UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Tese de Doutorado

Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero

Marciel Medeiros de Oliveira

Campina Grande, Paraíba, Brasil

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Centro de Engenharia Elétrica e Informática
Programa de Pós-Graduação em Engenharia Elétrica

Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero

Marciel Medeiros de Oliveira

Tese de doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande como parte dos requisitos necessários para obtenção do título de Doutor em Engenharia Elétrica.

Área de Concentração: Processamento da Informação
Linhas de Pesquisa: Eletrônica e Telecomunicações

Orientador: Francisco Marcos de Assis, Dr.

Campina Grande, Paraíba, Brasil

Novembro, 2024.

O48a Oliveira, Marciel Medeiros de.
Aplicações do teorema de Shemesh e dos conceitos de subespaço invariante e canal quântico não-ergódico na teoria da informação quântica erro-zero / Marciel Medeiros de Oliveira. – Campina Grande, 2024.
101 f. : il. color.

Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e informática, 2024.
"Orientação: Prof. Dr. Francisco Marcos de Assis".
Referências.

1. Processamento da Informação. 2. Teoria da Informação Quântica. 3. Canal Quântico e Canal Quântico Não-Ergódico. 4. Capacidade Erro-Zero. 5. Estado Próprio Comum. 6. Subespaço Comum Invariante. 7. Teorema de Shemesh. 8. Eletrônica e Telecomunicações. I. Assis, Francisco Marcos de. II. Título.

CDU 621.391:530.145(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero

MARCIEL MEDEIROS DE OLIVEIRA

TESE APROVADA EM 28/11/2024

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)

RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG
Examinador(a)

HELDER ALVES PEREIRA, Dr., UFCG
Examinador(a)

GIULIANO GADIOLI LA GUARDIA, Dr., UEPG-PR
Examinador(a)

NADJA KOLB BERNARDES, Dr, UFPE
Examinador(a)

CAMPINA GRANDE - PB

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
POS-GRADUACAO EM ENGENHARIA ELETRICA
Rua Aprigio Veloso, 882, - Bairro Universitario, Campina Grande/PB, CEP 58429-900

REGISTRO DE PRESENÇA E ASSINATURAS

1. ATA DA DEFESA PARA CONCESSÃO DO GRAU DE DOUTOR EM CIÊNCIAS, NO DOMÍNIO DA ENGENHARIA ELÉTRICA, REALIZADA EM 28 DE NOVEMBRO DE 2024
(Nº 388)

CANDIDATO(A): **MARCIEL MEDEIROS DE OLIVEIRA.** COMISSÃO EXAMINADORA: RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG - Presidente da Comissão e Examinador Interno, FRANCISCO MARCOS DE ASSIS, Dr., UFCG - Orientador, HELDER ALVES PEREIRA, D.Sc., UFCG - Examinador Interno, este por motivos superiores não participou de modo remoto da referida tese, entretanto enviou o parecer por escrito para o Presidente da Comissão, bem como os questionamentos e sugestões, explicitando que considera o trabalho de tese aprovado. GIULIANO GADIOLI LA GUARDIA, Dr., UEPG - Examinador Externo, NADJA KOLB BERNARDES, Dr., UFPE - Examinador Externo. TÍTULO DA TESE: Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero. ÁREA DE CONCENTRAÇÃO: Processamento da Informação. HORA DE INÍCIO: **14h00** – LOCAL: **Sala Virtual, conforme Art. 5º da PORTARIA SEI Nº 01/PRPG/UFCG/GPR, DE 09 DE MAIO DE 2022.** Em sessão pública, após exposição de cerca de 45 minutos, o(a) candidato(a) foi arguido(a) oralmente pelos membros da Comissão Examinadora, tendo demonstrado suficiência de conhecimento e capacidade de sistematização, no tema de sua tese, obtendo conceito APROVADO. Face à aprovação, declara o presidente da Comissão, achar-se o examinado, legalmente habilitado a receber o Grau de Doutor em Ciências, no domínio da Engenharia Elétrica, cabendo a Universidade Federal de Campina Grande, como de direito, providenciar a expedição do Diploma, a que o(a) mesmo(a) faz jus. Na forma regulamentar, foi lavrada a presente ata, que é assinada por mim, Leandro Ferreira de Lima, e os membros da Comissão Examinadora. Campina Grande, 28 de Novembro de 2024.

LEANDRO FERREIRA DE LIMA
Secretário

RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr. UFCG
Presidente da Comissão e Examinador Interno

FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador

HELDER ALVES PEREIRA, D.Sc., UFCG
Examinador Interno

GIULIANO GADIOLI LA GUARDIA, Dr., UEPG
Examinador Externo

NADJA KOLB BERNARDES, Dr., UFPE
Examinador Externo

MARCIEL MEDEIROS DE OLIVEIRA

Candidato

2 - APROVAÇÃO

2.1. Segue a presente Ata de Defesa de Tese de Doutorado do candidato **MARCIEL MEDEIROS DE OLIVEIRA**, assinada eletronicamente pela Comissão Examinadora acima identificada.

2.2. No caso de examinadores externos que não possuam credenciamento de usuário externo ativo no SEI, para igual assinatura eletrônica, os examinadores internos signatários **certificam** que os examinadores externos acima identificados participaram da defesa da tese e tomaram conhecimento do teor deste documento.

Documento assinado eletronicamente por **LEANDRO FERREIRA DE LIMA**, **SECRETÁRIO (A)**, em 29/11/2024, às 11:44, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **RAIMUNDO CARLOS SILVERIO FREIRE**, **PROFESSOR 3 GRAU**, em 29/11/2024, às 12:39, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **HELDER ALVES PEREIRA**, **PROFESSOR(A) DO MAGISTERIO SUPERIOR**, em 29/11/2024, às 15:03, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **FRANCISCO MARCOS DE ASSIS**, **PROFESSOR 3 GRAU**, em 29/11/2024, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Marciel Medeiros de Oliveira**, **Usuário Externo**, em 16/12/2024, às 11:08, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.ufcg.edu.br/autenticidade, informando o código verificador **5072010** e o código CRC **2258D13B**.

Referência: Processo nº 23096.086211/2024-91 SEI nº 5072010

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CNPJ nº 05.055.128/0001-76
POS-GRADUACAO EM ENGENHARIA ELETRICA
Rua Aprigio Veloso, 882, - Bairro Universitario, Campina Grande/PB, CEP 58429-900

DECLARAÇÃO

Processo nº 23096.086211/2024-91

DECLARAMOS para fins de comprovação que, os Professores RAIMUNDO CARLOS SILVÉRIO FREIRE, Dr., UFCG - Presidente da Comissão e Examinador Interno, FRANCISCO MARCOS DE ASSIS, Dr., UFCG - Orientador, HELDER ALVES PEREIRA, D.Sc., UFCG - Examinador Interno, este por motivos superiores não participou de modo remoto da referida tese, entretanto enviou o parecer por escrito para o Presidente da Comissão, bem como os questionamentos e sugestões, explicitando que considera o trabalho de tese aprovado. GIULIANO GADIOLI LA GUARDIA, Dr., UEPG - Examinador Externo, NADJA KOLB BERNARDES, Dr., UFPE - Examinador Externo., participaram da Banca de Defesa Final da Tese de Doutorado, do Programa de Pós-Graduação em Engenharia Elétrica da UFCG, intitulada TÍTULO DA TESE: **Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero**, de autoria do doutorando **MARCIEL MEDEIROS DE OLIVEIRA,** no dia 28 de novembro de 2024.

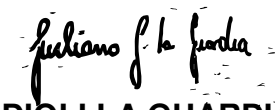
Documento assinado eletronicamente por **ALEXANDRE JEAN RENE SERRES**, **COORDENADOR(A)**, em 09/12/2024, às 09:21, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.ufcg.edu.br/autenticidade, informando o código verificador **5072086** e o código CRC **8838BBA6**.

Referência: Processo nº 23096.086211/2024-91 SEI nº 5072086

Caro Professor
Alexandre Jean Rene Serres
Coordenador do PPgEE/UFCG.

Eu, **GIULIANO GADIOLI LA GUARDIA, Dr., UEPG,** na qualidade de membro da comissão examinadora da defesa de tese intitulada **“** Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero”**,** de **MARCIEL MEDEIROS DE OLIVEIRA**, da qual participei por videoconferência, no dia 28 de Novembro de 2024, declaro ter recebido cópia da ata, que consta nos autos do processo n° 23096.086211/2024-91 como documento n° (5072010), a qual li e, embora não tenha podido assinar, é para todos os efeitos como se eu tivesse, pois está em perfeita conformidade com o que foi deliberado pela comissão e, portanto, estou de pleno acordo com seus termos.



GIULIANO GADIOLI LA GUARDIA, Dr., UEPG.

Caro Professor
Alexandre Jean Rene Serres
Coordenador do PPgEE/UFCG.

Eu, **NADJA KOLB BERNARDES, Dr., UFPE,** na qualidade de membro da comissão examinadora da defesa de tese intitulada **“** Aplicações do Teorema de Shemesh e dos Conceitos de Subespaço Invariante e Canal Quântico Não-Ergódico na Teoria da Informação Quântica Erro-Zero”**,** de **MARCIEL MEDEIROS DE OLIVEIRA**, da qual participei por videoconferência, no dia 28 de Novembro de 2024, declaro ter recebido cópia da ata, que consta nos autos do processo n° 23096.086211/2024-91 como documento n° (5072010), a qual li e, embora não tenha podido assinar, é para todos os efeitos como se eu tivesse, pois está em perfeita conformidade com o que foi deliberado pela comissão e, portanto, estou de pleno acordo com seus termos.

gov.br
Documento assinado digitalmente
NADJA KOLB BERNARDES
Data: 02/12/2024 11:41:55-0300
Verifique em https://validar.iti.gov.br

NADJA KOLB BERNARDES, Dr., UFPE.

Este trabalho é dedicado à minha mãe, Maria Zeth, e ao meu pai, Cicero Gomes.

Agradecimentos

Chegar ao final deste doutorado é uma conquista que não teria sido possível sem o apoio de pessoas especiais e, acima de tudo, sem a graça divina. A todos que contribuíram de alguma forma para este momento, expresso minha profunda gratidão.

Primeiramente, agradeço a Deus por me conceder força, sabedoria e perseverança para enfrentar os desafios ao longo dessa trajetória.

À minha família, que sempre foi meu alicerce, oferecendo amor incondicional, apoio e confiança durante essa conquista.

À Kelly, pelo carinho, paciência, compreensão e companheirismo ao longo desta jornada.

Agradeço aos amigos e amigas pelos incentivos e pela força ao longo dessa formação. Vocês foram fundamentais para que eu chegasse até aqui.

Ao Professor Francisco Marcos de Assis, sou imensamente grato pela orientação, paciência, ensinamentos, compreensão, conselhos e generosidade. O senhor possui uma mente brilhante.

Aos meus amigos e parceiros de estudos do IQuanta, que se mantiveram próximos e me acompanharam ao longo dessa caminhada, minha gratidão. Vocês foram a fonte de ânimo nos momentos de desânimo e sempre me lembraram da importância de manter o bom humor e o equilíbrio, mesmo em tempos de grande pressão. Em especial, à Andresso, Rávila, Micael, Milena e Professor Bruno.

Ao Programa de Pós-Graduação em Engenharia Elétrica (PPgEE - COPELE) da UFCG, pelo suporte administrativo. À CAPES, pelo suporte financeiro para a publicação do artigo na *IEEE Access*.

Por fim, expresso minha gratidão às instituições de ensino superior UEPB, UFCG e UniFip, nas quais sou professor. Em particular, agradeço à UEPB pelo afastamento das minhas atividades docentes durante o doutorado, e à UFCG e à UniFip pela compreensão e flexibilização das atividades acadêmicas ao longo de toda a minha formação.

"Nada te turbe, nada te espante. Tudo passa, Deus não muda. ***A paciência tudo alcança****. Quem a Deus tem, nada lhe falta. Só Deus basta."*

Santa Teresa d'Ávila, 1751

Resumo

A Teoria da Informação Quântica é uma ciência que utiliza os paradigmas da Mecânica Quântica para realizar estudos sobre os limites máximos possíveis para o processamento e transmissão da informação por meio de um canal quântico. Uma das subáreas de pesquisa é a capacidade dos canais quânticos, que é entendida como o supremo das taxas para as quais a probabilidade de erro tende assintoticamente a zero à medida que o comprimento do código tende ao infinito, quando a informação é transmitida por meio de canais quânticos. Em determinados contextos, há interesse no estudo da capacidade dos canais quânticos de enviar informações com probabilidade de erro exatamente igual a zero. Neste caso, o canal é dito ter capacidade erro-zero positiva ou não trivial. Para que um canal quântico transmita informações com probabilidade de erro exatamente igual a zero, é necessário que o canal satisfaça determinadas condições. Dessa forma, com a proposta da definição de capacidade de erro-zero de um canal quântico na primeira década deste século, foi demonstrada uma condição necessária para a capacidade de erro-zero de um canal quântico, baseada na ortogonalidade de estados quânticos na saída do canal. Mais recentemente, no ano de dois mil e dezenove, foi provada outra condição para a capacidade erro-zero de canais quânticos, baseada na ortogonalidade de estados quânticos com o subespaço gerado por todas as arrumações de produtos aos pares de operadores de Kraus que representam o canal quântico. Na linha de proposição de condições de capacidade erro-zero de canais quânticos, este trabalho de tese tem como eixo central o estudo de condições matemáticas para que os canais quânticos tenham capacidade erro-zero. Nesse sentido, é apresentada uma condição de capacidade baseada nos estados próprios comuns aos operadores de Kraus que representam o canal quântico. Também é provado que canais quânticos com subespaços invariantes comuns também são capazes de enviar informações com probabilidade de erro exatamente igual a zero. Ainda dando ênfase ao conceito de capacidade erro-zero dos canais quânticos, é apresentada uma classe de canais quânticos com capacidade de erro-zero positiva, denominados canais quânticos não ergódicos. Além disso, também são apresentadas algumas conexões entre o conceito de capacidade de erro-zero de um canal quântico e o Teorema de Shemesh.

Palavras-Chave: Canal Quântico. Capacidade Erro-Zero. Estado Próprio Comum. Subespaço Comum Invariante. Teorema de Shemesh. Canal Quântico Não-Ergódico.

Abstract

Quantum Information Theory is a science that utilizes the paradigms of Quantum Mechanics to study the ultimate limits of processing and transmitting information through a quantum channel. One of its sub-area of research is the capacity of quantum channels, which is understood as the supremum of rates at which the probability of error asymptotically tends to zero as the code length approaches infinity when information is transmitted through quantum channels. In certain contexts, there is interest in studying the capacity of quantum channels to transmit information with an error probability exactly equal to zero. In this case, the channel is said to have positive or non-trivial zero-error capacity. For a quantum channel to transmit information with an error probability exactly equal to zero, certain conditions must be satisfied. With the proposal of the definition of zero-error capacity of a quantum channel in the first decade of this century, a necessary condition for the zero-error capacity of a quantum channel was demonstrated, based on the orthogonality of quantum states at the channel output. More recently, in 2019, another condition for the zero-error capacity of quantum channels was proven, based on the orthogonality of quantum states with the subspace spanned by all pairwise products of Kraus operators representing the quantum channel. Following the line of proposing conditions for the zero-error capacity of quantum channels, this thesis focuses on the study of mathematical conditions for quantum channels to have zero-error capacity. In this regard, a capacity condition is presented based on the common eigenstates of the Kraus operators representing the quantum channel. It is also proven that quantum channels with common invariant subspaces are capable of transmitting information with an error probability exactly equal to zero. Continuing the emphasis on the concept of zero-error capacity of quantum channels, a class of quantum channels with positive zero-error capacity, called non-ergodic quantum channels, is presented. Additionally, some connections between the concept of zero-error capacity of a quantum channel and the Shemesh Theorem are discussed.

Keywords: Quantum Channel. Zero-Error Capacity. Common Eigenstate. Common Invariant Subspace. Shemesh Theorem. Non-Ergodic Quantum Channel.

Lista de Figuras

Lista de abreviaturas e siglas

DFS	*Subespaços e Subsistemas Livres de Descoerência*
DMC	*Canal Clássico Discreto e Sem Memória*
HSW	*Capacidade Holevo-Schumacher-Westmoreland*
qubit	*Quantum Bit*
POVM	*Positive Operator-Valued Measure*
OSR	*Operator-Sum Representation*

Lista de símbolos

$\mathcal{B}(\cdot)$	Conjunto de operadores de um espaço de Hilbert
$C(\cdot)$	Capacidade ordinária de um canal clássico
$C_0(\cdot)$	Capacidade erro-zero de um canal clássico
$C^{(0)}(\cdot)$	Capacidade erro-zero de um canal quântico
$H(\cdot)$	Entropia de Shannon
$I(X;Y)$	Informação mútua de Shannon das variáveis aleatórias X e Y
$\mathcal{H}$	Espaço de Hilbert
χ_{XY}	Informação de Holevo
$S(\cdot)$	Entropia de von Neumann
$H(\cdot)$	Entropia
$tr(\cdot)$	traço parcial
log	logaritmo na base 2

Sumário

Capítulo 1

Introdução

Neste capítulo é apresentada a motivação da proposta de tese, incluindo uma breve revisão bibliográfica, seguida pelos objetivos principais e a organização do documento. Além disso, apresentamos um esboço das contribuições deste trabalho e elencamos a produção científica desenvolvida.

1.1 Motivação

A Teoria da Informação, em linhas gerais, pode ser entendida como uma ciência cujos elementos centrais são a quantificação, o armazenamento e a transmissão da informação [1].

Os primeiros registros de estudos sobre a Teoria da Informação datam de 1924, com Nyquist [2], sobre a transmissão de informações por telégrafo, e de 1928, com Hartley [3]. No trabalho de Nyquist [2], o principal resultado das investigações sobre repetidores e transmissão de portadora de voz mostra que a quantidade total de informação que pode ser transmitida é proporcional à faixa de frequências transmitidas e ao tempo de transmissão. O trabalho de Hartley [3] é considerado o precursor mais importante para que, posteriormente, em 1948, o matemático e engenheiro eletricista Shannon fundamentasse matematicamente a Teoria da Informação por meio de métodos algébricos, lógicos, analíticos e probabilísticos [4].

Os estudos sobre a Teoria da Informação são conduzidos em dois cenários: o clássico e o quântico. No cenário clássico, a denominada Teoria da Informação Clássica tem como unidade básica o *bit* clássico (ou simplesmente *bit*), e a transmissão, o processamento e o armazenamento da informação seguem as leis da Mecânica Clássica. Uma caracterização da Teoria da Informação Clássica pode ser encontrada em [1].

No cenário quântico, a Teoria da Informação Quântica é vista como um novo para-

digma para o processamento e a transmissão de informação por meio de canais quânticos, que, evidentemente, consideram as leis da Mecânica Quântica [5], [6]. Consequentemente, a informação é representada em forma de *qubits* (do inglês: *quantum bits*), em vez de *bits* clássicos, como zeros e uns no caso do alfabeto binário. Em contrapartida, a abordagem dos conceitos da Teoria da Informação no cenário quântico é feita de forma análoga ao cenário clássico. Os dois grandes desafios para a Teoria da Informação Quântica são: o primeiro, do ponto de vista teórico, e o segundo, em relação à aplicação prática.

No que diz respeito ao aspecto teórico, um dos desafios é a tradução dos conceitos do paradigma clássico para o paradigma quântico. Outro desafio significativo é a determinação dos limites da classe de tarefas de processamento de informação possíveis utilizando as leis da Mecânica Quântica. Isso inclui, inclusive, investigar a possibilidade de obter resultados e realizar tarefas por meio da Teoria da Informação Quântica que não são factíveis pela Teoria da Informação Clássica. Com relação à aplicação prática, o principal desafio é desenvolver dispositivos e tecnologias capazes de implementar, no mundo real, as tarefas idealizadas no campo teórico [7], [8].

Um caminho natural para contribuir na resolução do primeiro desafio da Teoria da Informação Quântica é a tradução dos conceitos do paradigma clássico para o paradigma quântico. Um desses conceitos é o da Teoria da Informação Erro-Zero, que trata do envio de informações por meio de canais discretos sem memória, com probabilidade de ocorrência de erros de decodificação exatamente igual a zero [9]. Nesse contexto, o trabalho de Medeiros e Assis, em 2005 [10], é pioneiro ao estender os conceitos de capacidade erro-zero de canais clássicos para os canais quânticos. Posteriormente, em 2008, na tese de doutorado de Medeiros [11], foi desenvolvida a caracterização da Teoria da Informação Quântica Erro-Zero, mantendo o pioneirismo na área.Em sua tese, Medeiros construiu um conjunto de conceitos teóricos e apresentou condições necessárias para que um canal quântico discreto sem memória pudesse ser utilizado para transmitir mensagens com erro-zero de decodificação. Em outras palavras, ele propôs a definição de capacidade erro-zero para canais quânticos, entendida como o supremo das taxas em que a informação clássica pode ser transmitida por um canal quântico com probabilidade de erro igual a zero. Assim, utilizando códigos quânticos, a informação clássica é codificada em estados quânticos e transmitida por meio de um DMC *(Discrete Memoryless Channel)*. Na recepção, como parte do processo, os estados quânticos são medidos. Nesse caso, a transmissão é realizada com uma taxa de erro exatamente igual a zero.

É interessante destacar que o estudo da capacidade de canais quânticos constitui uma das áreas de pesquisa mais relevantes da Teoria da Informação Quântica. Também é importante ressaltar que os recursos da Mecânica Quântica possibilitam definir a capacidade dos canais quânticos de diversas maneiras, dependendo do tipo de informação a

ser transmitida (informação clássica ou estados quânticos), dos recursos físicos utilizados na transmissão, como o emaranhamento, e do protocolo de comunicação empregado [12], [13], [14].

Após os trabalhos originais propostos por Medeiros e Assis [10] e Medeiros [11], outros pesquisadores direcionaram sua atenção para a temática, identificando novas propriedades, propondo aplicações e outras abordagens sobre a capacidade erro-zero dos canais quânticos. Como exemplo, em 2008, o trabalho de Beigi e Shor [15] utilizou as ideias formuladas por Medeiros [11] para explicar a relação entre as classes de complexidade NP-completo e QMA-completo. Em 2010, Sanz *et al.* [58] provaram a Desigualdade de Wielandt para canais quânticos, que consiste em encontrar um limite superior para o número de vezes que um canal deve ser aplicado, de modo que tal canal mapeie qualquer operador densidade em um operador com classificação completa. Usando esse limite, estabeleceram o teorema da dicotomia universal para a capacidade de erro-zero dos canais quânticos. Em 2013, inspirados nos trabalhos desenvolvidos por Medeiros [11] e por Beigi e Shor [15], Duan *et al.* [17] realizaram um estudo sobre os grafos não-comutativos. Nesse trabalho, propuseram uma versão quântica para a função ϑ de Lovász e mostraram que essa função é um limitante superior para a capacidade erro-zero dos canais quânticos. Em 2019, Yamasaki e Murao [18] utilizaram as ideias desenvolvidas por Guedes *et al.* [19] e por Medeiros e Assis [10] para realizar um trabalho sobre processamento de informação quântica utilizando computadores quânticos. Nesse trabalho, investigaram o custo de emaranhamento necessário para a fusão de estados quânticos *one-shot*, visando à transformação de estados quânticos em escalas pequenas e intermediárias de até várias dezenas de *qubits.* Um trabalho mais recente nesta área é o de Dereniowski e Jurkiewicz [20]. Nesse estudo, investigaram grafos característicos de canais quânticos de linha e/ou coluna simétrica para encontrar suas caracterizações estruturais e, além disso, analisaram as condições sob as quais um grafo é característico de algum canal quântico simétrico discreto.

Além dos aspectos sobre a capacidade erro-zero abordados por Beigi e Shor [15], Sanz et al. [58] e Duan et al. [17], um outro aspecto importante envolvendo essa temática é a verificação de quando um canal quântico tem ou não capacidade erro-zero positiva (ou não trivial). Nesse contexto, Medeiros e Rex [10], [21] e Gupta et al. [22] propuseram condições para que um canal quântico tenha ou não capacidade erro-zero positiva. Ainda considerando esse aspecto, em 2022, uma nova condição para a capacidade erro-zero dos canais quânticos foi proposta por Oliveira e Assis [23]. Essa condição, baseada no Teorema de Shemesh [24], ainda permanece em forma de conjectura e, provavelmente, representa uma ideia original.

Outro exemplo que relaciona o Teorema de Shemesh à caracterização de canais

quânticos está no trabalho de Białończyk *et al.* [25]. Nele, os autores realizam um estudo sobre as propriedades espectrais dos canais quânticos e observam uma conexão entre as propriedades do espectro periférico dos canais quânticos e a álgebra gerada por seus operadores de Kraus, que representam os canais quânticos. As conclusões dessas conexões são baseadas no Teorema de Shemesh e no Teorema de Amitsur-Levitzki [26], [27]. O Teorema de Amitsur-Levitzki é um resultado central no estudo das PI-Álgebras [28], e também desempenha um papel importante no estudo e análise das estruturas internas dos canais quânticos. Como exemplos, podemos citar sua utilização na análise de canais quânticos [29] e para a demonstração do Teorema de Shemesh generalizado [30].

O Teorema de Shemesh generalizado fornece condições para que n operadores lineares ou matrizes quadradas tenham autovetor(es) comum(uns). Este teorema desempenha um papel importante neste trabalho de tese, pois as conexões que faremos entre conceitos matemáticos (por exemplo, o conceito de subespaço comum invariante dos canais quânticos) e a capacidade erro-zero dos canais quânticos estão intimamente relacionadas com conceitos consequentes do Teorema de Shemesh generalizado.

1.2 Objetivos

Este trabalho de tese tem como objetivo apresentar aplicações do Teorema de Shemesh e dos conceitos de subespaços invariantes de canais quânticos e canais quânticos não-ergódicos na Teoria da Informação Quântica Erro-Zero.

De forma mais específica, este trabalho de tese tem os seguintes objetivos:

- Apresentar uma condição para a capacidade erro-zero dos canais quânticos.
- Mostrar conexões entre o Teorema de Shemesh e o conceito de capacidade erro-zero dos canais quânticos;
- Verificar conexões entre os conceitos de capacidade erro-zero e subespaços invariantes dos canais quânticos;
- Discutir a relação entre os conceitos de capacidade erro-zero e canais quânticos não-ergódicos.

1.3 Contribuições e Produção Científica

As contribuições deste trabalho de tese, que o distinguem de outros trabalhos na literatura, estão listadas a seguir:

- Apresenta um teste para a capacidade de erro-zero dos canais quânticos, baseado nos estados próprios comuns dos operadores de Kraus que representam o canal quântico;
- Relaciona o Teorema de Shemesh com o conceito de capacidade de erro-zero de um canal quântico;
- Estuda as conexões entre os subespaços comuns invariantes de um canal quântico e a capacidade de erro-zero de um canal quântico;
- Discute resultados envolvendo a classe de canais quânticos não-ergódicos relacionados ao conceito de capacidade de erro-zero de um canal quântico.

Os resultados dessas contribuições foram publicados em congressos de abrangência nacional e internacional, e também serão publicados em um periódico da área. São os seguintes:

- M. M. de Oliveira e F. M. Assis, "Uma conjectura: o teorema de Shemesh e a capacidade erro-zero de canais quânticos com dois operadores de kraus,"em Anais do XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, 2022, doi: 10.14209/sbrt.2022.1570824539.
- M. M. de Oliveira, F. M. de Assis and M. A. Dias, "A condition for the zero-error capacity of quantum channels,"em Anais do XLI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, 2023, doi: 10.14209/sbrt.2023.1570917602.
- M. M. de Oliveira, A. da Silva, M. A. Dias e F. M. de Assis, "Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels,"aceito no VII Workshop Escola de Computação e Informação Quântica - WECIQ, 21 a 23 de agosto de 2024, Rio de Janeiro-RJ.
- M. M. de Oliveira, A. da Silva, M. A. Dias e F. M. de Assis, "Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels,"XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais De 01 a 04 de outubro de 2024, Belém - PA.

  Trabalho publicado:

- M. M. de Oliveira, M. A. Dias, A. da Silva and F. M. de Assis, "Shemesh Theorem and its Relation with the Zero-Error Quantum Information Theory,"*IEEE Access*, 09 December 2024, doi: 10.1109/ACCESS.2024.3514518.

1.4 Organização do Documento

Este documento está dividido em oito capítulos. No capítulo de introdução, são abordadas as motivações e os objetivos deste trabalho de tese. No Capítulo 2, faremos uma introdução aos conceitos da Mecânica Quântica. O Capítulo 3 apresentará tópicos referentes à Teoria da Informação, nos quais serão definidos os conceitos de Teoria da Informação Clássica, como entropia, entropia relativa, informação mútua e capacidade ordinária de canais clássicos. Ainda neste capítulo, será apresentada uma fundamentação básica da Teoria da Informação Quântica, contemplando os conceitos de entropia, entropia relativa e informação mútua; por fim, será apresentada uma caracterização dos canais quânticos. No Capítulo 4, será feita uma discussão sobre a Teoria da Informação Clássica Erro-Zero e a Teoria da Informação Quântica Erro-Zero, destacando o conceito de capacidade de erro-zero dos canais quânticos e condições matemáticas para que os canais quânticos possuam capacidade erro-zero positiva. O Capítulo 5 será dedicado a apresentar uma condição de capacidade erro-zero dos canais quânticos, baseada em estados próprios comuns aos operadores de Kraus que representam o canal quântico. O Capítulo 6 apresentará o Teorema de Shemesh e a sua generalização, além das conexões deste com o conceito de capacidade erro-zero dos canais quânticos. No Capítulo 7, discutiremos algumas conexões entre os conceitos de capacidade erro-zero e subespaços invariantes dos canais quânticos. Essa discussão será realizada em duas etapas: a primeira etapa contempla uma discussão particular, e a segunda etapa contempla o caso geral. O Capítulo 8 tratará dos canais quânticos não-ergódicos e da relação dessa classe de canais com o conceito de capacidade erro-zero dos canais quânticos. No Apêndice A, serão recomendados teoremas básicos de Álgebra Linear e da PI-Álgebra que serão utilizados ao longo desta tese.

Capítulo 2

Introdução à Mecânica Quântica

Neste introdução à Mecânica Quântica, apresentamos uma discussão básica dos conceitos de representação da informação, processamento da informação e medição da informação. Dividimos essas temáticas em seções, cujas disposições estão apresentadas da seguinte maneira: a Seção 2.1 é destinada a discutir o conceito de representação da informação; na Seção 2.2, introduzimos o conceito de processamento da informação; e, na Seção 2.3, apresentamos uma discussão sobre a medida da informação.

Na construção desta introdução, utilizamos como referências base os livros de Chuang [5], Wilde [12] e Jordan [31], além das teses de doutorado de Guedes [8] e de Dias [32].

2.1 A Representação da Informação

A unidade básica de informação clássica é o *bit* clássico ou *bit*, que assume dois valores lógicos 0 (falso) ou 1 (verdadeiro). A representação de uma informação é feita por meio da sua codificação em uma sequência finita de *bits*.

Por outro lado, o *bit* quântico, ou *qubit* é a unidade básica de informação quântica. Esta informação é descrita por um vetor de estado em um sistema de mecânica quântica de dois níveis. Matematicamente, um *bit* quântico é representado por um vetor $|\psi\rangle$[1] de um espaço vetorial complexo de dimensão dois. A seguir, apresentamos a definição de *qubit* e uma introdução ao conceito de sistemas quânticos de múltiplos *qubits*.

Definição 2.1 (Qubit) *Seja $\mathcal{H}$ um espaço vetorial complexo de dimensão 2, o qual é um espaço de Hilbert. Definimos um qubit $|\psi\rangle$ em $\mathcal{H}$ como sendo um vetor vetor unitário*

[1] Quando escrevemos um vetor com a notação $|\cdot\rangle$, dizemos que ele está escrito na notação de Dirac, a qual é a notação padrão para estados na mecânica quântica e foi discutida no Apêndice A.1.2 deste trabalho.

em $\mathbb{C}^2$*, cuja expressão geral é dada por*

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

em que $\alpha, \beta \in \mathbb{C}$ *tais que*

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

Nesta Definição 2.1, os números complexos α e β são chamados amplitudes de probabilidade e, na mecânica quântica, significa que, ao medir um *qubit* ou obtemos o resultado 0, com probabilidade $|\alpha|^2$, ou obtemos 1, com probabilidade $|\beta|^2$. Nos casos em que os valores de α e β são simultaneamente diferentes de zero ($\alpha, \beta \neq 0$), dizemos também que o estado está em superposição dos estados $|0\rangle$ e $|1\rangle$. Quando um *qubit* está em superposição, não é possível afirmar se este *qubit* está em $|0\rangle$ ou $|1\rangle$. Os estados $|0\rangle$ e $|1\rangle$ são chamados de estados da base computacional de $\mathcal{H}$ sobre $\mathbb{C}$, a qual é uma base ortonormal para este espaço vetorial e podemos representar essa base como

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{2.3}$$

e, em geral, um *qubit* $|\psi\rangle$ pode ser escrito da seguinte forma

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle && (2.4)\\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} && (2.5)\\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. && (2.6) \end{aligned}$$

Uma observação importante a respeito das unidades básicas da informação clássica e quântica é que enquanto o *bit* somente pode assumir dois valores distintos, 0 (falso) ou 1 (verdadeiro), o *qubit* pode assumir infintos estados, contanto que os números complexos α e β, da Equação 2.1 satisfaçam a condição $|\alpha|^2 + |\beta|^2 = 1$.

Na Computação e Comunicação Clássicas, um *bit* pode representar somente dois valores lógicos, enquanto n *bits* podem representar 2^n valores lógicos diferentes, sendo apenas um valor por vez. Pouco podemos fazer na Computação e Comunicação Clássicas com um único *bit*, por isso quase sempre é necessário usar sistemas de n *bits* para desenvolver os processos. De modo análogo, na Computação e Comunicação Quânticas, há sempre a necessidade de trabalhar com n *qubits*. Semelhantemente à Computação e Comunicação Clássicas, n *qubits* pode representar 2^n valores diferentes, no entanto, graças a superposição, na Computação e Comunicação Quânticas, todos 2^n valores podem ser representados simultaneamente.

Os sistemas de múltiplos *qubits* são produtos tensoriais[2] de *qubits*. Assim, suponha que $|\psi\rangle$ seja um estado de 2 *qubits*, então a representação geral de $|\psi\rangle$ é dada por

$$
\begin{aligned}
|\psi\rangle &= |\alpha\rangle \otimes |\beta\rangle && (2.7)\\
&= (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) && (2.8)\\
&= a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle && (2.9)\\
&= a_{00} |00\rangle + a_{01} |01\rangle + b_{10} |10\rangle + b_{11} |11\rangle && (2.10)\\
&= a'_0 |0\rangle + a'_1 |1\rangle + a'_2 |2\rangle + a'_3 |4\rangle && (2.11)\\
&= \sum_{i=0}^{2^2-1} a'_i |i\rangle . && (2.12)
\end{aligned}
$$

Observe que o estado $|\psi\rangle$ de dois *qubits*, contém os estados $|0\rangle, |1\rangle, |2\rangle$ e $|3\rangle$ simultaneamente, cada um deles com amplitude a'_i, respectivamente. Observe ainda que, se todas as amplitudes a'_i forem não nulas, então o estado $|\psi\rangle$ está em superposição dos estados $|0\rangle, |1\rangle, |2\rangle$ e $|3\rangle$.

De modo geral, podemos denotar um estado de n *qubits* por

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle \tag{2.13}$$

em que $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$ e $\{|0\rangle, |1\rangle, ..., |2^n - 1\rangle\}$ é a base computacional.

2.2 O Processamento da Informação

O processamento da informação quântica é realizado por meio de operadores lineares. De maneira formal, podemos definir isso como segue.

Definição 2.2 (Operador Quântico) *A evolução de um sistema quântico isolado, originalmente no $|\psi\rangle$, para o estado $|\psi'\rangle$, é dada por meio de um operador quântico unitário U, isto é,*

$$|\psi'\rangle = U |\psi\rangle . \tag{2.14}$$

Os operadores quânticos são unitários, pois preservam a norma dos vetores, e devem possuir a seguinte propriedade

$$U^\dagger U = U U^\dagger = I. \tag{2.15}$$

[2]No Apêndice A.1.10, apresentamos o conceito de produto tensorial e algumas de suas propriedades.

em que † *é o conjugado transposto do operador* U *e* I *é a matriz identidade (Veja Definição A.15).*

No estudo da informação em sistemas quânticos, é mais comum utilizar operadores unitários que apresentam comportamento de portas quânticas análogas ao modelo clássico de computação. No universo possível de operadores unitários na computação quântica, destacamos as matrizes de Pauli [3](A.20)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.16}$$

Dentre essas matrizes de Pauli, o operador X merece uma menção particular, visto que é o análogo quântico da porta NOT clássica. Por exemplo, que quando aplicamos $X \cdot |0\rangle = |1\rangle$ e $X \cdot |1\rangle = |0\rangle$, por isso a matriz X de Pauli recebe o nome de *bit flip*.

2.3 A Medida da Informação

Uma passagem pelas páginas iniciais do livro do Jordan [31], possibilita entender que uma medição é a única forma de obtermos informação sobre o mundo, e somente a partir dos dados colhidos podemos começar a formular teorias sobre o mundo que nos rodeia. No contexto de um sistema quântico isolado, já vimos que ele evolui conforme um operador unitário. Porém, para acessar o estado do sistema, é necessário realizar uma medição, a qual possibilita colher informações úteis sobre os estados do sistema após determinado processamento e, assim, poder formular teorias baseadas nas informações colhidas.

A realização da medição dos estados de um sistema quântico[4] não é uma tarefa simples. Esse processo interfere no sistema quântico isolado, ocasionando, após sua execução, o fenômeno conhecido como colapso ou redução dos estados do sistema.

A seguir apresentamos a definição da medição chamada de medição projetiva.

Definição 2.3 (Medição projetiva) *Seja o conjunto de projetores* M_m *que atuam sobre o espaço de estados de um sistema quântico. Então, sendo* $|\psi\rangle$ *o estado deste sistema*

[3]É interessante destacar que as matrizes de Pauli formam um grupo multiplicativo. O grupo de Pauli é o grupo de n *qubits*. Para um único qubit, o grupo de Pauli G_1 é definido como o conjunto de todas as matrizes de Pauli e fatores multiplicativos $\pm 1, \pm i$. Ou seja, $G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. Para ver mais detalhes sobre o grupo de Pauli sugerimos a leitura da Seção 10.5.1 [5].

[4][33] Após a medição, não há como restaurar o sistema ao estado anterior, tornando-a a única operação irreversível em um sistema quântico isolado.

quântico, imediatamente antes da medição, então a probabilidade $p(m)$ do resultado da aplicação dos operadores de medição resultar no índice de medição m é dada por

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{2.17}$$

e o estado $|\psi'\rangle$ deste sistema quântico após a medição é dado por

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.18}$$

Ainda neste capítulo, voltamos com mais detalhes sobre a medição projetiva.

2.4 O Operador Densidade

Os estados puros, também conhecidos como vetores unitários, são representados na base de um espaço de Hilbert. Esses estados refletem o mínimo de ignorância sobre o sistema, já que nada além do próprio estado precisa ser determinado. No entanto, há situações em que esse formalismo não é adequado. Em particular [8]:

1. Um sistema está em um dos estados puros $|\psi_1\rangle , |\psi_1\rangle , ..., |\psi_N\rangle$ com respectivas probabilidades, $p_1, p_2, ..., p_N$;
2. Um sistema, denominado A, é parte de um sistema maior AB.

Matematicamente, o operador densidade é usado para lidar com essa situação, sendo definido a seguir.

Definição 2.4 (Operador densidade) *Definimos o operador densidade $\hat{\rho}$ como as possíveis combinações dos estados quânticos $|\psi_1\rangle , |\psi_1\rangle , ..., |\psi_N\rangle$ com respectivas probabilidades $p_1, p_2, ..., p_N$ $(\sum_i p_i = 1)$ do sistema quântico estar no i-ésimo estado, tal que*

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i| . \tag{2.19}$$

O operador densidade é também designado por *matriz de densidade* do sistema. Uma caracterização para operador de densidade é dada no teorema a seguir.

Teorema 2.1 *Um operador $\hat{\rho}$ é operador densidade associado a um ensemble $\{p_i, |\psi_i\rangle\}$ se, e somente se, são satisfeitas as duas condições:*

1. *O traço do operador densidade é sempre unitário*[5], $\mathrm{tr}(\hat{\rho}) = 1$.

2. *O operador densidade* $\hat{\rho}$ *é positivo*[6].

Quando um sistema quântico se encontra em um único estado $|\psi\rangle$ conhecido, dizemos que o sistema é puro. Denotamos um sistema quântico puro em termos de operador densidade como $\hat{\rho} = |\psi\rangle\langle\psi|$. Quando o sistema quântico não se encontra em um único estado quântico, dizemos que o estado quântico $\hat{\rho}$ é uma mistura de operadores densidade, isto é, uma mistura de estados puros no agrupamento $\hat{\rho}$.

Para ilustrar o conceito de mistura de estados puros, suponhamos que um sistema quântico se encontra no estado ρ_j com probabilidade p_j. Pela Equação 2.19, podemos escrever $\rho_j = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, em que os estados $|\psi_i\rangle$, $i = 1, 2, ...N$ são estados puros. Ademais, vamos denotar por $\hat{\rho} = \sum_j p_j \rho_j$, o estado $\hat{\rho}$ que é uma mistura de estados ρ_j com probabilidade p_j.

2.5 Os Postulados da Mecânica Quântica

Postulado 2.1 (Espaço dos estados) *Associado a qualquer sistema quântico isolado, existe um espaço vetorial complexo com produto interno (isto é, um espaço de Hilbert)* $\mathcal{H}$*, chamado de espaço de estados do sistema. O sistema quântico é completamente descrito por um vetor de estado unitário no espaço de estados.*

É por meio de um operador unitário U que o sistema quântico fechado evolui. Assim, se o sistema inicialmente está no estado $|\psi_i\rangle$ com probabilidade p_i, então, após a atuação do operador unitário U, o sistema estará no estado $U|\psi_i\rangle$ com probabilidade p_i. Dessa forma, a evolução do sistema, mediante o operador densidade, é descrita pela expressão abaixo

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i| \stackrel{U}{=} \sum_i p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U\hat{\rho}U^\dagger. \tag{2.20}$$

Postulado 2.2 (Evolução do sistema quântico) *A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Um estado do sistema* $\hat{\rho}$ *no tempo* t_1 *evolui para o estado* $\hat{\rho}'$ *no tempo* t_2 *por meio de um operador unitário* U*, de modo que*

$$\hat{\rho}' = U\hat{\rho}. \tag{2.21}$$

[5]O traço é a soma dos elementos da diagonal principal da matriz.

[6]Dizemos que um $\hat{\rho}$ é operador positivo, se para todo $|u\rangle$ em um espaço de Hilbert $\mathcal{H}$, vale a condição $\langle u|\hat{\rho}|u\rangle \geq 0$.

A linguagem dos operadores densidade também descreve facilmente medições. Para ver isso, suponha que um conjunto de operadores $\{M_m\}$ descreva uma medição. Então, se o estado inicial do sistema era $|\psi_i\rangle$, a probabilidade de obter m após a medição é dada pela expressão[7]

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|). \tag{2.22}$$

Assim, a probabilidade de obter m, é dada por[8]

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \hat{\rho}) \tag{2.23}$$

em que $\hat{\rho} = |\psi_i\rangle\langle\psi_i|$. Além disso, se o estado inicial do sistema antes da medição era $|\psi_i\rangle$ e foi m o resultado da medição, então o estado que o sistema assume é dado pela expressão

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{p(m|i)}}, \tag{2.24}$$

ou ainda, de modo mais explicito

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}}. \tag{2.25}$$

Portanto, o operador densidade correspondente é dado por

$$\hat{\rho}_m = \frac{M_m \hat{\rho} M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \hat{\rho})}. \tag{2.26}$$

Postulado 2.3 (Medidas) *Medições projetivas são descritas por uma coleção de operadores de medição $\{M_m\}$, os quais atuam no espaço de estados do sistema que está sendo medido. Se o estado do sistema quântico se encontra no estado $\hat{\rho}$ imediatamente antes da medição, então a probabilidade de que seja obtido o resultado m como resultado da medição é dada pela expressão*

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \hat{\rho}), \tag{2.27}$$

e o sistema assumirá o estado

$$\hat{\rho}_m = \frac{M_m \hat{\rho} M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \hat{\rho})}. \tag{2.28}$$

Os operadores de medição devem satisfazer à relação de completude, $\sum_m M_m^\dagger M_m = I$.

[7] $p(m|i)$ significa a probabilidade de medir m, dado que o índice do estado inicial sistema era i.
[8] A expressão $p(m)$ é obtida conforme a Lei das probabilidades total.

Medição POVM

O Postulado 2.3 expressa dois procedimentos sobre medição. O primeiro trata das probabilidades associadas aos diferentes resultados da medição. O segundo elemento diz respeito à descrição do estado do sistema após a medição. Em algumas situações, o estado do sistema após a medição pode ter maior foco; em outras situações as probabilidades dos resultados possíveis após a medição podem ser mais interessante. Neste último caso, medições POVM's *(Positive Operator-Valued Measure)* são mais adequadas.

Para definirmos um POVM, considere o estado do sistema $|\psi\rangle$ e suponha que uma medição projetiva, que atua sobre $|\psi\rangle$, seja descrita pelos operadores de medição $\{M_m\}$. Ao efetuar a medição, a probabilidade de um certo índice m é dada pela expressão

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{2.29}$$

Definindo,

$$E_m \equiv M_m^\dagger M_m, \tag{2.30}$$

então, a partir do Postulado 2.3 e de conceitos da Álgebra Linear, é possível verificar que:

1. E_m é um operador positivo.
2. $\sum_m E_m = 1$.
3. $p(m) = \langle\psi| E_m |\psi\rangle$.

Definição 2.5 (POVM) *Definimos um POVM como sendo o conjunto $\{E_m\}$ dado na Equação 2.30, cujos elementos do POVM são os operadores E_m.*

A interação entre sistemas quânticos individuais produz sistemas quânticos compostos. O postulado a seguir determina que o espaço de estados do sistema composto é representado pelo produto tensorial de espaços de estados individuais.

Postulado 2.4 (Sistemas compostos) *O espaço de estados de um sistema quântico composto é representado pelo produto tensorial dos espaços de estados dos sistemas físicos que o compõem. Isto é, para n sistemas, onde o sistema i é preparado no estado $|\psi_i\rangle$, o sistema composto total é dado por $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.*

É importante destacar a importância que o Postulado 2.4 exerce na Mecânica Quântica, pois devido a este postulado, é possível definir o conceito de emaranhamento. Por definição, um sistema composto está emaranhado se não pudermos escrever o estado de todo o sistema como um produto tensorial dos estados de cada um dos sistemas individuais.

Capítulo 3

Tópicos em Teoria da Informação

Neste capítulo abordamos uma fundamentação básica da Teoria da Informação, na qual definimos as quantidades de entropia, entropia relativa e informação mútua, que são vistas como medidas razoáveis de informação. A partir dessas definições, apresentamos a capacidade de um canal de comunicação. Dividimos essa fundamentação em duas seções, cuja disposição está da seguinte forma: a Seção 3.1 é destinada a apresentar uma fundamentação da Teoria da Informação Clássica e a Seção 3.3 contempla uma discussão sobre a Teoria da Informação Quântica, com ênfase especial na definição e nas propriedades da capacidade erro-zero de canais quânticos.

Para a construção deste capítulo, utilizamos como referências: Chuang [5], Wilde [12] e Guedes *et al.* [19], além das teses de doutorado de Medeiros [11], Guedes [8] e Dias [32].

3.1 Teoria da Informação Clássica

Iniciaremos esta seção introduzindo o conceito de entropia, a qual é uma medida de incerteza de uma variável aleatória[1].

Definição 3.1 (Entropia) *Seja* X *uma variável aleatória discreta com alfabeto* $\mathcal{X}$ *e função densidade de probabilidade* $p(x) = P[X = x], x \in \mathcal{X}$. *Definimos a entropia de* X*, que denotamos por* $H(X)$*, como sendo*

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log(p(x)). \tag{3.1}$$

[1]Para mais detalhes sobre o conceito de variável aleatória, sugerimos a leitura do Capítulo 3 da referência [34].

Vamos considerar que o logaritmo é tomado na base 2 e que a entropia é expressa em termos de bits por símbolo. Admitiremos também que $0log(0) = 0$, o que se justifica pelo fato de que o limite $xlog(x) \to 0$ à medida que x se aproxima de zero, e mantendo a continuidade. É interessante destacar que a entropia não possui relação com os valores que a variável assume, depende apenas das probabilidades associadas a esses valores. Além disso, é importante notar que a entropia é uma medida positiva, isto é, $H(X) \geq 0$.

A definição de entropia pode ser ampliada para um par de variáveis aleatórias conjuntamente distribuídas. Essa extensão é chamada de entropia conjunta, a qual é definida a seguir.

Definição 3.2 (Entropia conjunta) *Sejam duas variáveis aleatórias X e Y com distribuição conjunta de probabilidades $p(x, y)$. Definimos a entropia conjunta, que denotamos por $H(X, Y)$, como sendo*

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y) log\, p(x,y). \tag{3.2}$$

Também definimos a entropia de uma variável aleatória, dada outra variável aleatória. Essa entropia é chamada de entropia condicional.

Definição 3.3 (Entropia condicional) *Sejam duas variáveis aleatórias X e Y com distribuição conjunta de probabilidades $p(x, y)$. Definimos a entropia de Y condicionada à X, que denotamos por $H(Y|X)$, como sendo*

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X}} p(x) H(Y|X=x) && (3.3)\\ &= -\sum_{x\in\mathcal{X}} p(x) \sum_{y\in\mathcal{Y}} p(y|X=x)\log(p(y|X=x)) && (3.4)\\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log(p(y|X=x)). && (3.5) \end{aligned}$$

A entropia relativa, também conhecida como distância de Kullback-Leibler, pode ser encarada como uma maneira de mensurar a ineficiência de se assumir a distribuição de probabilidade q, dado que a real distribuição utilizada é p.

Definição 3.4 (Entropia relativa) *Sejam duas funções massa de probabilidade $p(x)$ e $q(x)$. Definimos a entropia relativa entre essas duas funções, que denotamos por $D(p||q)$, como sendo*

$$D(p||q) = \sum_{x\in\mathcal{X}} p(x)\log\left(\frac{p(x)}{q(x)}\right). \tag{3.6}$$

É interessante destacar que, de acordo com a Definição 3.4 de entropia relativa, dado algum $x \in \mathcal{X}$ tal que $p(x) > 0$ e $q(x) = 0$, então temos que $D(p||q) = \infty$. Também é interessante mencionar que a entropia relativa é sempre não negativa e somente é zero quando $p = q$.

A informação mútua é outra medida bastante importante, pois esta informa qual a redução da incerteza de X, quando Y é conhecido, e vice-versa.

Definição 3.5 (Informação Mútua) *Sejam duas variáveis aleatórias X e Y com distribuição conjunta de probabilidade $p(x, y)$ e distribuições marginais $p(x)$ e $p(y)$. Definimos a informação mútua, que denotamos por $I(X;Y)$, como sendo a entropia relativa entre a distribuição conjunta e o produto das distribuições marginais*

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) && (3.7)\\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log\left(\frac{p(x,y)}{p(x)\cdot p(y)}\right). && (3.8) \end{aligned}$$

Nota

Pelas Equações (3.1), (3.2) e (3.5), podemos concluir que

$$H(X|Y) = H(X) + H(Y|X). \tag{3.9}$$

Além disso, a informação mútua é uma medida simétrica, ou seja,

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X). \tag{3.10}$$

Das Equações (3.9) e (3.10), obtemos que

$$I(X;Y) = H(X) + H(Y) - H(X,Y). \tag{3.11}$$

3.2 Capacidade Ordinária de Canais Clássicos

Para iniciar a discussão sobre Capacidade Ordinária de Canais Clássicos, tomamos como ponto de partida a apresentação de um modelo de um sistema de comunicações digitais ponto a ponto. Então, vamos supor que um emissor (Alice) deseje enviar uma mensagem M para um receptor (Bob), cujo modelo é ilustrado na Figura 1 a seguir.

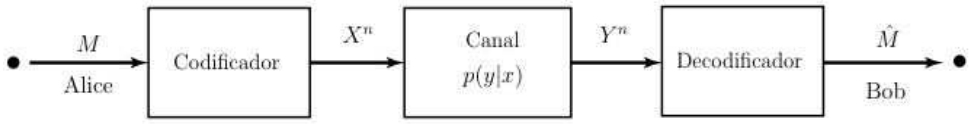


Figura 1: Modelo de um sistema de comunicações digitais ponto-a-ponto [1].

Neste modelo, o primeiro etapa é a codificação, na qual os símbolos da mensagem M são mapeados em símbolos do canal, formando uma palavra-código que é enviada pelo canal. O canal pode ser qualquer meio físico, como uma linha telefônica, o ar, a internet, entre outros.

Os dados que trafegam pelo canal estão sujeitos a distorções, ruído e interferências. Por conta disso, dizemos que a saída do canal é um mapeamento aleatório, cuja distribuição de probabilidade depende da sequência de entrada. A partir da sequência de saída do canal, tenta-se recuperar a mensagem M por meio de um processo de decodificação. Dizemos, então, que a comunicação entre Alice e Bob é bem-sucedida se Alice e Bob concordam com o que foi enviado.

Definição 3.6 (Canal discreto sem memória) *Sejam um alfabeto de entrada $\mathcal{X}$ e um alfabeto de saída $\mathcal{Y}$. Definimos um canal discreto sem memória (DMC) $W : \mathcal{X} \longrightarrow \mathcal{Y}$, que denotamos por $(\mathcal{X}, p(y|x), \mathcal{Y})$, como sendo uma matriz estocástica cujas linhas são indexadas por elementos do conjunto finito $\mathcal{X}$, enquanto que as colunas são indexadas por índices de $\mathcal{Y}$. O elemento (x, y) da matriz estocástica é a probabilidade $p(y|x)$ de receber $y \in \mathcal{Y}$, dado que $x \in \mathcal{X}$ é transmitido. Dizemos que o canal é discreto sem memória se a distribuição de probabilidade da saída depende somente da entrada naquele tempo e é condicionalmente independente de entradas ou saídas prévias.*

Na literatura é muito comum usar iniciais DMC para denotar o canal discreto sem memória, em virtude da escrita em inglês *DMC - Discrete Memoryless Channel*.

Definição 3.7 (Código clássico) *Um código de blocos (m, n) para um canal DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ é composto por:*

1. *Um conjunto de índices $M = \{1, ..., m\}$, em que cada índice está associado a uma mensagem clássica;*

2. *Uma função de codificação*

$$X^n : \{1, ..., m\} \longrightarrow \mathcal{X}^n$$

originando palavras-código $\boldsymbol{x}^1 = X^n(1), ..., \boldsymbol{x}^m = X^n(m)$.

3. Uma função de decodificação

$$g : \mathcal{Y}^n \longrightarrow \{1, ..., m\}$$

que mapeia cada palavra-código recebida numa mensagem do conjunto $\{1, ..., m\}$.

A taxa R do código é definida como sendo

$$R = \frac{1}{n} \log\ m \text{ (\textit{bits} por símbolo)}, \tag{3.12}$$

isto é, a razão entre o logaritmo do número de mensagens possíveis e o número de palavras-código existentes.

Ao enviar dados através do canal, estes estão sujeitos distorções, interferências e ruído. Devido a essas causas, a saída do canal é entendida como um mapeamento aleatório em que a distribuição de probabilidade depende da sequência de entrada. Em ou outras palavras, o canal pode introduzir erros, o que implica que a mensagem recebida possa ser diferente da mensagem original. Vamos, então, definir a probabilidade média de erro de decodificação como sendo

$$P_e = \frac{1}{m} \sum_{i \in M} \Pr(g(Y^n) \neq i \mid X^n = X^n(i)). \tag{3.13}$$

A definição de probabilidade média leva em consideração a ocorrência de erros quando todas as mensagens em M são equiprováveis. A partir desses conceitos, podemos definir quando uma taxa é alcançável.

Definição 3.8 (Taxa alcançável) *Vamos dizer que uma taxa R de transmissão de um código (m, n) é alcançável por um canal DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$, se existe uma sequência $(\lceil 2^{nR} \rceil, n)$ de códigos tal que, para $\epsilon > 0$, vale*

$$\lim_{n \to \infty} \inf\ R \ > \ R - \epsilon, \tag{3.14}$$

$$\lim_{n \to \infty}\ P_e \ < \ \epsilon. \tag{3.15}$$

A partir do conceito de taxas alcançáveis, é possível definir a capacidade ordinária de canais clássicos.

Definição 3.9 (Capacidade ordinária de um canal clássico) *Definimos a capacidade ordinária de um canal clássico, que denotamos pela letra C, como sendo o supremo de todas as taxas alcançáveis por um canal DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$. De forma simplificada, escrevemos,*

$$C = \sup\ \{R\ ;\ R \ \ \textit{alcançável}\}. \tag{3.16}$$

Nota

Shannon [4] mostrou que a capacidade ordinária de um canal DMC é dada por

$$C = \max_{p(x)} \; I(X;Y) \tag{3.17}$$

em que o máximo é tomado sobre todas as distribuições de entrada $p(x)$ possíveis, e $I(X;Y)$ é a informação mútua entre as variáveis aleatórias X e Y, que representam a entrada e a saída do canal DMC, respectivamente.

3.3 Teoria da Informação Quântica

Na Teoria da Informação Clássica, a entropia é uma função da distribuição de probabilidade que rege a variável aleatória e que informa uma "quantidade de incerteza"da distribuição. Uma vez que a incerteza é um conceito muito importante para a Teoria da Informação Quântica, medidas entrópicas ocupam um lugar de ampla importância [35]. Nos sistemas quânticos, os estados do sistema são "objetos probabilísticos", apresentando um tipo de distribuição de probabilidades por meio dos seus autovalores. Logo, a entropia de um sistema (que é uma medida de incerteza) é uma função do operador de densidade do sistema, seguindo os mesmos padrões da entropia de Shannon.

Definição 3.10 (Entropia de Von Neuman) *Seja ρ um estado do sistema quântico $\mathcal{H}$. A entropia $S(\rho)$ do estado é definida como sendo:*

$$S(\rho) = -\operatorname{tr}(\rho \log \rho). \tag{3.18}$$

Na Equação 3.18, o logaritmo é na base 2, além disso $0log0 = 0$. O logaritmo do operador densidade é calculado a partir da decomposição espectral $\rho = \sum_i \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ do operador densidade, em que $\log \rho = \sum_i \log \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$.

A entropia de von Neumann possui algumas propriedades interessantes que devem ser destacadas.

1. A entropia é não negativa ($S(\rho) \geq 0$). O valor $S(\rho) = 0$ se, e somente se, ρ é um estado quântico puro.

2. Em um espaço de Hilbert $\mathcal{H}$ de dimensão d, o máximo valor da entropia é $\log d$, correspondente ao estado $\rho = I/d$, que é o estado maximamente misturado do sistema.

3. Supondo que um sistema composto AB está num estado puro, então $S(A) = S(B)$;

4. Se os estados ρ_i tem suporte em subespaços ortogonais, então a entropia da mistura ρ será dada por

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i). \tag{3.19}$$

Definição 3.11 (Entropia conjunta) *Definimos a entropia conjunta $S(A, B)$ de um sistema composto AB como sendo:*

$$S(\rho_{AB}) = -\operatorname{tr}(\rho_{AB} \log \rho_{AB}), \tag{3.20}$$

em que ρ_{AB} é o operador densidade do sistema AB.

Definição 3.12 (Entropia quântica condicional) *Definimos a entropia quântica condicional $S(A|B)$ como sendo a diferença entre a entropia conjunta $S(\rho_{AB})$ e a entropia marginal $S(B) = S(\rho_B)$, isto é,*

$$S(A|B) = S(A, B) - S(B). \tag{3.21}$$

em que AB é um sistema quântico composto.

Definição 3.13 (Informação mútua quântica) *Sejam A e B dois sistemas quânticos. A informação mútua de von Neumann $S(A : B)$ para estes dois sistemas é definida por*

$$S(A : B) = S(A) + S(B) - S(A, B) \tag{3.22}$$

$$= S(A) - S(A|B) = S(B) - S(B|A), \tag{3.23}$$

É importante destacar que as definições de entropia conjunta, condicional e de informação mútua de von Neumann representa uma contrapartida quântica das medidas de informação na Teoria da Informação Clássica.

3.4 Uma Caracterização de Canais Quânticos

Seja um sistema quântico fechado ρ e um sistema aberto, denominado de *ambiente*. Suponha que ρ interaja com o ambiente e, após essa interação, ρ volte a ser fechado novamente. A evolução de um sistema quântico fechado ρ é completamente descrita pela atuação de operadores unitários. O estado do sistema após a interação é denotado por $\mathcal{E}(\rho)$. Porém, diferentemente do que ocorre em sistemas quânticos fechados, nem sempre

é o caso que $\mathcal{E}(\rho)$ pode ser relacionado ao estado inicial ρ por meio de operações unitárias [5].

O formalismo adequado para descrever esses cenários é o das operações quânticas. Esse formalismo é uma ferramenta geral para descrever a evolução de sistemas quânticos sob diversas circunstâncias, como mudanças estocásticas nos estados quânticos [5], [8].

Uma operação quântica pode ser vista como um mapa £ que atua no estado inicial da seguinte forma:

$$\sigma = \mathcal{E}(\rho). \tag{3.24}$$

As operações unitárias e medição são dois exemplos de operações quânticas. Uma operação quântica captura a mudança dinâmica de estado que ocorre como resultado de um processo físico. considerando ρ como o estado inicial antes do processo e $\mathcal{E}(\rho)$ como o estado final após a ocorrência do processo, este pode estar sujeito a um fator de normalização [5], [8].

Definimos uma operação quântica $\mathcal{E}$ como um mapa do conjunto de operadores de densidade do espaço de entrada $\mathcal{H}_1$ para o conjunto de operadores de saída $\mathcal{H}_2$, com três propriedades axiomáticas que devem ser respeitadas (considerando $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}$) [8]:

1. Supondo que ρ seja o estado inicial, então o valor $\operatorname{tr}\mathcal{E}(\rho)$ é a probabilidade de que o processo descrito por $\mathcal{E}$ ocorra. Ademais, $0 \leq \operatorname{tr}\mathcal{E}(\rho) \leq 1$ para qualquer estado inicial ρ.

2. O mapa $\mathcal{E}$ é linear e convexo no conjunto dos operadores de densidade. Ou seja, considerando as probabilidades p_i, é válido que:

$$\mathcal{E}\left(\sum_i p_i\sigma_i\right) = \sum_i p_i\mathcal{E}(\rho_i). \tag{3.25}$$

3. O mapa linear $\mathcal{E}$ é completamente positivo. Isso significa que, se $\mathcal{E}$ mapeia operadores do espaço $\mathcal{H}_1$ em operadores do espaço $\mathcal{H}_2$, então para qualquer operador positivo A, $\mathcal{E}(A)$ deve ser positivo.

Para um mapa linear $\mathcal{E}$ e levando em consideração as Propriedades 1, 2 e 3 apresentadas, pode-se apresentar o seguinte teorema, cuja prova é encontrada em Chuang [5].

Teorema 3.1 *Um mapa linear $\mathcal{E}$ satisfaz as Propriedades 1,2 e 3, se, e somente se,*

$$\mathcal{E}(\rho) = \sum_i E_i\rho E_i^\dagger \tag{3.26}$$

para um conjunto de operadores lineares E_i satisfazendo a condição $\sum_i E_i^\dagger E_i \leq I$.

A Equação 3.26 é conhecida como a representação da soma de operadores (OSR-*Operator-Sum Representation*) do canal quântico $\mathcal{E}$, e os operadores lineares $\{E_i\}$ são chamados de elementos de operação ou de operadores de Kraus[2].

Canais quânticos são modelados por operações quânticas que preservam o traço dos operadores de densidade. Isto é, canais quânticos são operações quânticas lineares, completamente positivas e que preservam o traço. Dessa forma, dado um operador de densidade ρ, tem-se que:

$$1 = \text{tr } \rho = \text{tr}\,\mathcal{E}(\rho) = \text{tr}\sum_i E_i \rho E_i^\dagger = \text{tr}\sum_i E_i^\dagger E_i \rho. \tag{3.27}$$

Como essa relação é válida para qualquer ρ, segue que

$$\sum_i E_i^\dagger E_i = I. \tag{3.28}$$

Definição 3.14 (Canal quântico) *Um canal quântico $\mathcal{E}$ é um mapa linear completamente positivo com preservação de traço que atua em um estado de entrada como segue:*

$$\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} E_i \rho E_i^\dagger \tag{3.29}$$

em que $\{E_i\}_{i=1}^{\kappa}$ satisfaz a relação $\sum_{i=1}^{\kappa} E_i^\dagger E_i = I$.

3.5 Capacidades Clássicas de Canais Quânticos

As características da Mecânica Quântica permitem que a capacidade de um canal quântico possa ser definida de várias formas, cada uma delas dependendo do tipo de informação a transmitir (informação clássica ou estados quânticos), das características físicas utilizadas na transição, como o emaranhamento, e do protocolo de comunicação utilizado [5]. Ilustramos isso apresentando as definições de duas capacidades para canais quânticos.

A Capacidade *one-shot*

Seja uma fonte quântica que emite estados ρ_i com probabilidades p_i. Suponhamos que, após cada emissão, seja realizada uma medição nos estados, e que as variáveis aleatórias X e Y sejam associadas, respectivamente, aos índices dos estados e às saídas das

[2]Para mais detalhes sobre o canal quântico com esses dois operadores de Kraus, veja [25].

medições. Definimos a informação acessível, que denotamos por I_{acc}, como sendo o máximo da informação mútua $I(X;Y)$, em que o máximo é tomado sobre todas as medições POVMs,

$$I_{acc} = \max_{M_m} I(X;Y). \tag{3.30}$$

Além disso, seja $\rho = \sum_i p_i \rho_i$. Definimos a quantidade de Holevo como sendo

$$\chi = S(\rho) - \sum_i p_i S(\rho_i). \tag{3.31}$$

É possível provar que vale $I_{acc} \leq \chi$, sendo que a igualdade somente acorre se os estados quânticos comutarem entre si [5].

Para definir a capacidade *one-shot*, consideramos a definição de canal quântico $\mathcal{E}(\cdot)$ caracterizado na Seção 3.4.

Definição 3.15 (Capacidade *one-shot*) *Definimos a capacidade one-shot de um canal quântico $\mathcal{E}(\cdot)$, que denotamos por $C_{1,1}(\mathcal{E})$, com sendo o máximo da informação acessível na saída de um canal quântico, em que o máximo é tomado sobre todas as famílias na entrada do canal. Matematicamente, podemos expressar isso como*

$$C_{1,1}(\mathcal{E}) = \max_{\{\rho_x, p_x\}} I_{acc_{out}} \tag{3.32}$$

em que $I_{acc_{out}}$ é a informação acessível da família $\{\mathcal{E}(\rho_x), p_x\}$.

A capacidade de Holevo-Schumacher-Westmoreland

No protocolo para envio de uma mensagem clássica por meio de canal quântico, escolhida aleatoriamente de um conjunto $\{1, ...2^{nR}\}$, é permitido que Alice prepare palavras-código como sendo produtos tensoriais e que Bob possa realizar medições coletivas na saída do canal. Então, a capacidade de Holevo-Schumacher-Westmoreland (HSW)de um canal quântico $\mathcal{E}(\cdot)$, que denotamos por $C_{1,\infty}(\mathcal{E})$, é dada pelo teorema a seguir:

Teorema 3.2 (Holevo-Schumacher-Westmoreland [13] [14]) *Seja um canal quântico $\mathcal{E}(\cdot)$. Então, a capacidade HSW é*

$$C_{1,\infty}(\mathcal{E}) \equiv \max_{\{p_i, \rho_i\}} \left[S\left(\mathcal{E}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i S(\mathcal{E}(\rho_i)) \right], \tag{3.33}$$

em que o máximo é tomado sobre todas as famílias $\{p_i, \rho_i\}$ de estados quânticos de entrada.

A demonstração do teorema faz uso da codificação aleatória e dos subespaços típicos. A demonstração detalhada pode ser encontrada em [5].

Capítulo 4

Tópicos em Teoria da Informação Erro-Zero

Este capítulo é dedicado a apresentar uma fundamentação elementar da Teoria da Informação Erro-Zero, na qual definimos capacidade erro-zero de canais clássicos e de canais quânticos, entre outros conceitos. Dividimos essa apresentação em duas seções, nas quais, na Seção 4.1 apresentamos uma discussão básica sobre temas da Teoria da Informação Clássica Erro-Zero e na Seção 4.2 fazemos uma fundamentação básica dos conceitos da Teoria da Informação Quântica Erro-Zero.

Para elaborar este capítulo, usamos como referências base os livros de Chuang [5], Gupta [22] e de Guedes *et al.* [19] e os artigos de Shannon [4], de Medeiros [10], [37] e de Medeiros *et al.* [21], além das teses de doutorado de Medeiros [11] e de Guedes [8].

4.1 Teoria da Informação Clássica Erro-Zero

Para apresentar alguns conceitos relacionados à Teoria da Informação Clássica Erro-Zero, vamos inicialmente definir código clássico erro-zero de um canal discreto sem memória - DMC W (Definição 3.6). Então, sendo um alfabeto de entrada $\mathcal{X} = \{x_1, x_2, ..., x_n\}$ e um alfabeto de saída $\mathcal{Y} = \{y_1, y_2, ..., y_m\}$, um DMC é uma aplicação de $\mathcal{X}$ em $\mathcal{Y}$ que é caracterizada por uma matriz estocástica cujas linhas são indexadas por elementos do conjunto finito $\mathcal{X}$, enquanto que as colunas são indexadas por índices de $\mathcal{Y}$. O elemento $(i, j) \in W$ é a probabilidade $p(y_j|x_i)$ que $y_j \in \mathcal{Y}$ seja recebido dado que $x_i \in \mathcal{X}$ é transmitido.

Definição 4.1 (Código clássico erro-zero) *Um código de blocos (m, n) de erro-zero para um canal DMC é composto por:*

1. *Um conjunto de índices* $M = \{1, ..., m\}$*, em que cada índice está associado a uma mensagem clássica.*

2. *Uma função de codificação*

$$X^n : \{1, ..., m\} \longrightarrow \mathcal{X}^n$$

originando palavras-código $\boldsymbol{x}^1 = X^n(1), ..., \boldsymbol{x}^m = X^n(m)$.

3. *Uma função de decodificação*

$$g : \mathcal{Y}^n \longrightarrow \{1, ..., m\}$$

que mapeia cada palavra-código recebida numa mensagem do conjunto $\{1, ..., m\}$*, com a seguinte propriedade*

$$\Pr(g(Y^n) \neq i \mid X^n(i)) = 0 \ \forall \ i \in \{1, ..., m\} \tag{4.1}$$

que garante a inexistência de erros de decodificação.

No contexto da inexistência de erros de decodificação, existe o interesse particular nos chamados símbolos não-adjacentes, isto é, símbolos que possam ser completamente distinguíveis na saída do canal clássico.

Definição 4.2 (Símbolos clássicos adjacentes) *Sejam* $\mathcal{X}$ *um alfabeto de entrada de um DMC e* $x_i, x_j \in \mathcal{X}$*. Dizemos que* x_i *e* x_j *são adjacentes (ou indistinguíveis) quando existe um* $y \in \mathcal{Y}$ *tais que* $p(y|x_i)$ *e* $p(y|x_j)$ *são maiores que zero. Caso contrário, dizemos que os símbolos* x_i *e* x_j *são ditos não-adjacentes (ou distinguíveis).*

Seja uma sequência $\mathbf{x} = x_1x_2...x_n$ transmitida pelo *DMC* W, tal que a sequência $\mathbf{y} = y_1y_2...y_n$ é recebida com probabilidade[1]

$$p^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i). \tag{4.2}$$

Se as duas sequências $\mathbf{x}'$ e $\mathbf{x}''$ podem resultar numa sequência $\mathbf{y}$ com probabilidade positiva, então dizemos que as sequências são adjacentes (ou indistinguíveis), visto que o decodificador não consegue fazer a distinção entre uma e outra sequência na saída do canal. Caso contrário, vamos dizer que as duas sequências são não-adjacentes (ou distinguíveis) na saída do canal.

[1]O produtório significa a ausência de memória do canal, como também a estacionariedade do mesmo, pois as probabilidades são advindas de uma mesma matriz.

Para reforçar a importância da distinguibilidade de sequências na saída do DMC W, vamos pensar na distribuição de probabilidades $p(\cdot|x)$ e $p^n(\cdot|\mathbf{x})$ como vetores de dimensão $|\mathcal{X}|$ e $|\mathcal{X}^n|$. Então, podemos afirmar que duas sequências $\mathbf{x}', \mathbf{x}'' \in \mathcal{X}$ são não-adjacentes (ou distinguíveis) na saída do DMC W se, e somente se, os vetores correspondentes $p^n(\cdot|\mathbf{x}')$ e $p^n(\cdot|\mathbf{x}'')$ são ortogonais. Ou equivalentemente, as sequências $\mathbf{x}'$ e $\mathbf{x}''$ são não-adjacentes (ou distinguíveis) se, e somente se, existe pelo menos um dos índices $i \leq i \leq n$, tal que x'_i e x''_i sejam não-adjacentes (ou distinguíveis).

$$\begin{array}{rcl} \mathbf{x}' & = & x'_1 x'_2 \ldots \boxed{x'_i} \ldots x'_{n-1} x'_n \\ \mathbf{x}'' & = & x''_1 x''_2 \ldots \boxed{x''_i} \ldots x''_{n-1} x''_n \end{array}$$

Figura 2: Duas sequências $\mathbf{x}'$ e $\mathbf{x}''$ são não-adjacente (ou distinguíveis), quando existe pelo menos um dos índices $i \leq i \leq$ é tal que x'_i e x''_i são não-adjacentes (ou distinguíveis) [19].

Considerando estes conceitos apresentados podemos definir a capacidade clássica erro-zero como segue:

Definição 4.3 (Capacidade clássica erro-zero [9]) *Seja $N(n)$ a cardinalidade máxima de um conjunto de vetores mutuamente ortogonais de $p^n(\cdot|\boldsymbol{x})$, com $\boldsymbol{x} \in \mathcal{X}^n$. Vamos definir a capacidade clássica erro-zero de um DMC W, como sendo*

$$C_0 = \lim_{n\to\infty} \sup \ \frac{1}{n} \log \ N(n). \tag{4.3}$$

Intuitivamente, a capacidade C_0 é a taxa máxima de informação que um DMC pode transmitir sem erro.

O número $N(n)$ é super multiplicativo, ou seja, $N(n+m) \leq N(n) \cdot N(m)$ e o limite superior coincide com o supremo (em n) dos números $\frac{1}{n} \log \ N(n)$.

Nota

Shannon [4] reformulou o problema de determinar a capacidade erro-zero de um canal em termos da Teoria dos Grafos. Sendo um canal DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ é possível construir um grafo característico G como segue: tome tantos vértices quanto for o número de símbolos em $\mathcal{X}$ e conecte dois vértices se os símbolos correspondentes são não-adjacentes (ou distinguíveis). Defina o n-ésimo produto de Shannon de G como sendo um grafo para o qual $V(G^n) = \mathcal{X}^{\times n}$ e $\{\mathbf{x}', \mathbf{x}''\} \in E(G^n)$ se para pelo menos um i, $1 \leq i \leq n$ as i-ésimas coordenadas de $\mathbf{x}'$ e $\mathbf{x}''$ satisfazem $\{\mathbf{x}'_i, \mathbf{x}''_i\} \in E(G)$. Ademais, é possível verificar que o

número máximo de seqüências não-adjacentes (ou distinguíveis) de comprimento n é o número de cliques de G^n, denotado por $\omega(G)$ ou seja, que $N(m) = \omega(G^n)$. Portanto, a capacidade clássica erro-zero de um DMC, em termos de grafo característico, é definida como sendo

$$C_0 = \sup_m \ \frac{1}{n} \log \ \omega(G^n). \tag{4.4}$$

Para ver maiores detalhes e exemplos ilustrando essa definição, sugerimos o leitor ver a Subseção 2.2.1, referência [8] e a Subseção 2.1.1, referência [11].

4.2 Teoria da Informação Quântica Erro-Zero

Sendo uma subárea da Teoria da Informação Quântica, a Teoria da Informação Quântica Erro-Zero objetiva o estudo e a proposição de técnicas, protocolos e medidas para a transmissão de informação clássica por canais quânticos ruidosos, livres de erros de decodificação. O ano de 2005 marca o primeiro trabalho envolvendo a Teoria da Informação Quântica Erro-Zero, mais especificamente o trabalho intitulado *Quantum Zero-Error Capacity* [19], dos pioneiros da área Medeiros e Assis, que propuseram uma extensão dos conceitos de capacidade erro-zero de canais clássicos, propostos por Shannon [4], para canais quânticos. Três anos depois, Medeiros [11], em sua Tese de Doutorado, orientado por Assis, avançou mais em trabalhos transpondo conceitos da Teoria da Informação Clássica Erro-Zero, proposta por Shannon [4], para o cenário quântico. Na sua tese, Medeiros estabeleceu condições necessárias para realizar o envio de informação clássica por canais quânticos ruidosos, livres de erros de decodificação.

Nesse sentido, dado um canal quântico, desejamos saber qual o máximo de informação clássica que pode ser transmitida por esse canal quântico com uma probabilidade exatamente igual a zero. Para este propósito, vamos supor um canal quântico $\mathcal{E} \equiv \{E_i\}_{i=1}^{\kappa}$ sobre um espaço Hilbert $\mathcal{H}$, d-dimensional, modelado por um mapa linear completamente positivo com preservação de traço. Além disso, vamos denotar por $\mathcal{S} = \{\rho_1, ..., \rho_\ell\}$, um subconjunto finito de $\mathcal{H}$, constituído por estados quânticos, em que os ρ_i são denominados de estados de entrada do canal quântico.

A ideia de um protocolo quântico de comunicações erro-zero tem início com um emissor (Alice) escolhendo uma mensagem de um conjunto de m mensagens clássicas $\{1, ..., m\}$. Essas mensagens são mapeadas pelo codificador em um produto tensorial de n estados quânticos de $\mathcal{S}$, gerando um estado pertencente ao espaço de Hilbert $\mathcal{H}^n$, e é chamado de palavra-código quântica. O estado palavra-código quântica é enviado pelo canal ruidoso $\mathcal{E}$. O receptor (Bob) realiza uma medição coletiva com um POVM no

estado recebido. As saídas da medição são os argumentos para a função de decodificação. O decodificador tem que decidir qual mensagem foi enviada por Alice, considerando que erros não são permitidos [11], [19], [8]. Este protocolo de comunicações quântico erro-zero é sintetizado na Figura 4, a seguir.

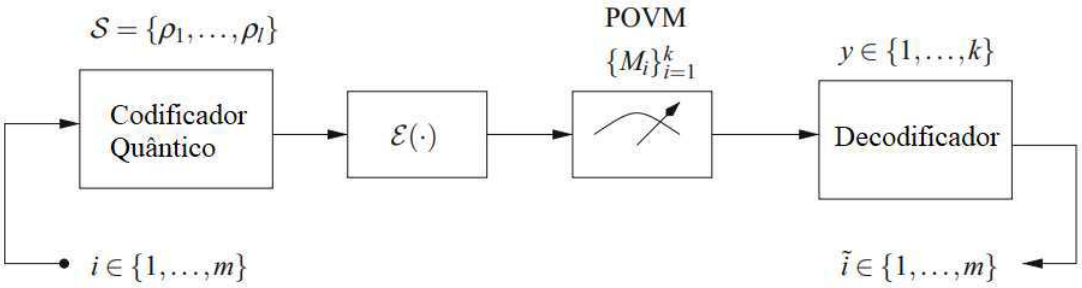


Figura 3: Protocolo de comunicações quântico erro-zero [11].

Levando em consideração essas discussões, vamos definir um código quântico de erro-zero da seguinte forma:

Definição 4.4 (Código quântico erro-zero) *Um código quântico* (m, n) *erro-zero para um canal quântico* $\mathcal{E}$ *é composto por:*
1. Um conjunto de índices $\{1, ..., m\}$*, em que cada índice está associado a uma mensagem clássica;*
2. Uma função de codificação

$$X^n : \{1, ..., m\} \longrightarrow \mathcal{S}^{\otimes n} \tag{4.5}$$

levando às palavras-código quânticas $X^n(1) = \overline{\rho}_1, ..., X^n(m) = \overline{\rho}_m$;
3. Uma função de decodificação

$$g : \{1, ..., k\} \longrightarrow \{1, ..., m\} \tag{4.6}$$

que associa deterministicamente uma mensagem a um dos possíveis resultados de medição $y \in \{1, ..., k\}$ *realizado pelo POVM* $\{M_i\}_{i=1}^k$*. Além disso, a função de decodificação possui a propriedade seguinte:*

$$\Pr(g(Y^n = y) \neq i \mid X^n(i)) = 0 \ \forall \ i \in \{1, ..., m\}. \tag{4.7}$$

A taxa deste código é dada por $R_n = \frac{1}{n} \log\ m$, *bits* por uso do canal.

O conceito de código quântico erro-zero possibilita que apresentemos a definição de capacidade quântica de erro-zero (QZEC - *Quantum Zero-Error Capacity*).

Definição 4.5 (Capacidade erro-zero dos canais quânticos[11]) *Definimos a capacidade erro-zero de um canal quântico, $\mathcal{E}(\cdot)$, que denotamos por $C^{(0)}(\mathcal{E})$, como sendo o maior limite superior das taxas alcançáveis com probabilidade de erro de decodificação igual a zero,*

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \ \sup_{n} \ \frac{1}{n} \log \ m \tag{4.8}$$

em que m é o número máximo de mensagens clássicas que o sistema pode transmitir sem erro quando um código de bloco quântico de erro-zero (m, n) e o alfabeto de entrada é $\mathcal{S}$.

Estamos interessados em situações em que a capacidade clássica de erro-zero de um canal quântico é não trivial ou positiva. Há uma relação entre a capacidade erro-zero positiva dos canais quânticos e a garantia de que pelo menos dois estados quânticos na saída do canal quântico sejam não-adjacentes (ou distinguíveis). Assim, vamos formalizar o conceito de adjacência e não-adjacência de estados quânticos.

Definição 4.6 (Estados quânticos adjacentes) *Sejam $\rho_i, \rho_j \in \mathcal{S}$ com $i \neq j$, então dizemos que ρ_i e ρ_j são não-adjacentes (ou distinguíveis) na saída do canal quântico $\mathcal{E}$ se $\mathcal{E}(\rho_i)$ e $\mathcal{E}(\rho_j)$ pertencem a subespaços ortogonais. Caso contrário, dizemos que ρ_i e ρ_j são adjacentes (ou indistinguíveis) na saída de $\mathcal{E}$.*

Vamos usar a notação $\rho_i \perp_{\mathcal{E}} \rho_j$ para denotar que os estados quânticos ρ_i e ρ_j são não-adjacentes (ou distinguíveis). Além disso, sendo duas sequências de produtos tensoriais $\hat{\rho}_i = \rho_{i,1} \otimes ... \otimes \rho_{i,n}$ e $\hat{\rho}_j = \rho_{j,1} \otimes ... \otimes \rho_{j,n}$, então vamos dizer que $\hat{\rho}_i$ e $\hat{\rho}_j$ são não-adjacentes (ou distinguíveis), o que denotamos por $\hat{\rho}_i \perp_{\mathcal{E}} \hat{\rho}_j$, se existe pelo menos um $\rho_{i,k} \perp_{\mathcal{E}} \rho_{j,k}$, $1 \leq k \leq n$.

$$\begin{aligned} \mathcal{E}(\hat{\rho}_i) &= \mathcal{E}(\rho_{i_1}) \otimes \cdots \otimes \mathcal{E}(\rho_{i_k}) \otimes \cdots \otimes \mathcal{E}(\rho_{i_n}) \\ \mathcal{E}(\hat{\rho}_j) &= \mathcal{E}(\rho_{j_1}) \otimes \cdots \otimes \mathcal{E}(\rho_{j_k}) \otimes \cdots \otimes \mathcal{E}(\rho_{j_n}) \end{aligned}$$

Figura 4: Dois estados quânticos $\hat{\rho}_i$ e $\hat{\rho}_j$ são não-adjacentes (ou distinguíveis) na saída de um canal $\mathcal{E}$, se existe pelo menos um $\rho_{i,k} \perp_{\mathcal{E}} \rho_{j,k}$, $1 \leq k \leq n$ [11].

A seguir, apresentaremos uma condição para que um canal quântico tenha capacidade erro-zero positiva. Essa condição, juntamente com sua demonstração matemática, pode ser encontrada em [10].

Teorema 4.1 ([10]) *Seja $\mathcal{S} = \{\rho_1, ..., \rho_\ell\}$, $\mathcal{S} \subset \mathcal{X}$ um conjunto de estados quânticos, e seja $\mathcal{P} = \{M_1, ..., M_m\}$ um POVM, em que $m \geqslant \ell$ e tais que $\sum_{j=1}^{m} M_j = \mathbb{I}$. Considere os*

subconjuntos

$$A_k = \{j \in \{1, ..., m\}; \mathrm{tr}[\sigma_k M_j] > 0\};\ k \in \{1, ..., \ell\}, \tag{4.9}$$

com $\sigma_k = \mathcal{E}(\rho_k)$. *Então, o canal quântico* $\mathcal{E}$ *possui uma capacidade positiva (ou não trivial) se, e somente se, existir um conjunto* $\mathcal{S}$ *e um um POVM* $\mathcal{P}$ *tal que, para pelo menos um par* $(i, j) \in \{1, ..., \ell\}^2$, *com* $i \neq j$, *os subconjuntos* A_i *e* A_j *são disjuntos.*

Os estados quânticos ρ_i e ρ_j são ditos não-adjacentes (ou distinguíveis) em $\mathcal{E}$ para o POVM $\mathcal{P}$.

Prova: Seja $\rho_i, \rho_j \in \mathcal{S}$ tais que os subconjuntos A_i e A_j são disjuntos para um determinado POVM $\mathcal{P}$. Então, é possível construir um código de bloco quântico para mapear duas mensagens clássicas nos estados ρ_i e ρ_j. Ademais, a taxa deste código é igual a 1, e, portanto, $C^{(0)}(\mathcal{E}) \geq 1$, isto é, o canal quântico tem capacidade erro-zero positiva.

Por outro lado, suponha que $C^{(0)}(\mathcal{E})$ é positiva. Então, pelo menos dois estados quânticos ρ_i e ρ_j de um determinado $\mathcal{S}$ são não-adjacentes (ou distinguíveis) em relação ao POVM $\mathcal{P}$, ou seja, A_i e A_j são subconjuntos disjuntos.

□

No artigo [21], os autores apresentam outro resultado para garantir que um canal quântico tem capacidade erro-zero positiva. No resultado, foi mostrado que um canal $\mathcal{E}$ possui capacidade erro-zero positiva quando estados de entrada escolhidos não-adjacentes são levados pelo canal a espaços vetoriais ortogonais, considerando o produto interno de Hilbert-Schmidt.[2] Segue o resultado:

Teorema 4.2 ([21]) *Seja um canal quântico* $\mathcal{E}$ *com operadores de Kraus* E_i. *Dois estados de entrada* $\rho_1, \rho_2 \in \mathcal{S}$ *são não-adjacentes para um dado POVM* $\mathcal{P} = M_1, ..., M_m$ *se, e somente se, os respectivos* $\mathcal{E}(\rho_1)$ *e* $\mathcal{E}(\rho_2)$ *pertencem a subespaços vetoriais ortogonais, ou seja,* $\mathrm{tr}[\mathcal{E}(\rho_1)\mathcal{E}(\rho_2)] = 0$.

Este resultado, cuja demonstração matemática é uma consequência direta da Definição 4.5, pode ser encontrado na [21, Proposição 3] e é utilizado para verificar a capacidade erro-zero do canal de despolarização.

Exemplo 4.1 ***(Canal de despolarização [19])*** *O canal de despolarização em um espaço de Hilbert com dimensão d atua sobre um estado de entrada* ρ *da seguinte forma:*

[2] O produto interno de Hilbert-Schmidt entre dois operadores A e B é o produto interno definido pelo traço, $\langle A, B\rangle = \mathrm{tr}[A^\dagger B]$, em que $A^\dagger$ é o conjugado transposto de A.

$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{1}{d}I \tag{4.10}$$

com $0 < p < 1$ *e* I *a matriz identidade de dimensão* d*. Um estado quântico de entrada* ρ *pode ser transmitido intacto com probabilidade* $1-p$ *ou é trocado por um estado completamente misto com probabilidade* p*.*

Para calcular a capacidade erro-zero desse canal, basta verificar se dois estados quaisquer distintos são distinguíveis na saída do canal, isto é,

$$\operatorname{tr}[\mathcal{E}(\rho_i)\mathcal{E}(\rho_j)] = \operatorname{tr}\left[\left((1-p)\rho_i + p\frac{1}{d}I\right)\left((1-p)\rho_j + p\frac{1}{d}I\right)\right] \tag{4.11}$$

$$= \operatorname{tr}\left[(1-p)^2\rho_i\rho_j + (1-p)\rho_i\frac{1}{d}I + (1-p)\rho_j\frac{1}{d}I + \frac{p^2}{d^2}I\right] \tag{4.12}$$

$$= (1-p)^2\operatorname{tr}[\rho_i\rho_j] + \frac{p(1-p)}{d}\operatorname{tr}(\rho_i+\rho_j) + \frac{p^2}{d^2} > 0, \tag{4.13}$$

em que $0 < p < 1$*. Logo, a capacidade erro-zero do canal de despolarização* $\mathcal{E}$ *é igual a zero, ou seja,* $C^{(0)}(\mathcal{E}) = 0$*.*

Para calcular a capacidade erro-zero do canal *Phase Flip*, vamos primeiramente apresentar a seguinte definição.

Definição 4.7 (Mapa ótimo) *Seja um conjunto* $\mathcal{S} = \{\rho_1, ..., \rho_\ell\}$ *e* $\mathcal{P} = \{M_1, ..., M_m\}$ *um POVM . Dizemos que* $(\mathcal{S},\ \mathcal{P})$ *é um mapa ótimo para um canal quântico* $\mathcal{E}$ *se a capacidade erro-zero é alcançada com* $(\mathcal{S},\ \mathcal{P})$*.*

Existe uma relação entre a capacidade de erro-zero e o ponto fixo do canal quântico $\mathcal{E}$, a qual apresentamos no teorema abaixo. Ademais, dizemos que um estado quântico ρ é *ponto fixo* para um canal quântico $\mathcal{E}$, se $\mathcal{E}(\rho) = \rho$. O teorema do ponto fixo de Schauder's [36, Teorema 2.3.7] garante que todo canal quântico possui pelo menos um ponto fixo.

Teorema 4.3 ([10]) *Seja* $\mathcal{E}$ *um canal quântico com* N_f *pontos fixos. Então, a capacidade erro-zero de* $\mathcal{E}$ *é pelo menos* $\log N_f$*.*

A demonstração matemática do resultado pode ser encontrada em [10, Proposição 2].

Exemplo 4.2 ***(Phase Flip [5])*** *O canal Phase Flip em um espaço de Hilbert de dimensão 2, cuja caracterização é dada pelos elementos de operação*

$$E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad E_2 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.14}$$

Matematicamente, esse canal tem probabilidade p de levar um qubit intacto até a saída e probabilidade $1-p$ *de trocar a sua fase. O canal phase flip possui dois pontos fixos, que são os estados* $\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle$ *. Para ver isso, observe que se*

$$|\psi_0\rangle = |0\rangle \qquad e \qquad |\psi_1\rangle = |1\rangle\,, \tag{4.15}$$

então $\mathcal{E}(|0\rangle\langle 0|) = |0\rangle$ *e* $\mathcal{E}(|1\rangle\langle 1|) = |1\rangle$ *. Observando a Proposição 4.3 e que a dimensão do espaço de Hilbert é 2, concluímos que*

$$C^{(0)}(\mathcal{E}) = \frac{1}{1}\log(2) = 1 \tag{4.16}$$

para um mapa $(\mathcal{S}, \mathcal{P})$ *ótimo dado por*

$$\mathcal{S} = \{|0\rangle\,, |1\rangle\} \quad e \quad \mathcal{P} = \{E_1 = |0\rangle\langle 0|\,,\ E_2 = |1\rangle\langle 1|\}. \tag{4.17}$$

A capacidade foi encontrada para $n = 1$*. Isso significa que podemos transmitir um bit por uso do canal com probabilidade de erro-zero igual a 1.*

Exemplo 4.3 ***(Amplitude Damping [5])*** *Dado um qubit na entrada do canal, a saída é dada por*

$$\mathcal{E}(\rho) = E_1\rho E_1^\dagger + E_2\rho E_2^\dagger \tag{4.18}$$

em que

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \quad e \quad E_2 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \tag{4.19}$$

Matematicamente, se um qubit está em $|0\rangle$*, então ele é levado intacto pelo canal, porém, se um qubit possui uma componente no estado* $|1\rangle$*, então o canal atenua sua amplitude. Ademais, a capacidade erro-zero desse canal é igual a zero. Para ver isso, é suficiente ver que, num espaço de Hilbert de dimensão 2, não é possível distinguir perfeitamente entre um estado puro e um estado misto*[3]*.*

Uma outra condição de capacidade erro-zero de um canal quântico é apresentada no trabalho citado em [22]. Essa condição, juntamente com a demonstração matemática, está reproduzida no teorema a seguir.

[3][37] **Corolário 1** *Num espaço de Hilbert de dimensão dois, não é possível distinguir perfeitamente entre um estado puro* $|\psi\rangle$ *e um estado misto* ρ*.*
A única entrada desse canal que resulta em um estado puro na saída é o estado fixo $|0\rangle$. Dessa forma, quaisquer dois estados quânticos puros distintos aplicados na entrada do canal produzirão, na saída, ou um estado puro (caso $|0\rangle$ seja usado) e um estado misto, ou dois estados mistos.

Teorema 4.4 ([22]) *Seja um canal quântico $\mathcal{E}$ com operadores de Kraus $\{E_i\}$. Sendo $|\psi_m\rangle \neq |\psi_{m'}\rangle$ para $m \neq m'$ estados de entrada no canal, então a capacidade erro-zero do canal $\mathcal{E}$ é positiva se, e somente se, $|\psi_{m'}\rangle\langle\psi_m|$, para $m \neq m'$, for ortogonal ao subespaço*

$$S := \text{span}\{E_i^\dagger E_j,\ i,j\} \tag{4.20}$$

com a ortogonalidade definida em termos do produto interno de Hilbert-Schmidt.

Prova: Como os estados $\{\mathcal{E}(\rho_m)\}$ são operadores semi-definidos positivos, então sendo ρ_m e $\rho_{m'}$ ortogonais, implica-se que

$$\text{tr}[\mathcal{E}(\rho_m)\mathcal{E}(\rho_{m'})] = 0,\ \forall\ m \neq m'. \tag{4.21}$$

Suponha uma representação de Kraus particular para $\mathcal{E}$, então $\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} E_i \rho E_i^\dagger$. Assim, basta mostrar que

$$\sum_{i,j}^{\kappa} \text{tr}[E_i \rho_m E_i^\dagger E_j \rho_{m'} E_j^\dagger] = 0,\ \forall\ m \neq m'. \tag{4.22}$$

Sem perda de generalidade, escolhemos estados de entrada ortogonais ψ_m e $\psi_{m'}$, com operadores $\rho_m = |\psi_m\rangle\langle\psi_m|$ e $\rho_{m'} = |\psi_{m'}\rangle\langle\psi_{m'}|$, respectivamente. Então

$$|\langle\psi_m| E_i^\dagger E_j |\psi_{m'}\rangle|^2 = 0,\ \forall\ m \neq m' \tag{4.23}$$

$$\langle\psi_m| E_i^\dagger E_j |\psi_{m'}\rangle = 0,\ \forall\ m \neq m',\ \forall\ i,j \tag{4.24}$$

$$\text{tr}[|\psi_{m'}\rangle\langle\psi_m| E_i^\dagger E_j] = 0\ \forall\ m \neq m',\ \forall\ i,j. \tag{4.25}$$

□

ara ilustrar o Teorema 4.4, apresentamos, a seguir, um exemplo de um canal quântico $\mathcal{E}$ que não satisfaz as exigências deste teorema. Consequentemente, a capacidade erro-zero do canal é igual a zero.

Exemplo 4.4 *Seja o canal quântico $\mathcal{E}$ representado pelos dois operadores de Kraus seguintes:*

$$E_1 = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{12}} & \frac{\sqrt{2}}{\sqrt{6}} & 0 \\ -\frac{1}{\sqrt{12}} & 0 & \frac{\sqrt{2}}{\sqrt{6}} \end{pmatrix} \ e\ E_2 = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{6}} & \frac{1}{\sqrt{12}} & -\frac{1}{\sqrt{12}} \\ \frac{-1}{\sqrt{6}} & \frac{3}{2\sqrt{6}} & \frac{1}{2\sqrt{6}} \\ \frac{1}{\sqrt{6}} & \frac{1}{2\sqrt{6}} & \frac{3}{2\sqrt{6}} \end{pmatrix}. \tag{4.26}$$

Considerando o subespaço vetorial

$$S := Span\{E_1^\dagger E_1, E_1^\dagger E_2, E_2^\dagger E_1, E_2^\dagger E_2\} \tag{4.27}$$

e sejam

$$|1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ |2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \ e \ |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{4.28}$$

Observando que

$$\mathrm{tr}[|1\rangle \langle 2| \, E_2^\dagger E_2] \neq 0, \tag{4.29}$$

concluímos que $|i\rangle \langle j|$*, com* $i \neq j$*, não é ortogonal a* S*. Portanto, o canal quântico* $\mathcal{E}$ *possui capacidade erro-zero igual a zero.*

Nota

Nesta seção, fizemos alguns recortes dos conceitos da Teoria da Informação Quântica Erro-Zero, direcionados à definição de capacidade erro-zero de um canal quântico e aos resultados consequentes dessa definição, que possibilitam a verificação da capacidade erro-zero de um canal quântico. A explicação para esse recorte está relacionada às questões centrais deste trabalho de tese, que busca apresentar alguns resultados na área de capacidade erro-zero de um canal quântico. No próximo capítulo, será apresentado o primeiro resultado, que relaciona estados próprios comuns aos operadores de Kraus de um canal quântico à Teoria da Informação Quântica Erro-Zero, especialmente voltada para a capacidade erro-zero de um canal quântico.

Capítulo 5

Estado Próprio Comum aos Operadores de Kraus e Teoria da Informação Quântica Erro-Zero

Neste capítulo, apresentaremos uma condição para a capacidade de erro-zero de canais quânticos, que relaciona os operadores de Kraus que representam o canal ao número de estados próprios comuns a esses operadores [38]. A conclusão da prova do resultado utiliza o Teorema 4.3, apresentado anteriormente. Essa condição, juntamente com as condições apresentadas no capítulo anterior nos Teoremas 4.1, 4.2 e 4.4, constitui o conjunto de quatro condições de capacidade de erro-zero de canais quânticos conhecidas na literatura.

Para apresentar a condição de capacidade de erro-zero de canais quânticos, começamos introduzindo algumas notações, algumas das quais já foram mencionadas no Apêndice A, mas entendemos que relembrá-las enriquece o entendimento do leitor.

Seja $\mathcal{H}$ um espaço de Hilbert de dimensão d. Por $\mathcal{B}(\mathcal{H})$, denotamos o conjunto de todos os operadores lineares em $\mathcal{H}$. Por $M_d(\mathbb{C})$, denotamos o conjunto de todas as matrizes quadradas complexas de ordem d. Assumindo que $\mathcal{H} \cong \mathbb{C}^d$ e $\mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$, o canal quântico $\mathcal{E}$ pode ser visto como um superoperador quântico que preserva o traço $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$, ou $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$.

Antes de provarmos o seguinte lema dado a seguir, precisamos chamar a atenção para o fato de que, para estados puros $|\psi\rangle$ no espaço de Hilbert $\mathcal{H}$, temos que

$$\mathcal{E}(|\psi\rangle) = \sum_{i=1}^{\kappa} E_i \, |\psi\rangle\langle\psi| \, E_i^{\dagger}. \tag{5.1}$$

Lema 5.1 ([38]) *Seja um canal quântico $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ com operadores de Kraus $E_1, ..., E_\kappa$. Se $|\varphi\rangle$ é um estado próprio comum dos operadores E_i, então é um ponto fixo de $\mathcal{E}$.*

Prova: Devemos mostrar que $\mathcal{E}(|\psi\rangle \langle\psi|) = |\psi\rangle \langle\psi|$. Por uma questão de generalidade, vamos considerar que $E_i |\psi\rangle = \lambda_i |\psi\rangle$ pode ser associado a diferentes estados próprios para diferentes operadores de Kraus. Então,

$$\mathcal{E}(|\psi\rangle\langle\psi|) \overset{(a)}{=} \sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger \tag{5.2}$$

$$\overset{(b)}{=} \sum_i \lambda_i |\psi\rangle \lambda_i^* \langle\psi| \tag{5.3}$$

$$= |\psi\rangle\langle\psi| \sum_i |\lambda_i|^2 \tag{5.4}$$

$$\overset{(c)}{=} |\psi\rangle\langle\psi|, \tag{5.5}$$

em que (a) utilizamos a representação de Kraus do canal quântico, em (b) o fato de $|\varphi\rangle$ ser um estado próprio de cada E_i (por hipótese) e (c) porque $\mathcal{E}$ é preservador de traços.

□

Provamos no Lema 5.1 que cada estado próprio comum dos operadores de Kraus que representam o canal quântico é um ponto fixo do canal.

5.1 Condição para Capacidade de Erro-Zero dos Canais Quânticos

A partir do Lema 5.1, vamos concluir que a capacidade de erro-zero dos canais quânticos é positiva se os operadores de Kraus tiverem pelo menos dois estados próprios comuns. Detalhamos isso a seguir, antes vamos apresentar a seguinte definição:

Definimos $N_\mathcal{E} = \{|\psi\rangle \in \mathcal{S} \ : \ E_i |\psi\rangle = \lambda_i |\psi\rangle\}$ como o conjunto de estados próprios comuns para cada operador de Kraus do canal quântico $\mathcal{E}$. Denotamos por $|N_\mathcal{E}|$ a cardinalidade de $N_\mathcal{E}$.

Teorema 5.1 ([38]) *Seja N_f o número de pontos fixos de um canal quântico $\mathcal{E}$. Então, $N_f \geq |N_\mathcal{E}|$ e $C^{(0)}(\mathcal{E}) \geq log\ |N_\mathcal{E}|$.*

Prova: Mostramos no Lema 5.1 que os estados em $N_\mathcal{E}$ são pontos fixos do canal. Como um ponto fixo não precisa ser um estado comum de cada operador de Kraus, a desigualdade $N_f \geq |N_\mathcal{E}|$ é válida. Para o limite inferior da capacidade de erro-zero, é possível

construir um código de bloco quântico trivial com probabilidade de erro-zero, codificando a informação clássica nos estados em $N_{\mathcal{E}}$ e, então, é possível transmitir pelo menos $\log |N_{\mathcal{E}}|$ *bits* através do canal quântico sem erro. Assim, temos $C^{(0)}(\mathcal{E}) \geq \log |N_{\mathcal{E}}|$.

□

É interessante chamar a atenção que o Teorema 5.1 também funciona como um limite para a capacidade de erro-zero dos canais quânticos. Por conseguinte, por esta condição, a capacidade de erro-zero de um canal quântico é limitada inferiormente por $\log |N_{\mathcal{E}}|$.

A recíproca do Teorema 5.1 não é válida, ou seja, um canal quântico $\mathcal{E}$ pode ter capacidade de zero-erro positiva e os seus operadores de Kraus não terem um estado próprio comum. O exemplo seguinte mostra um canal quântico com capacidade de erro-zero positiva, mas os operadores de Kraus não tem um estado próprio comum.

Exemplo 5.1 *Seja o canal quântico $\mathcal{E}$ representado pelos operadores de Kraus E_1, E_2 e E_3, dados por:*

$$E_1 = \begin{pmatrix} 0.5 & 0 & 0 & 0 & \frac{\sqrt{49902}}{620} \\ 0.5 & -0.5 & 0 & 0 & 0 \\ 0 & 0.5 & -0.5 & 0 & 0 \\ 0 & 0 & 0.5 & -\frac{\sqrt{457}}{50} & \frac{\sqrt{457}}{50} \\ 0 & 0 & 0 & -0.62 & \frac{289}{1550} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0.5 & 0 & 0 & 0 & \frac{\sqrt{49902}}{620} \\ 0.5 & 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & \frac{\sqrt{457}}{50} & -\frac{\sqrt{457}}{50} \\ 0 & 0 & 0 & 0.5 & 0.5 \end{pmatrix},$$

$$E_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.3 \end{pmatrix}.$$

Os operadores de Kraus E_1, E_2 e E_3 não têm um estado próprio comum, mas o canal tem capacidade de erro-zero positiva [21, Exemplo 5.4].

A seguir apresentamos alguns exemplos que ilustram a condição de capacidade de erro-zero de canais quânticos.

Exemplo 5.2 ([38]) *O canal quântico $\mathcal{E}$ com os operadores de Kraus E_1 e E_2, dados por*

$$E_1 = \begin{pmatrix} \frac{3}{10} & 0 & -\frac{3}{10} \\ 0 & 0 & 0 \\ -\frac{3}{10} & 0 & \frac{3}{10} \end{pmatrix} \quad e \quad E_2 = \begin{pmatrix} -\frac{1}{10} & 0 & -\frac{9}{10} \\ 0 & 0 & 0 \\ -\frac{9}{10} & 0 & -\frac{1}{10} \end{pmatrix},$$

os três vetores $|\psi\rangle = (1,0,1)$, $|\phi\rangle = (0,1,0)$ *e* $|\varphi\rangle = (-1,0,1)$ *são estados próprios comuns a* E_1 *e* E_2*, logo, pelo Lema 5.1, são pontos fixos do canal quântico. Pela condição de capacidade de erro-zero do Teorema 5.1, temos que* $C^{(0)}(\mathcal{E}) \geq log\ 3$.

Exemplo 5.3 ([38]) *Dado que* $p \in (0,1)$*, considere o canal quântico* $\mathcal{E}$ *com os operadores de Kraus* E_1 *e* E_2*, dados por:*

$$E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad e \quad E_2 = \sqrt{1-p}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

os dois vetores $|\psi\rangle = (1,0,0,0)$ *e* $|\varphi\rangle = (0,0,0,1)$ *são estados próprios comuns a* E_1 *e* E_2*, logo, pelo Lema 5.1, são pontos fixos do canal quântico. Pela condição de capacidade de erro-zero do Teorema 5.1, temos que* $C^{(0)}(\mathcal{E}) \geq log\ 2$.

Exemplo 5.4 ([38]) *Seja o canal quântico* $\mathcal{E}$ *representado pelos operadores de Kraus* E_1*,* E_2 *e* E_3*, dados por:*

$$E_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0.5 \\ 0 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0.5 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & -0.5 \\ 0 & -0.5 & 0 & 0 & 0 \\ 0 & 0 & -0.5 & 0 & 0 \\ 0 & 0 & 0 & -0.5 & 0 \\ 0 & 0 & 0 & 0 & -0.5 \end{pmatrix}$$

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{0.5} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{0.5} & 0 & 0 \\ 0 & 0 & 0 & \sqrt{0.5} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Os operadores de Kraus E_1*,* E_2 *e* E_3 *têm quatro estados próprios comuns que são* $|\psi\rangle = (1,0,0,0,0)$, $|\phi\rangle = (0,1,0,0,0,0)$, $|\varphi\rangle = (0,0,1,0,0)$ *e* $|\mu\rangle = (0,0,0,1,0)$*. Esses estados próprios são pontos fixos do canal quântico pelo Lema 5.1. Pela condição de capacidade de erro-zero do Teorema 5.1, temos que* $C^{(0)}(\mathcal{E}) \geq log\ 4 = 2$.

Neste capítulo, apresentamos uma condição de capacidade de erro-zero de canais quânticos. A condição mostra que se os operadores de Kraus do canal quântico tiverem pelo menos dois estados próprios comuns, isso implica que o canal tem capacidade de erro-zero não trivial. Uma particularidade dessa condição é o fato de ser fácil verificar a condição de capacidade de erro-zero do canal quando se dispõem dos operadores de Kraus que representam o canal. Além disso, a condição é um limite inferior para a capacidade de erro-zero do canal, quando se demonstra que $C^{(0)}(\mathcal{E}) \geq log\ |N_{\mathcal{E}}|$.

Capítulo 6

O Teorema de Shemesh e a Teoria da Informação Quântica Erro-Zero

Neste capítulo, estabelecemos resultados relacionando o Teorema de Shemesh à Teoria da Informação Quântica Erro-Zero. Para tanto, começaremos com o Teorema de Shemesh e sua demonstração, assim como enunciaremos o Teorema de Shemesh generalizado. Logo em seguida, apresentaremos algumas conexões entre este teorema e a capacidade de erro-zero de canais quânticos. A primeira conexão é o resultado proposto na Conjectura 6.1 [23]. Em seguida, demonstramos que os estados próprios comuns aos operadores de Kraus que representam o canal pertencem ao subespaço de Shemesh. Como consequência, os pontos fixos do canal quântico atuam como uma ponte entre o Teorema de Shemesh e a Teoria da Informação Quântica Erro-Zero, permitindo assim a derivação de novos resultados sobre a capacidade de erro-zero dos canais quânticos. Essa segunda parte, envolvendo essas conexões, encontrou-se nas Proposições 6.1 e 6.2 e no Corolário 6.1.

6.1 O Teorema de Shemesh

O Teorema de Shemesh 6.1 apresenta um critério garantindo que, dadas duas matrizes quadradas, elas possuem um autovetor comum, bem como um critério para uma matriz ter um autovetor em um dado subespaço. No contexto do estudo dos canais quânticos, o Teorema de Shemesh tem uma importância significativa, na medida em que funciona como uma ferramenta primordial na sondagem da estrutura interna da álgebra $\mathcal{A}(E_1, \ldots, E_\kappa)$ gerada pelos operadores de Kraus $E_1, \ldots, E_\kappa$, os quais representam o canal quântico $\mathcal{E}$, e utilizando apenas seus geradores. Uma dessas sondagens assegura que, num

canal quântico $\mathcal{E} : M_5(\mathbb{C}) \longrightarrow M_5(\mathbb{C})$ com dois operadores de Kraus, o espectro periférico[1] é um grupo cíclico com ordem no máximo 25 [25]. Outra questão que se pode concluir, usando o Teorema 6.1, é sobre a irredutibilidade de um canal quântico $\mathcal{E}$. Ou seja, na representação de Kraus de qualquer canal quântico $\mathcal{E}$, se pelo menos dois operadores de Kraus não têm um autovetor comum, então o mapa é irredutível[2].

Teorema 6.1 (Shemesh [24]) *Sejam $E_1,\ E_2 \in M_d(\mathbb{C})$. Então E_1 e E_2 possuem autovetores comuns se, e somente se, o subespaço*

$$\mathcal{M} = \cap_{k,l=1}^{d-1} \ker\ [E_1^k, E_2^l] \tag{6.1}$$

é um subespaço não trivial, ou seja, existe algum $x \in \mathcal{M}$ com $0 \neq x \in \mathbb{C}^d$. O símbolo $[\cdot,\cdot]$ denota o comutador de matrizes e $k, l \in \{1, 2, ..., d-1\}$, enquanto E_1^k e E_2^l denotam as k-ésima e l-ésima potências de E_1 e E_2, respectivamente.

A demonstração do Teorema de Shemesh é apresentada em [24] e vamos reproduzi-la neste trabalho de tese. Antes, porém, é necessário apresentar o Teorema auxiliar 6.2, cuja demonstração pode ser encontrada em [39].

Teorema 6.2 *Sejam $E_1,\ E_2 \in M_d(\mathbb{C})$. Existe um autovetor $x \in \mathbb{C}^d$ satisfazendo $E_2 x = 0$ se, e somente se, $\cap_{k=0}^{q-1} \ker(E_2 E_1^k) \neq \{0\}$, em que q é um número inteiro maior do que ou igual ao grau do polinômio minimal de E_1.*

Prova do Teorema de Shemesh: Suponha que $x \neq 0$ seja um autovetor comum de E_1 e E_2. Então, $E_1 x = \lambda x$ e $E_2 x = \mu x$, implicando que

$$E_1^k E_2^l x = E_2^l E_1^k x = \lambda^k \mu^l x. \tag{6.2}$$

Assim,

$$[E_1^k, E_2^l] x = E_1^k E_2^l x - E_2^l E_1^k x = 0. \tag{6.3}$$

Isto é, $0 \neq x \in \mathcal{M} = \cap_{k,l=1}^{d-1} \ker\ [E_1^k, E_2^l]$.

Reciprocamente, considere o subespaço $\mathcal{M} = \cap_{k,l=1}^{d-1} \ker\ [E_1^k, E_2^l]$ e suponha que $\mathcal{M} \neq \{0\}$ e que $\mathcal{M}$ é invariante sob E_1 e E_2. Note que E_1 e E_2 comutam com os elementos de $\mathcal{M}$ ($[E_1, E_2]x = 0$ para todo $x \in \mathcal{M}$). Assim, as restrições dos operadores representados

[1] O espectro periférico de um canal quântico $\mathcal{E}$, denotado por $\mathrm{Spec}(\mathcal{E})$, é o conjunto de todos os autovalores de $\mathcal{E}$ com módulo 1. O conjunto $\mathrm{Spec}(\mathcal{E})$ de $\mathcal{E}$ é um subgrupo do grupo $U(1)$ dos números complexos com módulo 1 [40].

[2] Seja um canal quântico $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ com operadores de Kraus $E_1, ..., E_\kappa$. Dizemos $\mathcal{E}$ é irredutível, se operadores de Kraus $E_1, ..., E_\kappa$, não têm nenhum subespaço invariante comum não trivial (ou seja, os únicos subespaços invariante comum são $\{0\}$ e $\mathbb{C}^n$) [29].

por E_1 e E_2 ao subespaço $\mathcal{M}$ são comutativas e, portanto, têm um autovetor comum, que é um autovetor comum de E_1 e E_2.

Para concluir a prova, resta mostrar que $\mathcal{M}$ é invariante sob E_1 e E_2. Então, seja $x \neq 0$ um vetor pertencente ao subespaço $\mathcal{M}$ e defina $\mathcal{M}_x = \{p(E_1, E_2)x \mid p \in \mathcal{P}\}$ em que $\mathcal{P}$ é o conjunto de todos os polinômios complexos a duas variáveis não comutativas. Observe que $\mathcal{M}_x$ é um subespaço invariante sob E_1 e E_2. Além disso, como $x \in \mathcal{M}$ tem-se $E_1^k E_2^l x = E_2^l E_1^k x$ e, portanto, todo monômio em E_1 e E_2 operando em x tem a forma $E_1^r E_2^s x$. Isso significa que qualquer elemento de $\mathcal{M}_x$ é da forma $y = (\sum_{i,j} a_{ij} E_1^i E_2^j)x$, e usando o argumento acima, obtém-se

$$E_1 E_2 y = E_2 E_1 y = (\sum_{i,j} a_{ij} E_1^{i+1} E_2^{j+j})x. \tag{6.4}$$

Assim, E_1 e E_2 comutam com $\mathcal{M}_x$. Além disso, note que $\mathcal{M}_x \subset \mathcal{M}$ e dessa forma

$$\mathcal{M} = \cup_{x \in \mathcal{M}} \mathcal{M}_x = \sum_{x \in \mathcal{M}} \mathcal{M}_x. \tag{6.5}$$

Assim, $\mathcal{M}$, como uma soma de subespaços invariantes, é invariante tanto sob E_1, quanto sob E_2.

□

O Teorema de Shemesh 6.1 pode ser generalizado para uma quantidade s de matrizes e dar condições para que as mesmas tenham autovetores comuns. Esta generalização é feita com o uso do conceito de polinômio standard A.38 e do Teorema de Amitsur-Levitzki A.1. O Teorema de Shemesh generalizado é enunciado a seguir, cuja demonstração o leitor pode encontrar em [30, Teorema 2.4].

Teorema 6.3 (Shemesh generalizado [30]) *As matrizes $E_1, ..., E_s \in M_d(\mathbb{C})$ possuem autovetores comuns se, e somente se, o subespaço*

$$\mathcal{M} = \cap_{\alpha_i, l_i = 1}^{d-1} \ker\, [E_1^{\alpha_1} ... E_s^{\alpha_s}, E_1^{l_1} ... E_s^{l_s}] \tag{6.6}$$

é um subespaço não trivial, ou seja, existe algum $x \in \mathcal{M}$ com $0 \neq x \in \mathbb{C}^d$ e $\sum_i \alpha_i \neq 0$ e $\sum_i l_i \neq 0$.

O Teorema de Shemesh generalizado continua bastante importante no estudo dos canais quânticos. Uma contribuição é a verificação se uma álgebra $\mathcal{A}$ gerada pelos operadores de Kraus tem ou não um *DFS* (Subespaços e Subsistemas Livres de Descoerência)

de dimensão maior do que ou igual a 2 [29]. No contexto deste trabalho, o Teorema de Shemesh generalizado ganha especial importância, pois um dos objetivos é utilizá-lo para generalizar o resultado da Conjectura 6.1 para canais quânticos com n operadores de Kraus

6.2 Conexões entre o Teorema de Shemesh e a Capacidade de Erro-Zero dos Canais Quânticos

Nesta seção, apresentamos algumas conexões entre o Teorema de Shemesh e a capacidade de erro-zero dos canais quânticos. Iniciamos com a apresentação de uma conjectura. A elaboração dessa conjectura tem como base as verificações feitas com alguns canais quânticos, tais como o canal de despolarização, o canal *phase flip*, o canal *amplitude damping*, entre outros.

Conjectura 6.1 (Condição para capacidade erro-zero [23]) *Seja um canal quântico* $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ *com dois operadores de Kraus* E_1 *e* E_2*. Todo vetor* $x \in \mathbb{C}^d$ *pertence ao subespaço*

$$\mathcal{M} = \cap_{k,l=1}^{d-1} ker\ [E_1^k, E_2^l], \tag{6.7}$$

se, e somente se, a capacidade de erro-zero do canal $\mathcal{E}$ *é positiva.*

Exemplo 6.1 *O canal Phase Flip em um espaço de Hilbert de dimensão 2 é caracterizado pelos operadores de Kraus*

$$E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad E_2 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{6.8}$$

O canal pode transmitir um bit por uso do canal, com probabilidade de erro-zero igual a 1, ou seja, capacidade de erro-zero do canal é positiva. Ademais, observe que,

$$\mathcal{M} = \ker\ [E_1, E_2] = \ker\{E_1E_2 - E_2E_1\} = \ker\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}, \tag{6.9}$$

dessa forma, qualquer vetor em $\mathbb{C}^2$ *pertence a* $\mathcal{M}$*. Logo, a condição apresentada da Conjectura 6.1 assegura, que a capacidade de erro-zero deste canal é positiva.*

Exemplo 6.2 *O canal Bit Flip em um espaço de Hilbert de dimensão 2 é caracterizado pelos dois operadores de Kraus*

$$E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad E_2 = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6.10}$$

O canal pode transmitir um bit por uso do canal, com probabilidade de erro-zero igual a 1, ou seja, capacidade de erro-zero do canal é positiva. Ademais, observe que,

$$\mathcal{M} = \ker\,[E_1, E_2] = \ker\{E_1E_2 - E_2E_1\} = \ker\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}, \tag{6.11}$$

dessa forma, qualquer vetor em $\mathbb{C}^2$ pertence a $\mathcal{M}$. Logo, a condição apresentada da Conjectura 6.1 assegura, mais uma vez, que a capacidade de erro-zero deste canal é positiva.

Exemplo 6.3 *O canal Amplitude Damping em um espaço de Hilbert de dimensão 2 é caracterizado pelos dois operadores de Kraus*

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \quad e \quad E_2 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \tag{6.12}$$

A capacidade de erro-zero desse canal é igual a zero. Além disso, observe que

$$\mathcal{M} = \ker\,[E_1, E_2] = \ker\{E_1E_2 - E_2E_1\} = \ker\left\{\begin{pmatrix} 0 & \sqrt{p} - \sqrt{p(1-p)} \\ 0 & 0 \end{pmatrix}\right\}, \tag{6.13}$$

de tal forma que nem todo vetor $x \in \mathbb{C}^2$ pertence a $\mathcal{M}$ e a capacidade de erro-zero do canal é igual a zero, em conformidade com o resultado apresentado na Conjectura 6.1.

Exemplo 6.4 *O canal quântico $\mathcal{E}$ dado pelos dois operadores de Kraus*

$$E_1 = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{12}} & \frac{\sqrt{2}}{\sqrt{6}} & 0 \\ -\frac{1}{\sqrt{12}} & 0 & \frac{\sqrt{2}}{\sqrt{6}} \end{pmatrix} e\ E_2 = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{6}} & \frac{1}{\sqrt{12}} & -\frac{1}{\sqrt{12}} \\ \frac{-1}{\sqrt{6}} & \frac{3}{2\sqrt{6}} & \frac{1}{2\sqrt{6}} \\ \frac{1}{\sqrt{6}} & \frac{1}{2\sqrt{6}} & \frac{3}{2\sqrt{6}} \end{pmatrix}, \tag{6.14}$$

tem capacidade de erro-zero igual a zero. Além disso, observe que nem todo vetor de $\mathbb{C}^3$ pertence ao subespaço

$$\mathcal{M} = \cap_{k,l=1}^{2} ker\ [E_1^k, E_2^l] \neq \left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}. \tag{6.15}$$

E, pela Conjectura 6.1, reafirma-se que a capacidade de erro-zero do canal é igual a zero.

É interessante destacar que a Conjectura 6.1 funciona como uma condição para a capacidade de erro-zero dos canais quânticos com dois operadores de Kraus.

A seguir, apresentamos um resultado que possibilita aprofundar as conexões entre o Teorema de Shemesh e o conceito de capacidade de erro-zero dos canais quânticos.

Proposição 6.1 *Seja um canal quântico $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ com operadores de Kraus $E_1, ..., E_\kappa$. Então, cada estado próprio de $N_\mathcal{E}$ pertence ao subespaço*

$$\mathcal{M} = \cap_{\alpha_i, l_i = 1}^{d-1} ker\, [E_1^{\alpha_1} ... E_\kappa^{\alpha_\kappa}, E_1^{l_1} ... E_\kappa^{l_\kappa}] \tag{6.16}$$

em que $\sum_i \alpha_i \neq 0$ e $\sum_i l_i \neq 0$.

Prova: Vamos supor que $|\varphi\rangle \in N_\mathcal{E}$, então $|\varphi\rangle$ é um estado próprio comum a $E_1, ..., E_\kappa$, isto é,

$$E_1 |\varphi\rangle = \lambda_1 |\varphi\rangle\,,\ E_2 |\varphi\rangle = \lambda_2 |\varphi\rangle\,, ..., E_\kappa |\varphi\rangle = \lambda_\kappa |\varphi\rangle\,. \tag{6.17}$$

Pelo Teorema 6.3, temos o subespaço $\mathcal{M} \neq 0$, então suponhamos $a_1, ..., a_\kappa \in \{1, ..., d-1\}$ e $b_1, ..., b_\kappa \in \{1, ..., d-1\}$ e consideremos o comutador

$$[E_1^{a_1} ... E_\kappa^{a_\kappa}, E_1^{b_1} ... E_\kappa^{b_\kappa}] = (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_\kappa^{b_\kappa}) - (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_\kappa^{a_\kappa}). \tag{6.18}$$

Note que

$$\Big((E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_\kappa^{b_\kappa}) - (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_\kappa^{a_\kappa})\Big) |\varphi\rangle \tag{6.19}$$

$$= (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_{\kappa-1}^{b_{\kappa-1}}) E_\kappa^{b_\kappa} |\varphi\rangle - (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_{\kappa-1}^{a_{\kappa-1}}) E_\kappa^{a_\kappa} |\varphi\rangle \tag{6.20}$$

$$= (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_{\kappa-1}^{b_{\kappa-1}}) \lambda_\kappa^{b_\kappa} |\varphi\rangle - (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_{\kappa-1}^{a_{\kappa-1}}) \lambda_\kappa^{a_\kappa} |\varphi\rangle \tag{6.21}$$

$$= \lambda_\kappa^{b_\kappa} (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_{\kappa-1}^{b_{\kappa-1}}) |\varphi\rangle - \lambda_\kappa^{a_\kappa} (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_{\kappa-1}^{a_{\kappa-1}}) |\varphi\rangle \tag{6.22}$$

$$= \lambda_\kappa^{b_\kappa} (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_{\kappa-2}^{b_{\kappa-2}}) E_{\kappa-1}^{b_{\kappa-1}} |\varphi\rangle - \lambda_\kappa^{a_\kappa} (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_{\kappa-2}^{a_{\kappa-2}}) E_{\kappa-1}^{a_{\kappa-1}} |\varphi\rangle \tag{6.23}$$

$$= \lambda_\kappa^{b_\kappa} \lambda_{\kappa-1}^{b_{\kappa-1}} (E_1^{a_1} ... E_\kappa^{a_\kappa})(E_1^{b_1} ... E_{\kappa-2}^{b_{\kappa-2}}) |\varphi\rangle - \lambda_\kappa^{a_\kappa} \lambda_{\kappa-1}^{a_{\kappa-1}} (E_1^{b_1} ... E_\kappa^{b_\kappa})(E_1^{a_1} ... E_{\kappa-2}^{a_{\kappa-2}}) |\varphi\rangle \tag{6.24}$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$= \lambda_\kappa^{b_\kappa} \lambda_{\kappa-1}^{b_{\kappa-1}} ... \lambda_1^{b_1} \lambda_\kappa^{a_\kappa} \lambda_{\kappa-1}^{a_{\kappa-1}} ... \lambda_1^{a_1} |\varphi\rangle - \lambda_\kappa^{a_\kappa} \lambda_{\kappa-1}^{a_{\kappa-1}} ... \lambda_1^{a_1} \lambda_\kappa^{b_\kappa} \lambda_{\kappa-1}^{b_{\kappa-1}} ... \lambda_1^{b_1} |\varphi\rangle \tag{6.25}$$

$$= (\lambda_\kappa^{b_\kappa + a_s} \lambda_{\kappa-1}^{b_{\kappa-1} + a_{\kappa-1}} ... \lambda_1^{b_1 + a_1} - \lambda_\kappa^{a_\kappa + b_\kappa} \lambda_{\kappa-1}^{a_{\kappa-1} + b_{\kappa-1}} ... \lambda_1^{a_1 + b_1}) |\varphi\rangle \tag{6.26}$$

$$= 0 \cdot |\varphi\rangle = 0. \tag{6.27}$$

Em outras palavras, o estado próprio $|\varphi\rangle$ pertence ao subespaço

$$\mathcal{M} = \cap_{\alpha_i, l_i=1}^{d-1} \ker\, [E_1^{\alpha_1} ... E_\kappa^{\alpha_\kappa}, E_1^{l_1} ... E_\kappa^{l_\kappa}]. \tag{6.28}$$

Logo, todos os estados próprios de $N_\mathcal{E}$ pertencem ao subespaço $\mathcal{M}$.

□

A Proposição 6.1 mostra que, se $|\varphi\rangle \in N_\mathcal{E}$, então $|\varphi\rangle \in \mathcal{M}$, isto é, $N_\mathcal{E} \subseteq \mathcal{M}$. Além disso, vamos considerar o seguinte conjunto

$$\mathcal{M}_\mathcal{E} = \{|\varphi\rangle \in \mathcal{M} \ : \ \mathcal{E}(|\varphi\rangle) = |\varphi\rangle\,, \text{ com pelo menos um } |\varphi\rangle \in N_\mathcal{E}\}.$$

Vamos denotar por $|\mathcal{M}_\mathcal{E}|$ a cardinalidade de $\mathcal{M}_\mathcal{E}$. Portanto, com base neste parágrafo, temos o seguinte corolário.

Corolário 6.1 *A cardinalidade do conjunto $|\mathcal{M}_\mathcal{E}|$ é maior ou igual à cardinalidade do conjunto $|N_\mathcal{E}|$.*

Prova: Seja $\mathcal{E}$ um canal quântico com operadores de Kraus $E_1, ..., E_\kappa$. Então, é possível ter um $|\varphi\rangle \in \mathcal{M}_\mathcal{E}$ que não é um estado próprio comum dos operadores $E_1, ..., E_\kappa$, ou seja, $|\varphi\rangle \in \mathcal{M}_\mathcal{E}$ e $|\varphi\rangle \notin N_\mathcal{E}$. Portanto, $|\mathcal{M}_\mathcal{E}| \geq |N_\mathcal{E}|$.

□

Proposição 6.2 *Suponha que $|\mathcal{M}_\mathcal{E}| \geq 2$, então $C^{(0)}(\mathcal{E}) > 0$.*

Prova: Por hipótese, os estados pertencentes a $\mathcal{M}_\mathcal{E}$ são pontos fixos de $\mathcal{E}$ e temos pelo menos dois estados em $\mathcal{M}_\mathcal{E}$, pelo que se segue que $C^{(0)}(\mathcal{E}) \geq \log\, |\mathcal{M}_\mathcal{E}|$.

□

O resultado da Proposição 6.2 estabelece uma ligação entre o Teorema de Shemesh e a capacidade de erro-zero dos canais quânticos.

Exemplo 6.5 *Se $p \in (0, 1)$, então considere o canal quântico $\mathcal{E}$ com operadores de Kraus E_1 e E_2, dados por*

$$E_1 = \sqrt{p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ E_2 = \sqrt{1-p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Para $p = \frac{1}{4}$*, temos que* E_1 *e* E_2 *têm a forma:*

$$E_1 = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & \frac{\sqrt{3}}{4} & 0 \\ 0 & \frac{\sqrt{3}}{4} & -\frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}, \; E_2 = \begin{pmatrix} \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{4} & -\frac{3}{4} & 0 \\ 0 & -\frac{3}{4} & -\frac{\sqrt{3}}{4} & 0 \\ 0 & 0 & 0 & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

Os estados próprios $|\psi\rangle = (1,0,0,0)$ *e* $|\varphi\rangle = (0,0,0,1)$ *são comuns a* E_1 *e* E_2*. Pelo Lema 5.1, os estados próprios* $|\psi\rangle$ *e* $|\varphi\rangle$ *são pontos fixos do canal quântico. Portanto,* $|\psi\rangle, |\varphi\rangle \in \mathcal{M}_{\mathcal{E}}$*, isto é,* $|\mathcal{M}_{\mathcal{E}}| \geq 2$ *e, pela Proposição 6.2, temos que* $C^{(0)}(\mathcal{E}) > 0$.

Capítulo 7

Subespaço Comum Invariante de um Canal Quântico e a Teoria da Informação Quântica Erro-Zero

NNeste capítulo, vamos apresentar algumas conexões entre subespaços invariantes de um canal quântico $\mathcal{E}$ e a capacidade erro-zero do canal. Didaticamente, dividimos essa apresentação em duas partes. Na primeira parte, que chamamos de "caso particular", vamos abordar as conexões entre subespaços gerados por estados próprios comuns aos operadores de Kraus que representam o canal quântico e a capacidade erro-zero dos canais quânticos. Na segunda parte, que também chamamos de "caso geral", vamos analisar as conexões entre subespaços invariantes dos canais quânticos, cujos geradores desses subespaços são vetores quaisquer, e a capacidade de erro-zero dos canais quânticos.

7.1 Primeira parte: Conexões entre Capacidade de Erro-Zero e Subespaço Invariante de um Canal Quântico - Caso particular

Seja $W \subseteq \mathbb{C}^d$ um subespaço vetorial. Dizemos que W é um subespaço invariante (em inglês: *invariant subspace*) para um operador $E \in M_d(\mathbb{C})$, ou seja, *E-invariante*, se $E|\nu\rangle \in W$ para todo $|\nu\rangle \in W$ [41]. Dizemos ainda que W é um subespaço comum invariante (em inglês: *common invariant subspace*) para um conjunto de operadores $E_1, \ldots, E_s \in M_d(\mathbb{C})$, se W é E_i-invariante para todo $i = 1, \ldots, s$, isto é, $E_i|\nu\rangle \in W$ para todo $|\nu\rangle \in W$.

No contexto dos estudos envolvendo subespaços invariantes para matrizes ou ope-

radores lineares, sabemos que, os subespaços nulo e $\mathbb{C}^d$ são invariantes, sendo chamados de subespaços invariantes triviais. Portanto, no que segue, quando nos referirmos a subespaços invariantes ou subespaços comuns invariantes, sempre estaremos nos referindo a subespaços não triviais.

No campo da Teoria da Informação Quântica, podemos transpor o conceito de subespaço comum a operadores lineares para canais quânticos, cuja definição está posta abaixo.

Definição 7.1 (Subesp. invar. de um canal quântico [42]) *Seja $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ um canal quântico representado por operadores de Kraus $E_1, \ldots, E_\kappa$. Um subespaço $W \subseteq \mathbb{C}^d$ é invariante para um canal quântico $\mathcal{E}$ quando W é um subespaço comum invariante para os operadores E_i com $i = 1, \ldots, \kappa$, isto é, $E_i |\nu\rangle \in W$ para todo $|\nu\rangle \in W$.*

Na definição de subespaço invariante de um canal quântico com representação em termos de operadores de Kraus E_i, observe que a invariância do subespaço $W \subseteq \mathbb{C}^d$ através do canal quântico $\mathcal{E}$ depende de o subespaço W ser comum invariante aos operadores E_i com $i = 1, \ldots, \kappa$.

O fato de os operadores de Kraus E_i, que representam um canal quântico $\mathcal{E}$, possuírem um estado próprio comum, conforme estabelecido pelo Teorema de Shemesh generalizado, implica que o canal quântico $\mathcal{E}$ possui um subespaço $W \subseteq \mathbb{C}^d$ invariante, com $\dim(W) = 1$, gerado pelo estado próprio comum a todos os operadores de Kraus E_i . Este resultado é demonstrado na proposição a seguir.

Proposição 7.1 ([43]) *Seja $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ um canal quântico com uma representação de Kraus dada pelos operadores E_i, onde $i = 1, \ldots, \kappa$. Se os operadores E_i possuem um estado próprio comum $|\psi\rangle$, então o subespaço $W = Span\{|\psi\rangle\}$ é invariante comum para o canal quântico $\mathcal{E}$.*

Prova: Como $|\psi\rangle$ é um estado próprio comum aos operadores E_i, então temos $E_i |\psi\rangle = \lambda_i |\psi\rangle$ para $i = 1, \ldots, \kappa$. Supondo que $|\nu\rangle \in W = \text{Span}\{|\psi\rangle\}$, temos que $|\nu\rangle = \lambda |\psi\rangle$. Assim,

$$E_i |\nu\rangle = \lambda E_i |\psi\rangle = \lambda\lambda_i |\psi\rangle \tag{7.1}$$

ou seja, $E_i |\nu\rangle \in W = \text{Span}\{|\psi\rangle\}$, implicando que $W = \text{Span}\{|\psi\rangle\}$ é um subespaço invariante para E_i, com $i = 1, \ldots, \kappa$, isto é, $W = \text{Span}\{|\psi\rangle\}$ é um subespaço invariante de $\mathcal{E}$.

□

Para iniciar a discussão envolvendo as relações entre o subespaço invariante de um canal quântico $\mathcal{E}$ e a capacidade de erro-zero dos canais quânticos, podemos propor uma questão bastante relevante, que é a seguinte: seja um canal quântico $\mathcal{E}$ com representação por operadores de Kraus E_i e suponha que E_i, com $i = 1, \ldots, \kappa$, possua um estado próprio comum. Consequentemente, o canal quântico $\mathcal{E}$ tem um subespaço invariante de dimensão um (Proposição 7.1). Diante disso, é possível afirmar que o canal tem capacidade de erro-zero positiva? A resposta a esta questão é negativa. Para ver isso, considere o canal quântico *Amplitude Damping* $\mathcal{E}$ [37], definido em um espaço de Hilbert de dimensão 2 e representado pelos operadores de Kraus

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \quad \text{e} \quad E_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \tag{7.2}$$

em que $\gamma = \sin^2\theta$ é a probabilidade de um fóton ser perdido em uma cavidade sujeita a atenuação. O canal *Amplitude Damping* tem capacidade de erro-zero igual a zero, mas possui um subespaço invariante comum de dimensão um

$$W = Span\{|\psi\rangle\} \tag{7.3}$$

gerado pelo estado próprio $|\psi\rangle = (1, 0)$ comum aos operadores de Kraus E_1 e E_2.

Por outro lado, quando se trata de um subespaço invariante do canal quântico $\mathcal{E}$, gerado por pelo menos dois estados próprios comuns aos operadores de Kraus E_i que representam o canal $\mathcal{E}$, existe uma relação direta com a capacidade de erro-zero dos canais quânticos. A seguir, apresentamos o resultado que prova essa relação.

Teorema 7.1 ([43]) *Seja $\mathcal{E} : M_d(\mathbb{C}) \longrightarrow M_d(\mathbb{C})$ um canal quântico com operadores de Kraus $E_1, \ldots, E_\kappa$. Se $W \subset \mathbb{C}^d$ é um subespaço com dim $W = s$, onde $2 \leq s < d$, gerado por s estados próprios $\{|\psi_j\rangle : j = 1, \ldots, s\}$ comuns aos operadores E_i, então W é um subespaço invariante de $\mathcal{E}$, e $C^{(0)}(\mathcal{E}) \geq \log s$.*

Prova: Por hipótese, os $|\psi_j\rangle$ com $j = 1, \ldots, s$ são estados próprios comuns aos operadores de Kraus E_i, com $i = 1, \ldots, \kappa$. Assim, por definição, temos que

$$E_i |\psi_j\rangle = \lambda_j |\psi_j\rangle, \quad i = 1, \ldots, \kappa, \quad \text{e} \quad j = 1, \ldots, s. \tag{7.4}$$

Também por hipótese, o subespaço W é gerado por esses s estados próprios comuns aos operadores de Kraus E_i. Em notação de subespaço gerado, isso é expresso como

$$W = Span\{|\psi_j\rangle : j = 1, \ldots, s\}. \tag{7.5}$$

Para mostrar que W é invariante a cada operador de Kraus E_i, suponha que $|\nu\rangle \in W$. Então, podemos escrever $|\nu\rangle$ como combinação linear dos estados próprios $|\psi_j\rangle$ com $j = 1, \ldots, s$, ou seja, $|\nu\rangle = \alpha_1 |\psi_1\rangle + ... + \alpha_s |\psi_s\rangle$, ou, em notação de somatório,

$$|\nu\rangle = \sum_{j=1}^{s} \alpha_j |\psi_j\rangle . \tag{7.6}$$

Aplicando os operadores de Kraus E_i na equação (7.6) e utilizando as propriedades de linearidade desses operadores, temos

$$E_i |\nu\rangle = \sum_{j=1}^{s} \alpha_j E_i |\psi_j\rangle = \sum_{j=1}^{s} \alpha_j \lambda_j |\psi_j\rangle . \tag{7.7}$$

Como $\sum_{j=1}^{s} \alpha_j \lambda_j |\psi_j\rangle \in W$, visto que W é gerado pelos estados próprios $|\psi_j\rangle$, então $E_i |\nu\rangle \in W$, para todo $i = 1, ..., \kappa$. Logo, W é E_i-invariante e, consequentemente, um subespaço invariante de $\mathcal{E}$. Além disso, os estados $\{|\psi_j\rangle : j = 1, ..., s\}$ que geram o subespaço W são estados próprios comuns aos operadores de Kraus E_i e, portanto, são pontos fixos para o canal quântico $\mathcal{E}$ (Lema 5.1).Assim, como o número de estados próprios comuns satisfaz $s \geq 2$, pelo Teorema 5.1, podemos concluir que $C^{(0)}(\mathcal{E}) \geq \log s$.

□

A seguir, ilustraremos as ideias apresentadas neste artigo com um exemplo de um canal quântico $\mathcal{E}$ que possui um subespaço invariante gerado por dois estados próprios comuns aos operadores de Kraus que representam o canal.

Exemplo 7.1 ([43]) *Dado $p \in (0, 1)$, considere o canal quântico $\mathcal{E}$ representado pelos operadores de Kraus E_1 e E_2 dados a seguir*

$$E_1 = \sqrt{p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_2 = \sqrt{1-p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Para o caso particular $p = 0,5$, temos que $|\phi\rangle = (1, 0, 0, 0)$ e $|\varphi\rangle = (0, 0, 0, 1)$ são estados próprios comum aos operadores de Kraus E_1 e E_2. Dessa forma pelas ideias desenvolvidas no Teorema 7.1, o subespaço $W = Span\{|\phi\rangle, |\varphi\rangle\}$ é um subespaço invariante comum aos operadores de Kraus E_1 e E_2 e consequentemente é invariante para o canal quântico $\mathcal{E}$. Além disso, também podemos concluir, pelas ideias desenvolvidas que a capacidade erro-zero do canal $C^{(0)}(\mathcal{E}) \geq log\ 2$.

Nesta seção, apresentamos alguns resultados preliminares sobre a relação entre a capacidade de erro-zero de um canal quântico e um subespaço invariante comum gerado por estados próprios comuns aos operadores de Kraus que representam o canal. Consequentemente, tal subespaço é também invariante para o canal quântico.

Foi caracterizado, através de um contraexemplo, que um canal quântico que possui um subespaço invariante gerado por um único autovetor comum aos operadores de Kraus que representam o canal não implica, necessariamente, que a capacidade de erro-zero do canal quântico seja positiva. Por outro lado, concluímos que, quando o canal possui pelo menos dois estados próprios comuns a esses operadores, então a capacidade de erro-zero do canal é positiva. Noutras palavras, é possível construir um código de bloco quântico trivial com probabilidade de erro-zero, codificando a informação clássica em pelo menos dois estados do subespaço invariante para o canal quântico.

7.2 Segunda parte: Conexões entre Capacidade de Erro-Zero e Subespaço Invariante de um Canal Quântico - Caso geral

Nesta seção, apresentaremos dois resultados relacionados à capacidade de erro-zero e ao subespaço invariante de um canal quântico. O primeiro resultado estabelece uma relação entre subespaços invariantes de um canal quântico que se intersectam apenas trivialmente, o que implica na capacidade de erro-zero positiva do canal quântico.

Antes de iniciarmos a apresentação dos resultados desta seção, revisaremos brevemente a definição de canal quântico, com o objetivo de definir a combinação convexa, a multiplicação (aplicação recursiva) e o canal quântico adjunto.

Seja $\mathcal{H}$ um espaço de Hilbert de dimensão d. Vamos denotar por $\mathcal{B}(\mathcal{H})$, o espaço de Hilbert dos operadores lineares definidos em $\mathcal{H}$, de dimensão d^2.

Um canal quântico definido no espaço de Hilbert $\mathcal{H}$, é um mapa linear $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$, completamente positivo e que preserva o traço das matrizes densidade. Através de uma coleção de operadores de Kraus $\{E_i\}_{i=1}^{\kappa}$, é possível representar um canal quântico $\mathcal{E}$, e podemos escrever

$$\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} E_i \rho E_i^{\dagger} \quad \text{e} \quad \sum_{i}^{\kappa} E_i^{\dagger} E_i = I, \tag{7.8}$$

para todo $\rho \in \mathcal{B}(\mathcal{H})$.

Além disso, vamos denotar por $\mathcal{C}(\mathcal{H})$ o conjunto formado por todos os canais quânticos no espaço de Hilbert $\mathcal{H}$, o qual é fechado em relação à combinação convexa e à

composição. Isto é, para $\mathcal{E}_1, \mathcal{E}_2 \in \mathcal{C}(\mathcal{H})$ e $p \in [0,1]$ as transformações definidas pelos mapas

$$p\mathcal{E}_1(\rho) + (1-p)\mathcal{E}_2(\rho), \quad \rho \in \mathcal{B}(\mathcal{H}) \tag{7.9}$$

$$(\mathcal{E}_1 \circ \mathcal{E}_2)(\rho) := \mathcal{E}_1(\mathcal{E}_2(\rho)), \quad \rho \in \mathcal{B}(\mathcal{H}) \tag{7.10}$$

também são elementos de $\mathcal{C}(\mathcal{H})$.

Sendo $\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} E_i \rho E_i^\dagger$ um canal quântico com representação de Kraus $\{E_i\}_{i=1}^{\kappa}$, vamos definir o adjunto de $\mathcal{E}$, que denotamos por $\mathcal{E}^\dagger$,como o canal quântico representado pelos adjuntos dos operadores de Kraus. Ou seja,

$$\mathcal{E}^\dagger(\rho) = \sum_{i=1}^{\kappa} E_i^\dagger \rho E_i \text{ e } \sum_{i}^{\kappa} E_i E_i^\dagger = I \tag{7.11}$$

para todo $\rho \in \mathcal{B}(\mathcal{H})$.

Ademais, é importante ressaltar que $\mathcal{E}$ e $\mathcal{E}^\dagger$ apresentam espectros idênticos, ou seja, possuem os mesmos autovalores.

Por outro lado, suponhamos que $\mathcal{E}$ e $\mathcal{E}^\dagger$ estejam representados em (7.8) e (7.11), respectivamente. Vamos denotar por $\mathcal{E}^\dagger \circ \mathcal{E}$ o canal quântico obtido a partir da composição de $\mathcal{E}^\dagger$ e $\mathcal{E}$, com representação por operadores de Kraus. Podemos escrever,

$$(\mathcal{E}^\dagger \circ \mathcal{E})(\rho) = \sum_{i=1}^{\kappa} \sum_{j=1}^{\kappa} E_i^\dagger E_j \rho E_j^\dagger E_i. \tag{7.12}$$

Observe que, para todo $\rho \in \mathcal{B}(\mathcal{H})$, temos

$$(\mathcal{E}^\dagger \circ \mathcal{E})(\rho) = \sum_{i=1}^{\kappa} \sum_{j=1}^{\kappa} E_i^\dagger E_j \rho E_j^\dagger E_i \tag{7.13}$$

$$= \sum_{i=1}^{\kappa} E_i^\dagger \left(\sum_{j=1}^{\kappa} E_j \rho E_j^\dagger \right) E_i \tag{7.14}$$

$$= \sum_{i=1}^{\kappa} E_i^\dagger \mathcal{E}(\rho) E_i, \tag{7.15}$$

isto é, a aplicação do canal $\mathcal{E}^\dagger \circ \mathcal{E}$ no estado ρ significa que o estado recebido $\mathcal{E}(\rho)$ é enviado pelo adjunto $\mathcal{E}^\dagger$.

Seja $W \subseteq \mathcal{H}$ um subespaço vetorial. Dizemos que W é subespaço invariante (em inglês: *invariant subspace*) de um operador $E \in \mathcal{B}(\mathcal{H})$, ou *E-invariante*, se $E|\nu\rangle \in W$ para todo $|\nu\rangle \in W$ [41]. Dizemos ainda que W é um subespaço comum invariante (em

inglês: *common invariant subspace*) para um conjunto de $E_1, ..., E_s \in \mathcal{B}(\mathcal{H})$, se W é E_i-invariante para todo $i = 1, ..., s$, isto é, $E_i |\nu\rangle \in W$ para todo $|\nu\rangle \in W$.

Em estudos envolvendo subespaços invariantes de operadores lineares, os subespaços nulo e o espaço de Hilbert $\mathcal{H}$ são sempre invariantes e são chamados de subespaços invariantes triviais. Se existirem outros, serão chamados de subespaços invariantes não triviais.

No campo da Teoria da Informação Quântica, podemos transpor o conceito de subespaço comum a operadores lineares para canais quânticos, cuja definição está posta abaixo.

Definição 7.2 (Subesp. invar. de um canal quântico [42]) *Seja $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ um canal quântico representado por operadores de Kraus $E_1, ..., E_\kappa$. Um subespaço $W \subseteq \mathcal{H}$ é invariante para um canal quântico $\mathcal{E}$ quando W é um subespaço comum invariante para os operadores E_i, com $i = 1, ..., \kappa$, isto é, $E_i |\nu\rangle \in W$ para todo $|\nu\rangle \in W$.*

Antes de iniciar a apresentação destes resultados, vamos chamar a atenção para o fato de que a condição de W ser um subespaço invariante para um canal quântico $\mathcal{E}$ (Definição 7.2) pode ser expressa de forma equivalente pelas seguintes propriedades [44],[42]:

1. $E_i P = P E_i P$ para $i = 1, ..., s$ e P é um projetor sobre W.
2. $\mathcal{E}(P) = P\mathcal{E}(P)P$.
3. Supp$[\mathcal{E}(\rho)] \subseteq W$ para todo estado ρ com Supp$(\rho) \subseteq W$ (o Supp(ρ) representa o suporte do estado ρ).

Lema 7.1 ([42]) *Sejam $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, então podemos escrever*

$$\rho = q\sigma + (1 - q)\tau \tag{7.16}$$

em que $q \in (0, 1]$ e $\tau \in \mathcal{B}(\mathcal{H})$ se, e somente, se Supp$(\sigma) \subseteq$ Supp(ρ).

A demonstração deste resultado pode ser encontrada em [42, Lemma 8].

Proposição 7.2 ([42]) *Se ρ é um ponto fixo de $\mathcal{E}$, então o subespaço gerado por Supp(ρ) é um subespaço invariante de $\mathcal{E}$. Além disso, se $W \subset \mathcal{H}$ é um subespaço invariante de $\mathcal{E}$, então existe um ponto fixo $\rho_W \in W$ tal que Supp$(\rho_W) \subset W$.*

Prova: Dado $|\psi\rangle \in \text{Supp}(\rho)$, então, pelo Lema 7.1, existe uma probabilidade $p > 0$ e um estado σ, tal que

$$\rho = p\,|\psi\rangle\langle\psi| + (1-p)\sigma. \tag{7.17}$$

Dessa forma, aplicando o canal $\mathcal{E}$ na equação (7.17) e usando a linearidade, obtemos

$$\mathcal{E}(\rho) = p\mathcal{E}(|\psi\rangle\langle\psi|) + (1-p)\mathcal{E}(\sigma). \tag{7.18}$$

Pelo Lema 7.1, temos que

$$\text{Supp}[\mathcal{E}(|\psi\rangle\langle\psi|)] \subseteq \text{Supp}[\mathcal{E}(\rho)]. \tag{7.19}$$

Seja agora, ρ ponto fixo de $\mathcal{E}$, então $\mathcal{E}(\rho) = \rho$ e pela equação (7.19),

$$\text{Supp}[\mathcal{E}(|\psi\rangle\langle\psi|)] \subseteq \text{Supp}(\rho), \tag{7.20}$$

isto permite concluir que $\text{Supp}(\rho)$ é um subespaço invariante de $\mathcal{E}$. Por outro lado, suponha W um subespaço invariante de $\mathcal{E}$, então a restrição de $\mathcal{E}|_W$ ao subespaço W é um canal em $\mathcal{C}(W)$. Logo, $\mathcal{E}|_W$ possui um ponto fixo $\rho_W \in W$, ou seja, $\mathcal{E}|_W(\rho_W) = \rho_W$. Usando a primeira parte desta Proposição e a propriedade equivalente (3) da Definição 7.2, temos que o $\text{Supp}(\rho_W) \subset W$.

□

Proposição 7.3 ([42]) *Seja $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ um canal quântico. Um subespaço $W \subset \mathcal{H}$ é um subespaço invariante para $\mathcal{E}$ se, e somente se,*

$$W^{\perp} = \{|\varphi\rangle \in W : \langle\varphi|\psi\rangle = 0,\ \forall\,|\psi\rangle \in W\}$$

é um subespaço invariante para $\mathcal{E}^{\dagger}$.

Esboço da Prova: Suponha os projetores P e $P^{\perp}$ dos subespaços W e $W^{\perp}$, respectivamente. Como W é subespaço invariante de $\mathcal{E}$, segue que $\mathcal{E}(P) = P\mathcal{E}(P)P$. Dessa forma, é possível mostrar que $\langle\mathcal{E}^{\dagger}(P^{\perp}), P\rangle = 0$, implicando que $P\mathcal{E}^{\dagger}(P^{\perp})P = 0$. Assim, temos que $\mathcal{E}^{\dagger}(P^{\perp}) = P^{\perp}\mathcal{E}^{\dagger}(P^{\perp})P^{\perp}$, implicando que $W^{\perp}$ é subespaço invariante de $\mathcal{E}^{\dagger}$. A ideia da prova da recíproca é análoga.

Teorema 7.2 ([45]) *Seja $\mathcal{E} \in \mathcal{C}(\mathcal{H})$ um canal quântico representado por operadores de Kraus $E_1, ..., E_\kappa$. Sejam $W_1 \neq \{0\}$ e $W_2 \neq \{0\}$ subespaços vetoriais de $\mathcal{H}$ invariantes de $\mathcal{E}$, tais que $W_1 \cap W_2 = \{0\}$, então $C^{(0)}(\mathcal{E})$ é positiva.*

Prova: Por hipótese, temos que $W_1 \neq \{0\}$ e $W_2 \neq \{0\}$ são subespaços vetoriais de $\mathcal{H}$ invariantes de $\mathcal{E}$ e com a propriedade de que $W_1 \cap W_2 = \{0\}$. Então pela Proposição 7.2, podemos afirmar que existem pontos fixos distintos $\rho_{W_1} \in W_1$ e $\rho_{W_2} \in W_2$ do canal quântico $\mathcal{E}$, tais que $\text{Supp}(\rho_{W_1}) \subset W_1$ e $\text{Supp}(\rho_{W_2}) \subset W_2$. Dessa forma, pelo [42, Corolário 1], os subespaços gerados por $\text{Supp}(\rho_{W_1})$ e $\text{Supp}(\rho_{W_2})$ são subespaços ortogonais. Logo, para os estados $\rho_{W_1} \in W_1$ e $\rho_{W_2} \in W_2$, temos que $tr[\mathcal{E}(\rho_{W_1})\mathcal{E}(\rho_{W_2})] = 0$, e isso significa que a capacidade de erro-zero do canal quântico $\mathcal{E}$ é positiva.

□

Para apresentar o segundo resultado envolvendo a conexão entre a capacidade de erro-zero e o subespaço invariante de um canal quântico, necessitamos apresentar uma discussão sobre o comutador de ruídos de um canal quântico.

Sendo $\mathcal{E}$ um canal quântico representado por operadores de Kraus $E_1, ..., E_\kappa$, vamos definir o *comutador de ruídos* [44] para $\mathcal{E}$, e vamos denotar por $\mathcal{A}'$, como sendo o conjunto de todos os operadores de $\mathcal{B}(\mathcal{H})$ que comutam com E_i e $E_i^\dagger$, isto é,

$$\mathcal{A}' = \{\rho \in \mathcal{B}(\mathcal{H}); [\rho, E] = 0 = [\rho, E^\dagger], \forall E \in \{E_i\}_{i=1}^\kappa\}. \tag{7.21}$$

Para canais unitais, ou seja, canais quânticos que fixam o operador identidade ($\mathcal{E}(I) = I$), todos os $\rho \in \mathcal{A}'$ que satisfazem $\mathcal{E}(\rho) = \rho$. Da mesma forma, o canal adjunto $\mathcal{E}^\dagger$ também fixa a identidade ($\mathcal{E}^\dagger(I) = I$) [42] e assim para todos $\rho \in \mathcal{A}'$, temos que $\mathcal{E}^\dagger(\rho) = \rho$. De fato, observe que

$$\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} E_i \rho E_i^\dagger = \sum_{i=1}^{\kappa} \rho E_i E_i^\dagger = \sum_{i=1}^{\kappa} \rho \mathcal{E}(I) = \rho \tag{7.22}$$

e

$$\mathcal{E}^\dagger(\rho) = \sum_{i=1}^{\kappa} E_i^\dagger \rho E_i = \sum_{i=1}^{\kappa} \rho E_i^\dagger E_i = \sum_{i=1}^{\kappa} \rho \mathcal{E}^\dagger(I) = \rho. \tag{7.23}$$

Por outro lado, os pontos fixos dos canais unitais $\mathcal{E}$ e $\mathcal{E}^\dagger$, pertencem a $\mathcal{A}'$ [46]. Ou seja, os pontos fixos de $\mathcal{E}$ e $\mathcal{E}^\dagger$ são os mesmos.

A seguir, demonstraremos que, para um canal quântico unital que tenha um subespaço invariante com dimensão no mínimo dois, o canal possui a capacidade de erro-zero positiva.

Teorema 7.3 ([45]) *Seja $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ um canal quântico unital com operadores de Kraus $E_1, ..., E_\kappa$. Se $W \subset \mathcal{H}$ é um subespaço invariante de $\mathcal{E}$ com dim $W = s$ e $2 \leq s < d$, então $C^{(0)}(\mathcal{E})$ é positiva.*

Prova: Temos que espaço de Hilbert $\mathcal{H}$ pode ser escrito como soma direta do subespaço invariante W e do subespaço ortogonal $W^{\perp}$, isto é, $\mathcal{H} = W \oplus W^{\perp}$. Como $dim\ W \geq 2$, então podemos afirmar que $dim\ W^{\perp} \geq 1$. Além disso, por hipótese, o subespaço W é invariante de $\mathcal{E}$, então, pela Proposição 7.3, o subespaço $W^{\perp}$ é invariante de $\mathcal{E}^{\dagger}$. Ainda pelo fato de que W é subespaço invariante de $\mathcal{E}$, temos, pela Proposição 7.2, que existe um $|\psi\rangle \in W$ que é ponto fixo de $\mathcal{E}$, ou seja, $\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. Pela equação (7.23), temos que $|\psi\rangle$ também é ponto fixo para $\mathcal{E}^{\dagger}$, isto é, $\mathcal{E}^{\dagger}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. Por outro lado, vamos supor que $|\phi\rangle \in W^{\perp}$, então, temos que $|\psi\rangle$ e $|\phi\rangle$ são estados ortogonais. Denotemos $a = |\psi\rangle\langle\psi|$ e $b = |\phi\rangle\langle\phi|$. Então para provar que $C^{(0)}(\mathcal{E})$ é positiva, em conformidade com a discussão desenvolvida na Seção III deste estudo, basta provar que

$$tr(\mathcal{E}(a)\mathcal{E}(b)) = 0. \tag{7.24}$$

De fato,

$$tr(\mathcal{E}(a)\mathcal{E}(b)) = tr\left(\sum_{i=1}^{\kappa} E_i\,|\psi\rangle\langle\psi|\,E_i^{\dagger}\sum_{j=1}^{\kappa} E_j\,|\phi\rangle\langle\phi|\,E_j^{\dagger}\right) \tag{7.25}$$

$$= tr\left[\left(\sum_{i,j=1}^{\kappa} E_j^{\dagger}E_i\,|\psi\rangle\langle\psi|\,E_i^{\dagger}E_j\right)|\phi\rangle\langle\phi|\right] \tag{7.26}$$

$$= tr[(\mathcal{E}^{\dagger}\circ\mathcal{E})(|\psi\rangle\langle\psi|)\,|\phi\rangle\langle\phi|] \tag{7.27}$$

$$= tr[(\mathcal{E}^{\dagger}(\mathcal{E}(|\psi\rangle\langle\psi|))\,|\phi\rangle\langle\phi|] \tag{7.28}$$

$$= tr[\mathcal{E}^{\dagger}(|\psi\rangle\langle\psi|)\,|\phi\rangle\langle\phi|] \tag{7.29}$$

$$= tr[|\psi\rangle\langle\psi|\,|\phi\rangle\langle\phi|] = 0. \tag{7.30}$$

Assim sendo, se $W \subset \mathcal{H}$ é um subespaço invariante de um canal quântico unital $\mathcal{E}$, com $dim\ W = s$ e $2 \leq s < d$, então $C^{(0)}(\mathcal{E})$ é positiva.

□

O exemplo a seguir apresenta o modelo matemático de um canal quântico unital, com um subespaço invariante de dimensão dois.

Exemplo 7.2 ([45]) *Seja um canal quântico $\mathcal{E}$ representado por operadores de Kraus E_1, E_2 e E_3, dados por*

$$E_1 = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{2} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{\sqrt{2}}{2} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{\sqrt{2}}{2} & 0 \end{pmatrix}, E_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\sqrt{2}}{2} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \frac{\sqrt{2}}{2} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

O canal quântico $\mathcal{E}$ é unital, pois $\mathcal{E}(I) = \sum_{i=1}^{3} E_i^\dagger I E_i = I$. Além disso, o subespaço

$$W = Span\{|\psi_1\rangle, |\psi_2\rangle\} \tag{7.31}$$

em que $|\psi_1\rangle = (0,1,0,0,0)$ e $|\psi_1\rangle = (0,0,1,0,0)$ tem dimensão 2 e é subespaço invariante de $\mathcal{E}$, logo, pelo Teorema 7.3, temos que $C^{(0)}(\mathcal{E})$ é positiva.

Ao fim desta seção, podemos apresentar algumas conclusões relacionadas ao objetivo proposto, que é investigar as relações entre a capacidade de erro-zero e os subespaços invariantes dos canais quânticos. Inicialmente, podemos afirmar que existem duas conexões entre esses conceitos. A primeira, apresentada no Teorema 7.2, assegura que canais quânticos com subespaços invariantes que apenas se interceptam trivialmente resultam na capacidade de erro-zero positiva do canal quântico. Já a segunda, provada no Teorema 7.3, mostra que um canal quântico unital com subespaço invariante de dimensão no mínimo 2 tem capacidade de erro-zero positiva. Para estudos futuros, temos a pretensão de provar o último resultado, retirando a hipótese de que o canal seja unital.

Capítulo 8

Canais Quânticos Não-Ergódicos e a Teoria da Informação Quântica Erro-Zero

A definição rigorosa de canais ergódicos remonta a uma série de trabalhos surgidos no final da década de 1970, que estabeleceram o contexto matemático adequado e exploraram algumas aplicações do conceito [47], [48]. Uma definição de canais ergódicos pode ser dada da seguinte forma: dizemos que um canal quântico é ergódico quando admite um ponto fixo único no espaço das matrizes de densidade [49]. O estudo da ergodicidade de um canal quântico tem sido objeto de muita investigação e tem encontrado aplicações em várias subáreas da Teoria da Informação Quântica [42], [50], [51].

Definição 8.1 ([42]) *Seja um canal quântico* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$. *Dizemos que* $\mathcal{E}$ *é ergódico quando admite um único ponto fixo.*

No trabalho [42], Burgarth apresenta uma caracterização sistemática dos canais quânticos ergódicos em espaços vetoriais com dimensão finita, em termos de subespaços invariantes dos canais quânticos. Como ponto de partida para essa caracterização, é apresentado o seguinte resultado:

Lema 8.1 ([42]) *Seja um canal quântico* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ *e* $A \in \mathcal{B}(\mathcal{H})$ *um ponto fixo de* $\mathcal{E}$, *escreva* $A = (X_+ - X_-) + i(Y_+ - Y_-)$, *em que* X_+, X_-, Y_+ *e* Y_- *são operadores positivos em* $\mathcal{B}(\mathcal{H})$ *tais que* $X_+X_- = X_-X_+ = Y_+Y_- = Y_-Y_+ = 0$. *Então,* X_+, X_-, Y_+ *e* Y_- *são pontos fixos de* $\mathcal{E}$.

Como consequência deste resultado, Burgarth [42] afirma que os canais quânticos não-ergódicos são canais quânticos que admitem pelo menos dois pontos fixos distintos.

Corolário 8.1 ([42]) *Seja um canal quântico $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ tais que ρ e ρ' são dois pontos fixos distintos de $\mathcal{E}$. Então, ρ e ρ' tem suportes ortogonais.*

Diante do exposto, propomos a seguinte definição para canais quânticos não-ergódicos:

Definição 8.2 *Seja um canal quântico $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$. Dizemos que $\mathcal{E}$ é não-ergódico se $\mathcal{E}$ possui pelo menos dois pontos fixos distintos.*

A seguir, apresentamos um resultado que relaciona a classe dos canais quânticos não-ergódicos com o conceito de capacidade de erro-zero dos canais quânticos.

Teorema 8.1 *Seja $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ um canal quântico não-ergódico. Então a capacidade de erro-zero de $\mathcal{E}$ é positiva.*

Prova: Temos por hipótese que $\mathcal{E}$ é um canal não-ergódico. Então, por definição, $\mathcal{E}$ possui pelo menos dois pontos fixos distintos. Pelo Teorema 4.3, a capacidade de erro-zero de um canal quântico é limitada inferiormente pelo *log* do número de pontos fixos distintos do canal. Portanto, para um canal não-ergódico $\mathcal{E}$, a capacidade de erro-zero é dada por $C^{(0)}(\mathcal{E}) \geq log\ 2$.

□

A recíproca do Teorema 8.1 é inválida, isto é, existe um canal quântico com capacidade de erro-zero positiva que tem um único ponto fixo. Abaixo, segue um exemplo ilustrando isso:

Exemplo 8.1 ([19]) *Seja um canal quântico $\mathcal{E}$, representado pelos operadores de Kraus a seguir:*

$$E_1 = \alpha(|00\rangle\langle 00| + |11\rangle\langle 11|) + |01\rangle\langle 01| + |10\rangle\langle 10| \tag{8.1}$$

$$E_2 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|) \tag{8.2}$$

$$E_3 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| - |01\rangle\langle 01| - |10\rangle\langle 10|) \tag{8.3}$$

em que o escalar q é tal que $0 < p < 1$ e $\alpha = \sqrt{1-2q}$, $\beta = \sqrt{q/2}$. O canal possui um único ponto fixo e não é unital, isto é, $\mathcal{E}(I) = \sum_{i=1}^{3} E_i E_i^\dagger \neq I$. Isso significa, que o ponto fixo de $\mathcal{E}$ é algum operador diferente da identidade. Além disso, neste modelo de canal, existe apenas um único estado ρ tal que $\mathcal{E}(\rho) = \rho$ [19, Exemplo 6.2]. A capacidade de

erro-zero deste canal é positiva. Para ver isso, escolhendo os estados $|00\rangle = (1,0,0,0)$ *e* $|10\rangle = (0,0,1,0)$*, temos que* $tr(\mathcal{E}(|00\rangle)\mathcal{E}(|10\rangle)) = 0$*, e dessa forma a capacidade de erro-zero deste canal quântico é positiva.*

O resultado a seguir apresentar mostra uma condição para que um canal quântico, simultaneamente, ter capacidade erro-zero positiva e ser não-ergódico.

Teorema 8.2 *Seja* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ *um canal quântico tais que* $W_1 \neq \{0\}$ *e* $W_2 \neq \{0\}$ *são subespaços invariantes de* $\mathcal{E}$ *e* $W_1 \cap W_2 = \{0\}$*. Então,* $\mathcal{E}$ *tem capacidade de erro-zero positiva e é também não-ergódico.*

Prova: Como $W_1 \neq \{0\}$ e $W_2 \neq \{0\}$ são subespaços invariantes de $\mathcal{E}$, então, pela segunda parte da Proposição 7.2, temos que existem $\rho_{W_1} \in W_1$ e $\rho_{W_2} \in W_2$ que são pontos fixos de $\mathcal{E}$. Assim, a capacidade de erro-zero de $\mathcal{E}$ é tal que $C^0(\mathcal{E}) > log\ 2$. Além disso, como $\mathcal{E}$ possui pelo menos dois pontos fixos, segue que $\mathcal{E}$ é não-ergódico.

□

Teorema 8.3 *Seja* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ *um canal quântico unital e não-ergódico. Então, o adjunto* $\mathcal{E}^\dagger$ *possui capacidade de erro-zero positiva.*

Prova: Por hipótese, o canal $\mathcal{E}$ é unital. Então, pelas Equações (7.22) e (7.23), temos que $\mathcal{E}$ e $\mathcal{E}^\dagger$ têm os mesmos pontos fixos. Como $\mathcal{E}$ é não-ergódico, então $\mathcal{E}$ possui pelo menos dois pontos fixos; consequentemente, o mesmo acontece com $\mathcal{E}^\dagger$. Portanto, pelo Teorema 4.3, concluímos que a capacidade de erro-zero do canal adjunto $\mathcal{E}^\dagger$ é positiva.

□

A partir do que provamos no Teorema 8.3, vamos fazer algumas observações a respeito dos pontos fixos de $\mathcal{E}$ e $\mathcal{E}^\dagger$, que são muito importantes para o cálculo da capacidade de erro-zero desses canais. Antes, enunciaremos o lema a seguir, cuja prova é baseada em [42, Teorema 1, Teorema 7].

Lema 8.2 *Seja* $\mathcal{E} : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$ *um canal quântico não-ergódico. Então,* $\mathcal{E}$ *e* $\mathcal{E}^\dagger$ *possuem, respectivamente, subespaços invariantes não triviais.*

Primeiramente, a partir das ideias no parágrafo que antecede imediatamente as Equações (7.22) e (7.23), temos que, sendo canal $\mathcal{E}$ unital, então o canal fixa a identidade

($\mathcal{E}(I) = I$). Da mesma forma, o canal adjunto $\mathcal{E}^\dagger$ fixa também a identidade ($\mathcal{E}^\dagger(I) = I$). Além disso, exite um projetor $0 < P < I$ tal que

$$\mathcal{E}(P) = P, \tag{8.4}$$

ou, equivalentemente,

$$\mathcal{E}^\dagger(P) = P. \tag{8.5}$$

Para provar as Equações (8.4) e (8.5), note que, sendo $\mathcal{E}$ um canal não-ergódico, então, pelo Lema 8.2, $\mathcal{E}$ possui um subespaço W não trivial invariante. Assim, pelas propriedades equivalentes da definição de subespaço invariante de $\mathcal{E}$, existe um projetor P tal que

$$E_i P = P E_i P \quad \text{e} \quad E_i^\dagger P = P E_i^\dagger P \tag{8.6}$$

para $i = 1, ..., \kappa$. A partir destas relações obtemos, $E_i P = P E_i$ e $E_i^\dagger P = P E_i^\dagger$ para $i = 1, ..., \kappa$. Dessa forma,

$$\mathcal{E}(P) = \sum_{i=1}^{\kappa} E_i P E_i^\dagger = \sum_{i=1}^{\kappa} E_i E_i^\dagger P = \sum_{i=1}^{\kappa} \mathcal{E}(I) P = P. \tag{8.7}$$

De modo análogo, podemos provar que $\mathcal{E}^\dagger(P) = P$. A partir de análises preliminares, podemos concluir que a capacidade de erro-zero do canal $\mathcal{E}$ unital não-ergódico, e, consequentemente, de canal adjunto $\mathcal{E}^\dagger$, está diretamente relacionada ao número de projetores P (incluindo o projetor indentidade I), fixados pelos canais $\mathcal{E}$ e $\mathcal{E}^\dagger$, respectivamente.

Capítulo 9

Considerações Finais

Na Teoria da Informação Quântica Erro-Zero, uma das subáreas de pesquisa é a capacidade de erro-zero dos canais quânticos, que é o estudo do limite máximo das taxas em que os canais quânticos podem enviar mensagens com erro de decodificação exatamente igual a zero. Dessa forma, saber se os canais quânticos têm ou não capacidade de erro-zero positiva é muito importante. Nesse sentido, existem, então, na literatura à qual tivemos acesso, três testes que verificam se os canais quânticos têm ou não, capacidade de erro-zero positiva, os quais foram mencionados ao longo do Capítulo 4 deste trabalho. Esses testes requerem um trabalho matemático bastante denso, ao passo que necessitam verificar condições matemáticas em d^2 estados quânticos, caso o espaço Hilbert do sistema tenha dimensão d, para decidir se o canal quântico tem ou não capacidade de erro-zero positiva. Diante disso, propusemos no Capítulo 5 deste trabalho de tese, um teste de capacidade de erro-zero para canais quânticos representados por operadores de Kraus. O nosso teste leva em consideração estados próprios comuns aos operadores de Kraus do canal; consequentemente, requer uma verificação de d estados próprios, isto é, acaba sendo um teste vantajoso em relação aos anteriores.

Ainda nessa linha de contribuir para a subárea de capacidade de erro-zero dos canais quânticos, no Capítulo 6, desenvolvemos algumas conexões entre o Teorema de Shemesh e a capacidade de erro-zero dos canais quânticos. Até então, já existiam relações importantes do Teorema de Shemesh com os estudos dos canais quânticos, por exemplo, a sondagem da estrutura interna da álgebra gerada pelos operadores de Kraus que representam os canais quânticos e também o uso do teorema para decidir sobre a irredutibilidade ou não dos canais quânticos. No nosso trabalho de tese, fizemos uma abordagem provavelmente original, ao passo que relacionamos o Teorema de Shemesh com a capacidade de erro-zero dos canais quânticos, mostrando, por exemplo, que os pontos fixos dos canais quânticos pertencem ao subespaço de Shemesh. Como a capacidade de erro-zero do canal se relaciona com o número de pontos fixos do canal, dessa forma, segue uma conclusão sobre as

conexões entre o Teorema Shemesh e a capacidade de erro-zero dos canais quânticos.

Outra questão relevante que trouxemos para este trabalho de tese é o que fizemos no Capítulo 7, quando relacionamos o conceito de subespaço invariante e o conceito de capacidade de erro-zero dos canais quânticos. Em outras palavras, obedecendo às hipóteses matemáticas da dimensão ≥ 2 do subespaço invariante do canal quântico, o subespaço funciona como "um lugar de erro-zero"para os canais quânticos. Isso, ao nosso entender, é muito significativo para as pesquisas envolvendo capacidade de erro-zero dos canais quânticos.

Por fim, no Capítulo 8 investigamos uma classe de canais bastante importante para a Teoria da Informação Quântica, que são os canais ergódicos. Nessa investigação, conseguimos propor uma definição para outra classe de canais, os chamados canais quânticos não-ergódicos, que são aqueles que possuem pelo menos dois pontos fixos. Ora, há uma relação entre o número de pontos fixos e a capacidade de erro-zero dos canais quânticos. Dessa forma, conseguimos organizar algumas conexões iniciais entre canais quânticos não-ergódicos e a capacidade erro-zero dos canais quânticos.

9.1 Trabalhos Futuros

Nos desenvolvimentos realizados neste trabalho de tese, temos a percepção de que dá para ir mais além em alguns resultados apresentados.

- **Em relação às conexões do teorema de Shemesh e à capacidade de erro-zero dos canais quânticos.**
  Compreendemos que um estudo mais refinado do subespaço de Shemesh pode apontar novos limitantes para a capacidade de erro-zero dos canais quânticos representados por operadores de Kraus.

- **Em relação ao subespaço invariante e à capacidade de erro-zero dos canais quânticos.**
  Entendemos que esse "lugar de erro-zero"pode ainda ser explorado com mais profundidade. Na tese, mostramos que, se o canal quântico tem um subespaço invariante de dimensão ≥ 2, isso implica que a capacidade de erro-zero do canal é positiva. Então, uma ideia é investigar a recíproca deste resultado.

- **Em relação aos canais quânticos não-ergódicos.**
  Neste trabalho de tese, compreendemos que os resultados desenvolvidos são embrionários, diante do que pode ser explorado. Por exemplo, será possível relacionar os

canais quânticos não-ergódicos com o limite quântico proposto pela desigualdade de Wielandt [58]?

São questões e perguntas ainda em fase inicial de reflexão.

Referências Bibliográficas

1 COVER, T. M.; THOMAS, J. A. *Elements of Information Theory.* John Wiley & Sons, 2006. Citado nas páginas 8, 13 e 31.

2 NYQUIST, H. Certain Factors Affecting Telegraph Speed. *Transactions of the American Institute of Electrical Engineers,* v. XLIII, p. 412-422, 1924. Citado na página 13.

3 HARTLEY, R.V.L. Transmission of Information. *Bell System Technical Journal,* v. 7, p. 535-563, 1928. Citado na página 13.

4 SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948. Citado nas páginas 13, 33, 38, 40 e 41.

5 NIELSEN, M.A; CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* [S.l.]: Cambridge University Press, 2010. Citado nas páginas 14, 19, 22, 28, 35, 36, 37, 38, 45 e 46.

6 BENNETT, C. H.; SHOR, P. W. Quantum information theory. *IEEE Trans. Info. Theory*, v. 44, n. 6, p. 2724–2755, 1998. Citado na página 14.

7 NIELSEN, M. A. *Quantum Information Theory.* Tese (Doutorado) — University of New México - Albuquerque, New México, USA, 1998. Citado na página 14.

8 GUEDES, E. B. *Capacidade Quântica de Sigilo Erro-Zero e Informação Acessível Erro-Zero de Fontes Quânticas.* Tese (Doutorado)- Universidade Federal de Campina Grande - Campina Grande, Paraíba, Brasil, 2013. Citado nas páginas 14, 19, 23, 28, 35, 38, 41 e 42.

9 SHANNON, C. E. The zero error capaciy of a noisy channel. *IRE Trans. Inform. Theory,* IT-2(3):8–19, 1956. Citado nas páginas 14 e 40.

10 MEDEIROS, R. A. C.; ASSIS F. M. de. Quantum Zero-Error Capacity. *International Journal of Quantum Information,* v. 3, n. 1, p. 135-139, 2005. Citado nas páginas 14, 15, 38, 43 e 45.

11 MEDEIROS, Rex A. da C. *Capacidade Erro-Zero de Canais Quânticos*. Tese (Doutorado)- Coordenação dos Cursos de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, Brasil, e de TELECOM ParisTech, França - Campina Grande, Paraíba, Brasil, 2008. Citado nas páginas 8, 14, 15, 28, 38, 41, 42 e 43.

12 WILDE, M. M. *From Classical to Quantum Shannon Theory*. Cambridge, New York: Cambridge University Press, 2019. Citado nas páginas 15, 19 e 28.

13 HOLEVO, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Info. Theory*, v. 44, n. 1, p. 269–273, 1998. Citado nas páginas 15 e 37.

14 SCHUMACHER, B.; WESTMORELAND, M. D. Sending classical information via noisy quantum channels. *Phys. Rev. A*, v. 56, n. 1, p. 131–138, 1997. Citado nas páginas 15 e 37.

15 BEIGI, S.; SHOR, P. W. On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels. *arXiv:quant-ph/*0709.2090, 2008. Citado na página 15.

16 SANZ, M.; PÉREZ-GARCIA, D.; WOLF, M. M.; CIRAC, J. I. A Quantum Version of Wielandt's Inequality. *IEEE Transactions On Information Theory*, v. 56, n. 9, 2010. Citado nas páginas 15 e 79.

17 DUAN, R.; SEVERINI, S.; WINTER, A. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz ϑ function. *IEEE International Symposium on Information Theory*. São Petersburgo, Rússia: IEEE Press, p. 64-68, 2011. Citado na página 15.

18 YAMASAKI, H; MURAO, M. Quantum State Merging for Arbitrarily Small-Dimensional Systems. *IEEE Transactions On Information Theory*, v. 65, n. 6, p. 3950-3972, 2019. Citado na página 15.

19 GUEDES, E. B.; ASSIS, F. M.; MEDEIROS, R. A.C. *Quantum Zero-Error Information Theory*. Springer, 2016. Citado nas páginas 8, 15, 28, 38, 40, 41, 42, 44 e 74.

20 DERENIOWSKI, D; JURKIEWICZ, M. On the Characteristic Graph of a Discrete Symmetric Channel. *IEEE Transactions On Information Theory*, V. 67, N. 6, P. 3818-3823, 2021. Citado na página 15.

21 MEDEIROS, R. A. C.; ALLEAUME, R., COHEN, G.; ASSIS, F. M. de. Zero-Error Capacity of Quantum Channels and Noiseless Subsystems. *IEEE International Telecommunications Symposium,* p. 900 - 905, 2006. Citado nas páginas 15, 38, 44 e 51.

22 GUPTA, V. P., MANDAYAM P.; SUNDER, V.S. *The Functional Analysis of Quantum Information Theory.* Springer, 2015. Citado nas páginas 15, 38, 46 e 47.

23 OLIVEIRA, M. M. de; ASSIS, F. M. de. Uma conjectura: o teorema de Shemesh e a capacidade erro-zero de canais quânticos com dois operadores de kraus. *XL Simpósio Brasileiro de Telecomunicações - SBrT 2022*, Sta. Rita do Sapucaí - MG, 2022. DOI: 10.14209/sbrt.2022.1570824539. Citado nas páginas 15, 54 e 57.

24 SHEMESH, D. Common Elgenvectors of Two Matrices. *Department of Mathematics, Technion* - Israel Institute of Technolog, 1984. Citado nas páginas 15 e 55.

25 BIAŁOŃCZYK, M.; JAMIOŁKOWSKI A.; ZYCZKOWSKI, K. Application of Shemesh theorem to quantum channels. *Journal of Mathematical Physics*, 59, 102-204, 2018. Citado nas páginas 16, 36, 55 e 101.

26 AMITSUR, S. A.; LEVITZKI, J. Minimal identities for algebras. *Proc. Amer. Math. Soc.,* v.1, p. 449-463, 1950. Citado nas páginas 16, 99 e 100.

27 KOSTANT, B. *A theorem of Frobenius, a theorem of Amitsur-Levitski and cohomology theory.* J. Math. Mech. 7, 237-264 (1958). Citado na página 16.

28 DRENSKY, V. *Free algebras and PI algebras: Graduate Course in Algebra.* Springer Verlag PTE.LTD, 1999. Citado na página 16.

29 JAMIOŁKOWSKI A. On applications of PI-algebras in the analysis of quantum channels. *International Journal of Quantum Information*, vol. 10, n. 8, 2012. Citado nas páginas 16, 55 e 57.

30 JAMIOŁKOWSKI A.; PASTUSZAK, G. Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive superoperators. *arXiv:1306.0083,* v.1, [math.QA], p. 1-17, 2013. Citado nas páginas 16, 56 e 101.

31 JORDAN, A. N.and SIDDIQI, I. A. *Quantum Measurement: Theory and Practice.* Cambridge University Press, 2024. Citado nas páginas 19 e 22.

32 DIAS, M. A. *Distribuição Quântica de Chaves com Modulação não Gaussiana: Protocolos, Desempenho e Segurança.* Tese (Doutorado)- Universidade Federal de Campina Grande - Campina Grande, Paraíba, Brasil, 2023. Citado nas páginas 19 e 28.

33 MERMIN, N. D., *Quantum Computer Science - An Introduction.* Cambridge, Inglaterra: Cambridge University Press, 2007 Citado na página 22.

34 BLITZSTEIN, J. K. and HWANG, J. *Introduction to Probability.* 2nd edition. Chapman and Hall/CRC,2019. Citado na página 28.

35 COLES, P. J. *et al.* Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, v. 89, n. 1, 2017. Citado na página 33.

36 SMART, D. R. *Fixed point theorems*, Cambridge University Press, 1974. Citado na página 45.

37 MEDEIROS, R. A. C.; ASSIS, F. M. de. Capacidade erro-zero de canais quânticos e estados puros. *XXXI Simpósio Brasileiro de Telecomunicações - SBrT 2013*, Fortaleza, Ceará, Brasil, 2013. Citado nas páginas 38, 46 e 64.

38 OLIVEIRA, M. M. de, ASSIS, F. M. de and DIAS, M. A. *A condition for the zero-error capacity of quantum channels.* Em Anais do XLI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais, 2023, doi: 10.14209/sbrt.2023.1570917602. Citado nas páginas 49, 50, 51 e 52.

39 MCCOY, N. H. On the characteristic roots of matric polynomials. *Bull. Amer. Math. Sot.* 42:592-600, 1936. Citado na página 55.

40 FRALEIGH, J. B. *A First Course in Abstract Algebra.* 7th ed., Pearson, 2002. Citado na página 55.

41 GOHBERG, I., LANCASTER, P. and RODMAN, L. *Invariant Subspaces of Matrices with Applications.* Wiley-Interscience, New York, 1986. Citado nas páginas 62 e 67.

42 BURGARTH, D., CHIRIBELLA, G., GIOVANNETTI, V., PERINOTTI, P. and YUASA K. Ergodic and mixing quantum channels in finite dimensions. *New Journal of Physics*, vol. 15 073045, 2013, doi: 10.1088/1367-2630/15/7/073045. Citado nas páginas 63, 68, 69, 70, 73, 74 e 75.

43 OLIVEIRA, M. M. de, SILVA, A. da, DIAS, M. A. and ASSIS F. M. de. *Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels.* VII Workshop Escola de Computação e Informação Quântica - WECIQ, 21 a 23 de agosto de 2024, Rio de Janeiro-RJ. Citado nas páginas 63, 64 e 65.

44 CHOI, Man-Duen and KRIBS, D. W. A Method to Find Quantum Noiseless Subsystems. *Phys. Rev. Lett.* 96, 050501 – Published 6 February 2006, doi:10.1103/PhysRevLett.96.050501. Citado nas páginas 68 e 70.

45 OLIVEIRA, M. M. de, SILVA, A. da, DIAS, M. A. and ASSIS F. M. de. *Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels.* XLII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais De 01 a 04 de outubro de 2024, Belém - PA. Citado nas páginas 69, 70 e 71.

46 KRIBS, D. W. Quantum channels, wavelets, dilations, and representations of on. *Proc. Edin. Math. Soc.*, vol. 46, pp. 421–433, 2003, doi::10.1017/S0013091501000980. Citado na página 70.

47 SPOHN, H. *Kinetic equations from Hamiltonian dynamics: Markovian limits*. Rev. Mod. Phys. 52, 569, 1980 Citado na página 73.

48 RUELLE, D. *Ergodic theory of differentiable dynamic systems*. IHES Publ. Math. 50 (1): 27–58, 1979, doi:10.1007/BF02684768. Citado na página 73.

49 STREATER, R. F. *Statistical Dynamics: A Stochastic Approach To Nonequilibrium Thermodynamics*. 2nd ed.,World Scientific Publishing Company, 2009. Citado na página 73.

50 BRÉMAUD, P. *Probability Theory and Stochastic Processes*. Springer, 2020. Citado na página 73.

51 WOLF, M. M. *Quantum channels and operations: Guided tour*. unpublished, 2012. Citado na página 73.

52 DIRAC, P. *The principies of Quantum Mechanics*. 4th. ed. Oxford, Inglaterra: Oxford University Press, 1982. Citado na página 87.

53 HORN, R. A.; JOHNSON, C. R. *Topics in Matrix Analysis*. [U.K.]: Cambridge University Press, 1991. Citado na página 85.

54 BHATIA, R. *Positive Definite Matrices*. Princeton University Press, 2007. Citado na página 85.

55 ZHANG, F. *Matrix Theory: Basic Results and Techniques*. 2nd ed. Springer, 2011. Citado na página 85.

56 HOFFMAN, K. ; KUNZE R. *Linear Algebra*. 2th ed. PRENTICE-HALL, Inc., Englewood Cliffs, New Jersey, 2001. Citado na página 90.

57 GIAMBRUNI, A.; ZAICEV, M. *Polynomial identities and asymptotic methods*. Amercan Mathematical Society, v. 122, 2005. Citado na página 99.

58 SANZ, M.; PÉREZ-GARCIA, D.; WOLF, M. M.; CIRAC, J. I. A Quantum Version of Wielandt's Inequality. *IEEE Transactions On Information Theory*, v. 56, n. 9, 2010. Citado nas páginas 15 e 79.

Apêndice A

Conceitos Básicos de Álgebra Linear e a PI-Álgebras

Nesta seção, apresentaremos uma síntese dos conceitos básicos de Álgebra Linear, tomando como base os livros *Matrix Analysis* dos autores Horn e Johnson [53], *Positive Definite Matrices* de Bhatia [54] e *Matrix Theory: Basic Results and Techniques* de Zhang [55].

A.1 Revisão de álgebra linear

A.1.1 Espaço Vetorial

Nesta seção, revisamos a estrutura básica da Álgebra Linear, que é a do espaço vetorial. A definição de um espaço vetorial V, cujos elementos são chamados de vetores, envolve um corpo matemático F arbitrário, cujos elementos são chamados de escalares. Corrigir tempo verbal.

Definição A.1 (Espaço vetorial) *Seja V um conjunto não-vazio de vetores e F um corpo matemático, munido com duas operações:*

*i. (Adição de vetores) Associa a quaisquer $u, v \in V$ a **soma** $u + v \in V$.*

*ii. (Multiplicação por escalar) Associa a quaisquer $u \in V$, $a \in F$ o **produto de vetor por escalar** $au \in V$.*

Então, dizemos que V é um espaço vetorial (sobre o corpo F) se os axiomas seguintes forem válidos.

1. *Associatividade:* $u + (v + w) = (u + v) + w$, *para todos* $u, v, w \in V$.

2. *Elemento neutro: existe* $0 \in V$ *tal que* $u + 0 = u$, *para todo* $u \in V$.

3. *Elemento oposto: para cada* $u \in V$, *existe* $-u \in V$ *tal que* $u + (-u) = 0$.

4. *Comutatividade:* $u + v = v + u$, *para todos* $u + v \in V$.

5. *Associatividade da multiplicação por escalar:* $a(bu) = (ab)u$, *para todos* $a, b \in F$ *e* $u \in V$.

6. *Distributiva da soma de escalares em relação a um vetor:* $(a + b)u = au + bu$, *para todos* $a, b \in F$ *e* $u \in V$.

7. *Distributiva de um escalar em relação à soma de vetores:* $a(u + v) = au + bv$, *para todos* $u, v \in V$ *e* $a \in F$.

8. $1u = u$, *para todo* $u \in V$.

A fim de contextualizar o conceito de espaço vetorial para este trabalho de tese, vamos considerar um vetor como sendo uma d-upla ordenada de números

$$u = (a_1, ..., a_d). \tag{A.1}$$

Se os números $a_i \in \mathbb{R}$, então dizemos que o espaço vetorial é um espaço vetorial real. Por outro lado, se os números $a_i \in \mathbb{C}$, então dizemos que o espaço vetorial é um espaço vetorial complexo. No campo da Mecânica Quântica e da Teoria da Informação Quântica, os espaços vetoriais de interesse são os espaços vetoriais complexos.

No contexto deste trabalho de tese, considere o conjunto $\mathbb{C}^d$, consistindo de todas as d-uplas de números complexos, as quais são muito importantes. Isto é, para cada número inteiro $d \geq 1$, seja $\mathbb{C}^d$ o conjunto de vetores-colunas

$$\begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix} \tag{A.2}$$

tais que $a_i \in \mathbb{C}, \forall i = 1, \ldots, d$. Assim, definindo as operações de soma e produto de vetor por escalar, respectivamente, como sendo:

1. $\begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix} + \begin{pmatrix} b_1 \\ : \\ b_d \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ : \\ a_d + b_d \end{pmatrix}, \ \forall \begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix}, \begin{pmatrix} b_1 \\ : \\ b_d \end{pmatrix} \in \mathbb{C}^d.$

$$2.\ a\begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix} = \begin{pmatrix} aa_1 \\ : \\ aa_d \end{pmatrix},\ \forall a \in \mathbb{C}, \begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix} \in \mathbb{C}^d.$$

Temos que duas operações satisfazem os itens da Definição A.1 de espaço vetorial, de modo que $\mathbb{C}^d$ é um espaço vetorial sobre $\mathbb{C}$.

É oportuno fazermos alguns comentários sobre os elementos do espaço vetorial $\mathbb{C}^d$, uma vez que, dado um vetor coluna $u \in \mathbb{C}^d$, o transposto do vetor u é o vetor linha, denotado por u^T. Isto é, dado um vetor

$$u = \begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix} \in \mathbb{C}^d,\ \text{escrevemos } u^T = (a_1, ..., a_d)^T. \tag{A.3}$$

O conjugado complexo de um vetor u é denotado por u^*. O transposto conjugado do vetor u é denotado por $u^\dagger$, ou seja,

$$u^\dagger = (u^*)^T = (u^T)^*. \tag{A.4}$$

Além deste exemplo, vamos considerar o conjunto das matrizes $M_d(\mathbb{C})$ quadradas de ordem d com entradas no corpo dos complexos $\mathbb{C}$. Então, considerando as operações usuais de soma de matrizes e de multiplicação de matrizes por escalares, é possível verificar que essas duas operações satisfazem os itens da Definição A.1 de espaço vetorial, de modo que $M_d(\mathbb{C})$ é um espaço vetorial sobre $\mathbb{C}$.

No que se refere ao conceito de transposto e conjugado complexo dos elementos do espaço vetorial $M_d(\mathbb{C})$, vamos dizer que, dado $A \in M_d(\mathbb{C})$, então A^T é a transposta da matriz A e o conjugado de A será denotado por A^*. Além disso, o transposto conjugado de A será denotado por $A^\dagger$, ou seja,

$$A^\dagger = (A^*)^T = (A^T)^*. \tag{A.5}$$

A.1.2 A Notação de Dirac

No desenvolvimento da Mecânica Quântica, uma notação bastante particular para os elementos de espaços vetoriais é a notação de Dirac [52]. A notação de Dirac é uma maneira concisa de representar os conceitos da Mecânica Quântica, que implica uma simplificação dos cálculos a serem realizados. *Bra's* e *ket's* são nomes diferentes para vetores linha e coluna:

- Um vetor coluna $u \in \mathbb{C}^d$ é um *ket*,

$$|u\rangle = u = \begin{pmatrix} a_1 \\ : \\ a_d \end{pmatrix}. \tag{A.6}$$

- Um vetor de linhas $u^\dagger \in \mathbb{C}^d$ é um *bra*,

$$\langle u| = u^\dagger = (a_1^*, ..., a_d^*). \tag{A.7}$$

Observe que a mudança de *bra* para *ket* também inclui a conjugação complexa. Na notação de Dirac, a notação para o vetor nulo do espaço vetorial é ainda a notação tradicional 0, visto que as notações $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ são utilizados, respectivamente, para designar os estados 0 e 1 de um *qubit*.

A.1.3 Base e Dimensão

Nesta seção, vamos resumir os conceitos de base e dimensão de um espaço vetorial, os quais também são muito importantes no estudo das estruturas dos espaços vetoriais.

Definição A.2 (Combinação linear) *Seja V um espaço vetorial sobre $\mathbb{C}$. Um vetor $|u\rangle$ em V é uma combinação linear dos vetores $|u_1\rangle, ..., |u_d\rangle$ em V, se exitem escalares $a_1, ..., a_d \in \mathbb{C}$ tais que*

$$|u\rangle = a_1 |u_1\rangle + ... + a_d |u_d\rangle = \sum_{i=1}^{d} a_i |u_i\rangle . \tag{A.8}$$

Como consequência da propriedade associativa da adição de vetores e da propriedade distributiva da multiplicação de vetor por escalar, temos que para combinações lineares:

$$\sum_{i=1}^{d} a_i |u_i\rangle + \sum_{i=1}^{d} b_i |u_i\rangle = \sum_{i=1}^{d} (a_i + b_i) |u_i\rangle \tag{A.9}$$

$$c \sum_{i=1}^{d} a_i |u_i\rangle = \sum_{i=1}^{d} (ca_i) |u_i\rangle . \tag{A.10}$$

Definição A.3 (Independência e dependência linear) *Seja V um espaço vetorial sobre o corpo $\mathbb{C}$. Dizemos que o conjunto de vetores $\beta = |u_1\rangle, \ldots, |u_d\rangle$ em V é linearmente independente quando uma combinação linear dos vetores que resulta no vetor*

nulo implica que todos os escalares são iguais a zero. Em outras palavras, se

$$a_1 |u_1\rangle + ... + a_d |u_d\rangle = 0, \tag{A.11}$$

então, o conjunto de vetores $\beta = \{|u_1\rangle, ..., |u_d\rangle\}$ *em* V *é linearmente independentes, se* $a_1 = ... = a_n = 0$. *Caso contrário, dizemos que o conjunto vetores* $\beta = \{|u_1\rangle, ..., |u_d\rangle\}$ *é linearmente dependente.*

A partir da Definição A.3, podemos apontar algumas consequências imediatas:

1. Qualquer conjunto que contenha um conjunto linearmente dependente é linearmente dependente.
2. Qualquer subconjunto de um conjunto linearmente independente é linearmente independente.
3. Qualquer conjunto que contenha o vetor nulo é linearmente dependente.
4. Um conjunto β de vetores é linearmente independente se, e somente se, cada subconjunto finito de β é linearmente independente.

Definição A.4 (Base) *Seja* V *um espaço vetorial sobre o corpo* $\mathbb{C}$. *Definimos uma base para* V *como sendo um conjunto de vetores* β *em* V *que é linearmente independente e que gera o espaço vetorial* V. *O espaço vetorial* V *é dito ter dimensão finita se possui uma base com uma quantidade finita de vetores.*

Seja V um espaço vetorial sobre $\mathbb{C}$. Definimos a dimensão de V como sendo o número de vetores em uma base de V. Denotamos por dim V a dimensão de um espaço vetorial finito V. Por exemplo, a dimensão do espaço vetorial $\mathbb{C}^d$ é d e a dimensão do espaço vetorial $M_d(\mathbb{C})$ é d^2, ou seja, dim $\mathbb{C}^d = d$ e dim $M_d(\mathbb{C}) = d^2$.

A.1.4 Subespaço

Nesta seção, vamos resumir o conceito de subespaço de um espaço vetorial, o qual é bastante importante para a compreensão de alguns resultados neste trabalho de tese.

Definição A.5 (Subespaço) *Seja* V *um espaço vetorial sobre* $\mathbb{C}$. *Um subespaço de* V *é um subconjunto não vazio* U *de* V *que é, ele próprio, um espaço vetorial sobre* $\mathbb{C}$, *com as operações de adição vetorial e multiplicação por escalar em* V.

A partir dos axiomas de definição de espaço vetorial, podemos verificar de forma imediata que um subconjunto não vazio U de V é um subespaço vetorial se, para quaisquer $|u\rangle, |v\rangle \in U$ e $a \in \mathbb{C}$, temos:

1. $|u\rangle + |v\rangle \in U$
2. $a\,|u\rangle \in U$.

Observe ainda que o vetor nulo pertence ao subespaço U e que, para cada $|u\rangle \in U$, o vetor oposto $(-|u\rangle)$ também pertence ao subespaço U.

Exemplo A.1 *Seja V um espaço vetorial sobre F. A interseção de qualquer conjunto de subespaços de V é um subespaço de V. Para ver isso, considere uma coleção U_t de subespaços de V e seja $U = \bigcap_t U_t$. Então, dados $|u\rangle, |v\rangle \in U_t$ e $a \in F$, temos que $|u\rangle + |v\rangle$ e $a\,|u\rangle$ pertencem a todo U_t. Assim, $|u\rangle + |v\rangle \in \bigcap_t U_t$ e $a\,|u\rangle \in \bigcap_t U_t$. Dessa forma, concluímos que $U = \bigcap_t U_t$ é um subespaço de V.*

Definição A.6 (Subespaço gerado) *Seja $\beta = \{|u_1\rangle, \ldots, |u_d\rangle\}$ um conjunto finito de vetores de um espaço vetorial V. O subespaço gerado por β, o qual denotamos por span(β), é definido como sendo a interseção U de todos os subespaços de V que contêm β.*

Em outras palavras, o subespaço de V gerado por $\beta = \{|u_1\rangle, \ldots, |u_d\rangle\}$ é o conjunto de todas as combinações lineares dos vetores em β. Podemos encontrar mais detalhes sobre essa afirmação no Teorema 3 da referência [56].

A.1.5 Espaço de Hilbert

Definição A.7 (Produto interno) *Seja V um espaço vetorial sobre $\mathbb{C}$. Definimos o produto interno entre dois elementos $|u\rangle, |v\rangle \in V$, como uma função*

$$\begin{array}{rccc} \langle \cdot, \cdot \rangle & : & V \times V & \longrightarrow & \mathbb{C} \\ & & \langle u, v \rangle & \longmapsto & \langle u|v\rangle = a, \end{array}$$

que seguintes às propriedades:

1. *Linearidade: $\langle u|v\rangle = \langle u| \sum_i a_i v_i\rangle = \sum_i a_i \langle u|v_i\rangle$, $|u\rangle, |v_i\rangle \in V$ e $a_i \in \mathbb{C}$.*
2. *Simétrico conjugado: $\langle u|v\rangle = \langle v|u\rangle^*$, $|u\rangle, |v\rangle \in V$.*
3. *Definido positivo: $\langle u|u\rangle > 0$, se $|u\rangle \neq 0$, $\langle u|u\rangle = 0$, se, e somente se, $|u\rangle = 0$, $|u\rangle, |v\rangle \in V$.*

4. Linearidade do conjugado: $\langle \sum_i a_i u_i | v \rangle = \sum_i a_i^* \langle u_i | v \rangle$, $|u_i\rangle, |v\rangle \in V$ *e* $a_i^* \in \mathbb{C}$.

Explicitamente, no espaço vetorial $\mathbb{C}^d$, o produto interno é o produto elementar do *bra* e do *ket*, conforme segue:

$$\langle u|v\rangle = \begin{pmatrix} a_1^*, a_2^*, ..., a_d^* \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ : \\ b_d \end{pmatrix} = \sum_{i=1}^{d} a_i^* b_i. \tag{A.12}$$

Por outro lado, seja V um espaço vetorial sobre $\mathbb{C}$ e $|u\rangle, |v\rangle \in V$. Dizemos que $|u\rangle$ e $|v\rangle$ são ortogonais se:

$$\langle u|v\rangle = \langle v|u\rangle = 0. \tag{A.13}$$

Definimos, ainda, a norma de $|u\rangle \in V$ como:

$$|| \, |u\rangle \, || = \sqrt{\langle u|u\rangle}. \tag{A.14}$$

Dizemos também que o vetor $|u\rangle$ é unitário se $|| \, |u\rangle \, || = 1$. É importante destacar que, a partir de qualquer vetor não nulo $|u\rangle$, podemos construir um vetor unitário $|u\rangle_{\text{normal}}$, definindo:

$$|u\rangle_{normal} = \frac{|u\rangle}{|| \, |u\rangle \, ||}. \tag{A.15}$$

O vetor $|u\rangle_{\text{normal}}$ é chamado de vetor normalizado. É importante destacar que um estado quântico é representado por um vetor normalizado. Além disso, devemos ressaltar que dois vetores normalizados $|u\rangle$ e $e^{i\phi}|u\rangle$, que diferem por uma fase $\phi \in \mathbb{R}$, representam o mesmo estado quântico. Um conjunto de vetores $|i\rangle$ é dito ortonormal se $\langle i|j\rangle = \delta ij$ (delta de *Kronecker*) e se todos são unitários. Uma base ortogonal para um espaço vetorial de dimensão d é um conjunto de d vetores mutuamente ortogonais. Uma base ortogonal é ortonormal se todos os vetores forem unitários.

O conceito de métrica é necessário para definir o espaço vetorial de Hilbert.

Definição A.8 (Métrica) *Seja um conjunto* M *não vazio. Uma função* $d : M \times M \longrightarrow \mathbb{R}$ *é uma métrica no conjunto* M *quando, para todo par* $x, y \in M$*, o número real* $d(x, y)$ *satisfaz às seguintes condições:*

1. $d(x, y) = 0$ *se, e somente se,* $x = y$.

2. $d(x, y) \geq 0$.

3. $d(x, y) = d(y, x)$.

4. $d(x, z) \leq d(x, y) + d(x, z)$ *(Desigualdade triangular).*

Um espaço métrico, que denotamos por (M, d), é um par formado por um conjunto não vazio M e uma métrica $d(x, y)$.

Definição A.9 (Sequência de Cauchy) *Uma sequência $\{x_n\}$ em um espaço métrico (M, d) é uma sequência de Cauchy se, para cada $\epsilon > 0$, existe um número natural n_0 tal que $d(x_n, x_m) \leq \epsilon$ para $n, m \geq n_0$.*

Um espaço métrico (M, d) é completo quando todas as sequências de Cauchy convergem para um limite que pertence ao espaço. Por definição, todo espaço vetorial com produto interno tem uma métrica associada e, portanto, são espaços métricos.

Definição A.10 (Espaço de Hilbert) *Seja $\mathcal{H}$ um espaço vetorial sobre $\mathbb{C}$ e $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$ um produto interno. Dizemos que $\mathcal{H}$ é um espaço de Hilbert se for completo com a norma induzida pelo produto interno.*

A.1.6 Operadores lineares

Nesta seção, vamos introduzir as transformações lineares, que são funções que relacionam espaços vetoriais e levam em consideração as operações desses espaços vetoriais. Ao longo desta introdução, vamos nos concentrar em alguns aspectos das transformações lineares do espaço vetorial nele mesmo (ou seja, operadores lineares) que consideramos importantes para este trabalho de tese.

Definição A.11 (Transformação linear) *Sejam V e W espaços vetoriais sobre $\mathbb{C}$. Definimos uma transformação linear A de V em W, como uma função $A : V \longrightarrow W$ que satisfaz às seguintes condições:*

1. $A(|u\rangle + |u\rangle) = A(|u\rangle) + A(|v\rangle)$
2. $A(a\,|u\rangle) = aA(|u\rangle)$

para todo $|u\rangle, |u\rangle \in V$ e $a \in \mathbb{C}$.

Sendo uma transformação linear $A : V \longrightarrow W$ tal que A é injetora e sobrejetora simultaneamente, então A é chamada de isomorfismo. Neste caso, os espaços vetoriais V e W são ditos isomorfos e denotamos por $V \backsimeq W$. Matematicamente, dois subespaços vetoriais isormorfos preservam as mesmas estrtuturas algébricas.

Na Definição A.11, quando os espaço vetoriais são os mesmos, isto é, $V = W$, então a transformação linear $A : V \longrightarrow V$ é chamada de operador linear de V.

É importante notar que, sendo A um operador linear de V, então vale que $A(0) = 0$. Além disso, um operador linear preserva combinações lineares, ou seja,

$$A(a_1 |u_1\rangle + \cdots + a_d |u_d\rangle) = a_1 A(|u_1\rangle) + \cdots + a_d A(|u_d\rangle), \tag{A.16}$$

para $|u_1\rangle, ..., |u_d\rangle \in V$ e $a_1, ..., a_d \in F$. Além dessas duas propriedades, outra propriedade importante de um operador linear é que, se considerarmos uma base ordenada $\beta = |u_1\rangle, ..., |u_d\rangle$ de um espaço vetorial V sobre $\mathbb{C}$, então existe um único operador linear de V tal que $A |u_i\rangle = |u_j\rangle$, $j = 1, ..., d$.

Exemplo A.2 *Seja V um espaço vetorial sobre $\mathbb{C}$ e $|v\rangle \in V$. O operador identidade I, definido por $I |v\rangle = |v\rangle$, é um operador linear de V. O operador nulo $\mathbf{0}$, definido por $\mathbf{0}|v\rangle = 0$, é outro operador linear de V.*

Exemplo A.3 *Seja V um espaço vetorial sobre $\mathbb{C}$ com dimensão finita d, e sejam A e $\widetilde{A}$ operadores lineares de V. Então, definindo $(A + \widetilde{A}) |u\rangle = A(|u\rangle) + \widetilde{A}(|u\rangle)$ e $a(A |u\rangle) = A(a |u\rangle)$, o conjunto de todos os operadores lineares de V, juntamente com a adição e a multiplicação por escalar definidas acima, é um espaço vetorial sobre $\mathbb{C}$. Vamos denotar por $L(V)$ o espaço vetorial de todos os operadores lineares de V.*

Definição A.12 (Núcleo e imagem) *Sejam V um espaço vetorial sobre $\mathbb{C}$ e $A : V \longrightarrow W$ um operador linear de V. Definimos:*

1. *O núcleo de A é o conjunto dos $|u\rangle \in V$ tais que $A(|u\rangle) = 0$, e denotamos por $Ker(A)$.*
2. *A imagem de A é o conjunto $A(|u\rangle)$ tais que $|u\rangle \in V$, e denotamos por $Im(A)$.*

É oportuno destacar que o $Ker(A)$ e a $Im(A)$ são subespaços vetoriais de V e W, respectivamente. Além disso, o operador linear A do espaço vetorial V é sobrejetor se, e somente se, $Im(A) = W$. Além do mais, o operador linear A é injetor se, e somente se, $Ker(A) = 0$.

A.1.7 Representação de transformações lineares por matrizes

Nesta seção, vamos verificar que o estudo dos operadores lineares em espaços vetoriais de dimensão finita pode ser reduzido ao estudo de matrizes.

Sejam dadas duas bases ordenadas $\beta = \{|v_1\rangle, ..., |v_d\rangle\}$ de V e $\beta' = \{|w_1\rangle, ..., |w_D\rangle\}$ de W, e $A : V \longrightarrow W$ uma transformação linear de V em W. Então, para cada $j \in$

$\{1, ..., D\}$, existe um conjunto de escalares $A_{1j}, ..., A_{Dj}$ tais que

$$A(|v_j\rangle) = \sum_{i=1}^{D} A_{ij} |w_i\rangle . \tag{A.17}$$

Os escalares A_{ij} formam uma representação matricial $d \times D$ da transformação linear A nas bases ordenadas β e β' de V e W, respectivamente. No caso em que os espaços vetoriais $V = W$, o operador linear A de V é representado por uma matriz quadrada A_{ij} de ordem $d \times d$. Por outro lado é importante destacar que sendo V um espaço vetorial com $dim\ V = d$ sobre o corpo $\mathbb{C}$ e considerando os espaços vetoriais $L(V)$ e $M_d(\mathbb{C})$, então é possível mostrar $L(V)$ e $M_d(\mathbb{C})$ são isomorfos. Diante disso, temos que $dim\ M_d(\mathbb{C}) = L(V) = d^2$.

Os elementos da matriz A_{ij} podem ser calculados através do produto interno de $|w_i\rangle$ com $|v_j\rangle$, como segue:

$$A_{ij} = \langle w_i| A |v_j\rangle . \tag{A.18}$$

Equivalentemente, se $\{|j\rangle\} \in V$ e $\{|i\rangle\} \in W$ são bases ortonormais ordenadas de V e W, respectivamente, então

$$A_{ij} = \langle i| A |j\rangle . \tag{A.19}$$

Observe que a notação *bra-ket* expressa de forma compacta os elementos da matriz. Além disso, é preciso ter sempre em mente que a matriz que representa A depende da base ordenada, e que existe uma matriz que representa A em cada base ordenada.

Os operadores de Pauli I, X, Y, Z desempenham um papel central na Teoria da Informação Quântica. O espaço vetorial desses operadores é $\mathbb{C}^2$ e, em relação à base $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ tem a representação matricial

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{A.20}$$

A.1.8 Produto externo e relação de completude

Na primeira parte desta seção, vamos resumir o conceito de produto externo de vetores, que consiste em multiplicar vetores formando as transformações lineares que atuam sobre o espaço vetorial.

Definição A.13 *Sejam V e W espaços vetoriais sobre $\mathbb{C}$. Sendo $|v\rangle \in V$ e $|w\rangle \in W$, definimos o produto externo de $|v\rangle$ com $|w\rangle$ como sendo a transformação linear $|w\rangle \langle v| : V \longrightarrow W$ tal que*

$$(|w\rangle \langle v|)(|v'\rangle) \equiv |w\rangle (\langle v|v'\rangle) = \langle v|v'\rangle |w\rangle . \tag{A.21}$$

em que $|v'\rangle \in V$.

Devemos lembrar que $\langle v|v'\rangle$ é um escalar; portanto, a Equação A.21 tem duas interpretações:

1. A ação de um operador linear sobre um vetor $|v'\rangle$.
2. O produto de um escalar com o vetor $|w\rangle$.

Na segunda parte desta seção, vamos introduzir a relação de completude, que é um resultado importante sobre o produto externo.

Sejam V um espaço vetorial sobre $\mathbb{C}$ e $|v\rangle \in V$. Seja $\{|j\rangle\}$ uma base ortonormal de V e $|v\rangle = \sum_i a_i |v_i\rangle$, com $a_i \in \mathbb{C}$. Observe que o resultado da aplicação do operador linear $|j\rangle \langle j|$ no vetor $|v\rangle$ é

$$(\sum_j |j\rangle \langle j|) |v\rangle = \sum_j |j\rangle \langle j| \sum_i a_i |i\rangle = \sum_{ij} a_i |j\rangle \langle j|i\rangle = \sum_{ij} a_i |j\rangle \delta_{ij} = \sum_i a_i |i\rangle = |v\rangle . \tag{A.22}$$

Portanto, o operador devolve o próprio vetor e, por conseguinte, o operador é o operador de identidade,

$$\sum_i |i\rangle\langle i| = I. \tag{A.23}$$

Esta equação é conhecida como a relação de completude, ou, também, como a resolução da identidade.

A.1.9 Operadores unitários e hermitianos

Seja V um espaço vetorial sobre $\mathbb{C}$ e A um operador linear em V cuja representação matricial é A_{ij}. Então, a transposta conjugada de A_{ij} é denotada por A^*_{ji} e representa o operador adjunto $A^\dagger$, também chamado de conjugado hermitiano de A.

Definição A.14 (Operador auto-adjunto) *Seja V um espaço vetorial sobre $\mathbb{C}$ e A um operador linear em V. Dizemos que A é auto-adjunto ou Hermitiano, se $A = A^\dagger$.*

Se $|u\rangle = A^\dagger |w\rangle$, então é possível verificar que:

$$\langle w| A |v\rangle = \langle u|v\rangle , \ \forall |u\rangle , |v\rangle , |w\rangle \in V. \tag{A.24}$$

E também que:

$$(|w\rangle \langle v|)^\dagger = |v\rangle \langle w| , \ \forall |v\rangle , |w\rangle \in V. \tag{A.25}$$

Por outro lado, supondo que o operador linear A seja invertível, então existe um operador linear A^{-1} tal que $AA^{-1} = A^{-1}A = I$.

Definição A.15 (Operador unitário) *Seja V um espaço vetorial sobre $\mathbb{C}$ e A um operador linear em V. Dizemos que A é unitário, se $A^\dagger A = AA^\dagger = I$.*

Uma propriedade importante é que os operadores unitários preservam produto interno, isto é, dado um operador unitário A em V tal que $|u'\rangle = A|u\rangle$ e $|v'\rangle = A|v\rangle$ com $|u'\rangle, |u\rangle, |v'\rangle, |v\rangle \in V$, então

$$\langle u'|v'\rangle = \langle u| A^\dagger A |v\rangle = \langle u| I |v\rangle = \langle u|v\rangle . \tag{A.26}$$

Um conjunto importante de operadores unitários, com utilização recorrente no estudo da Teoria da Informação Quântica, são os operadores de Pauli A.20.

A.1.10 Espaço vetorial do produto tensorial

Nesta seção, vamos construir o espaço vetorial do produto tensorial, o que matematicamente significa construir espaços vetoriais maiores a partir de espaços menores utilizando o produto tensorial.

Sejam V e W espaços vetoriais finitos sobre $\mathbb{C}$, com $\dim V = m$ e $\dim W = n$. O espaço vetorial do produto tensorial, $\mathcal{T} = V \otimes W$, é também um espaço vetorial com dimensão mn, cujos elementos de $\mathcal{H}_1 \otimes \mathcal{H}_2$ são combinações lineares de produtos tensoriais

$$|t\rangle = |v\rangle \otimes |w\rangle = |vw\rangle = |v\rangle |w\rangle , \tag{A.27}$$

em que $|v\rangle \in V$ e $|w\rangle \in W$. Então, supondo

$$|v\rangle = \begin{pmatrix} a_1 \\ a_2 \\ : \\ a_m \end{pmatrix} \in V \text{ e } \quad |w\rangle = \begin{pmatrix} b_1 \\ b_1 \\ : \\ b_n \end{pmatrix} \in W, \tag{A.28}$$

temos que

$$|t\rangle = |v\rangle \otimes |w\rangle = \begin{pmatrix} a_1 \\ a_2 \\ : \\ a_m \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_1 \\ : \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 |w\rangle \\ a_2 |w\rangle \\ : \\ a_m |w\rangle \end{pmatrix} . \tag{A.29}$$

Por outro lado, se $|i\rangle \in V$ e $|j\rangle \in W$ são bases ortonormais de V e W, respectivamente, então

$$|k\rangle = |i\rangle \otimes |j\rangle \tag{A.30}$$

é uma base ortonormal de $\mathcal{T} = V \otimes W$.

Por construção, o espaço vetorial do produto tensorial satisfaz os axiomas da definição A.1 de um espaço vetorial:

1. Para $\alpha \in \mathbb{C}$, $|v\rangle \in V$ e $|w\rangle \in W$,

$$\alpha(|v\rangle \otimes |w\rangle = (\alpha(|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha\,|w\rangle).$$

2. Para $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle\,.$$

3. Para $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$,

$$|v\rangle\,(|w_1\rangle \otimes |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle\,.$$

O produto interno do espaço vetorial do produto tensorial pode ser obtido a partir do produto interno de suas componentes. Isto é, dados dois vetores $|u\rangle$ e $|u'\rangle$ no espaço do produto tensorial $\mathcal{T} = V \otimes W$, tais que

$$|u\rangle = \sum_i a_i\,|v_i\rangle \otimes |w_i\rangle$$

$$|u'\rangle = \sum_j b_j\,|v'_j\rangle \otimes |w'_j\rangle\,.$$

O produto interno

$$\langle u|u'\rangle = \sum_i a_i^*(\langle v_i| \otimes |w_i\rangle) \sum_j b_j\,|v'_j\rangle \otimes |w'_j\rangle =$$

$$\sum_{ij} a_i^* b_j(\langle v_i|v'_j\rangle \otimes \langle w_i|w'_j\rangle) = \sum_{ij} a_i^* b_j\,\langle v_i|v'_j\rangle\,\langle w_i|w'_j\rangle\,, \tag{A.31}$$

transforma os vectores de $\mathcal{T} = V \otimes W$ em escalares.

Além disso, podemos definir operadores lineares no espaço vetorial do produto tensorial. Para isso, sejam A e B operadores lineares sobre os espaços vetoriais V e W,

respectivamente. Então, definimos um operador linear C no espaço vetorial do produto tensorial $\mathcal{T} = V \otimes W$ como sendo

$$C = A \times B, \tag{A.32}$$

e se $|t\rangle = |v\rangle \otimes |w\rangle$ é um vetor em $\mathcal{T} = V \otimes W$, então

$$C\,|t\rangle = (A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle\,. \tag{A.33}$$

A.1.11 Autovetor e autovalor

Nesta seção, vamos resumir os conceitos de autovetor e autovalor de um operador linear. Esses dois conceitos são bastante importantes no contexto deste trabalho de tese.

Definição A.16 (Autovetor e autovalor) *Seja V um espaço vetorial sobre $\mathbb{C}$ e A um operador linear de V. Definimos um autovetor (ou vetor próprio) de A como sendo um vetor não nulo $|v\rangle \in V$, tal que*

$$A\,|v\rangle = \lambda\,|v\rangle\,. \tag{A.34}$$

O número complexo λ é chamado de autovalor (ou valor próprio) associado ao autovetor $|v\rangle$.

No contexto deste trabalho de tese, vamos usar os termos autoestado (ou estado próprio) para nos referirmos ao autovetor (ou vetor próprio) de um operador linear A.

Para um operador linear A do espaço vetorial V sobre o corpo $\mathbb{C}$, a representação diagonal é definida como

$$A = \sum_i \lambda_i\,|\psi_i\rangle\,\langle\psi_i| \tag{A.35}$$

em que $|\psi_i\rangle$ é um conjunto de autovetores de A, associados aos seus correspondentes autovalores.

Os operadores hermitianos e unitários são ambos diagonalizáveis. Os autovalores de um operador hermitiano são números reais, e os autovalores de um operador unitário são números complexos cujo valor absoluto é igual a um.

Além disso, dado um operador linear A do espaço vetorial V sobre o corpo $\mathbb{C}$, vamos definir o traço de A e denotá-lo por tr, A como sendo a soma dos elementos diagonais principais de sua representação matricial, ou seja,

$$\mathrm{tr}, A = \sum_i A_{ii}. \tag{A.36}$$

Ademais, o traço de um operador diagonalizável é a soma dos autovalores, e o determinante é o produto dos autovalores.

A.2 PI-Álgebra

Nesta seção, são apresentados alguns conceitos envolvendo o estudo das álgebras, e será enunciado o teorema de Amitsur-Levitzki. Esses tópicos são abordados tomando como base as referências [26], [57].

A.2.1 Álgebra

Definição A.17 (Álgebra) *Seja $\mathcal{A}$ um espaço vetorial sobre $\mathbb{C}$. Dizemos que $\mathcal{A}$ é um álgebra sobre $\mathbb{C}$, se a operação $** : V \times V \longrightarrow \mathcal{A}$ é bilinear, ou seja:*

1. $(a+b)*c = a*c + b*c$
2. $a*(b+c) = a*b + a*c$
3. $\lambda(a*b) = (\lambda a)*b = a*(\lambda b)$

para quaisquer $a, b, c \in \mathcal{A}$ e $\lambda \in \mathbb{C}$.

Na Definição A.17, a operação $*$ é chamada de *produto* ou *multiplicação*. Por simplicidade de notação, vamos denotar $(\mathcal{A},)$ simplesmente por $\mathcal{A}$ e $a*b$ por ab, para $a, b \in \mathcal{A}$. Definimos também $a_1a_2a_3$ como sendo $(a_1a_2)a_3$ e, indutivamente, $a_1a_2 \ldots a_na_{n+1}$ como sendo $(a_1a_2 \ldots a_n)a_{n+1}$ para $a_i \in \mathcal{A}$. Sendo $\mathcal{A}$ uma álgebra, vamos dizer que um subconjunto β é uma *base* de $\mathcal{A}$ se β for uma base de $\mathcal{A}$ como espaço vetorial. Com isso, definimos a dimensão de uma álgebra $\mathcal{A}$ como sendo a dimensão de $\mathcal{A}$ como espaço vetorial, e ela será denotada por dim $\mathcal{A}$.

Seja $\mathcal{A}$ uma álgebra. Então:

1. $\mathcal{A}$ é *associativa* se $(ab)c = a(bc)$ para quaisquer $a, b, c \in \mathcal{A}$.
2. $\mathcal{A}$ é *comutativa* se $ab = ba$ para quaisquer $a, b \in \mathcal{A}$.
3. $\mathcal{A}$ é *unitária* (ou *com unidade*) se existe $1 \in \mathcal{A}$ tal que $1a = a1 = a$ para todo $a \in \mathcal{A}$.

Ademais, as álgebras $\mathcal{A}$ consideradas neste trabalho são associativas e com unidade; caso contrário, isso será informado ao leitor.

O espaço vetorial $M_d(\mathbb{C})$ de todas as matrizes $d \times d$ com entradas sobre $\mathbb{C}$, munido do produto usual de matrizes, é uma álgebra associativa com unidade, cuja dim $M_d(\mathbb{C}) = d^2$. De maneira geral, se $\mathcal{A}$ é uma álgebra, podemos considerar o espaço vetorial de todas as

matrizes $d \times d$ com entradas em $\mathcal{A}$, denotando-o por $M_d(\mathcal{A})$. O produto de matrizes em $M_d(\mathcal{A})$ é análogo ao produto em $M_d(\mathbb{C})$ com entradas sobre $\mathbb{C}$. Ademais, este produto define em $M_d(\mathcal{A})$ a estrutura de uma álgebra.

Definição A.18 (Subálgebra) *Seja $\mathcal{A}$ uma álgebra. Um subespaço B de $\mathcal{A}$ é uma subálgebra de $\mathcal{A}$ se B for multiplicativamente fechado, ou seja, $BB \subseteq B$.*

Seja $\mathcal{A}$ uma álgebra e $S_1, \ldots, S_k \in \mathcal{A}$. O subespaço formado por todas as expressões $S_{i_1}^{n_1} S_{i_2}^{n_2} \ldots S_{i_k}^{n_k}$ e suas combinações lineares constitui uma subálgebra de $\mathcal{A}$. Um exemplo em particular é a subálgebra gerada por $S_1, \ldots, S_k \in M_d$.

A.2.2 PI-Álgebra

Definição A.19 (Identidade polinomial) *Sejam $f = f(x_1, x_2, \ldots, x_n)$ um polinômio nas variáveis não comutativas $x_1, x_2, \ldots, x_n$, cujos coeficientes pertencem a $\mathbb{C}$, e $\mathcal{A}$ uma álgebra associativa com unidade. O polinômio f é uma identidade polinomial para a álgebra $\mathcal{A}$ se*

$$f(a_1,\ a_2, ..., a_n) = 0 \tag{A.37}$$

para quaisquer $a_1,\ a_2, ..., a_n \in \mathcal{A}$.

Uma PI-álgebra é uma álgebra $\mathcal{A}$ que possui uma identidade polinomial $f \neq 0$.

O polinômio

$$St_d(x_1, x_2, ..., x_d) = \sum_{\sigma \in S_d} (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} ... x_{\sigma(d)} \tag{A.38}$$

em que S_d é o grupo simétrico das permutações e $(-1)^\sigma$ é o sinal da permutação σ é chamado de *polinômio standard de grau d.*

No ano de 1950, S. A. Amitsur e J. Levitzki [26], usando argumentos combinatórios, demonstraram que o polinômio standard St_{2d} é uma identidade polinomial para a álgebra $M_d(F)$[1]. A demonstração deste resultado, chamado de Teorema de Amitsur-Levitzki é considerada um marco na história da PI-Álgebra. O Teorema de Amitsur-Levitzki é enunciando a seguir:

[1]O espaço vetorial $M_d(F)$ de todas as matrizes $d \times d$ com entradas sobre o corpo F, munido do produto usual de matrizes, é uma álgebra associativa com unidade denota a álgebra de todas as matrizes $d \times d$.

Teorema A.1 (Amitsur-Levitzki) *Seja a álgebra $M_d(F)$, então:*

$$St_{2d}(A_1, A_2, ..., A_{2d}) = \sum_{\sigma \in S_{2d}} (-1)^{\sigma} A_{\sigma(1)} A_{\sigma(2)} ... A_{\sigma(2d)} = 0, \tag{A.39}$$

para quaisquer $A_1, ..., A_{2d} \in M_d(F)$. Em outras palavras a álgebra $M_d(F)$ satisfaz o polinômio standard de grau $2d$. Além disso, a álgebra $M_d(F)$ não satisfaz o polinômio standard de grau menor do que $2d$.

O Teorema de Amitsur-Levitzki desempenha um papel fundamental na teoria das PI-Álgebras, assegura que o polinômio standard é uma identidade polinomial para a álgebra $M_d(F)$. Além disso, o teorema tem sido explorado no contexto da Teoria da Informação Quântica, onde as álgebras de matrizes surgem naturalmente na descrição de sistemas quânticos e suas operações [25]. No contexto desta tese, o Teorema de Amitsur-Levitzki é utilizado na demonstração do teorema de Shemesh generalizado [30].