *Se E for projetado sobre Π_{init}* **then**
6 | Retorne (E, R) ;
7 **else**
8 | Retorne "falha";
9 **end**

Figura 5.4: Procedimento de Destilação

Lema 5.3.9. *Quando passamos como entrada o autovetor $|\phi_j\rangle$ de M_x associado ao maior autovalor λ_j, que é a probabilidade máxima de aceitação p_x, o Procedimento de Destilação, descrito na Figura 5.4, resulta no estado*

$$|\phi_j\rangle \otimes |\chi_p\rangle,$$

com probabilidade $2\lambda_j^2 - 2\lambda_j + 1$, ou falha, caso contrário.

Demonstração. Se projetarmos o estado após o passo 4 sobre o subespaço de estados iniciais válidos, temos que

$$\begin{aligned}
&(\Pi_{init} V_x^\dagger \Pi_{rej} V_x \Pi_{init} |\phi_j\rangle) \otimes |0\rangle + (\Pi_{init} V_x^\dagger \Pi_{acc} V_x \Pi_{init} |\phi_j\rangle) \otimes |1\rangle \\
&= (1 - \lambda_j)|\phi_j\rangle \otimes |0\rangle + \lambda_j |\phi_j\rangle \otimes |1\rangle \\
&= |\phi_j\rangle \otimes ((1 - \lambda_j)|0\rangle + \lambda_j |1\rangle).
\end{aligned}$$

Portanto, temos que a probabilidade de sucesso do procedimento é

$$(1 - \lambda_j)^2 + \lambda_j^2 = 2p_x^2 - 2p_x + 1,$$

e neste caso, temos como resultado

$$|\phi_j\rangle \otimes |\chi_p\rangle.$$

□

Simulando o Procedimento de Reflexão Usando duas cópias do resultado $|\chi_p\rangle$ do Procedimento de Destilação e duas cópias do estado de Choi-Jamiołkowski $|J(W_q)\rangle$ para $pq = \frac{1}{2}$, a Figura 5.5 descreve como simular o Procedimento de Reflexão. A simulação de W_p é feita a partir do estado $|J(W_p)\rangle$ que, como visto na Nota 5.3.8, pode ser obtido a partir de $|\chi_p\rangle$.

Input: Duas cópias de $|\chi_p\rangle$ e duas cópias de $|J(W_q)\rangle$
1 Simule a aplicação de $W_p \otimes W_q$ sobre $|00\rangle$;
2 Aplique $I - 2|11\rangle\langle 11|$;
3 Simule a aplicação $W_p \otimes W_q$ e se alguma das simulações falharem, retorne "falha" ;
4 Meça os qubits ;
5 **if** *resultado for* $|00\rangle$ **then**
6 | Rejeite ;
7 **else**
8 | Aceite ;
9 **end**

Figura 5.5: Simulação do Procedimento de Reflexão

Lema 5.3.10. *Se o estado* $|\chi_p\rangle^{\otimes 2} \otimes |J(W_q)\rangle^{\otimes 2}$ *for fornecido como entrada para a simulação do Procedimento de Reflexão, onde* $p, q \in [0, 1]$ *e* $pq = \frac{1}{2}$*, o teste irá falhar com probabilidade* $\frac{3}{4}$ *ou aceitar com probabilidade* $\frac{1}{4}$*.*

Demonstração. Seja $U = W_p \otimes W_q$. Se ambas simulações no passo 3 forem realizadas com sucesso, o que ocorre com probabilidade $\frac{1}{16}$, então o estado do sistema antes da medição será

$$\begin{aligned}
|00\rangle\langle 00|U^\dagger(I - |11\rangle\langle 11|)U(|00\rangle) &= |00\rangle\langle 00|U^\dagger U|00\rangle - 2|00\rangle\langle 00|U^\dagger|11\rangle\langle 11|U|00\rangle \\
&= |00\rangle - 2|||11\rangle\langle 11|U|00\rangle||^2|00\rangle \\
&= |00\rangle - 2\frac{1}{2}|00\rangle \\
&= 0,
\end{aligned}$$

portanto, a probabilidade de rejeição neste caso é 0, quando a simulação é bem sucedida. □

Lema 5.3.11. *Se* $|0\rangle^{\otimes 2} \otimes |J(W_q)\rangle^{\otimes 2}$ *for fornecido como entrada da simulação do Procedimento de Reflexão, para todo* $q \in [0,1]$*, o procedimento irá rejeitar com probabilidade* $\frac{1}{16}$*.*

Demonstração. Seja $U = W_0 \otimes W_q$. Se ambas simulações no passo 3 forem bem sucedidas, o que ocorre com probabilidade $\frac{1}{16}$, então o estado do sistema antes da medição será

$$\begin{aligned} U^\dagger(I - |11\rangle\langle 11|)U|00\rangle &= U^\dagger U|00\rangle - 2U^\dagger|11\rangle\langle 11|U|00\rangle \\ &= |00\rangle - 2U^\dagger|11\rangle\langle 11|(|0\rangle \otimes |\chi_q\rangle) \\ &= |00\rangle, \end{aligned}$$

onde a última igualdade vem do fato que $(|0\rangle \otimes |\chi_q\rangle)$ não está no subespaço gerado por $|11\rangle$. Portanto, a probabilidade de medir $|00\rangle$ quando as simulações foram realizadas com sucesso é 1. □

5.3.3 Lemas técnicos

Iremos agora provar uma série de lemas relativos aos passos propostos por KLGN[64] realizados pelo Verificador para certificar que o Provador enviou de fato cópias de um estado de Choi-Jamiołkowski associado a algum W_q, $|J(W_q)\rangle$. Estes passos serão todos utilizados na prova do Teorema 5.3.19.

Nesta seção, para $j \in \{1, ..., n\}$, $\mathcal{S}_j$ e $\mathcal{S}'_j$ são espaços de Hilbert 2-dimensionais complexos, $\mathcal{W}_j \subsetneq \mathcal{S}_j \otimes \mathcal{S}'_j$ o subespaço de $\mathcal{S}_j \otimes \mathcal{S}'_j$ gerado pelos vetores $|\Phi^-\rangle$ e $|\Psi^+\rangle$, $\mathcal{W} = \mathcal{W}_1 \otimes \mathcal{W}_2$ a composição de dois destes subespaços, $\Pi_{\mathcal{W}}$ o operador de projeção sobre $\mathcal{W}$ e $\mathbf{D}(\mathcal{W})$ o conjunto de estados mistos em $\mathcal{W}$. Para uma matriz de densidade ρ, denotamos por $||\rho||_{tr}$ sua norma de traço, que corresponde a $Tr(\sqrt{\rho\rho^\dagger})$. Dados dois estados cujas matrizes de densidade são ρ e σ, a distância de traço destes dois estados, $D(\rho, \sigma)$, é igual a $\frac{1}{2}||\rho - \sigma||_{tr}$, o que define uma métrica no espaço de matrizes de densidade.

Simulação de uma permutação aleatória

Veremos agora um processo de simulação de permutação aleatória entre registradores quânticos e suas consequências para o estado reduzido de alguns desses registradores. Para provar este lema, utilizaremos um resultado conhecido como Teorema de De Finetti, cuja prova está fora do escopo deste trabalho.

Teorema 5.3.12 (Teorema de De Finetti)**.** *Sejam n registradores quânticos $R_1, ..., R_n$, cada um formado por k qubits, e seu estado ρ, invariante sob qualquer permutação entre os registradores. Para todo $m < n$, seja também ρ_m o estado reduzido dos registradores $R_1, ..., R_m$. Existe um $c \in \mathbb{N}$ e um conjunto de estados $\{\xi_j\}$ de k qubits e uma distribuição de probabilidades $\{p_j\}$, para $1 \leq j \leq c$, tal que*

$$D\left(\rho_m, \sum_{j=1}^{c} p_j \xi_j^{\otimes m}\right) \leq \frac{2^{2k+1} m}{n}.$$

Lema 5.3.13. *Sejam N registradores de 2-qubits $(S_1, S_1'), ..., (S_N, S_N')$, para qubits S_i, S_i' no espaço $\mathcal{S}_i$, $\mathcal{S}_i'$, respectivamente, e seja $\epsilon \in (0, 1)$ uma constante. A Simulação de permutação aleatória, descrita na Figura 5.6, aplicada sobre esses N registradores falha com probabilidade $\frac{1}{N}$ e, se não falhar, o estado parcial dos dois primeiros registradores tem distância de traço no máximo $\frac{2^6}{N}$ do estado*

$$\sum_j \mu_j {\xi_j}^{\otimes 2},$$

para algum conjunto $\{\xi_j\}$.

Demonstração. Dado que a simulação falha somente quando $r_2 = 1$, a probabilidade de falha do procedimento é $\frac{1}{N}$.

Se o procedimento não falha, o estado misto dos dois primeiros registradores é igual ao estado misto que os dois registradores teriam caso uma permutação aleatória tivesse sido realizada. Neste caso, utilizando o Teorema de De Finetti, temos que estes registradores tem distância de traço no máximo $\frac{2^6}{N}$ a

$$\sum_j \mu_j {\xi_j}^{\otimes 2},$$

para algum conjunto de estados $\xi_j^{\otimes 2} \in \mathbf{D}(\mathcal{S}_1 \otimes \mathcal{S}_1' \otimes \mathcal{S}_2 \otimes \mathcal{S}_2')$ com probabilidade associada μ_j. □

Subespaço dos estados

Iremos agora limitar as probabilidades com que um estado $\rho = \sum_j \mu_j \xi_j^{\otimes 2}$ não está no subespaço gerado pelos vetores $\{|\Phi^-\rangle, |\Psi^+\rangle\}$, quando está próximo na distância de traço de uma mistura de estados mistos em $\mathbf{D}(\mathcal{W})$.

Input: N registradores de 2 qubits $R_1, ..., R_N$
1 Escolha $r_1, r_2 \in \{1, ..., N\}$ aleatoriamente de forma uniforme ;
2 Se $r_2 = 1$, retorne "falha" ;
3 Troque R_1 e R_{r_1} ;
4 Troque R_2 e R_{r_2} ;

Figura 5.6: Simulação de uma permutação aleatória em registradores

Lema 5.3.14. *Seja $\rho = \sum_j \mu_j \xi_j^{\otimes 2}$ um estado em $\mathcal{S}_1 \otimes \mathcal{S}'_1 \otimes \mathcal{S}_2 \otimes \mathcal{S}'_2$ tal que $Tr_{\mathcal{S}'_1 \otimes \mathcal{S}'_2}(\rho)$ tem distância de traço no máximo γ do estado $(\frac{1}{2}I)^{\otimes 2}$; e $\epsilon \in (0,1)$ uma constante. Neste caso, temos que um dos seguintes casos vale:*

1. *Se realizarmos uma projeção em ρ considerando os projetores $\{\Pi_{\mathcal{W}}, \Pi_{\mathcal{W}^\perp}\}$, o resultado estará em $\mathcal{W}^\perp$ com probabilidade pelo menos ϵ.*

2. *O estado ρ possui distância de traço no máximo $\sqrt{\epsilon}$ de*

$$\rho' = \sum_j \mu'_j {\xi'}_j^{\otimes 2},$$

para algum conjunto de $\mu'_j \in \mathbb{R}$ e $\xi'_j \in \boldsymbol{D}(\mathcal{W})$, e $Tr_{\mathcal{S}'_1 \otimes \mathcal{S}'_2}(\rho')$ tem distância de traço no máximo $\gamma + \sqrt{\epsilon}$ de $(\frac{1}{2}I)^{\otimes 2}$.

Demonstração. Se tivermos que $Tr(\Pi_{\mathcal{W}}\rho) < 1 - \epsilon$ então, quando aplicamos a projeção sobre $\{\Pi_{\mathcal{W}}, \Pi_{\mathcal{W}^\perp}\}$, o resultado estará em $\mathcal{W}^\perp$ com probabilidade pelo menos ϵ, satisfazendo o primeiro item.

Agora iremos demonstrar que se $Tr(\Pi_{\mathcal{W}}\rho) \geq 1 - \epsilon$, então o segundo item será satisfeito. Especificamente, provaremos que ρ possui distância de traço $\sqrt{\epsilon}$ do estado

$$\rho' = \sum_j \mu'_j {\xi'}^{\otimes 2}$$

onde

$$\mu'_j = \frac{1}{Tr({\Pi_{\mathcal{W}}}^{\otimes 2}\rho)} Tr(\Pi_{\mathcal{W}}\xi_j)^2 \mu_j \text{ e } \xi'_j = \frac{1}{Tr(\Pi_{\mathcal{W}}\xi_j)} \Pi_{\mathcal{W}}\xi_j\Pi_{\mathcal{W}} ,$$

para todos os valores de j. É fácil verificar que ρ' é um estado misto válido, sendo $\mu'_j \in [0,1]$ para todos os valores de j e $\sum_j \mu'_j = 1$. Além disso, temos que $\xi'_j \in \mathbf{D}(\mathcal{W})$.

Sejam $\mathcal{S}$ o espaço de Hilbert associado a ρ, $|\psi\rangle$ uma purificação de ρ tal que $|\psi\rangle$ está no espaço $\mathcal{S}\otimes\mathcal{T}$, e $|\psi'\rangle = \frac{1}{||(\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)|\psi\rangle||}(\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)|\psi\rangle$ a projeção normalizada de $|\psi\rangle$ sobre o subespaço $\mathcal{W}$.

Iniciaremos provando que $|\psi'\rangle$ é uma purificação de ρ':

$$\begin{aligned}
Tr_{\mathcal{T}}(|\psi'\rangle\langle\psi'|) &= \frac{1}{||(\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)|\psi\rangle||^2} Tr_{\mathcal{T}}((\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)|\psi\rangle\langle\psi|(\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)) \\
&= \frac{1}{Tr(\Pi_{\mathcal{W}}{}^{\otimes 2} Tr_{\mathcal{T}}(|\psi\rangle\langle\psi|))} \Pi_{\mathcal{W}}{}^{\otimes 2} Tr_{\mathcal{T}}(|\psi\rangle\langle\psi|)\Pi_{\mathcal{W}}{}^{\otimes 2} \\
&= \frac{1}{Tr(\Pi_{\mathcal{W}}{}^{\otimes 2}\rho)} \Pi_{\mathcal{W}}{}^{\otimes 2}\rho\Pi_{\mathcal{W}}{}^{\otimes 2} \\
&= \frac{1}{Tr(\Pi_{\mathcal{W}}{}^{\otimes 2}\rho)} \sum_j \mu_j (\Pi_{\mathcal{W}}\xi_j\Pi_{\mathcal{W}})^{\otimes 2} \\
&= \sum_j \frac{1}{Tr(\Pi_{\mathcal{W}}{}^{\otimes 2}\rho)} Tr(\Pi_{\mathcal{W}}\xi_j)^2 \mu_j \left(\frac{1}{Tr(\Pi_{\mathcal{W}}\xi_j)^2}\Pi_{\mathcal{W}}\xi_j\Pi_{\mathcal{W}}\right)^{\otimes 2} \\
&= \rho'.
\end{aligned}$$

Segue que

$$\begin{aligned}
D(\rho,\rho') \leq D(|\psi\rangle\langle\psi|, |\psi'\rangle\langle\psi'|) &= \sqrt{1-|\langle\psi|\psi'\rangle|^2} \\
&= \sqrt{1-||(\Pi_{\mathcal{W}}{}^{\otimes 2}\otimes I)|\psi\rangle||^2} \\
&= \sqrt{1-Tr(\Pi_{\mathcal{W}}{}^{\otimes 2}\rho)} \\
&\leq \sqrt{\epsilon}
\end{aligned}$$

Como $D(Tr_{\mathcal{S}_1'\otimes\mathcal{S}_2'}(\rho), (\frac{1}{2}I)^{\otimes 2}) \leq \gamma$ e $D(Tr_{\mathcal{S}_1'\otimes\mathcal{S}_2'}(\rho), Tr_{\mathcal{S}_1'\otimes\mathcal{S}_2'}(\rho')) \leq D(\rho,\rho')$, pela desigualdade triangular temos que $D(Tr_{\mathcal{S}_1'\otimes\mathcal{S}_2'}(\rho'), (\frac{1}{2}I)^{\otimes 2}) \leq \gamma + \sqrt{\epsilon}$. □

Verificação de estados puros

Agora faremos um teste que verifica se um estado que passou no teste anterior é uma mistura de estados puros ou está longe de o ser. Este teste é justamente o *Swap test* apresentado na Seção 2.5.4.

Lema 5.3.15. *Seja $\rho = \sum_j \mu_j \xi_j^{\otimes 2}$ o valor de dois registradores quânticos de 2 qubits (S_1, S_1', S_2, S_2'), tal que $\xi_j \in \boldsymbol{D}(\mathcal{W})$ e $D(Tr_{\mathcal{S}_1'\otimes\mathcal{S}_2'}(\rho), (\frac{1}{2}I)^{\otimes 2}) \leq \gamma$. Sejam também $\delta, \epsilon \in (0,1)$ duas constantes. Neste caso, um dos seguintes casos vale:*

1. *O Swap test entre* (S_1, S_1') *e* (S_2, S_2') *rejeita com probabilidade pelo menos* $\frac{1}{2}\epsilon\delta$.

2. ρ *tem distância de traço no máximo* $2\epsilon + \delta$ *de*

$$\rho' = \sum_j \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2},$$

para algum conjunto $|\psi_j\rangle\langle\psi_j| \in \mathcal{W}$ *e, neste caso,* $D(Tr_{S_1' \otimes S_2'}(\rho'), (\frac{1}{2}I)^{\otimes 2}) \leq \gamma + 2\epsilon + \delta$.

Demonstração. Sejam $S = \{j : Tr(\xi_j^2) \geq 1 - \epsilon\}$ e $\mu(S) = \sum_{j \in S} \mu_j$. Para todo $j \in S$, temos que o autovalor principal λ_j de ξ_j, associado ao autovetor $|\psi_j\rangle \in \mathcal{W}$, é no mínimo $1 - \epsilon$, portanto

$$\xi_j = \lambda_j |\psi_j\rangle\langle\psi_j| + (1 - \lambda_j)\upsilon_j,$$

para algum $v_j \in \mathbf{D}(\mathcal{W})$.

$$||\xi_j - |\psi_j\rangle\langle\psi_j|||_{tr} = ||\lambda_j|\psi_j\rangle\langle\psi_j| + (1-\lambda_j)\upsilon_j - |\psi_j\rangle\langle\psi_j|||_{tr} = (1-\lambda_j)||\upsilon_j - |\psi_j\rangle\langle\psi_j|||_{tr},$$

o que implica em

$$D(\xi_j, |\psi_j\rangle\langle\psi_j|) \leq (1 - \lambda_j) D(\upsilon_j, |\psi_j\rangle\langle\psi_j|) \leq 1 - \lambda_j \leq \epsilon.$$

Se $\mu(S) < 1 - \delta$, segundo o Teorema 2.5.6, o *Swap test* irá rejeitar com probabilidade pelo menos $\frac{1}{2}\epsilon\delta$, satisfazendo o primeiro caso.

Se $\mu(S) \geq 1 - \delta$, iremos provar que ρ é $2\epsilon + \delta$ distante do estado

$$\rho' = \frac{1}{\mu(S)} \sum_{j \in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2},$$

satisfazendo o segundo caso.

Vamos agora limitar a norma de traço entre os dois estados:

$$
\begin{aligned}
||\rho - \rho'||_{tr} &= \left|\left|\sum_j \mu_j {\xi_j}^{\otimes 2} - \frac{1}{\mu(S)} \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right|\right|_{tr} \\
&\leq \left|\left|\sum_j \mu_j {\xi_j}^{\otimes 2} - \left(\sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2} + \sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2}\right)\right|\right|_{tr} \\
&+ \left|\left|\left(\sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2} + \sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2}\right) - \frac{1}{\mu(S)} \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right|\right|_{tr} \\
&\leq \sum_{j\in S} \mu_j \left|\left|{\xi_j}^{\otimes 2} - |\psi_j\rangle\langle\psi_j|^{\otimes 2}\right|\right|_{tr} \\
&+ \left|\left|\sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2} - \left(\frac{1}{\mu(S)} - 1\right) \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right|\right|_{tr} \\
&\leq \sum_{j\in S} \mu_j \left(\left|\left|{\xi_j}^{\otimes 2} - \xi_j \otimes |\psi_j\rangle\langle\psi_j|\right|\right|_{tr} + \left|\left|\xi_j \otimes |\psi_j\rangle\langle\psi_j| - |\psi_j\rangle\langle\psi_j|^{\otimes 2}\right|\right|_{tr}\right) \\
&+ (1-\mu(S)) \left|\left|\frac{1}{1-\mu(S)} \sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2} - \frac{1}{\mu(S)} \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right|\right|_{tr} \\
&\leq 2 \sum_{j\in S} \mu_j \left|\left|\xi_j - |\psi_j\rangle\langle\psi_j|\right|\right|_{tr} \\
&+ (1-\mu(S)) \left|\left|\frac{1}{1-\mu(S)} \sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2} - \frac{1}{\mu(S)} \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right|\right|_{tr}
\end{aligned}
$$

Portanto temos que a distância de traço entre os dois estados é no mínimo

$$
\begin{aligned}
D(\rho,\rho') &\leq 2 \sum_{j\in S} \mu_j D(\xi_j, |\psi_j\rangle\langle\psi_j|) \\
&+ (1-\mu(S)) D\left(\frac{1}{1-\mu(S)} \sum_{i\notin S} \mu_j {\xi_j}^{\otimes 2}, \frac{1}{\mu(S)} \sum_{j\in S} \mu_j (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}\right) \\
&\leq 2\epsilon + \delta
\end{aligned}
$$

Pela desigualdade triangular, temos também que

$$
D\left(Tr_{S_1'\otimes S_2'}(\rho'), \left(\frac{1}{2}I\right)^{\otimes 2}\right) \leq \gamma + 2\epsilon + \delta.
$$

□

Estado de Choi-Jamiołkowski

Agora iremos utilizar o fato de que os primeiros *qubits* de cada registrador estão próximos do estado misto total para provar que os registradores também estão próximos a uma mistura de estados Choi-Jamiołkowski associados a algum operador W_q.

Inicialmente, iremos provar um lema auxiliar envolvendo distribuições de probabilidade.

Lema 5.3.16. *Seja* $\{p_j\}$ *uma distribuição de probabilidade e* $\{c_j\}$ *um conjunto de números reais tal que* $|c_j| \leq 1$. *Se* $\sum_j p_j c_j^2 \leq \delta$, *então* $\sum p_j |c_j| < 2\delta^{\frac{1}{3}}$.

Demonstração. Seja $A = \{j : c_j^2 \leq \delta^{\frac{2}{3}}\}$. Temos que

$$\sum_{j \in A} p_j |c_j| \leq \sum_{j \in A} p_j (\delta^{\frac{2}{3}})^{\frac{1}{2}} \leq \delta^{\frac{1}{3}} \sum_{j \in A} p_j \leq \delta^{\frac{1}{3}}.$$

Além disso, como

$$\delta \geq \sum_j p_j c_j^2 \geq \sum_{j \notin A} p_j c_j^2 > \delta^{\frac{2}{3}} \sum_{j \notin A} p_j,$$

segue que

$$\sum_{j \notin A} p_j |c_j| \leq \sum_{j \notin A} p_j < \delta^{\frac{1}{3}}.$$

Portanto

$$\sum_j p_j |c_j| < 2\delta^{\frac{1}{3}}.$$

□

Iremos agora provar um limitante inferior da distância dos primeiros *qubits* dos registradores para o estado misto total.

Lema 5.3.17. *Seja* $\rho = \sum_j \mu_j (|\xi_j\rangle\langle\xi_j|)^{\otimes 2}$, *para* $|\xi_j\rangle = \alpha_j |\Phi^-\rangle + \beta_j e^{i\theta_j} |\Psi^+\rangle$ *com* $\alpha_j, \beta_j \in \mathbb{R}$, $\alpha_j^2 + \beta_j^2 = 1$ *e* $\theta_j \in [0, 2\pi)$. *Segue-se então que*

$$D\left(Tr_{\mathcal{S}_1' \otimes \mathcal{S}_2'}(\rho), \left(\frac{1}{2} I\right)^{\otimes 2}\right) \geq \sum_j \mu_j \alpha_j^2 \beta_j^2 \sin^2 \theta_j.$$

Demonstração. Podemos ver que

$$\begin{aligned}|\xi_j\rangle &= \alpha_j|\Phi^-\rangle + \beta_j e^{i\theta_j}|\Psi^+\rangle \\ &= \frac{1}{\sqrt{2}}(\alpha_j(|00\rangle - |11\rangle) + \beta_j e^{i\theta_j}(|01\rangle + |10\rangle)) \\ &= \frac{1}{\sqrt{2}}((\alpha_j|0\rangle + \beta_j e^{i\theta_j}|1\rangle)\otimes|0\rangle + e^{i\theta_j}(\beta_j|0\rangle - \alpha_j e^{-i\theta_j}|1\rangle)\otimes|1\rangle),\end{aligned}$$

e, portanto, o estado reduzido de $Tr_{S_1'\otimes S_2'}(|\xi_j\rangle\langle\xi_j|^{\otimes 2})$ é

$$\begin{aligned}&\frac{1}{4}((\alpha_j|0\rangle + \beta_j e^{i\theta_j}|1\rangle)\otimes(\beta_j|0\rangle - \alpha_j e^{-i\theta_j}|1\rangle) \\ &+ (\beta_j|0\rangle - \alpha_j e^{-i\theta_j}|1\rangle)\otimes(\alpha_j|0\rangle + \beta_j e^{i\theta_j}|1\rangle) \\ &+ (\alpha_j|0\rangle + \beta_j e^{i\theta_j}|1\rangle)\otimes(\alpha_j|0\rangle + \beta_j e^{i\theta_j}|1\rangle) \\ &+ (\beta_j|0\rangle - \alpha_j e^{-i\theta_j}|1\rangle)\otimes(\beta_j|0\rangle - \alpha_j e^{-i\theta_j}|1\rangle)),\end{aligned}$$

cuja matriz de densidade é

$$\frac{1}{4}\begin{pmatrix} 1 & -2i\alpha_j\beta_j s_j & -2i\alpha_j\beta_j s_j & -4\alpha_j^2\beta_j^2 s_j^2 \\ 2i\alpha_j\beta_j s_j & 1 & 4\alpha_j^2\beta_j^2 s_j^2 & -2i\alpha_j\beta_j s_j \\ 2i\alpha_j\beta_j s_j & 4\alpha_j^2\beta_j^2 s_j^2 & 1 & -2i\alpha_j\beta_j s_j \\ -4\alpha_j^2\beta_j^2 s_j^2 & 2i\alpha_j\beta_j s_j & 2i\alpha_j\beta_j s_j & 1 \end{pmatrix},$$

onde $s_j = \sin\theta_j$.

Portanto temos que a matriz de diferença entre $Tr_{S_1'\otimes S_2'}(\rho)$ e $(\frac{1}{2}I)^{\otimes 2}$ é

$$A = \frac{1}{4}\begin{pmatrix} 0 & -2i\sum_j \mu_j\alpha_j\beta_j s_j & -2i\sum_j \mu_j\alpha_j\beta_j s_j & -4\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 \\ 2i\sum_j \mu_j\alpha_j\beta_j s_j & 0 & 4\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 & -2i\sum_j \mu_j\alpha_j\beta_j s_j \\ 2i\sum_j \mu_j\alpha_j\beta_j s_j & 4\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 & 0 & -2i\sum_j \mu_j\alpha_j\beta_j s_j \\ -4\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 & 2i\sum_j \mu_j\alpha_j\beta_j s_j & 2i\sum_j \mu_j\alpha_j\beta_j s_j & 0 \end{pmatrix}.$$

Podemos calcular os autovalores de A a partir de seu polinômio característico: $-\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2$ (com multiplicidade 2) e $\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 \pm |\sum_j \mu_j\alpha_j\beta_j s_j|$.

Temos que

$$\begin{aligned}
&D\left(Tr_{S_1'\otimes S_2'}(\rho), \left(\frac{1}{2}I\right)^{\otimes 2}\right) \\
&= \frac{1}{2}Tr(\sqrt{A^\dagger A}) \\
&= \frac{1}{2}\Bigg(2\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 + \left(\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 + \left|\sum_j \mu_j\alpha_j\beta_j s_j\right|\right) \\
&\qquad + \left(\left|\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 - \left|\sum_j \mu_j\alpha_j\beta_j s_j\right|\right|\right)\Bigg) \\
&= \sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2 + \max\left\{\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2, \sum_j \mu_j\alpha_j\beta_j s_j\right\} \\
&\leq 2\sum_j \mu_j\alpha_j^2\beta_j^2 s_j^2.
\end{aligned}$$

□

Finalmente iremos limitar a distância do estado quântico para algum estado de Choi-Jamiołkowski associado a algum operador W_q.

Lema 5.3.18. *Seja* $\rho = \sum_j \mu_j(|\xi_j\rangle\langle\xi_j|)^{\otimes 2}$, *para* $|\xi_j\rangle = \alpha_j|\Phi^-\rangle + \beta_j e^{i\theta_j}|\Psi^+\rangle$ *com* $\alpha_j, \beta_j \in \mathbb{R}$, $\alpha_j^2 + \beta_j^2 = 1$ *e* $\theta_j \in [0, 2\pi)$ *e tal que* $D\left(Tr_{S_1'\otimes S_2'}(\rho), \left(\frac{1}{2}I\right)^{\otimes 2}\right) \leq \epsilon$. *Então existe um estado* $\sigma = \sum_j \mu_j'(|J(W_{q_j})\rangle\langle J(W_{q_j})|)^{\otimes 2}$ *para algum* $q_j \in [0,1]$, *e tal que* $D(\sigma,\rho) \leq (32\epsilon)^{\frac{1}{3}}$.

Demonstração. Para todo $|\xi_j\rangle$, sejam

$$|\eta_j\rangle = \alpha_j|\Phi^-\rangle + \beta_j|\Psi^+\rangle = |J(W_{\sqrt{\beta_j}})\rangle,$$

e

$$\sigma = \sum_j \mu_j|\eta_j\rangle\langle\eta_j|^{\otimes 2}.$$

Iremos provar agora que $D(\sigma,\rho) \leq (32\epsilon)^{\frac{1}{3}}$. Temos que

$$D(\sigma,\rho) \leq \sum_j \mu_j D(|\xi_j\rangle\langle\xi_j|^{\otimes 2}, |\eta_j\rangle\langle\eta_j|^{\otimes 2}) = \sum_j \mu_j\sqrt{1-(|\langle\xi_j||\eta_j\rangle|^2)^2}.$$

Como

$$(||\langle\xi_j||\eta_j\rangle|^2)^2 = (\alpha_j^2+\beta_j^2 e^{i\theta_j})^2 = ((\alpha_j^2+\beta_j^2\cos\theta_j)^2+(\beta_j^2\sin\theta_j)^2)^2 = (1-2\alpha_j^2\beta_j^2\sin^2\theta_j)^2,$$

temos que

$$\sqrt{1-(|\langle\xi_j||\eta_j\rangle|^2)^2} = 2|\alpha_j\beta_j\sin\theta_j|\sqrt{1-2\alpha_j^2\beta_j^2\sin^2\theta_j} \leq 2|\alpha_j\beta_j\sin\theta_j|,$$

resultando em

$$D(\sigma,\rho) \leq 2\sum_j \mu_j|\alpha_j\beta_j\sin\theta_j|. \tag{5.1}$$

Pelo Lema 5.3.17, temos que $\sum_j \mu_j\alpha_j^2\beta_j^2\sin^2\theta_j < \frac{\epsilon}{2}$, e isso implica, pelo Lema 5.3.16, que

$$\sum_j \mu_j|\alpha_j\beta_j\sin\theta_j| < 2\left(\frac{\epsilon}{2}\right)^{\frac{1}{3}}. \tag{5.2}$$

Juntando as Equações 5.1 e 5.2, temos que

$$D(\sigma,\rho) \leq 4\left(\frac{\epsilon}{2}\right)^{\frac{1}{3}} = (32\epsilon)^{\frac{1}{3}}.$$

□

5.3.4 QMA $\subseteq$ QMA$_1^{\mathbf{k\cdot EPR}}$

Nesta seção, apresentaremos como estender um protocolo QMA, assumindo pares EPR compartilhados previamente pelos Provador e Verificador, de modo a atingir completude perfeita. A ideia geral do protocolo é utilizar os passos expostos nos lemas anteriores para garantir que temos dois estados de Choi-Jamiołkowski iguais para algum W_q. Informalmente, a ideia geral dos passos segue o seguinte roteiro:

1. Realizar a permutação para garantir que o estado reduzido dos dois primeiros registradores está próximo de algum estado $\sum_j \mu_j\xi_j^{\otimes 2}$;

2. Projetar sobre o espaço gerado por $|\Phi^-\rangle$ e $|\Psi^+\rangle$, pois os estados $|J(W_q)\rangle$ são uma combinação destes estados;

3. Realizar o *Swap test* para garantir que o estado reduzido está próximo de algum estado na forma $\sum_j \mu_j|\psi\rangle\langle\psi|^{\otimes 2}$ e, utilizando o resultado do item 2, temos que $|\psi\rangle$ está no subespaço gerado por $|\Phi^-\rangle$ e $|\Psi^+\rangle$;

1 Verificador e Provador compartilham N pares EPR. Sejam $S_1, ..., S_N$ os qubits do Verificador e $S'_1, ..., S'_N$ os qubits do Provador ;
2 **Provador:**
3 Aplique W_q em $S'_1, ..., S'_N$, onde p_x é a probabilidade máxima de aceitação no protocolo original, $p = \frac{p_x^2}{2p_x^2 - 2p_x + 1}$ e $pq = \frac{1}{2}$;
4 Envie para o Verificador o certificado original ótimo ψ do protocolo QMA e $S'_1, ..., S'_N$;
5 **Verificador:**
6 Prepare três qubits B, R_1, R_2 no estado $|0\rangle$, além do registrador auxiliar A do protocolo original;
7 Execute o Procedimento de destilação em $(R_i, A, M), i \in \{1, 2\}$ e se algum dos procedimentos falhar, aceite a entrada ;
8 Simule uma permutação aleatória entre os registradores (S_i, S'_i) e aceite se a simulação falhar ;
9 Verifique se (S_1, S'_1) e (S_2, S'_2) estão no subespaço gerado por $\{|\Phi^-\rangle$ e $|\Psi^+\rangle\}$ e rejeite se não estiverem ;
10 Realize o *Swap test* entre (S_1, S'_1) e (S_2, S'_2) e rejeite se o teste falhar ;
11 Simule o Procedimento de Reflexão com $(R_1, R_2, S_1, S'_1, S_2, S'_2)$, aceitando se a simulação falhar;
12 Aceite ou rejeite conforme o resultado da Simulação do Procedimento de Reflexão ;

Figura 5.7: Protocolo $\mathrm{QMA}^{\mathrm{k\cdot EPR}}{}_1$ para uma linguagem em QMA

4. Utilizando o fato de que metade dos possíveis estados de Choi-Jamiołkowski eram pares EPR, prova-se então que os estados $|\psi\rangle$ estão próximos de algum estado de Choi-Jamiołkowski.

Pode-se, então utilizar o Procedimento de Reflexão, que tem garantia de aceitar com probabilidade 1 instâncias positivas e rejeitar com probabilidade constante instâncias negativas.

Teorema 5.3.19. *Seja V o Verificador de um protocolo* QMA *que reconhece a linguagem L. O protocolo* $\mathrm{QMA}^{k\cdot EPR}$ *descrito na Figura 5.7 reconhece L com completude perfeita e robustez constante.*

Demonstração. Como descrito na Figura 5.7, para completude o certificado recebido pelo Verificador consiste no autovetor do protocolo original que resulta em máxima

probabilidade de aceitação p_x e N cópias da metade do par EPR que estava com o Provador, e sobre os quais foram aplicadas o operador W_q, onde $p = \frac{p_x^2}{2p_x^2-2p_x+1}$ e $pq = \frac{1}{2}$.

No passo 7, ou o Procedimento de Destilação falha, causando a aceitação, ou o algoritmo Verificador irá continuar e os valores de R_1 e R_2 serão $|\chi_p\rangle$.

Se o passo 8 não aceitar, continuando o algoritmo, não haverá nenhuma alteração no estado do sistema, dado que os registradores (S_i, S_i') contém N cópias idênticas e não-emaranhadas de $|J(W_q)\rangle$. Como estados de Choi-Jamiołkowski associados a W_q, por definição, estão no supespaço gerado por $|\Phi^-\rangle$ e $|\Psi^+\rangle$, concluímos que o passo 9 não rejeitará a entrada.

Novamente pelo fato de (S_1, S_1') e (S_2, S_2') possuírem duas cópias idênticas e não emaranhadas de $|J(W_q)\rangle$, o passo 10 também não rejeitará a entrada.

Finalmente, pelo Lema 5.3.10, a Simulação do Procedimento de reflexão irá aceitar com probabilidade $\frac{3}{4}$ dado à falha de simulação, caso contrário o procedimento de Reflexão irá aceitar a entrada com probabilidade 1.

Para instâncias negativas, temos que a probabilidade de aceitação p_x do protocolo original é no máximo $2^{-poly(|x|)}$. Pelo Lema 5.3.9, o procedimento de destilação do passo 7 irá falhar com probabilidade exponencialmente pequena, causando a aceitação da entrada. Se o procedimento não falhar, o estado dos registradores (R_1, R_2) terá distância de traço exponencialmente pequena ϵ_1 em relação a $|0\rangle^{\otimes 2}$, sendo que cada qubit R_1 e R_2 não estará emaranhado com nenhum outro sistema.

Seja ρ_0 o estado dos registradores $((S_1, S_1'), ..., (S_N, S_N'))$ antes do passo 8. Pelo Lema 5.3.13, a simulação de permutação no passo 8 em ρ_0 falhará com probabilidade $\frac{1}{N}$, causando aceitação. Com probabilidade $1 - \frac{1}{N}$, a simulação é bem-sucedida, e (S_1, S_1', S_2, S_2') estará a uma distância de traço de no máximo $\frac{2^6}{N}$ de um estado quântico na forma

$$\rho_1 = \sum_j \mu_j \xi_j^{\otimes 2},$$

para algum conjunto de $\xi_j \in D(\mathcal{S}_1 \otimes \mathcal{S}_1' \otimes \mathcal{S}_2 \otimes \mathcal{S}_2')$. Como originalmente tínhamos que $Tr_{\otimes_{i=1}^N \mathcal{S}_j'}(\rho_0) = (\frac{1}{2}I)^{\otimes N}$, temos agora que $D(Tr_{\mathcal{S}_1' \otimes \mathcal{S}_2'}(\rho_1), (\frac{1}{2}I)^{\otimes 2}) \leq \frac{2^6}{N}$.

Portanto, a probabilidade de entrar no passo 9 é exponencialmente perto de $1 - \frac{1}{N}$. Neste caso, para algum valor fixo $\epsilon_2 \in (0, 1)$, o Lema 5.3.14 diz que o passo 9 rejeitará

com probabilidade pelo menos

$$\epsilon_2 - \frac{2^6}{N}, \tag{5.3}$$

ou o estado dos pares de *qubits* (S_1, S_1', S_2, S_2') estará a uma distância de traço no máximo $\frac{2^6}{N} + \sqrt{\epsilon_2}$ de um estado

$$\rho_2 = \sum_j \mu_j \xi_j'^{\otimes 2},$$

onde $\xi' \in \mathbf{D}(\mathcal{W})$ e $\mathcal{W}$ é o espaço gerado pelos vetores $|\Phi^-\rangle$ e $|\Psi^+\rangle$. Temos que, neste caso, $D(Tr_{\mathcal{S}_1' \otimes \mathcal{S}_2'}(\rho_2), (\frac{1}{2}I)^{\otimes 2}) \leq \frac{2^6}{N} + \sqrt{\epsilon_2}$.

Dados $\epsilon_3, \epsilon_4 \in (0,1)$ fixos, o Lema 5.3.15 diz que o passo 10 irá rejeitar com probabilidade pelo menos

$$\frac{1}{2}\epsilon_3\epsilon_4 - \frac{2^6}{N} - \sqrt{\epsilon_2}, \tag{5.4}$$

ou o valor dos pares de *qubits* (S_1, S_1', S_2, S_2') estará a uma distância de traço no máximo $\frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4$ do estado

$$\rho_3 = \sum_j \mu_i (|\psi_j\rangle\langle\psi_j|)^{\otimes 2}$$

onde $|\psi_j\rangle = \alpha_j|\Phi^-\rangle + \beta_j e^{i\theta_j}|\Psi^+\rangle$ e $D(Tr_{\mathcal{S}_1' \otimes \mathcal{S}_2'}(\rho_2), (\frac{1}{2}I)^{\otimes 2}) \leq \frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4$.

Após o passo 10, pelo Lema 5.3.18, o valor dos pares de *qubits* (S_1, S_1', S_2, S_2') estará a uma distância $(32(\frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4))^{\frac{1}{3}}$ de algum estado

$$\rho_4 = \sum_j \mu_i (|J(W_q)\rangle\langle J(W_q)|)^{\otimes 2},$$

para algum valor de $q \in [0,1]$. Portanto, o valor de $(R_1, R_2, S_1, S_1', S_2, S_2')$ estará a uma distância de no máximo $\epsilon_1 + (32(\frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4))^{\frac{1}{3}}$ do estado

$$\sigma = |0\rangle\langle 0|^{\otimes 2} \otimes \rho_4.$$

Se o Procedimento de Reflexão fosse aplicado sobre σ a probabilidade de rejeição seria de $\frac{1}{16}$. Entretanto, como em cada passo consideramos uma distância de traço do estado ideal, e a distância de traço é um limitante superior para a distância estatística, temos que a probabilidade que a cadeia é rejeitada é de

$$\frac{1}{16} - \epsilon_1 - \frac{2^6}{N} - \sqrt{\epsilon_2} - 2\epsilon_3 - \epsilon_4 - \left(32\left(\frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4\right)\right)^{\frac{1}{3}}. \tag{5.5}$$

Tomando $\epsilon_2 = \frac{2^{10}}{N}$, $\epsilon_3 = \epsilon_4 = 2\epsilon_2^{\frac{1}{5}}$, $N = 2^{200}$ e considerando o erro ϵ_1 exponencialmente pequeno, baseados nas equações 5.3, 5.4 e 5.5 temos que se entrar no passo 8, a probabilidade de rejeição é ao menos

$$\min\left\{\begin{array}{l}\dfrac{2^{10}}{2^{200}} - \dfrac{2^6}{2^{200}},\\ \dfrac{2^6}{2^{40}} - \dfrac{2^6}{2^{200}} - \dfrac{2^5}{2^{100}},\\ \dfrac{1}{16} - \epsilon_1 - \dfrac{2^6}{2^{200}} - \dfrac{2^5}{2^{100}} - 3\dfrac{2^2}{2^{40}} - \left(32\left(\dfrac{2^6}{2^{200}} + \dfrac{2^5}{2^{100}} + 3\dfrac{2^2}{2^{40}}\right)\right)^{\frac{1}{3}}\end{array}\right\}$$
$$\geq 2^{-200}.$$

Como o Algoritmo Verificador entra no passo 8 com probabilidade exponencialmente próxima de $1 - \frac{1}{N}$, a probabilidade de rejeição é pelo menos

$$2^{-205}.$$

□

Destacamos que em provas alternativas deste resultado [64] [75] atinge-se probabilidade de rejeição mínima maior. Porém, com nossa análise podemos ainda obter o resultado principal que é a inclusão das classes de complexidade.

Teorema 5.3.20. $\mathrm{QMA} \subseteq \mathrm{QMA}_1^{k\text{-}EPR}$.

Demonstração. Direta do Teorema 5.3.19. □

5.3.5 QMA ⊆ QIP(q-poly, c-one, c-const)

Iremos agora demonstrar um protocolo baseado nas ideias propostas por KLGN[64]. Mas, ao invés do compartilhamento de pares EPR entre o Provador e o Verificador, o novo protocolo usará duas mensagens clássicas extras: o Verificador enviará um bit clássico para o Provador, que enviará de volta uma mensagem clássica de tamanho constante. Este resultado foi obtido no estágio feito pelo candidato em no *Laboratoire d'Informatique Algorithmique: Fondements et Applications, CNRS, Université Paris VII*, sob supervisão de Iordanis Kerenidis e Jamie Sikora.

A ideia geral do protocolo é que o Provador enviará, inicialmente, o certificado original do protocolo QMA e $2N$ metades de pares EPR. Então, o Verificador irá jogar uma moeda e enviará esse resultado para o Provador. Se o resultado foi "cara", o Verificador testará se as supostas metades de pares EPR são de fato metades de pares EPR. Para isso, o Provador irá fazer o teleporte quântico dos pares EPR e o Verificador irá confirmá-los. Se o resultado da moeda for "coroa", o Provador aplicará operações locais, transformando metade dos pares EPR compartilhados em estados de Choi-Jamiołkowski associados à matriz W_q, para o valor de q correto. O Provador irá, então, teleportar os estados de Choi-Jamiołkowski e o Verificador executará o Algoritmo Verificador original de KLGN, descrito na seção anterior.

Para instâncias positivas, não é difícil perceber que se o Provador seguir o protocolo, o Verificador irá aceitar com probabilidade 1.

Para instâncias negativas, a ideia é que o Provador não poderá enviar uma primeira mensagem que passe com alta probabilidade no teste de EPR e no teste de KLGN. Se o estado reduzido enviado pelo Provador estiver próximo do estado completamente misto, o algoritmo verificador de KLGN irá rejeitar com alta probabilidade. Se o estado reduzido dos *qubits* estiver longe do estado totalmente misto, segundo a distância de traço, a verificação dos pares EPR irá rejeitar a entrada com alta probabilidade.

Descrevemos nosso protocolo na Figura 5.8 e iremos agora provar sua completude e robustez.

Lema 5.3.21. *O protocolo descrito na Figura 5.8 apresenta completude perfeita.*

Demonstração. Se o resultado da moeda for "cara", o Provador não aplicará nenhuma operação sobre suas metades dos pares EPR, então o valor de (R_i, S_i, R'_i, S'_i) é

$$\begin{aligned}
&\frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) \\
&= \frac{1}{2\sqrt{2}}|\Phi^+\rangle(|00\rangle + |11\rangle) + \frac{1}{2\sqrt{2}}|\Phi^-\rangle(|00\rangle - |11\rangle) \\
&+ \frac{1}{2\sqrt{2}}|\Psi^+\rangle(|01\rangle + |10\rangle) + \frac{1}{2\sqrt{2}}|\Psi^-\rangle(|01\rangle - |10\rangle).
\end{aligned}$$

É fácil verificar que após a medição do Provador e a operação de correção feita pelo Verificador a partir do resultado da Medição, (S_i, S'_i) estará sempre com o valor $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$. Portanto, o teste na linha 11 irá sempre aceitar.

Provador:
Prepare $2N$ pares EPR (R_i, R'_i) e (S_i, S'_i), $0 \leq i < N$, e envie para o Verificador o certificado ótimo do protocolo original $|\psi\rangle$, e os qubits R'_i e S'_i ;
Verificador:
Jogue uma moeda aleatoriamente e envie o resultado para o Provador ;
Provador:
if *"coroa"* **then** Aplique W_q a R_i. Medir (R_i, S_i) na Base de Bell e envie os resultados v_i, classicamente, para o Verificador ;
Verificador:
Aplique a correção para cada S'_i de acordo com o valor de v_i:
if $|\Phi^+\rangle$*:* **then** Aplique I em S'_i **if** $|\Phi^-\rangle$*:* **then** Aplique Z em S'_i **if** $|\Psi^+\rangle$*:* **then** Aplique X em S'_i **if** $|\Psi^-\rangle$*:* **then** Aplique ZX em S'_i ;
if *"cara"* **then** Teste se todos (R'_i, S'_i) são $|\Psi^+\rangle$ e rejeite se algum deles não for **if** *"coroa"* **then** Execute o procedimento de Verificação proposto por KLGN com $|\psi\rangle$ e (R'_i, S'_i)

Figura 5.8: Protocolo $\mathrm{QIP}_1(q\text{-poly}, c\text{-one}, c\text{-const})$ para QMA

Se o resultado da moeda for "coroa", estão os valores de (R_i, S_i, R'_i, S'_i) após W_q ser aplicado à R'_i é

$$\begin{aligned}
&\frac{\sqrt{1-q}}{2}(|0000\rangle + |0101\rangle - |1010\rangle - |1111\rangle) \\
&+ \frac{\sqrt{q}}{2}(|1000\rangle + |1101\rangle + |0010\rangle + |0111\rangle) \\
&= \frac{1}{2\sqrt{2}}|\Phi^+\rangle(\sqrt{1-q}|00\rangle - \sqrt{1-q}|11\rangle + \sqrt{q}|01\rangle + \sqrt{q}|10\rangle) \\
&+ \frac{1}{2\sqrt{2}}|\Phi^-\rangle(\sqrt{1-q}|00\rangle + \sqrt{1-q}|11\rangle - \sqrt{q}|01\rangle + \sqrt{q}|10\rangle) \\
&+ \frac{1}{2\sqrt{2}}|\Psi^+\rangle(\sqrt{1-q}|01\rangle - \sqrt{1-q}|10\rangle + \sqrt{q}|00\rangle + \sqrt{q}|11\rangle) \\
&+ \frac{1}{2\sqrt{2}}|\Psi^-\rangle(\sqrt{1-q}|01\rangle + \sqrt{1-q}|10\rangle - \sqrt{q}|00\rangle + \sqrt{q}|11\rangle).
\end{aligned}$$

É fácil verificar que após a medição feita pelo Provador e a correção feita pelo Verificador, dado o resultado da medição, os valor de (R'_i, S'_i) será sempre $\sqrt{1-q}|\Phi^-\rangle + \sqrt{q}|\Psi^+\rangle = |J(W_q)\rangle$ e o algoritmo verificador proposto em KLGN irá aceitar com probabilidade 1, como demonstrado no Teorema 5.3.19. □

Agora, iremos mostrar alguns lemas auxiliares para que seja possível provar que se as supostas metades de pares EPR enviadas pelo Provador na primeira mensagem estiverem longe do estado totalmente misto, o teste de EPR irá rejeitar com alta probabilidade.

Lema 5.3.22. *Seja σ_{AB} um estado quântico de 2 qubits. Se $Tr(|\Phi^+\rangle\langle\Phi^+|\sigma_{AB}) > 1-\epsilon$, então $D(Tr_B(\sigma_{AB}), \frac{1}{2}I) < \sqrt{\epsilon}$.*

Demonstração. Seja $|\phi\rangle$ uma purificação de σ_{AB}. Dado que $|\Phi^+\rangle$ é uma purificação de $\frac{1}{2}I$, temos

$$\begin{aligned}
D(Tr_B(\sigma_{AB}), \frac{1}{2}I) &\leq D(\sigma_{AB}, |\Phi^+\rangle\langle\Phi^+|) \\
&\leq D\left(|\phi\rangle, \frac{1}{||(|\Phi^+\rangle\langle\Phi^+|\otimes I)|\phi\rangle||}(|\Phi^+\rangle\langle\Phi^+|\otimes I)|\phi\rangle\right) \\
&= \sqrt{1 - \left|\langle\phi|\frac{1}{||(|\Phi^+\rangle\langle\Phi^+|\otimes I)|\phi\rangle||}(|\Phi^+\rangle\langle\Phi^+|\otimes I)|\phi\rangle\right|^2} \\
&= \sqrt{1 - ||(|\Phi^+\rangle\langle\Phi^+|\otimes I)|\phi\rangle)||^2} \\
&= \sqrt{1 - Tr(|\Phi^+\rangle\langle\Phi^+|\sigma_{AB})} \\
&< \sqrt{\epsilon}.
\end{aligned}$$

□

Corolário 5.3.23. *Se $D(Tr_B(\sigma_{AB}), \frac{1}{2}I) \geq \sqrt{\epsilon}$, então $Tr(|\Phi^+\rangle\langle\Phi^+|\sigma_{AB}) \leq 1-\epsilon$, para um valor de $\epsilon \in (0,1)$ fixo.*

Provaremos agora a robustez do protocolo.

Lema 5.3.24. *Para instâncias negativas, a probabilidade máxima de aceitação é uma constante menor que* 1*.*

Demonstração. As operações feitas pelo Verificador entre os passos 8 e 9 são equivalentes a aplicar a seguinte porta controlada:

$$P_0 \otimes I_{R_i'} \otimes I + P_1 \otimes I_{R_i'} \otimes Z + P_2 \otimes I_{R_i'} \otimes X + P_3 \otimes I_{R_i'} \otimes ZX,$$

para algum conjunto de projetores $\{P_i\}$ atuando sobre o espaço privado do Provador.

Dado que nenhuma operação atua sobre R'_i, seu estado reduzido se mantém o mesmo desde o início do protocolo, na primeira mensagem. Iremos, então, provar que o teste de EPR irá rejeitar com probabilidade $\frac{\gamma}{2}$, para um valor $\gamma \in (0,1)$ fixo, ou todos os S_i estão $\sqrt{\gamma}$-próximos na distância de traço do estado $\frac{1}{2}I$ e, neste caso, o algoritmo de verificação de KLGN irá rejeitar a entrada com uma probabilidade constante.

Seja σ_i^{RS} o estado reduzido de (R'_i, S'_i) após a linha 9 e $\sigma_i^R = Tr_S(\sigma_i^{RS})$. Se $D(\sigma_i^R, \frac{1}{2}I) > \sqrt{\gamma}$ para algum i, pelo Corolário 5.3.23, temos que $Tr(|\Phi^+\rangle\langle\Phi^+|\sigma_i^{RS}) \leq 1-\gamma$. Portanto se aplicarmos o teste EPR, ele irá falhar com probabilidade pelo menos γ. Dado que o teste EPR é aplicado com probabilidade $\frac{1}{2}$, o protocolo rejeita neste caso com probabilidade pelo menos $\frac{\gamma}{2}$.

Se $D(\sigma_i^R, \frac{1}{2}I) \leq \sqrt{\gamma}$ para todos os i, então podemos utilizar o resultado do algoritmo verificador de KLGN, propagando a distância de traço entre R'_i e $\frac{1}{2}I$ na Demonstração do Teorema 5.3.19. Neste caso, a probabilidade de rejeição estará exponencialmente próxima de

$$\left(1-\frac{1}{N}\right)\min\left\{\epsilon_2 - \frac{2^6}{N}, \right.$$
$$\frac{1}{2}\epsilon_3\epsilon_4 - \frac{2^6}{N} - \sqrt{\epsilon_2},$$
$$\left.\frac{1}{16} - \epsilon_1 - \frac{2^6}{N} - \sqrt{\epsilon_2} - 2\epsilon_3 - \epsilon_4 - \left(32\left(\sqrt{\gamma} + \frac{2^6}{N} + \sqrt{\epsilon_2} + 2\epsilon_3 + \epsilon_4\right)\right)^{\frac{1}{3}}\right\},$$

para valores de $\epsilon_2, \epsilon_3, \epsilon_4, \gamma \in (0,1)$ fixos e ϵ_1 exponencialmente pequeno.

Escolhendo os valores adequados para as constantes, temos que a probabilidade de rejeição é pelo menos 2^{-206}. □

Portanto, vimos agora que é possível atingir completude perfeita adicionando uma rodada de comunicação clássica constante.

5.4 Conclusões

Neste capítulo, estudamos a questão QMA vs. QMA_1 apresentando dois resultados parciais.

O primeiro resultado mostra uma separação relativizada dessas classes. Se por um lado, isso pode não significar nada dado que classes que são iguais em um contexto não relativizado, não necessariamente são iguais relativas a um oráculo. Em especial, o resultado que mostramos utiliza um oráculo quântico e ainda não se sabe se com restrição a oráculos clássicos, se a desigualdade permanece. Esta pergunta é uma direção natural para novas tentativas de solucionar este problema. O que se obtém, entretanto, com este resultado parcial é que sabe-se que, para provar $\mathrm{QMA} = \mathrm{QMA}_1$, esta prova não pode se relativizar, ou seja, a prova deve ser invalidada em algum ponto ao colocarmos oráculos dentro de seu contexto.

O segundo resultado, apresenta um fato que, ao considerarmos recursos adicionais, como um número constante de pares EPR antes da execução do protocolo ou uma rodada de comunicação clássica constante, obtemos completude perfeita. O resultado que apresentamos é teórico, dado que a constante apresentada é de muito alta o que torna o método ainda inviável na prática. Porém, para efeitos de notação assintótica, temos a inclusão das classes de complexidade.

Capítulo 6

Conclusões

Vimos, neste trabalho, uma pequena lista de elementos da Computação Quântica que influenciam, de algum modo, tópicos em Teoria da Computação. Hoje, esta lista contém outros resultados muito importantes, inclusive que provam conjecturas abertas há décadas, porém que infelizmente não tiveram espaço dentro deste trabalho.

Os primeiros resultados importantes da Computação Quântica, os Algoritmos Quânticos que resolvem de maneira mais eficiente alguns problemas do que Algoritmos Clássicos conhecidos até hoje, foram apresentados no Capítulo 3. Em especial, apresentamos o Algoritmo de Shor, que fatora números em tempo polinomial, enquanto qualquer Algoritmo Clássico conhecido até hoje para o problema necessita tempo exponencial.

Foi visto, no Capítulo 4, um modelo de Autômato Finito que utiliza estados quânticos e clássicos para computar. Vimos que este modelo é mais poderoso que Autômatos Finitos Determinísticos, dado que reconhece inclusive algumas linguagens não livres de contexto. Porém, o poder exato deste modelo não está bem definido e apresentamos um resultado parcial neste sentido. Ressaltamos que este capítulo resulta de uma unificação da literatura e contém alguns resultados novos obtidos durante o mestrado [48][49][50].

Finalmente, vimos, no Capítulo 5, resultados parciais acerca de uma questão em aberto há algum tempo em Complexidade Computacional Quântica envolvendo a probabilidade de aceitação de instâncias positivas em protocolos QMA, o análogo quântico da classe NP. Foi mostrado, inicialmente, a separação relativizada das classes QMA, cuja probabilidade de aceitação de instâncias positivas é convencionada $\frac{2}{3}$, e QMA_1, cuja probabilidade de aceitação para instâncias positivas deve ser 1, o

que limita as possibilidades para provar que as duas classes são iguais. Em seguida, foi mostrado que com o recurso adicional de pares EPR compartilhados ou uma rodada de comunicação clássica constante, conseguimos decidir todos os problemas em QMA com probabilidade 1, neste novo modelo. Enfatizamos que o resultado envolvendo uma rodada adicional de comunicação clássica foi obtido pelo candidato durante seu mestrado.

Referências Bibliográficas

[1] Scott Aaronson. On perfect completeness for QMA. *Quantum Information & Computation*, 9(1):81–89, 2009.

[2] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter W. Shor. The Power of Unentanglement. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(051), 2008.

[3] Leonard M. Adleman, Jonathan Demarrais, and Ming deh A. Huang. Quantum computability. *SIAM Journal of Computation*, pages 1524–1540, 1997.

[4] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Ann. of Math*, 2:781–793, 2002.

[5] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013.

[6] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey. 2002.

[7] Dmitri Alekseevsky, Andreas Kriegl, Mark Losik, and Peter W. Michor. Choosing roots of polynomials smoothly. *Israel J. Math*, 105:203–233, 1998.

[8] Noga Alon and Joel Spencer. *The Probabilistic Method*. John Wiley, 1992.

[9] M. Amano and K. Iwama. Undecidability on quantum finite automata. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, STOC '99, pages 368–375, New York, NY, USA, 1999. ACM.

[10] A. Ambainis and R. Spalek. Quantum algorithms for matching and network flow. In *Proceedings of the 23rd International Symposium on Theoretical Aspects of Computer Science*, pages 172–183. Springer LNCS, 2006.

[11] A. Ambainis and J. Watrous. Two-way finite automata with quantum and classical states. *Theor. Comput. Sci.*, 287(1):299–311, September 2002.

[12] Andris Ambainis. Quantum lower bounds by quantum arguments. In *Proceedings of the ACM Symposium on Theory of Computing*, pages 636–643, 2000.

[13] Andris Ambainis. Quantum walks and their algorithmic applications. *International Journal of Quantum Information*, 1:507, 2003.

[14] Andris Ambainis and Robert Špalek. Quantum algorithms for matching and network flows. In *Proceedings of the 23rd Annual conference on Theoretical Aspects of Computer Science*, STACS'06, pages 172–183, Berlin, Heidelberg, 2006. Springer-Verlag.

[15] Howard Anton and Chris Rorres. *Álgebra Linear com Aplicações*. Bookman, 2001.

[16] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[17] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, May 1998.

[18] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of np. *J. ACM*, 45(1):70–122, January 1998.

[19] László Babai and Shlomo Moran. Arthur-merlin games: A randomized proof system, and a hierarchy of complexity class. *J. Comput. Syst. Sci.*, 36(2):254–276, April 1988.

[20] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001.

[21] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, July 2001.

[22] Salman Beigi. NP VS QMAlog(2). *Quantum Info. Comput.*, 10(1):141–151, January 2010.

[23] Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM J. Comput.*, 18(4):766–776, August 1989.

[24] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, October 1997.

[25] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM J. Comput.*, pages 1411–1473, 1997.

[26] Hugue Blier and Alain Tapp. All languages in NP have very short Quantum proofs. In *Proceedings of the 2009 Third International Conference on Quantum, Nano and Micro Technologies*, ICQNM '09, pages 34–37, Washington, DC, USA, 2009. IEEE Computer Society.

[27] V. D. Blondel, E. Jeandel, P. Koiran, and N. Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 34:14641473, 2005.

[28] C. H. Cardonha. Sistemas interativos de prova clássicos e quânticos. Master's thesis, Universidade de São Paulo, 2006.

[29] C. H. Cardonha, Silva M. K. de C., and C. G. Fernandes. Computação quântica: Complexidade e algoritmos. Technical report, Universidade de São Paulo, 2004.

[30] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285 – 290, 1975.

[31] Clay Mathematics Institue. P vs NP problem. `http://www.claymath.org/millenium-problems/p-vs-np-problem`.

[32] Clay Mathematics Institue. The Millennium Prize Problems. `http://www.claymath.org/millennium-problems/millennium-prize-problems`.

[33] Ronald de Wolf. Quantum communication and complexity. *Theor. Comput. Sci.*, 287(1):337–353, 2002.

[34] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97–117, 1985.

[35] David Deutsch. Quantum computational networks. *Royal Society of London Proceedings Series A*, 425:73–90, 1989.

[36] David Deutsch and Richard Jozsa. Rapid solutions of problems by quantum computation. In *Proceedings of the Royal Society of London A*, volume 439, pages 553–558, 1992.

[37] Irit Dinur. The pcp theorem by gap amplification. *J. ACM*, 54(3), June 2007.

[38] Andrew Drucker and Ronald de Wolf. *Quantum Proofs for Classical Theorems*. Number 2 in Graduate Surveys. Theory of Computing Library, 2011.

[39] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. *CoRR*, quant-ph/9607014, 1996.

[40] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[41] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. Wiley, January 1968.

[42] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.

[43] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds. In *STOC*, pages 95–106, 2012.

[44] Edward Fredkin and Tommaso Toffoli. Conservative logic. *International Journal of Theoretical Physics*, 21:219–253, 1982.

[45] François Le Gall, Shota Nakagawa, and Harumichi Nishimura. On QMA protocols with two short quantum proofs. *Quantum Info. Comput.*, 12(7-8):589–600, July 2012.

[46] Oded Goldreich, Rehovot Israel, and David Zuckerman. Another proof that BPP $\subseteq$ PH (and more). Technical report, Electronic Colloquium on Computational Complexity, 1997.

[47] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 291–304, New York, NY, USA, 1985. ACM.

[48] A. B. Grilo and A. V. Moura. Language classes and quantum finite automata. In *Proceedings of the the IV Workshop-School in Quantum Computation and Information*, WECIC '12, pages 90 – 95, 2012.

[49] A. B. Grilo and A. V. Moura. On finite automata with quantum and classical states. In *Abstracts of Reports and Other Materials of the 6th School "Computer Science Days in Ekaterinburg"*, CSEDays 2013, pages 32 – 35, 2013.

[50] A. B. Grilo and A. V. Moura. On finite automata with quantum and classical states. *Siberian Electronic Mathematical Reports*, 10:676–688, 2013.

[51] Lov Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[52] Aram Wettroth Harrow and Ashley Montanaro. Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization. *J. ACM*, 60(1):3, 2013.

[53] M. Hirvensalo. *Quantum computing*. Natural computing series. Springer, 2004.

[54] L. C. L. Hollenberg. Fast quantum search algorithms in protein sequence comparison - quantum biocomputing. Technical Report quant-ph/0002076, Feb 2000.

[55] J.E. Hopcroft and J.D. Ullman. *Introduction to automata theory, languages, and computation*. Addison-Wesley series in computer science. Addison-Wesley, 1979.

[56] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *J. ACM*, 58(6):30:1–30:27, December 2011.

[57] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275 – 278, 1972.

[58] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Info. Comput.*, 12(5-6):461–471, May 2012.

[59] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford University Press, 2007.

[60] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. In *Proceedings of 23rd IEEE Conference on Computational Complexity (CCC)*, pages 211–222, 2008.

[61] Iordanis Kerenidis. Quantum multiparty communication complexity and circuit lower bounds. *Mathematical Structures in Computer Science*, 19(1):119–132, 2009.

[62] Iordanis Kerenidis and Ronald De Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. In *Journal of Computer and System Sciences*, pages 106–115, 2003.

[63] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *In Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[64] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In Robert D. Kleinberg, editor, *ITCS*, pages 329–352. ACM, 2013.

[65] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? In Toshihide Ibaraki, Naoki Katoh, and Hirotaka Ono, editors, *Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer Berlin Heidelberg, 2003.

[66] A. Kondacs and J. Watrous. On the power of quantum finite state automata. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 66–, Washington, DC, USA, 1997. IEEE Computer Society.

[67] Ming Li, John Tromp, and Paul Vitanyi. Reversible simulation of irreversible computation. In *Physica D*, pages 301–306, 1996.

[68] Ludwig Mach. Über einen Interferenzrefraktor. *Zeitschrift für Instrumentenkunde*, 12, 1892.

[69] M. Macko. On closure properties of quantum finite automata. Master's thesis, Comenius University, 2006.

[70] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14, 2005.

[71] N.D. Mermin. *Quantum computer science: an introduction*. Cambridge University Press, 2007.

[72] Gary L. Miller. Riemann's hypothesis and tests for primality. In William C. Rounds, Nancy Martin, Jack W. Carlyle, and Michael A. Harrison, editors, *STOC*, pages 234–239. ACM, 1975.

[73] Cristopher Moore and James P. Crutchfield. Quantum automata and quantum grammars. *Theor. Comput. Sci.*, 237:275–306, April 2000.

[74] M.A. Nielsen and I.L. Chuang. *Quantum computation and quantum information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[75] Attila Pereszlényi. One-Sided Error QMA with Shared EPR Pairs - A Simpler Proof. *CoRR*, abs/1306.5406, 2013.

[76] R. Portugal, C.C. Lavor, L.M. Carvalho, and N. Maculan. *Uma introdução à computação quântica*. SBMAC, 2004.

[77] D. Qiu. Some observations on two-way finite automata with quantum and classical states. In *Proceedings of the 4th international conference on Intelligent Computing: Advanced Intelligent Computing Theories and Applications - with Aspects of Theoretical and Methodological Issues*, ICIC '08, pages 1–8, Berlin, Heidelberg, 2008. Springer-Verlag.

[78] Michael O Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128 – 138, 1980.

[79] S.C. Reghizzi. *Formal Languages and Compilation*. Texts in Computer Science. Springer, 2009.

[80] D. Qiu S. Zheng and L. Li. Some languages recognized by two-way finite automata with quantum and classical states. 2011.

[81] D. Qiu S. Zheng and L. Li. State succinctness of two-way finite automata with quantum and classical states. *CoRR*, abs/1202.2651, 2012.

[82] Peter Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 35:124–134, 1994.

[83] M. Sipser. *Introduction to the theory of computation*. Computer Science Series. Thomson Course Technology, 2006.

[84] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.

[85] A. L Vignatti, F.S. Netto, and L. F Bittencourt. Uma introdução à computação quântica. Technical report, Universidade Federal do Paraná, 2004.

[86] N. S. Volpato Filho and A. V. Moura. An $\mathcal{O}(n^{3/4}log^2n)$ quantum algorithm for the 1-dimensional closest pair problem. In *Workshop-Escola de Computação e Informação Quântica*, 2006.

[87] N. S. Volpato Filho and A. V. Moura. A quantum algorithm for finding the minimum pair. In *Workshop-Escola de Computação e Informação Quântica*, 2007.

[88] John Watrous. PSPACE has constant-round quantum interactive proof systems. In *Theoretical Computer Science*, pages 112–119. IEEE, 1999.

[89] John Watrous. Limits on the Power of Quantum Statistical Zero-Knowledge. In *FOCS*, pages 459–. IEEE Computer Society, 2002.

[90] John Watrous. Quantum computational complexity. In *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. 2009.

[91] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

[92] Abuzer Yakaryilmaz and A. C. Cem Say. Languages recognized by nondeterministic quantum finite automata. *Quantum Info. Comput.*, 10(9):747–770, September 2010.

[93] N.S. Yanofsky and M.A. Mannucci. *Quantum computing for computer scientists*. Cambridge University Press, 2008.

[94] Andrew Chi-Chih Yao. Quantum circuit complexity. In *34th Annual Symposium on Foundations of Computer Science, 3-5 November 1993, Palo Alto, California, USA*, pages 352–361. IEEE, 1993.

[95] Andrew Chi-Chih Yao. Quantum circuit complexity. In *FOCS*, pages 352–361. IEEE Computer Society, 1993.

[96] Stathis Zachos and Martin Furer. Probabilistic quantifiers vs. distrustful adversaries. In *Proc. Of the Seventh Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 443–455, London, UK, UK, 1987. Springer-Verlag.

[97] Ludwig Zehnder. Ein neuer Interferenzrefraktor. *Zeitschrift für Instrumentenkunde*, 11, 1891.

Apêndice A

Teoria dos Números

Iremos neste capítulo definir e enunciar Teoremas relativos a Teoria dos Números que são utilizados na prova de corretude do Algoritmo de Shor na Seção 3.2.3 e de um lema auxiliar no Apêndice B. Ressaltamos que as provas dos teoremas estão fora do escopo deste trabalho e podem ser facilmente encontrados em livros da área ou nos Apêndices dos livros sobre Computação Quântica como os de Nielsen e Chuang [74] ou Hirvensalo [53].

Assumimos familiaridade com conhecimentos básicos com Teoria de Grupos, mínimo múltiplo comum, máximo divisor comum, números primos e aritmética modular.

Iremos agora definir o conjunto de inteiros módulo n.

Definição A.1. $\mathbb{Z}_n = \{0, ..., n-1\}$.

Estaremos especialmente interessados no subconjunto de elementos de $\mathbb{Z}_n$ que são coprimos de n dado que este conjunto forma um grupo multiplicativo.

Definição A.2. $\mathbb{Z}_n^* = \{j \in \mathbb{Z}_n \mid mdc(n, j) = 1\}$

A cardinalidade de $\mathbb{Z}_n^*$ também é um elemento fundamental em várias provas em Teoria dos Números.

Definição A.3. *A função de Euler $\phi(n)$ representa o número de elementos em $\mathbb{Z}_n^*$, ou seja os número de elementos $0 \leq k < n$ tal que $mdc(k, n) = 1$.*

Enunciaremos agora um teorema que prova que todo $\mathbb{Z}_{p^c}^*$, para p primo ímpar e $c \in \mathbb{N}^*$, pode ser gerado por um elemento $g \in \mathbb{Z}_p^*$.

Teorema A.4. *Se p é um primo ímpar e c é um número natural positivo, $\mathbb{Z}^*_{p^c}$ é cíclico, ou seja, existe um valor $g \in \mathbb{Z}^*_{p^c}$ tal que $\{g^0 \mod p^c, g^1 \mod p^c, g^2 \mod p^c, ...\} = \mathbb{Z}^*_{p^c}$.*

Veremos agora a definição de um elemento fundamental para o Algoritmo de Shor, que é a ordem de um inteiro a em $\mathbb{Z}_n$. Este conceito será muito importante pois é o período da função $f_{a,n}(x) = a^x \mod n$, e encontrar este valor de forma eficiente é o ponto crucial da vantagem do modelo quântico sobre o modelo clássico.

Definição A.5. *A ordem r de a em $\mathbb{Z}_n$, denotada por $ord_n(a)$, é definida como o menor inteiro positivo r para o qual $a^r \equiv 1 \mod n$.*

Pode-se provar que para todo a, $ord_n(a)$ é um divisor de $\phi(n)$.

Teorema A.6. *Seja $r = ord_n(a)$ para um $a \in \mathbb{Z}^*_n$. Temos então que r divide $\phi(n)$.*

Finalmente enunciaremos o Famoso Teorema Chinês do Resto.

Teorema A.7 (Teorema Chinês do Resto)**.** *Seja $n = n_1 n_2 ... n_k$, com $mdc(n_i, n_j) = 1$ para $i \neq j$. Dados $k_i \in \mathbb{Z}_{n_i}$, para $1 \leq i \leq k$, existe um único $k \in \mathbb{Z}_n$ tal que $k \equiv k_i \mod n_i$*

Por fim, iremos enunciar um teorema que conecta o Teorema Chinês do Resto e o conceito de ordem.

Teorema A.8. *Sejam $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_n}$ a fatoração de n, um valor $a \in \mathbb{Z}^*_n$, $a_1, a_2, ..., a_n$ a decomposição de a através do Teorema Chinês do Resto e $r_i = ord_{p_i^{e_i}}(a_i)$. Então $ord_n(a) = mmc(r_1, ..., r_n)$.*

Apêndice B

Prova do Lema 3.2.4

Antes de provar o Lema 3.2.4 que fornece um limitante inferior para a probabilidade da ordem encontrada satisfazer as propriedades desejadas, vamos provar alguns lemas auxiliares. Os lemas apresentados aqui foram extraídos livro de Hirvensalo [53].

Como na Seção 3.2.3, assumiremos que o número que desejamos fatorar é um número composto, ímpar e que não é uma potência de um número primo. Também utilizaremos a notação de que n é o número que desejamos fatorar, $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, tal que $k \geq 2$, p_i são números primos distintos e $e_i \geq 1$ para $1 \leq i \leq k$. Denotaremos também $n_i = p_i^{e_i}$.

Lema B.1. *Dado um valor de $a \in Z_{p^e}^*$, escolhido aleatoriamente de maneira uniforme, a probabilidade de que $ord_{p^e}(a) = 2^s t$, com um $s \leq 0$ fixo e t ímpar, é no máximo $\frac{1}{2}$.*

Demonstração. Seja $\phi(p^e) = 2^u v$, onde p é um número primo, $u, v \geq 1$ e v ímpar. Se $s > u$ a probabilidade da ordem ser o valor $2^s t$ é 0 dado que a ordem é um divisor de $\phi(p^e)$ pelo Teorema A.6.

Temos então o caso de $s \leq u$. Como p^e é uma potência de um número primo, temos pelo Teorema A.4 que $Z_{p^e}^*$ é cíclico. Seja g um gerador de $Z_{p^e}^* = \{g^0, g^1, ..., g^{2^u(v-1)}\}$ e $ord_{p^e}(g^j) = \frac{2^u v}{mdc(j, 2^u v)}$. Portanto a ordem tem formato $2^s t$ se e somente se $j = 2^{u-s} w$, com w ímpar.

O conjunto $\{0, ..., 2^u(v-1)\}$ possui $2^s v$ múltiplos de 2^{u-s}:

$$0 \cdot 2^{u-s}, 1 \cdot 2^{u-s}, ... \text{ e } (2^s v - 1)s^{u-s}.$$

Entretanto, somente metade destes valores possuem multiplicador ímpar. Portanto a probabilidade de encontrar algum desses valores é $\frac{\frac{1}{2}2^s v}{2^u v} = \frac{1}{2}\frac{2^s}{2^u} \leq \frac{1}{2}$. □

Lema B.2. *A probabilidade de $r = ord_n(a)$ ser ímpar, para um a escolhido aleatoriamente de maneira uniforme dentre os elementos de $\mathbb{Z}_n^*$, é no máximo $\frac{1}{2^k}$.*

Demonstração. Pelo Teorema A.7, temos que a escolha de um valor aleatório de a do conjunto $\mathbb{Z}_n^*$ é equivalente a escolher aleatoriamente elementos a_i dos conjuntos $\mathbb{Z}_{n_i}$, $1 \leq i \leq k$.

Pelo Teorema A.8, temos $r = mmc\{r_1, ..., r_k\}$, para $r_i = ord_{n_i}(a_i)$, $1 \leq i \leq k$. Portanto r é ímpar se e somente se todos os r_i também o forem. Temos que r_i é ímpar com probabilidade no máximo $\frac{1}{2}$, pelo Lema B.1 com $s = 0$. Como a escolha dos valores de a_i são independentes, temos que a probabilidade de que todos os valores r_i sejam ímpares é de no máximo $\frac{1}{2^k}$. □

Lema B.3. *Seja $a \in \mathbb{Z}_n^*$ um valor selecionado aleatoriamente de maneira uniforme. Se $r = ord_n(a)$ é par, então a probabilidade de que $a^{\frac{r}{2}} \equiv -1 \mod n$ é de $\frac{1}{2^k}$.*

Demonstração. Se r é par e $a^{\frac{r}{2}} \equiv -1 \mod n$, então

$$a^{\frac{r}{2}} \equiv -1 \mod p_i^{e_i}, \tag{B.1}$$

para todo $1 \leq i \leq k$.

Sejam $r_i = ord_{n_i}(a_i)$, então temos que $r = mmc\{r_1, ..., r_k\}$. Vamos definir também $r = 2^s t$, com t ímpar e $s \geq 1$, e $r_i = 2^{s_i} t_i$, com s_i ímpar. Como r_i é um divisor de r, temos que $s_i \leq s$, para $1 \leq i \leq k$.

Na verdade, iremos mostrar que $s_i = s$ para todos os valores de i, caso contrário a Equação B.1 não será satisfeita. Se $s_j < s$ para algum valor de j, temos que r_j irá dividir $\frac{r}{2}$, o que implica que para algum valor $c \in \mathbb{Z}$, $a^{\frac{r}{2}} \equiv a^{cr_j} \mod p_j^{e_j} \equiv 1 \mod p_j^{e_j}$. Como $p_j \neq 2$ temos que este fato contradiz com o fato de que $a^{\frac{r}{2}} \equiv -1 \mod p_j^{e_j}$.

Para um dado s, a probabilidade de que $s_j = s$, e pelo Lema B.1 isso ocorre com probabilidade no máximo $\frac{1}{2}$. Portanto, a probabilidade de que esse fato ocorra para todo $1 \leq i \leq k$ é de no máximo $\frac{1}{2^k}$.

□

Finalmente provaremos o lema principal utilizado na Seção 3.2.3.

Lema 3.2.4. *Seja $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ a decomposição em fatores primos de um número ímpar composto n. A probabilidade de a ordem de a em $\mathbb{Z}_n$, $r = ord_n(a)$, ser par e $a^{\frac{r}{2}} \not\equiv -1 \mod n$ é pelo menos $\frac{9}{16}$.*

Demonstração. Pelo Lema B.2 temos que a probabilidade de r ser par é de pelo menos $1 - \frac{1}{2^k}$. Pelo Lema B.3 temos que se r é par, a probabilidade de que $a^{\frac{r}{2}} \not\equiv -1 \mod n$ é pelo menos $1 - \frac{1}{2^k}$.

Portanto, dado que $k \geq 2$, a probabilidade de que r seja par e $a^{\frac{r}{2}} \not\equiv -1 \mod n$ é pelo menos $(1 - \frac{1}{2^k})^2 \geq \frac{9}{6}$. □

Apêndice C

Classes de Complexidade Clássicas

Neste apêndices serão apresentadas brevemente as Classes de Complexidade determinísticas e probabilísticas referenciadas na Seção 3.3 a fim de comparação entre o modelo computacional quântico e clássico.

C.1 Classe P

A classe P contém os problemas que podem ser resolvidos de maneira eficiente no modelo computacional determinístico, também chamados, por este motivo, de problemas tratáveis.

Definição C.1. *A classe* P *é formada pelas linguagens que são decididas por um Algoritmo Determinístico em tempo polinomial em relação ao tamanho da entrada.*

C.2 Classe BPP

Para o modelo probabilístico, existem diferentes extensões da classe P, que diferem, em geral, na probabilidade de erro que o algoritmo pode ter ao decidir uma linguagem. Iremos apresentar aqui a classe BPP, que é reconhecida como a classe dos problemas que são resolvidos de forma eficiente no modelo probabilístico.

Definição C.2. *Uma linguagem* $L \in \{0,1\}^*$ *pertence à classe* BQP *se existe um Algoritmo Probabilístico* A_P *que para em tempo polinomial em relação ao tamanho da entrada e dada uma cadeia* $x \in \{0,1\}^*$

- *(Completude) se $x \in L$, A_P aceita x com probabilidade pelo menos $\frac{2}{3}$; e*
- *(Robustez) se $x \notin L$, A_P aceita x com probabilidade no máximo $\frac{1}{3}$*

As probabilidade $\frac{2}{3}$ e $\frac{1}{3}$ apresentadas na definição é arbitrária dado que é possível amplificar a probabilidade de acerto ao repetir o algoritmo verificador um número polinomial de vezes e o erro será exponencialmente pequeno.

A relação P $\subseteq$ BPP é direta e não se sabe se BPP $\subseteq$ P, porém acredita-se que este é o caso e todo algoritmo probabilístico pode ser desaleatorizado.

C.3 Classe NP

A classe NP tem muita importância em Teoria de Computação, especialmente em Otimização, dado que vários problemas de muita importância prática estão contidos nela. Na literatura, existem duas definições alternativas para esta classe, uma envolvendo algoritmos não-determinísticos e outra envolvendo algoritmos verificadores, e iremos agora apresentar ambas.

Começaremos com a definição original envolvendo algoritmos não-determinísticos.

Definição C.3. *Uma linguagem $L \subseteq \{0,1\}$ pertence à classe* NP*, se existe um algoritmo não-determinístico que decide L em tempo polinomial.*

E passaremos para a definição mais utilizada atualmente, envolvendo algoritmos verificadores. Intuitivamente, esta definição caracteriza NP como a classe dos problemas para os quais se consegue verificar soluções em tempo polinomial, dado um certificado provido por uma parte computacionalmente ilimitada.

Definição C.4. *Uma linguagem $L \in \{0,1\}^*$ pertence à classe* NP*, se existe um algoritmo determinístico V que possui complexidade polinomial em relação ao tamanho da entrada e um polinômio $p(x)$ tal que*

- *se $x \in L$, então existe uma cadeia $c \in \{0,1\}^{p(|x|)}$ tal que $\langle x, c\rangle$ é aceito por A; e*
- *se $x \notin L$, então para todas as cadeias $c \in \{0,1\}^{p(|x|)}$, $\langle x, c\rangle$ é rejeitada por A.*

O Algoritmo V da Definição C.4 é chamado de algoritmo verificador, e a cadeia c é chamada de certificado.

A relação P $\subseteq$ NP é direta e acredita-se que P $\subsetneq$ NP, entretanto este fato ainda não foi provado, sendo este um dos Problemas do Milênio do Clay Mathematics Institute [31] [32].

C.4 Classe PP

Veremos agora que o fato de que a probabilidade de erro na definição da classe BPP é uma grande restrição no poder computacional. Veremos agora uma definição em que a diferença entre a probabilidade de aceitação e rejeição pode ser exponencialmente pequena e veremos uma consequência disso.

Definição C.5. *Uma linguagem $L \in \{0,1\}$ está na classe* PP *se existe um algoritmo probabilístico A_P que para em tempo polinomial e*

- *se $x \in L$, A_P aceita x com probabilidade maior que $\frac{1}{2}$; e*
- *se $x \notin L$, A_P aceita x com probabilidade menor que $\frac{1}{2}$.*

Acredita-se que há problemas na classe PP não podem ser resolvidos de forma eficiente, dado que NP $\subseteq$ PP [16].

C.5 Classe MA

O conceito de algoritmos verificadores da classe NP também foi estendido ao modelo probabilístico com a classe MA. Entretanto, como no caso da classe BPP, como estão envolvidos passos probabilísticos, permite-se ao algoritmo verificador uma probabilidade de erro.

Definição C.6. *Uma linguagem $L \in \{0,1\}^*$ pertence à classe* MA*, se existe um algoritmo probabilístico V_P de complexidade polinomial em relação ao tamanho da entrada e um polinômio $p(x)$ tal que*

- *(Completude) se $x \in L$, então existe uma cadeia $c \in \{0,1\}^{p(x)}$ tal que $\langle x, c\rangle$ é aceito com probabilidade pelo menos $\frac{2}{3}$; e*

- *(Robustez) se $x \notin L$, então para todo $c \in \{0,1\}^{p(|x|)}$, $\langle x, c\rangle$ é aceito com probabilidade no máximo $\frac{1}{3}$.*

Assim como no caso da classe BQP, a probabilidade de acerto pode ser amplificada ao repetir o protocolo um número polinomial de vezes. Na verdade, para a classe MA o caso é ainda melhor, pois consegue-se chegar a probabilidade de aceitação 1 para instâncias positivas sem alteração no poder computacional do modelo [96] [46].

Temos que NP $\subseteq$ MA, pois basta remover o caráter probabilístico do algoritmo verificador, e BPP $\subseteq$ MA, bastando ignorar o certificado.

C.6 Classe #P

Vimos até agora classes que consistem de problemas de decisão. Iremos agora definir uma classe de complexidade relativa ao fato de contar os certificados que levam um algoritmo verificador a aceitar. Para esta generalização, temos que as classes de contagem não consistem de linguagens, mas de funções $f : \{0,1\}^* \to \mathbb{N}$.

Definição C.7. *Uma função $f : \{0,1\}^* \to \mathbb{N}$ está na classe* #P *se existem um algoritmo determinístico de complexidade em tempo polinomial A e um polinômio $p(x)$ tal que para uma entrada $x \in \{0,1\}^*$, temos*

$$f(x) = \left|\left\{y \in \{0,1\}^{p(|x|)} |\ A \text{ aceita } \langle x, y\rangle\right\}\right|.$$

Como está classe não é de decisão, comparamos seu poder computacional com a classe $\mathrm{P}^{\#\mathrm{P}}$ de problemas para os quais existem algoritmos determinísticos polinomiais com um oráculo para os problemas em #P.

Claramente se houver algoritmos eficientes para os problemas de #P, P = NP, dado que basta verificar se a resposta do algoritmo para #P é igual ou maior que 0. Foi provado por Toda que $\mathrm{P}^{\#\mathrm{P}} = \mathrm{P}^{\mathrm{PP}}$ [84].

C.7 Classe PSPACE

Até agora foram apresentadas classes de complexidade cuja restrição está na complexidade em tempo dos algoritmos. Iremos agora definir uma classe cuja restrição está na quantidade de memória utilizada pelo algoritmo.

Definição C.8. *A classe* PSPACE *é formada pelas linguagens que são decididas por um Algoritmo Determinístico utilizando uma quantidade de memória polinomial em relação ao tamanho da entrada.*

Como temos que os certificados de NP e MA são de tamanho polinomial, podemos fazer uma busca exaustiva de um certificado correto utilizando uma quantidade polinomial de memória, pois o gasto adicional nessa busca é logarítmico no número de possíveis certificados, que é exponencial. Portanto, PSPACE engloba todas as outras classes de decisão definidas até o momento.

C.8 Sistemas Interativos de Prova

Sistemas Interativos de Prova, ou Provas Interativas, generalizam o conceito de certificados e algoritmos verificadores introduzido nas definições das classes P e NP. Formalizados em um contexto na intersecção de Complexidade Computacional e Criptografia [47] [19], este tópico levou a descobertas importantes em Complexidade Computacional, como por exemplo o Teorema PCP [17] [18] [37].

Nos sistemas interativos de prova, existem dois participantes, o Verificador V, de poder computacional limitado, e o Provador P, de poder computacional ilimitado. Estes P e V trocam mensagens afim de que V possa reconhecer uma linguagem, sem ser enganado por algum Provador desonesto.

Para definir formalmente os Sistemas Interativos de Prova, precisaremos antes aprestar alguns outros conceitos iniciais.

Definição C.9. *Um interação de k mensagens entre um verificador V e um provador P é um conjunto de funções:*

$$\begin{aligned} m_1 &= f_1(x) \\ m_2 &= f_2(x, m_1) \\ m_2 &= f_3(x, m_1) \\ &\ldots \\ m_k &= f_3(x, m_1, \ldots m_{k-1}), \end{aligned}$$

tal que para k par, m_{2i} são mensagens enviadas de V para P e, portanto, f_{2i} deve ser computacionalmente eficiente e o Verificador pode fazer escolhas aleatórias em sua

computação; e m_{2i+1} são mensagens de P para V e não há restrição na eficiência de f_{2i+1}. Para k ímpar, o caso é inverso, dado que a última mensagem deve ser sempre do provador ao verificador.

Definição C.10. *Um Sistema Interativo de Prova com k mensagens é uma interação de k mensagens entre um Verificador V e um provador P e, ao final da troca de mensagens, o Verificador deve decidir aceitar ou rejeitar a cadeia inicial x.*

Veremos, finalmente, a definição da classe IP.

Definição C.11. *Uma linguagem L está na classe* $\mathrm{IP}(k, C, S)$ *se existe um Sistema Interativo de Prova com k mensagens que satisfaz as seguintes restrições:*

- *(Completude) $\forall x \in L$, o verificador aceita com probabilidade pelo menos C;*
- *(Robustez) $\forall x \notin L$, o verificador aceita x com probabilidade no máximo S.*

Definição C.12. $\mathrm{IP} = \mathrm{IP}(poly(|x|), \frac{2}{3}, \frac{1}{3})$.

Assim como na classe MA, pode-se repetir um protocolo IP a fim de amplificar a probabilidade de responder corretamente.

Um resultado é que PSPACE = IP, que foi provado utilizando uma técnica em Complexidade Computacional chamada algebrização.

Apêndice D

Prova do Lema 4.5.10

Neste anexo provaremos o Lema 4.5.10 utilizado na Seção 4.5.2 na prova de que palíndromos são reconhecidos pelo modelo 2QCFA com erro unilateral ϵ arbitrário. Porém, antes de apresentar a prova do lema, faremos a definição de elementos necessários e provaremos alguns lemas auxiliares.

Definição D.1. *Sejam*

$$A = \begin{pmatrix} 4 & 3 & 0 \\ -3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix} \text{ e } B = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & 4 \end{pmatrix}$$

duas matrizes 3×3*,*

$$f(u) = 4u_1 + 3u_2 + 3u_3$$

uma função $f : \mathbb{Z}^3 \to \mathbb{Z}$*, e*

$$K = \{u \in \mathbb{Z}^3 | u_1 \not\equiv 0 \mod 5, f(u) \not\equiv 0 \mod 5 \text{ e } u_2u_3 \equiv 0 \mod 5\}$$

um subconjunto de $\mathbb{Z}^3$*.*

Lema D.2. *Se* $u \in K$*, então* $Au \in K$ *e* $Bu \in K$*.*

Demonstração. Iremos provar inicialmente que $u \in K \implies Au \in K$. Seja

$$v = Au = \begin{pmatrix} 4u_1+3u_2 \\ -3u_1+4u_2 \\ 5u_3 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}.$$

Como $u \in K$, sabemos que $u_1 \not\equiv 0 \mod 5$, $4u_1 + 3u_2 + 3u_3 \not\equiv 0 \mod 5$ e além disso temos que $u_2 \equiv 0 \mod 5$ ou $u_3 \equiv 0 \mod 5$.

Se $u_2 \equiv 0 \mod 5$, temos que

$$v_1 = 4u_1 + 3u_2 \equiv 4u_1 \mod 5 \not\equiv 0 \mod 5$$

e que

$$\begin{aligned} f(v) &= 4v_1 + 3v_2 + 3v_3 \\ &= 16u_1 + 12u_2 - 9u_1 + 12u_2 + 15u_3 \\ &= 7u_1 + 24u_2 + 15u_3 \\ &\equiv 7u_1 \mod 5 \\ &\not\equiv 0 \mod 5. \end{aligned}$$

Se $u_3 \equiv 0 \mod 5$, temos que

$$v_1 = 4u_1 + 3u_2 \equiv 4u_1 + 3u_2 + 3u_3 \mod 5 \equiv f(u) \mod 5 \not\equiv 0 \mod 5$$

e que

$$\begin{aligned} f(v) &= 4v_1 + 3v_2 + 3v_3 \\ &= 16u_1 + 12u_2 - 9u_1 + 12u_2 + 15u_3 \\ &= 7u_1 + 24u_2 + 15u_3 \\ &\equiv 2u_1 + 4u_2 \mod 5 \\ &\equiv 12u_1 + 9u_2 + 9u_3 \mod 5 \\ &\equiv 3(4u_1 + 3u_2 + 3u_3) \mod 5 \\ &\equiv 3f(u) \mod 5 \\ &\not\equiv 0 \mod 5. \end{aligned}$$

Trivialmente, para os dois casos, temos que

$$v_2 v_3 = 5u_3(-3u_1 + 4_u 2) \equiv 0 \mod 5,$$

completando a prova.

□

Lema D.3. *Sejam $u, v, w \in \mathbb{Z}^3$ vetores tal que $u = Av = Bw$. Então $u \notin K$.*

Demonstração. Temos que $A^{-1} = \begin{pmatrix} \frac{4}{25} & -\frac{3}{25} & 0 \\ \frac{3}{25} & \frac{4}{25} & 0 \\ 0 & 0 & \frac{1}{25} \end{pmatrix}$ e, portanto, $v_1 = \frac{4u_1}{25} - \frac{3u_2}{25} \in \mathbb{Z}$. Como $v \in \mathbb{Z}^3$, resulta-se que $4u_1 - 3u_2 \equiv 0 \mod 5$. Do mesmo modo, a partir de B^{-1}, podemos deduzir que $u_2 = 5w_2 \equiv 0 \mod 5$.

Esses dois fatos juntos implicam que $u_1 \equiv 0 \mod 5$, resultando que $u \notin K$. □

Com estes elementos, podemos agora efetuar a prova do Lema 4.5.10.

Lema 4.5.10. *Seja* $u = Y_1^{-1}...Y_n^{-1}X_n...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, *tal que* $X_i, Y_i \in \{A, B\}$. *Se* $X_j \neq Y_j$ *para algum valor de* j, *então* $u_2^2 + u_3^2 > 25^{-n}$.

Demonstração. Como $\frac{1}{5}X_i$ e $5Y_i^{-1}$ são matrizes unitárias, temos que $||u|| = 1$. Além disso temos que $25^n u \in \mathbb{Z}^3$. Portanto, se provarmos que $u \neq \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, temos que que $u_1 < 1$ e portanto $u_1 \leq 1 - 25^n$.

Seja k o maior índice tal que $X_k \neq Y_k$ e suponha, sem perda de generalidade que $X_k = A$ e $Y_k = B$. Seja $v = X_{k-1}...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ e $w = Y_{k-1}...Y_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Como $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in K$, pelo Lema D.2, $Av, Bw \in K$. Pelo Lema D.3, $Av = Bw$ contradiz o fato de que $Av, Aw \in K$, portanto temos que $Aw \neq Bv$. Como para todo $j > k$ temos que $X_j = Y_j$, resulta-se que $Y_n..Y_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \neq X_n...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, e, portanto $u = Y_1^{-1}...Y_n^{-1}X_n...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

Como $\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \in K$, pelos mesmos argumentos apresentados anteriormente temos que $u = Y_1^{-1}...Y_n^{-1}X_n...X_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$. □