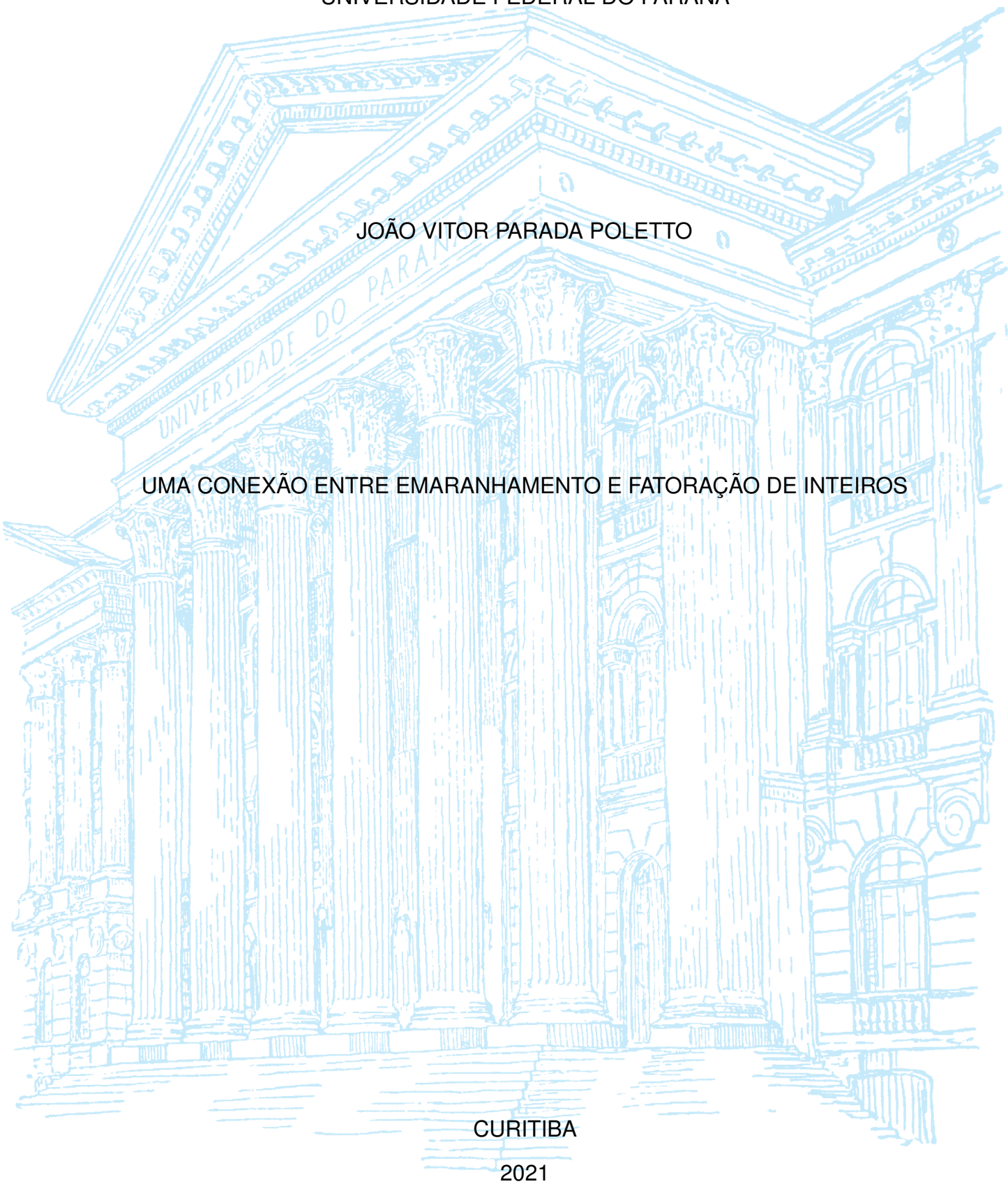
UNIVERSIDADE FEDERAL DO PARANÁ

JOÃO VITOR PARADA POLETTO



UMA CONEXÃO ENTRE EMARANHAMENTO E FATORAÇÃO DE INTEIROS

CURITIBA

2021

JOÃO VITOR PARADA POLETTO

UMA CONEXÃO ENTRE EMARANHAMENTO E FATORAÇÃO DE INTEIROS

Trabalho de conclusão de curso apresentado ao curso de Licenciatura em Física, Setor de Ciências Exatas, Universidade Federal do Paraná, como requisito parcial à obtenção de título de Licenciado em Física.

Orientador: Prof. Dr. Alexandre Dias Ribeiro

CURITIBA

2021

UNIVERSIDADE FEDERAL DO PARANÁ

ATA DE REUNIÃO

ATA DA APRESENTAÇÃO E ARGUIÇÃO ORAL DE

TRABALHO DE CONCLUSÃO DE CURSO

Aos 23 dias do mês de dezembro de 2021, às 14 horas, reuniram-se remotamente usando a Plataforma Teams, o acadêmico **João Vitor Parada Poletto**, aluno do Curso de Licenciatura em Física do Setor de Exatas da Universidade Federal do Paraná, para fazer a apresentação e arguição oral relativa ao seu **Trabalho de Conclusão de Curso (TCC)**, intitulado "**Uma conexão entre emaranhamento e fatoração de inteiros**", orientado pelo Prof. Dr. Alexandre Dias Ribeiro, perante a banca examinadora, que foi assim constituída: Prof. Dr. Alexandre Dias Ribeiro, como Presidente da Banca; a Prof.ª Dr.ª Alessandra Souza Barbosa, como 1° Membro da Banca e a Prof. Dr. Renato Moreira Angelo, como 2° Membro da Banca. Após assistirem a exposição do acadêmico, acima nomeado, e arguirem-no sobre diferentes aspectos do TCC apresentado, os membros da banca reuniram-se para a atribuição da nota final, a qual foi **99 (noventa e nove)**, de acordo com o **Relatório de Avaliação de TCC** , que acompanha esta Ata, estando o acadêmico aprovado na disciplina TCCB, com a recomendação de que todas as sugestões de correções indicadas pela Banca sejam atendidas e que a versão definitiva do TCC seja entregue conforme as regras estabelecidas pelo Colegiado de Curso e no prazo fixado. A nota final foi comunicada ao acadêmico. Nada mais havendo a ser tratado, o Presidente da Banca declarou encerrada a seção e todos os membros da Banca assinaram eletronicamente a presente Ata.

Curitiba, 23 de dezembro de 2021.

Documento assinado eletronicamente por **ALEXANDRE DIAS RIBEIRO**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/12/2021, às 16:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ALESSANDRA DE SOUZA BARBOSA**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/12/2021, às 16:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RENATO MOREIRA ANGELO**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/12/2021, às 16:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOÃO VITOR PARADA POLETTO**, **Usuário Externo**, em 27/12/2021, às 09:10, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **4145808** e o código CRC **C178CD0F**.

Referência: Processo nº 23075.074173/2021-29 SEI nº 4145808

À memória de minhas queridas avós, Maria e Marisa.

AGRADECIMENTOS

Agradeço ao professor Alexandre por todo o apoio e disposição em auxiliar-me em minhas dúvidas, desde as disciplinas básicas do curso de graduação. O incentivo e as sugestões ao longo de nossas conversas motivaram-me para que eu pudesse desenvolver esse trabalho, bem como trazer conceitos que aprendi nas disciplinas de matemática.

Aos meus pais, Jamerson e Marisa, que sempre me incentivaram a estudar e procurar fazer o melhor que posso. A vocês, meus sinceros agradecimentos por todo carinho e cuidado que recebi todos esses anos. Também agradeço ao meu irmão Daniel, pela paciência e companhia desde pequeno, e a todos os meus demais familiares.

À minha noiva Mahira, que sempre incentivou-me em todos os momentos ao longo da graduação e ajudou a tornar-me uma pessoa melhor, tanto pessoalmente e profissionalmente. Com certeza a minha trajetória acadêmica não seria a mesma se não estivesse com você ao meu lado, me suportando e incentivando com muito amor. Também sou grato por todos os bons momentos que passamos com sua família, em especial, com sua mãe Luciana e padrasto Maurício.

Aos meus colegas de graduação: Jhionathan, Egbert, Marcelo, Matheus e Yohan. Lembro-me das conversas sobre Física com o Jhionathan, às 23h30min, durante o retorno para casa. Meu aprendizado no curso não seria o mesmo se não fosse pela companhia de vocês.

Ao MUR Curitiba, por todo o apoio e auxílio durante a graduação, que me transformaram em uma pessoa melhor.

Ao professor Roberto Ribeiro, por todo o incentivo durante a realização das disciplinas de graduação e pós-graduação no departamento de matemática da universidade. O seu apoio foi fundamental para que eu pudesse ser aceito nos programas de pós-graduação que me inscrevi. Também agradeço ao CNPq pelo apoio financeiro quanto aluno do PICME, que foi fundamental para a minha formação acadêmica.

Ao professor Renato e à professora Alessandra, por se disponibilizarem em participar da banca de meu trabalho, mesmo com curtos prazos.

E por fim, o mais importante de todos, sou grato a Deus por tudo o que Ele fez em minha vida, me acompanhando nos momentos mais difíceis e mostrando que, independentemente da dificuldade, Ele estava e está sempre ao meu lado. Parafraseando São João Paulo II, quero unir fé e razão para contemplar a verdade.

“A humildade é o primeiro degrau para a sabedoria.”
(São Tomás de Aquino)

RESUMO

Estados quânticos emaranhados são considerados muito importantes, tanto a partir do ponto de vista fundamental quanto quando se considera suas possíveis aplicações tecnológicas. A importância desses estados pode ser ilustrada pelo seu papel fundamental na compreensão do famoso debate gerado por Einstein, Podolsky e Rosen, em 1935. Além disso, eles estão entre os protagonistas nos estudos relativos à implantação da computação quântica. Através de uma revisão de conceitos fundamentais para o estudo do emaranhamento, introduzimos propriedades básicas de vetores no espaço de Hilbert, bem como definimos o operador densidade nesse espaço. Em particular, para estados puros compostos por duas partes, ainda mostramos como obter o operador densidade reduzido, quantidade fundamental para a quantificação de emaranhamento. Em seguida, discorremos sobre o conceito de entropia, abordando-se a entropia de Shannon e a de von Neumann, da qual obtém-se a entropia linear. Esta última, quando aplicada ao operador densidade reduzido, torna-se uma expressão simples de quantidade de emaranhamento. Motivado por uma bem-sucedida conexão entre o tópico de partição de inteiros e a descrição quântica de um gás de bósons, investigamos um sistema físico particular para o qual é possível estabelecer uma conexão entre fatoração de inteiros e propriedades da dinâmica de emaranhamento. Embora não tenhamos estabelecido uma ligação clara entre os dois assuntos, neste trabalho indicamos um caminho a seguir.

Palavras-chaves: Emaranhamento. Entropia linear. Fatoração de inteiros.

ABSTRACT

Entangled quantum systems are considered very important, both from the fundamental and technological point of view. The importance of these states can be illustrated by their crucial role in comprehension of the famous debate brought by Einstein, Podolsky and Rosen, in 1935. Furthermore, they are among the protagonists in the study related to the implementation of quantum computing. Throughout a revision of fundamental concepts to study entanglement, we introduce basic properties of vectors in a Hilbert space, as well as define density operators in this space. Particularly, for pure states composed by two parts, we also show how to obtain the reduced density operator, a fundamental quantity for the quantification of entanglement. Thus, the concept of Shannon and von Neumann entropy are shown, from which we obtain the linear entropy. This last one, when applied to the reduced density operator, becomes a simple expression to quantify entanglement. Motivated by a successful connection between the integer partition topic and a bose gas description, we investigate a particular physical system, for which it is possible to establish a connection between integer factorization and properties of entanglement dynamics. Although we did not find a clear connection between these two subjects, in this work we indicate a route to follow.

Key-words: Entanglement. Linear entropy. Integer factorization.

SUMÁRIO

1 INTRODUÇÃO 10

2 CONCEITOS FUNDAMENTAIS 13
2.1 ESTADO PRODUTO 13
2.2 ESTADOS EMARANHADOS 13
2.3 OPERADOR DENSIDADE 14
2.3.1 Operador densidade em estados puros 14
2.3.2 Operador densidade em estados mistos 16
2.4 EXEMPLO: OPERADOR DENSIDADE APLICADO A ESTADOS SEPARÁVEIS 17
2.4.1 Dinâmica quântica 19

3 ENTROPIA 20
3.1 ENTROPIA DE SHANNON 20
3.1.1 Entropia binária 21
3.2 ENTROPIA DE VON NEUMANN 22
3.3 ENTROPIA LINEAR 24

4 ENTROPIA LINEAR E O EMARANHAMENTO 25
4.1 UM ESTUDO DE CASO 25
4.2 DINÂMICA DE EMARANHAMENTO 30
4.3 ENTROPIA LINEAR E A FATORAÇÃO DE INTEIROS 31
4.3.1 Transformada de Fourier 33
4.3.2 Modos de Fourier e a fatoração de inteiros 35

5 PARTIÇÃO E FATORAÇÃO DE INTEIROS APLICADOS À MECÂNICA QUÂNTICA 39
5.1 PARTIÇÃO DE INTEIROS NA MECÂNICA QUÂNTICA 39
5.2 DA MECÂNICA QUÂNTICA À FATORAÇÃO DE INTEIROS 41

6 CONSIDERAÇÕES FINAIS 43

REFERÊNCIAS 44

1 INTRODUÇÃO

Historicamente, o conceito de emaranhamento começou a receber sua devida importância a partir do famoso artigo de Einstein, Podolsky e Rosen (EPR), intitulado: *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, publicado em 1935 [1]. Naquela época, esta propriedade de estados quânticos ainda não era conhecida por esse nome. Não havia sequer uma formalização de suas características, porém atualmente reconhecemos a sua importância, por exemplo, quando buscamos compreender os incômodos gerados pela Mecânica Quântica, levantados por EPR. Um exemplo típico deste conflito é a existência de estados quânticos que violam desigualdades de Bell, que são construídas exclusivamente através de hipóteses amplamente aceitas no mundo clássico, conforme comentaremos logo abaixo.

EPR utilizaram-se dos conceitos de *realidade* e *localidade* para concluir que a mecânica quântica estava incompleta. Afinal, embora seus argumentos tenham chegado na conclusão de que, por exemplo, momento e posição de um sistema possam ter valores bem definidos, outros resultados, como o Princípio de Incerteza de Heisenberg, implicavam no contrário. Os autores sugeriram que a solução para o impasse seria se se tivesse o conhecimento do que foi chamado de *variáveis ocultas*, as quais, se fossem conhecidas, completariam a mecânica quântica, eliminando aquela contradição. Os conceitos de *realidade* e *localidade* apresentados por EPR foram debatidos por muitos autores, sendo que é possível encontrar uma análise detalhada sobre ambos na referência [2].

Por décadas, esse impasse gerado por EPR provocou desconfortos na comunidade científica, até que começou a ser efetivamente respondido por John Stewart Bell em 1964 [3]. No artigo, Bell baseou-se em argumentos probabilísticos de modo a colocar um limitante superior em uma determinada função de correlação que envolvia medidas em um sistema de duas partes. Neste trabalho, ele levava em consideração as hipóteses de localidade e realismo. Bell também mostrou que estados quânticos poderiam violar aquela desigualdade, concluindo que aquelas hipóteses não valeriam para a Mecânica Quântica [4]. Mais tarde, experimentos concordaram com o seu resultado avassalador, violando desigualdades similares, que atualmente são chamadas de *desigualdades de Bell*. Exemplos com a descrição desses experimentos podem ser encontrados nas referências [4, 5, 6], que envolvem medições da polarização de fótons.

A partir de então intensificou-se a importância do conhecimento sobre o emaranhamento, pois é possível demonstrar [7, 8] que, ao se considerar estados puros, os únicos que violam as desigualdades de Bell são os chamados *estados emaranhados*. Tais estados implicam que suas partes, após interação, estão *correlacionadas*,

ou seja, o conhecimento de alguma quantidade física de uma das partes implica em algum conhecimento sobre a outra. Para ilustrar correlação em um contexto clássico, considere a seguinte situação [9, p. 87-88]: na cidade de Curitiba, duas meias, uma verde e outra vermelha são postas em duas maletas distintas. Então, uma das maletas é enviada para o Japão, enquanto que a outra permanece em Curitiba. Se alguém abrir uma das maletas no Japão e constatar que a meia é vermelha, instantaneamente saberá que a meia verde está em Curitiba. Ou seja, mesmo que as duas meias estejam arbitrariamente afastadas, o conhecimento da cor de uma implica no conhecimento de outra, exemplificando a ideia de variáveis correlacionadas. Neste exemplo, a correlação foi atribuída às meias localmente, quando ambas ainda estavam em Curitiba. Além disso, montada uma mala, sabemos que a sua meia está definida, de modo que observar a sua cor significa apenas revelar aquela propriedade. Esta maneira de entender as propriedades dos sistemas, *grosso modo*, é sinônimo do conceito de realismo. Já no contexto da Mecânica Quântica, dizemos que estados emaranhados violam a desigualdade de Bell pois não são regidos por tais princípios, os quais muitas vezes são chamados de realismo local. As correlações quânticas, portanto, podem ir além das correlações clássicas, uma vez que incluem aspectos relacionados à não localidade e irrealismo.

O conceito de emaranhamento, além do que foi mencionado nos parágrafos anteriores, é fundamental no estudo da computação quântica. Por exemplo, propicia o estudo de teletransporte quântico, algoritmos quânticos rápidos e correção de erros quânticos. De acordo com a referência [10] essa é uma área que ainda requer muita exploração.

Neste trabalho, veremos como quantificar emaranhamento em alguns estados quânticos específicos, os chamados estados puros e bipartidos. Estados puros são estados completamente descritos por um vetor que o representa em seu espaço de Hilbert; enquanto que estados bipartidos são aqueles em que há interesse em apenas duas partes distintas do sistema. Apesar da maneira simplificada abordada aqui, os conceitos apresentados podem ser estendidos a sistemas quânticos mais complexos.

Para descrever emaranhamento, utilizamos do conceito de *entropia*, em particular, a *entropia linear* S_{lin} obtida a partir da entropia de von Neumann. O nosso objetivo está focado na dinâmica de emaranhamento de um sistema quântico específico, a qual pode ser caracterizada ao se analisar os estados reduzidos do sistema original. Finalmente, para um hamiltoniano particular, mostraremos que os modos de Fourier associados a S_{lin} estão ligados ao problema de fatoração de inteiros. Esta é uma contribuição original do trabalho.

Nossa motivação para indicar esta conexão entre a entropia linear e a Teoria de Números se origina em um outro cenário, em que relaciona-se a densidade de

níveis de energia a sistemas de muitos corpos. Ali, aproximações semiclássicas contribuem para encontrar expressões assintóticas de interesse, inclusive para a teoria matemática. Embora a partição de números inteiros pareça estar bem estruturada no mundo matemático [11], quando comparada à fatoração [12], esta ainda tem um potencial para se desenvolver e este trabalho aponta uma possível maneira disso ocorrer. Assim como a investigação de assuntos específicos da Mecânica Quântica trouxe um desenvolvimento na partição de inteiros, espera-se que esse trabalho aponte para uma possível contribuição ao estudo da fatoração.

O trabalho inicia-se com uma revisão sobre estado puro de tipo produto e como descrevê-lo, no capítulo 2. Então, apresenta-se a definição de estados emaranhados e o operador densidade, que é apropriado no cálculo da entropia de estados puros. Mostra-se como se dá a descrição de estados separáveis a partir desse operador.

Em seguida, no capítulo 3, é apresentada uma revisão sobre a entropia de Shannon e a entropia de von Neumann; enquanto a primeira é utilizada majoritariamente para a descrição de sistemas clássicos, a segunda é utilizada exclusivamente para sistemas quânticos. Ainda assim, utilizamos uma entropia mais simples associada a entropia de von Neumann: a entropia linear. Com ela, já no capítulo 4, através de um estudo de caso, vemos condições necessárias e suficientes para que um sistema bipartido, com dois níveis cada um, seja emaranhado. Esse estudo de caso prossegue pela descrição da dinâmica de emaranhamento. Consideramos que os estados são regidos por um hamiltoniano que não depende do tempo. Assim, através de um caso particular, vê-se como o emaranhamento de determinado sistema relaciona-se com a fatoração de números inteiros.

Por fim, no capítulo 5, com a motivação de que a mecânica quântica promoveu um desenvolvimento e aplicação da partição de números inteiros, pretende-se especular como o problema apresentado nesse trabalho pode contribuir para o estudo da fatoração de inteiros.

2 CONCEITOS FUNDAMENTAIS

Para que seja possível estudar a entropia e o emaranhamento, se faz necessária a utilização de conceitos matemáticos. Estados quânticos são descritos utilizando-se um espaço vetorial específico sobre $\mathbb{C}$, o chamado *espaço de Hilbert*. No caso geral, estados quânticos são descritos através de operadores, os quais podem ser representados por matrizes. No caso particular de estados puros, além da utilização de matrizes, pode-se associá-los a um vetor. Nesse trabalho, utilizaremos a notação de *Bra-ket*, de modo que o vetor será denotado por $|\psi\rangle$.

2.1 ESTADO PRODUTO

Para iniciar nossa discussão sobre estados produto, consideramos um espaço de estados de um sistema de dois objetos quânticos, como dois fótons. Trabalhamos com as definições de espaço de Hilbert, que será denotado pela letra $\mathscr{H}$. Neste caso bipartido, o espaço de Hilbert associado a cada parte é expresso por $\mathscr{H}_j$, com $j = 1$ ou 2. Considerando dois vetores, $|\phi\rangle \in \mathscr{H}_1$ e $|\psi\rangle \in \mathscr{H}_2$, sendo que os espaços tem dimensões N e M, respectivamente, consideramos o conjunto $\{|\phi\rangle, |\psi\rangle\}$ como um vetor produto de um espaço vetorial de dimensão $N \cdot M$, denotado por $\mathscr{H}_1 \otimes \mathscr{H}_2$. Para melhor exemplificar, considere $\{|n\rangle\}$, com $n = 1, \cdots, N$, uma base para o espaço $\mathscr{H}_1$, e $\{|m\rangle\}$, com $m = 1, \cdots, M$, uma base para o espaço $\mathscr{H}_2$. Podemos então escrever:

$$|\phi\rangle = \sum_{n=1}^{N} c_n |n\rangle \text{ e } |\psi\rangle = \sum_{m=1}^{M} d_m |m\rangle , \tag{2.1}$$

de forma que o par $\{|\phi\rangle, |\psi\rangle\}$ seja definido como:

$$|\phi\rangle \otimes |\psi\rangle = \sum_{n,m} c_n d_m |n\rangle \otimes |m\rangle . \tag{2.2}$$

Utilizaremos simplesmente a notação $|\phi\psi\rangle$ para se referir a $|\phi\rangle \otimes |\psi\rangle$ e, assim, para o par de vetores que define o estado produto.

2.2 ESTADOS EMARANHADOS

Assim como na seção anterior, aqui trabalhamos com um sistema quântico bipartido, porém nos restringiremos a $N = M = 2$. Conforme tratado em [9], podemos considerar que esses objetos quânticos são dois fótons, com dois possíveis estados individuais de polarização linear, a saber, $|h\rangle$ (horizontal) e $|v\rangle$ (vertical). A base de vetores para o espaço produto quadridimensional é dada por $\{|hh\rangle, |hv\rangle, |vh\rangle, |vv\rangle\}$. Nesse espaço vetorial, um estado puro geral pode ser definido pelo vetor:

$$|\Psi\rangle = a_{hh} |hh\rangle + a_{hv} |hv\rangle + a_{vh} |vh\rangle + a_{vv} |vv\rangle . \tag{2.3}$$

Agora, o questionamento que surge é saber se qualquer vetor que tem a forma (2.3) pode ser escrito como o produto de dois vetores individuais, um para cada fóton. Isto é, se, a partir desse estado geral, podemos escrever:

$$|\phi\rangle = a_{1h}\,|h\rangle + a_{1v}\,|v\rangle \quad \text{e} \quad |\psi\rangle = a_{2h}\,|h\rangle + a_{2v}\,|v\rangle\,, \tag{2.4}$$

que nos leva a:

$$|\phi\psi\rangle = a_{1h}a_{2h}\,|hh\rangle + a_{1h}a_{2v}\,|hv\rangle + a_{1v}a_{2h}\,|vh\rangle + a_{1v}a_{2v}\,|vv\rangle\,, \tag{2.5}$$

também chamado de estado **fatorável**. Ao compará-lo com o estado geral (2.3), vemos que, para que este seja fatorável, seus coeficientes devem respeitar:

$$a_{hh} = a_{1h}a_{2h}, \quad a_{hv} = a_{1h}a_{2v}, \quad a_{vh} = a_{1v}a_{2h}, \quad \text{e} \quad a_{vv} = a_{1v}a_{2v},$$

a partir das quais, conclui-se que $a_{hh}a_{vv} = a_{1h}a_{2h}a_{1v}a_{2v} = a_{hv}a_{vh}$. Portanto, um estado expresso por (2.3) só pode ser produto de estados de dois objetos quânticos individuais se a relação

$$a_{hh}a_{vv} = a_{hv}a_{vh} \tag{2.6}$$

for respeitada. Caso isto não ocorra, o estado é dito **estado emaranhado**.

Um exemplo de estado emaranhado é dado por:

$$|\Psi\rangle = \frac{|hv\rangle - |vh\rangle}{\sqrt{2}}, \tag{2.7}$$

em que a condição (2.6) é claramente violada.

2.3 OPERADOR DENSIDADE

No estudo de estados quânticos, nem sempre conseguimos descrever todas as informações relevantes se expressamos tais estados através de vetores no espaço de Hilbert [9]. Por isso precisamos de um outro objeto, obtido com a utilização do operador densidade (também chamado matriz densidade). Este objeto se faz necessário para o estudo de estados mistos e, mesmo não sendo fundamental para estados puros, continua válida sua utilização para estes. Adiante, veremos que o emaranhamento de um estado quântico, para estados puros e bipartidos, pode ser quantificado através do operador densidade reduzido obtido a partir do operador densidade original. Para prosseguir, vejamos as definições do operador e dos estados puros e mistos.

2.3.1 Operador densidade em estados puros

Definimos um estado puro como aquele que pode ser representado por um vetor $|\psi\rangle$ em um espaço de Hilbert $\mathscr{H}$. Esse estado também pode ser representado por:

$$\hat{\rho} = |\psi\rangle\,\langle\psi|\,, \tag{2.8}$$

que recebe o nome de *operador densidade*.

A primeira observação a ser feita é que, quando utilizamos o operador densidade, a fase de um vetor mostra-se claramente irrelevante. Considere, por exemplo, um vetor $|\psi\rangle$ no espaço de Hilbert $\mathscr{H}$. Ao adicionarmos uma fase alfa, ele passa a ser representado por:

$$e^{i\alpha}\,|\psi\rangle\,. \tag{2.9}$$

Para o operador densidade $\hat{\rho}'$, levando em conta a fase, obtemos:

$$\hat{\rho}' = e^{i\alpha}\,|\psi\rangle\,\langle\psi|\,e^{-i\alpha} = \hat{\rho}. \tag{2.10}$$

Outro ponto importante a ser ressaltado é que, considerando o estado $|\psi\rangle$ normalizado, o operador densidade é uma *projeção* (somente para estados puros), pois:

$$\hat{\rho}^2 = |\psi\rangle\,\langle\psi|\psi\rangle\,\langle\psi| = |\psi\rangle\,\langle\psi| = \hat{\rho};\ \hat{\rho}^\dagger = \hat{\rho}. \tag{2.11}$$

Podemos agora verificar que quantidades mensuráveis, como o valor esperado, por exemplo, podem ser obtidas em termos do operador $\hat{\rho}$. Para isso é importante relembrar o conceito de traço de um operador $\hat{A}$, denotado por $\mathrm{tr}(\hat{A})$. Considerando uma base $\{|n\rangle\}$ para o espaço de Hilbert, obtemos:

$$\mathrm{tr}(\hat{A}) = \sum_n \langle n|\,\hat{A}\,|n\rangle\,. \tag{2.12}$$

Com essa observação, podemos escrever o valor médio de um operador $\hat{A}$ para o estado $|\psi\rangle$ como (consideramos $\hat{I}$ como um operador identidade):

$$\langle\hat{A}\rangle = \langle\psi|\,\hat{A}\,|\psi\rangle = \langle\psi|\,\hat{I}\hat{A}\hat{I}\,|\psi\rangle\,. \tag{2.13}$$

E lembramos que, como $\{|n\rangle\}$ é uma base para o espaço, a seguinte igualdade é válida:

$$\hat{I} = \sum_n |n\rangle\,\langle n|\,. \tag{2.14}$$

Como $\langle\psi|\,, |\psi\rangle$ e $\hat{A}$ são independentes dos índices dos somatórios, podemos escrever o valor médio de A como:

$$\langle\hat{A}\rangle = \sum_m \langle\psi|\,\hat{A}\,|m\rangle\,\langle m|\psi\rangle = \sum_m \langle m|\psi\rangle\,\langle\psi|\,\hat{A}\,|m\rangle = \sum_m \langle m|\,\hat{\rho}\hat{A}\,|m\rangle\,. \tag{2.15}$$

E, portanto, obtemos:

$$\langle\hat{A}\rangle = \sum_m \langle m|\,\hat{\rho}\hat{A}\,|m\rangle = \mathrm{tr}(\hat{\rho}\hat{A}). \tag{2.16}$$

Para a próxima observação sobre o operador densidade, note que, uma vez definido um conjunto ortonormal para o sistema $\{|n\rangle\}$, podemos definir:

$$|\psi\rangle = \sum_n \langle n|\psi\rangle\,|n\rangle = \sum_n c_n\,|n\rangle\,, \tag{2.17}$$

com $\sum_n |c_n|^2 = 1$, porque estamos considerando $\langle\psi|\psi\rangle = 1$. Desta forma, o traço de $\hat{\rho}$ é igual a 1:

$$\mathrm{tr}(\hat{\rho}) = \sum_n \langle n|\psi\rangle \langle\psi|n\rangle = \sum_n |c_n|^2 = 1. \tag{2.18}$$

Por fim, conseguimos escrever $\hat{\rho}$ em termos de uma matriz de coeficientes. Para isso notamos que $\langle\psi|$ pode ser escrito como:

$$\langle\psi| = |\psi\rangle^\dagger = \left(\sum_n c_n |n\rangle\right)^\dagger = \sum_n \langle n| c_n^*. \tag{2.19}$$

Com isso, obtemos:

$$\hat{\rho} = |\psi\rangle \langle\psi| = \sum_{n,m} c_n c_m^* |n\rangle \langle m|. \tag{2.20}$$

E, então, os coeficientes da matriz $\hat{\rho}$ são dados por:

$$\hat{\rho}_{nm} = c_n c_m^* \text{ ou } \hat{\rho} \cong \begin{pmatrix} c_1c_1^* & c_1c_2^* & \cdots \\ c_2c_1^* & c_2c_2^* & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}, \tag{2.21}$$

onde o símbolo $(\cong)$ foi utilizado para identificar $\hat{\rho}$ como uma matriz.

Ressaltamos que as entradas da diagonal principal da matriz $\hat{\rho}$ são chamadas de *populações* ou *números de ocupação*, enquanto as outras entradas recebem o nome de *coerências* ou *termos de interferência*.

Agora vamos ver um resultado para a matriz densidade de um *estado puro*, que será importante posteriormente, na comparação da matriz densidade quando o estado é *misto*.

Para isso, consideramos um vetor $|\psi\rangle$ no espaço de Hilbert bidimensional. O operador $\hat{\rho}$ é descrito como:

$$\hat{\rho} = \begin{pmatrix} c_1c_1^* & c_1c_2^* \\ c_2c_1^* & c_2c_2^* \end{pmatrix}. \tag{2.22}$$

Note que, considerando $|\psi\rangle \neq 0$, a matriz $\hat{\rho}$ apresenta uma das entradas não nulas ou todas as entradas não nulas. De fato, se $c_1, c_2 \neq 0$, então todas as entradas são não nulas. Se $c_1 = 0$, então apenas $c_2c_2^* \neq 0$; analogamente para c_2 = 0, nesse caso a única entrada não nula é $c_1c_1^*$.

2.3.2 Operador densidade em estados mistos

De maneira geral, não se sabe se determinado estado quântico está precisamente descrito por um estado $|\psi\rangle$, como é o caso, por exemplo, do estudo de um gás a partir da *Teoria Cinética dos Gases* [9, p. 120-123]. Nesse caso, somente o estado

macroscópico é conhecido e, normalmente, existe uma infinidade de configurações microscópicas $|\psi_n\rangle$ ($n = 1, \ldots$) capazes de respeitar tal vínculo. Consideramos que a probabilidade do sistema estar no estado microscópico $|\psi_n\rangle$ é p_n, onde $0 \leq p_n \leq 1$. Assim, uma completa descrição do sistema pode ser descrita pelo seguinte operador:

$$\hat{\rho}_{stat} = \sum_n p_n |\psi_n\rangle \langle\psi_n| . \tag{2.23}$$

Por exemplo, assumindo que um estado é descrito por $\{|\psi_1\rangle, |\psi_2\rangle\}$, onde $|\psi_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |\psi_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $p_1 = p_2 = \frac{1}{2}$, segue que:

$$\hat{\rho}_{stat} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} . \tag{2.24}$$

Note que é impossível escrever a matriz em (2.24) como uma matriz densidade obtida a partir de um único $|\psi\rangle$, devido à restrição imposta por (2.22).

No decorrer deste trabalho, estados mistos voltarão a aparecer somente em algumas descrições de estados reduzidos. Portanto, uma análise mais detalhada destes estados, neste ponto, não é necessária para o desenvolvimento dos objetivos propostos.

2.4 EXEMPLO: OPERADOR DENSIDADE APLICADO A ESTADOS SEPARÁVEIS

Considere o estado representado pelo vetor $|\Psi\rangle$ em (2.3). Nesse caso, o vetor representa o estado geral da polarização de dois fótons. O operador densidade definido para esse vetor é dado por:

$$\hat{\rho} = |\Psi\rangle \langle\Psi| . \tag{2.25}$$

Matricialmente, $\hat{\rho}$ pode ser representado por:

$$\hat{\rho} = \begin{bmatrix} |a_{hh}|^2 & a_{hh}a_{hv}^* & a_{hh}a_{vh}^* & a_{hh}a_{vv}^* \\ a_{hv}a_{hh}^* & |a_{hv}|^2 & a_{hv}a_{vh}^* & a_{hv}a_{vv}^* \\ a_{vh}a_{hh}^* & a_{vh}a_{hv}^* & |a_{vh}|^2 & a_{vh}a_{vv}^* \\ a_{vv}a_{hh}^* & a_{vv}a_{hv}^* & a_{vv}a_{vh}^* & |a_{vv}|^2 \end{bmatrix} . \tag{2.26}$$

Vejamos agora como ficam os operadores $\hat{\rho}_1 = |\psi_1\rangle \langle\psi_1|$ e $\hat{\rho}_2 = |\psi_2\rangle \langle\psi_2|$, em que $|\psi_1\rangle$ e $|\psi_2\rangle$ assumem a forma de $|\phi\rangle$ e $|\psi\rangle$, respectivamente, segundo a equação (2.4). Encontramos:

$$\begin{aligned} \hat{\rho}_1 &= |\psi_1\rangle \langle\psi_1| \\ &= (a_{1h} |h\rangle + a_{1v} |v\rangle)(a_{1h}^* \langle h| + a_{1v}^* \langle v|) \\ &= \begin{bmatrix} |a_{1h}|^2 & a_{1h}a_{1v}^* \\ a_{1v}a_{1h}^* & |a_{1v}|^2 \end{bmatrix} . \end{aligned} \tag{2.27}$$

Analogamente:

$$\begin{aligned}\hat{\rho}_2 &= |\psi_2\rangle \langle\psi_2| \\ &= (a_{2h}|h\rangle + a_{2v}|v\rangle)(a_{2h}^* \langle h| + a_{2v}^* \langle v|) \\ &= \begin{bmatrix} |a_{2h}|^2 & a_{2h}a_{2v}^* \\ a_{2v}a_{2h}^* & |a_{2v}|^2 \end{bmatrix}. \end{aligned} \tag{2.28}$$

Lembramos agora que, se $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, os coeficiente acima satisfazem:

$$a_{hh} = a_{1h}a_{2h}, \quad a_{hv} = a_{1h}a_{2v}, \quad a_{vh} = a_{1v}a_{2h}, \quad e \quad a_{vv} = a_{1v}a_{2v}. \tag{2.29}$$

Podemos definir o traço parcial sobre a segunda variável, definido segundo a operação:

$$\mathrm{tr}(\hat{\rho})_2 = \sum_{i=1}^{2} \langle i|_2 \, \hat{\rho} \, |i\rangle_2 , \tag{2.30}$$

onde $\{|i\rangle_2\} = \{|h\rangle, |v\rangle\}$ diz respeito à segunda variável dos vetores da base do espaço original, isto é, atua-se somente na segunda parte do sistema. No próximo capítulo, será demonstrado com mais detalhes o cálculo do traço parcial de um operador $\hat{\rho}$ em um estado puro e bipartido. Vemos que essa operação, ao contrário do traço usual de um operador, que resulta em um escalar, fornece um novo operador com dimensão igual à da parte não traçada. Analogamente, definimos o traço parcial sobre a primeira variável. Esses operadores resultantes do traço parcial são denominados *operadores densidade reduzidos*.

Dito isso, segue que:

$$\mathrm{tr}(\hat{\rho})_2 = \begin{bmatrix} |a_{hh}|^2 + |a_{hv}|^2 & a_{hh}a_{vh}^* + a_{hv}a_{vv}^* \\ a_{hh}^*a_{vh} + a_{hv}^*a_{vv} & |a_{vh}|^2 + |a_{vv}|^2 \end{bmatrix}. \tag{2.31}$$

Ainda, é possível reescrever $\mathrm{tr}(\hat{\rho})_2$ para o caso do estado produto. Para isso, note que, como os vetores $|\psi_1\rangle$ e $|\psi_2\rangle$ são normalizados, tem-se que $|a_{1h}|^2 + |a_{1v}|^2 = 1$ e $|a_{2h}|^2 + |a_{2v}|^2 = 1$. Então:

- Entrada $(\mathrm{tr}(\hat{\rho})_2)_{11}$:

$$|a_{hh}|^2 + |a_{hv}|^2 = |a_{1h}a_{2h}|^2 + |a_{1h}a_{2v}|^2 = |a_{1h}|^2[|a_{2h}|^2 + |a_{2v}|^2] = |a_{1h}|^2. \tag{2.32}$$

- Entrada $(\mathrm{tr}(\hat{\rho})_2)_{12}$:

$$a_{hh}a_{vh}^* + a_{hv}a_{vv}^* = a_{1h}a_{2h}a_{1v}^*a_{2h}^* + a_{1h}a_{2v}a_{1v}^*a_{2v}^* = a_{1h}a_{1v}^*[|a_{2h}|^2 + |a_{2v}|^2] = a_{1h}a_{1v}^*. \tag{2.33}$$

- Entrada $(\mathrm{tr}(\hat{\rho})_2)_{21}$:

$$a^*_{hh}a_{vh} + a^*_{hv}a_{vv} = a^*_{1h}a^*_{2h}a_{1v}a_{2h} + a^*_{1h}a^*_{2v}a_{1v}a_{2v} = a^*_{1h}a_{1v}[|a_{2h}|^2 + |a_{2v}|^2] = a^*_{1h}a_{1v}. \tag{2.34}$$

- Entrada $(\mathrm{tr}(\hat{\rho})_2)_{22}$:

$$|a_{vh}|^2 + |a_{vv}|^2 = |a_{1v}a_{2h}|^2 + |a_{1v}a_{2v}|^2 = |a_{1v}|^2[|a_{2h}|^2 + |a_{2v}|^2] = |a_{1v}|^2. \tag{2.35}$$

Assim, escrevemos $\mathrm{tr}(\hat{\rho})_2$ como:

$$\mathrm{tr}(\hat{\rho})_2 = \begin{bmatrix} |a_{1h}|^2 & a_{1h}a^*_{1v} \\ a^*_{1h}a_{1v} & |a_{1v}|^2 \end{bmatrix}. \tag{2.36}$$

Note que $\mathrm{tr}(\hat{\rho})_2$ é escrito completamente em termos dos coeficientes de $|\psi_1\rangle$, ou seja, não é influenciado por $|\psi_2\rangle$. Mais ainda, $\mathrm{tr}(\hat{\rho})_2 = \hat{\rho}_1$, conforme (2.27). Isso era de se esperar, pois o estado inicial $|\Psi\rangle$ é separável e, ao tomar o traço parcial sobre a segunda variável, estamos reduzindo o sistema somente à primeira parte. Veremos, no próximo capítulo, um caso em que, assumindo um estado geral, não é possível obter essa mesma conclusão.

2.4.1 Dinâmica quântica

Em determinados sistema quânticos, é relevante considerar a evolução temporal. Para isso, podemos utilizar a representação de Schrödinger, onde a dependência temporal de um sistema representado por um vetor $|\psi\rangle$ é descrita através dos coeficientes de sua expansão em alguma base. Por exemplo, sendo $\{|n\rangle\}$ uma base ortonormal para o vetor $|\psi\rangle$, podemos escrevê-lo como:

$$|\psi(t)\rangle = \sum_n c_n(t)\,|n\rangle\,. \tag{2.37}$$

Consequentemente, o operador densidade $\hat{\rho}$ também apresenta dependência temporal, pois $\hat{\rho} = |\psi(t)\rangle\,\langle\psi(t)|$. A partir desse operador, podemos analisar como se dá a dinâmica de emaranhamento de determinado sistema, conforme descrito no capítulo 4.

3 ENTROPIA

O conceito de entropia assume diferentes significados para áreas distintas da Física. Por exemplo, para a Termodinâmica, entropia diz respeito à *desordem de um sistema*, está relacionada ao número de configurações microscópicas possíveis para um conhecido estado macroscópico [13]. Na teoria da informação clássica, a entropia utilizada é a *entropia de Shannon*, que diz respeito à incerteza acerca de uma variável antes de se realizar sua medida. De maneira similar, para sistemas quânticos, a entropia utilizada de maneira geral é a entropia de von Neumann, que é caracterizada através do operador densidade de determinado sistema. Podemos dizer que, nesses sistemas, a entropia também está relacionada com o número de microestados, porém, neste contexto, o microestado é caracterizado por um vetor de estado no subespaço de Hilbert do sistema [10].

Neste capítulo, serão apresentados conceitos e resultados acerca da entropia de Shannon e de von Neumann, bem como uma versão simplificada motivada pela última, chamada de entropia linear, que será a mais conveniente para o alcance dos objetivos propostos pelo trabalho.

3.1 ENTROPIA DE SHANNON

De acordo com a referência [10], entropia é a medida de quanta incerteza há no estado de um sistema físico. Em particular, a *entropia de Shannon* é fundamental para o entendimento da teoria da informação clássica. De maneira geral, tomando-se uma variável aleatória X, a entropia de Shannon de X indica a quantidade de incerteza sobre X, antes de uma medição de seu valor, ou a quantidade de informação ganha após a medição da variável. Ela é definida em termos das probabilidades $(p_1, \cdots, p_n)$ da variável assumir determinados valores $(x_1, \cdots, x_n)$, respectivamente. A entropia de Shannon é definida por:

$$H(X) \equiv H(p_1, \cdots, p_n) \equiv -\sum_{i=1}^{n} p_i \log_2 p_i. \tag{3.1}$$

Escrita desta forma, a entropia tem unidade de "bit", enquanto que na base natural a unidade é "nat". Note que, como a probabilidade p_j de um evento ocorrer pode ser nula, definimos:

$$p_j \log_2 p_j = 0 \log_2 0 \equiv 0, \quad \text{pois} \quad \lim_{x \to 0} x \log x = 0. \tag{3.2}$$

A definição de entropia é construída assim para que seja possível quantificar os recursos necessários para armazenar informações.

Iremos agora tratar de alguns exemplos para nos familiarizar com este conceito de entropia. Suponha que uma variável X seja tal que apenas um único evento possa acontecer. Isto é, há 100% de chance dele ocorrer. Nesse caso não há entropia no sistema pois $H(X) = 1 \cdot \log_2 1 = 0$. Concluímos, então, que a entropia é nula para variáveis que estão 100% determinadas antes da medição.

Outro exemplo típico consiste no lançamento de uma moeda justa, onde há 50% de chance de obtermos coroa e 50% de chance de se obter cara. Então, temos que a entropia associada ao lançamento vale:

$$H(X) = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{1}{2}\log_2\left(\frac{1}{2}\right) = 1. \tag{3.3}$$

Portanto, após ler a face da moeda, teremos ganho um bit de informação. E se, por algum motivo, a probabilidade de sair cara fosse 75% e a de sair coroa fosse de 25%, então a entropia associada ao sistema seria:

$$H(x) = -\frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{3}{4}\log_2\left(\frac{3}{4}\right) \approx 0,811. \tag{3.4}$$

Agora considere o exemplo do lançamento de um dado justo. Cada face do dado tem uma probabilidade de $1/6$ de aparecer após o lançamento. Então a entropia associada ao lançamento do dado é:

$$H(X) = -\sum_{1}^{6}\frac{1}{6}\log_2\left(\frac{1}{6}\right) = \log_2(6) \approx 2,585. \tag{3.5}$$

3.1.1 Entropia binária

Quando a entropia de uma variável aleatória depende somente de duas probabilidades, como no caso da moeda mostrado acima, nomeamos a entropia de H_{bin}, que pode ser definida como:

$$H_{\text{bin}}(p) \equiv -p\log p - (1-p)\log(1-p), \tag{3.6}$$

em que $0 \leq p \leq 1$. Tomando a derivada desta função, temos: $H'_{\text{bin}}(p) = -\log(p) - 1 + \log(1-p) + 1 = \log(1-p) - \log(p)$. Essa derivada é igual a 0 quando $\log(1-p) = \log(p) \Rightarrow (1-p) = p \Rightarrow p = 1/2$. Ou seja, a entropia binária apresenta valores estacionários somente quando $p = 1/2$. Para verificar que esse valor é um máximo global, tomamos a segunda derivada da entropia binária, dada por:

$$H''_{\text{bin}}(p) = -\frac{1}{1-p} - \frac{1}{p} = \frac{-p-(1-p)}{p(1-p)} = -\frac{1}{p(1-p)}. \tag{3.7}$$

Como $H''_{\text{bin}}(1/2) < 0$, concluímos que, de fato, o ponto $1/2$ maximiza a entropia binária. Isso concorda com o que foi ilustrado anteriormente, no caso do lançamento de uma moeda. A situação com maior entropia entre os dois exemplos analisados foi aquela em que consideramos uma moeda justa, com 50% de chance de se obter cada uma das faces.

3.2 ENTROPIA DE VON NEUMANN

Dado que estamos interessados em estados bipartidos, uma versão quântica da entropia binária mostrada acima é desejada. Assim como a entropia de Shannon mede a incerteza associada a uma probabilidade clássica, a entropia de estados quânticos é medida através de entropia de von Neumann. Para isto, é necessário utilizar o operador densidade $\hat{\rho}$ estudado nas seções anteriores. Como tal operador geralmente é representado por uma matriz e a definição de entropia envolve logaritmos, precisamos definir o logaritmo de um operador $\hat{A}$ qualquer:

$$\ln(\hat{A}) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(\hat{A} - I)^k}{k}. \tag{3.8}$$

Note que $\ln(\hat{A})$, dentro de certas condições de convergência[1], também é uma matriz.

Agora podemos definir a entropia de um estado quântico $\hat{\rho}$. Tal medida é dada pela fórmula:

$$S(\hat{\rho}) \equiv -\operatorname{tr}(\hat{\rho} \ln(\hat{\rho})). \tag{3.9}$$

Se λ_x são os autovalores de $\hat{\rho}$ então a entropia de von Neumann pode ser reescrita como:

$$S(\hat{\rho}) = -\sum_x \lambda_x \ln \lambda_x. \tag{3.10}$$

Vamos ver uma prova para a igualdade acima, no caso particular que $\ln(\hat{\rho})$ converge. Como a matriz $\hat{\rho}$ é complexa, esse é o caso onde $\hat{\rho}$ é invertível. Sabemos que qualquer matriz quadrada é semelhante a uma matriz de Jordan [15]. Mais precisamente, para uma matriz A quadrada qualquer vale a seguinte igualdade:

$$A = V^{-1} J V, \tag{3.11}$$

onde V é a matriz de autovetores (ou autovetores generalizados) de A e J, a matriz de Jordan, é uma matriz diagonal superior, cuja diagonal principal contém os autovalores da matriz A e as entradas da diagonal secundária superior são 1 ou 0.

Outro resultado importante é o binômio de Newton. Sejam $a, b \in \mathbb{C}$. Temos que:

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} (a^{n-p} \cdot b^p). \tag{3.12}$$

Esse resultado pode ser estendido também para o caso de matrizes, onde, ao invés de considerarmos a e b números reais, consideramos matrizes quadradas A e B de dimensão m, desde que elas comutem, isto é, que $AB = BA$. Em nosso caso, uma das matrizes é a identidade, por isso a extensão valerá.

[1] Uma matriz A com entradas complexas tem um logaritmo se, e somente se, é invertível [14].

Seja $\hat{\rho}$ o operador densidade descrito por $\hat{\rho} = V^{-1}JV$. Pelas equações (3.8) e (3.12) podemos escrever:

$$\ln\hat{\rho} = \sum_{k=1}^{\infty}(-1)^{k+1}\frac{(\hat{\rho}-I)^k}{k} = \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}(\hat{\rho}^{k-p}I^p). \tag{3.13}$$

Agora note que $I^p = I$ para qualquer valor de p. Utilizando a igualdade $\hat{\rho} = V^{-1}JV$ na relação acima, e observando que $\hat{\rho}^p = (V^{-1}JV)(V^{-1}JV)\cdots(V^{-1}JV) = V^{-1}J^pV$, podemos escrever:

$$\ln\hat{\rho} = \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}(V^{-1}J^{k-p}V). \tag{3.14}$$

Agora, como estamos considerando o caso em que $\ln\hat{\rho}$ converge, podemos escrever $\mathrm{tr}(\hat{\rho}\ln\hat{\rho})$ como (utilizando que o traço da soma de matrizes é igual a soma dos traços):

$$\begin{aligned}\mathrm{tr}(\hat{\rho}\ln\hat{\rho}) &= \mathrm{tr}\left(V^{-1}JV\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}(V^{-1}J^{k-p}V)\right)\\ &= \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}\mathrm{tr}(V^{-1}J^{k-p+1}V).\end{aligned} \tag{3.15}$$

Aqui utilizaremos a propriedade cíclica do traço para um produto de matrizes: $\mathrm{tr}(V^{-1}J^{k-p+1}V) = \mathrm{tr}(VV^{-1}J^{k-p+1}) = \mathrm{tr}(J^{k-p+1})$. Além disso, como J é triangular superior, se λ é um elemento da diagonal principal de J^{k-p+1}, então $\lambda = \lambda_0^m$, onde λ_0 é o elemento da entrada correspondente de J e $m = k-p+1$. Como a diagonal principal de J é composta de autovalores de $\hat{\rho}$, que serão denotados por λ_j, podemos escrever:

$$\begin{aligned}\mathrm{tr}(\hat{\rho}\ln\hat{\rho}) &= \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}\sum_{j=1}^{m}\lambda_j^{k-p+1}\\ &= \sum_{j=1}^{m}\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}(-1)^p\binom{k}{p}\lambda_j^{k-p+1}\\ &= \sum_{j=1}^{m}\lambda_j\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\sum_{p=0}^{k}\binom{k}{p}\lambda_j^{k-p}(-1)^p.\end{aligned} \tag{3.16}$$

Novamente, utilizando a equação (3.12), escrevemos:

$$\begin{aligned}\mathrm{tr}(\hat{\rho}\ln\hat{\rho}) &= \sum_{j=1}^{m}\lambda_j\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}(\lambda_j-1)^k\\ &= \sum_{j=1}^{m}\lambda_j\ln\lambda_j,\end{aligned} \tag{3.17}$$

o que prova a igualdade. Este último resultado também pode ser obtido, de maneira mais direta, tomando o traço da equação (3.9), utilizando a base que diagonaliza $\hat{\rho}$. Aqui, optamos por demonstrar tal resultado através desta maneira alternativa.

No caso em que $\hat{\rho}$ não é invertível, a mesma demonstração não se aplica, mas, nesse caso, sabemos que o operador apresenta algum autovalor nulo. De fato, se $\hat{\rho}v = 0$ para algum vetor v não nulo, então podemos escrever $0 = 0 \cdot v = \hat{\rho}v$. Nesse caso, ainda assumimos que a equação (3.10) vale, considerando que $0 \cdot \ln 0 \equiv 0$, uma vez que $\lim_{x \to 0^+} x \ln x = 0$.

3.3 ENTROPIA LINEAR

Vimos na seção anterior que a entropia de von Neumann é dada pela expressão (3.9). A partir dela, definimos a entropia linear associada ao operador $\hat{\rho}$, notando que, para uma aproximação de primeira ordem em x, $\ln(1 + x) \approx x$, para x suficientemente pequeno. Estendendo está condição diretamente a matrizes, podemos aproximar:

$$\begin{aligned} S(\hat{\rho}) &= -\operatorname{tr}(\hat{\rho}\ln(\hat{\rho})) = -\operatorname{tr}(\hat{\rho}\ln(1-(1-\hat{\rho}))) \\ &\approx -\operatorname{tr}(\hat{\rho}(-(1-\hat{\rho}))) = -\operatorname{tr}(\hat{\rho}^2 - \hat{\rho}) = \operatorname{tr}(\hat{\rho}) - \operatorname{tr}(\hat{\rho}^2) = 1 - \operatorname{tr}(\hat{\rho}^2), \end{aligned} \tag{3.18}$$

onde utilizamos que $\operatorname{tr}(\hat{\rho}) = 1$, conforme equação (2.18).

Definimos $\gamma(\hat{\rho}) \equiv \operatorname{tr}(\hat{\rho}^2)$ como a *pureza* de um estado $\hat{\rho}$, chamando de *entropia linear* o número $S_{\text{lin}}(\hat{\rho}) = 1 - \gamma(\hat{\rho})$. Apesar do motivação para se definir esta entropia ter partido da aproximação acima comentada, salientamos que o seu uso continua válido para situações que vão além desta restrição. Em outras palavras, S_{lin} ainda se caracteriza como uma entropia, mesmo que fora daquele limite.

Verifica-se que $\gamma(\hat{\rho}) = 1$ se, e somente se, $\hat{\rho}$ for um estado puro, conforme equação (2.11). Consequentemente, $S_{\text{lin}}(\hat{\rho}) = 0$ para qualquer estado puro.

Este resultado não nos surpreende porque, se temos um estado puro, então seu vetor de estado é conhecido, de modo que não há falta de informação. Na verdade, poderíamos dizer ainda que há uma incerteza genuinamente quântica presente no vetor de estado, mas esta não é contemplada pela entropia linear.

4 ENTROPIA LINEAR E O EMARANHAMENTO

Conforme abordado no capítulo anterior, a entropia linear é mais simples de ser calculada e é útil no estudo de emaranhamento de sistemas quânticos, como veremos a seguir. No capítulo 2, definiu-se o estado reduzido de um operador. Neste capítulo, retornamos a esse conceito e mostraremos sua importância na quantificação de emaranhamento.

Antes, porém, para nos familiarizar com os conceitos, vejamos um estudo de caso baseado em spins de dois elétrons.

4.1 UM ESTUDO DE CASO

Considere um sistema formado por dois elétrons, para os quais apenas o grau de liberdade de spin nos interessa. Podemos considerar que, em determinada direção, cada elétron pode ter spin *up*, que será denotado por $+$ e spin *down*, que será denotado por $-$. Podemos então definir o vetor estado puro geral como:

$$|\psi\rangle = a\,|{+}{+}\rangle + b\,|{+}{-}\rangle + c\,|{-}{+}\rangle + d\,|{-}{-}\rangle\,. \tag{4.1}$$

Então identificamos os quatro vetores de base acima com as seguintes matrizes:

$$|{+}{+}\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |{+}{-}\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |{-}{+}\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |{-}{-}\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{4.2}$$

O operador $\hat{\rho} = |\psi\rangle\langle\psi|$ será dado por:

$$\begin{aligned}
\hat{\rho} =& (a\,|{+}{+}\rangle + b\,|{+}{-}\rangle + c\,|{-}{+}\rangle + d\,|{-}{-}\rangle)(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|) \\
=& a\,|{+}{+}\rangle\,(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|) \\
&+ b\,|{+}{-}\rangle\,(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|) \\
&+ c\,|{-}{+}\rangle\,(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|) \\
&+ d\,|{-}{-}\rangle\,(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|).
\end{aligned} \tag{4.3}$$

Vejamos inicialmente qual o valor do primeiro termo da equação acima, pois os outros são análogos a este:

$$\begin{aligned}
&a\,|{+}{+}\rangle\,(a^*\langle{+}{+}| + b^*\langle{+}{-}| + c^*\langle{-}{+}| + d^*\langle{-}{-}|) = \\
&|a|^2\,|{+}{+}\rangle\langle{+}{+}| + ab^*\,|{+}{+}\rangle\langle{+}{-}| + ac^*\,|{+}{+}\rangle\langle{-}{+}| + ad^*\,|{+}{+}\rangle\langle{-}{-}|\,.
\end{aligned} \tag{4.4}$$

Utilizando a representação matricial, a última linha da expressão acima resulta na matriz:

$$\begin{bmatrix} |a|^2 & ab^* & ac^* & ad^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{4.5}$$

Utilizando a mesma ideia para os outros termos de $\hat{\rho}$, podemos escrever esse operador como:

$$\hat{\rho} = \begin{bmatrix} |a|^2 & ab^* & ac^* & ad^* \\ ba^* & |b|^2 & bc^* & bd^* \\ ca^* & cb^* & |c|^2 & cd^* \\ da^* & db^* & dc^* & |d|^2 \end{bmatrix}. \tag{4.6}$$

Como estamos considerando que o vetor $|\psi\rangle$ está normalizado, é imediato ver que $\mathrm{tr}(\hat{\rho}) = 1$.

Informações relevantes acerca do emaranhamento das duas partes de $\hat{\rho}$ são obtidas quando analisamos os operadores reduzidos.

Assim, podemos definir o traço parcial sobre a segunda variável, ao considerar a operação:

$$\mathrm{tr}_2(\hat{\rho}) = \sum_{i=+,-} \langle i|_2 \, \hat{\rho} \, |i\rangle_2 = \langle +|_2 \, \hat{\rho} \, |+\rangle_2 + \langle -|_2 \, \hat{\rho} \, |-\rangle_2 . \tag{4.7}$$

Para o primeiro termo da soma acima, temos:

$$\begin{aligned} \langle +|_2 \, \hat{\rho} \, |+\rangle_2 = \langle +|_2 \Big\{ & a \, |{+}{+}\rangle \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \\ & + b \, |{+}{-}\rangle \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \\ & + c \, |{-}{+}\rangle \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \\ & + d \, |{-}{-}\rangle \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \Big\} |+\rangle_2 \\ = \Big\{ & a \, |+\rangle_1 \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \\ & + c \, |-\rangle_1 \left(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \right) \Big\} |+\rangle_2 \\ = a \, |+\rangle_1 & \left(a^* \langle +|_1 + c^* \langle -|_1 \right) + c \, |-\rangle_1 \left(a^* \langle +|_1 + c^* \langle -|_1 \right). \end{aligned} \tag{4.8}$$

Para o segundo termo de $\mathrm{tr}_2(\rho)$ temos:

$$\begin{aligned}
\langle -|_2 \hat{\rho} |-\rangle_2 = \langle -|_2 \Big\{ & a |{+}{+}\rangle \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \Big) \\
& + b |{+}{-}\rangle \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \Big) \\
& + c |{-}{+}\rangle \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \Big) \\
& + d |{-}{-}\rangle \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d^* \langle {-}{-}| \Big) \Big\} |-\rangle_2 \\
= \Big\{ & b |+\rangle_1 \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d \langle {-}{-}| \Big) \\
& + d |-\rangle_1 \Big(a^* \langle {+}{+}| + b^* \langle {+}{-}| + c^* \langle {-}{+}| + d \langle {-}{-}| \Big) \Big\} |-\rangle_2 \\
= & \, b |+\rangle_1 \Big(b^* \langle +|_1 + d^* \langle -|_1 \Big) + d |-\rangle_1 \Big(b^* \langle +|_1 + d^* \langle -|_1 \Big).
\end{aligned} \tag{4.9}$$

Identificando os termos $|+\rangle_1 \langle +|_1, |+\rangle_1 \langle -|_1, |-\rangle_1 \langle +|_1$ e $|-\rangle_1 \langle -|_1$ com as matrizes:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ e } \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \tag{4.10}$$

respectivamente, temos que $\mathrm{tr}(\hat{\rho})_2$ pode ser representado por:

$$\mathrm{tr}(\hat{\rho})_2 = \begin{bmatrix} |a|^2 + |b|^2 & ac^* + bd^* \\ a^*c + b^*d & |c|^2 + |d|^2 \end{bmatrix} := \hat{\rho}_1. \tag{4.11}$$

De forma análoga, podemos escrever:

$$\mathrm{tr}(\hat{\rho})_1 = \begin{bmatrix} |a|^2 + |c|^2 & ab^* + cd^* \\ a^*b + c^*d & |b|^2 + |d|^2 \end{bmatrix} := \hat{\rho}_2. \tag{4.12}$$

Note que ambos os traços parciais acima dependem dos 4 coeficientes do vetor de estado original. Conforme comentado anteriormente, isso ocorreu porque o estado inicial não é necessariamente separável. Então, medidas somente sobre o elétron 1 ou 2, dependerá da configuração inicial de ambos, donde concluímos que o estado inicial é **emaranhado**. Em outras palavras, não conseguimos escrever os estados $\hat{\rho}_i$ como $\hat{\rho}_i = |\psi_i\rangle \langle \psi_i|$, onde $|\psi_i\rangle$ seria uma das partes do estado separável $|\psi_1\rangle \otimes |\psi_2\rangle$.

Chamamos de $\hat{\rho}_{\text{red}}$ os traços parciais $\hat{\rho}_1$ e $\hat{\rho}_2$ acima. Mostraremos que uma medida possível de emaranhamento para um estado puro, é tomar $S_{\text{lin}}(\hat{\rho}_{\text{red}})$.

Note também que $\mathrm{tr}(\hat{\rho}_1) = \mathrm{tr}(\hat{\rho}_2) = 1$, uma vez que o vetor $|\psi\rangle$ é normalizado. Agora perceba que:

$$\hat{\rho}_1^2 = \begin{bmatrix} t_{ab}^2 + (ac^* + bd^*)(a^*c + b^*d) & t_{ab}(ac^* + bd^*) + t_{cd}(ac^* + bd^*) \\ (ac^* + bd^*)t_{ab} + (|c|^2 + |d|^2)(a^*c + b^*d) & (ac^* + bd^*)(a^*c + b^*d) + t_{cd}^2 \end{bmatrix}, \tag{4.13}$$

em que $t_{ab} = (|a|^2 + |b|^2)$ e $t_{cd} = (|c|^2 + |d|^2)$. Então,

$$\mathrm{tr}(\hat{\rho}_1^2) = (|a|^2 + |b|^2)^2 + 2|a|^2|c|^2 + 2|b|^2|d|^2 + 2ab^*c^*d + 2a^*bcd^* + (|c|^2 + |d|^2)^2. \quad (4.14)$$

Analogamente, obtemos:

$$\mathrm{tr}(\hat{\rho}_2^2) = (|a|^2 + |c|^2)^2 + 2|a|^2|b|^2 + 2|c|^2|d|^2 + 2ab^*c^*d + 2a^*bcd^* + (|b|^2 + |d|^2)^2. \quad (4.15)$$

Comparando os termos da equação acima, é possível demonstrar que $\mathrm{tr}(\hat{\rho}_1^2) = \mathrm{tr}(\hat{\rho}_2^2)$. Mais ainda, esse resultado pode ser generalizado para qualquer operador $\hat{\rho}$ obtido a partir de um estado puro. Vejamos aqui uma demonstração desse fato, através do Teorema da decomposição de Schmidt [10, p. 109-110]:

Suponha que $|\psi\rangle$ é um estado puro de um sistema composto de 2 partes A e B. Então existem estados ortonormais $|i_A\rangle$, para o sistema A, e estados ortonormais $|i_B\rangle$, para o sistema B, tais que:

$$|\psi\rangle = \sum_{i}^{\min\{m,n\}} \lambda_i |i_A\rangle |i_B\rangle , \quad (4.16)$$

onde λ_i são valores reais não-negativos que satisfazem $\sum_i |\lambda_i|^2 = 1$, os quais são conhecidos como coeficientes de Schmidt, e m e n são as dimensões de A e B, respectivamente.

Para demonstrar esse enunciado, vamos utilizar a decomposição de uma matriz em valores singulares.

Toda matriz $A \in \mathbb{C}^{m\times n}$ com coeficientes reais ou complexos apresenta uma decomposição em valores singulares, isto é, A pode ser escrita como $A = U\Sigma V^T$, em que $U \in \mathbb{C}^{m\times m}$ e $V \in \mathbb{C}^{n\times n}$ são matrizes ortogonais, e $\Sigma \in \mathbb{R}^{m\times n}$ é uma matriz diagonal cujos elementos são não negativos; tais elementos são chamados de valores singulares da matriz. Suponha então que estamos trabalhando com dois sistemas A e B, cujas bases ortonormais são $|j\rangle$ e $|k\rangle$. Dessa forma, o vetor de estado geral $|\psi\rangle$ pode ser representado por:

$$|\psi\rangle = \sum_{jk} a_{jk} |j\rangle |k\rangle . \quad (4.17)$$

Considerando uma matriz com entradas a_{jk}, sabemos que ela pode ser escrita como $\sum_i u_{ji}\sigma_{ii}v_{ik}$, de acordo com sua decomposição em valores singulares. Aqui, assumimos que os valores i são tais que $1 \leq i \leq p$, onde $p = \min\{m, n\}$. Assim, o estado $|\psi\rangle$ assume a forma:

$$|\psi\rangle = \sum_{ijk} u_{ji}\sigma_{ii}v_{ik} |j\rangle |k\rangle . \quad (4.18)$$

Agora definamos $|i_A\rangle = \sum_j u_{ji} |j\rangle$, $|i_B\rangle = \sum_k v_{ik} |k\rangle$ e $\lambda_i = \sigma_{ii}$. Desta forma:

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle . \tag{4.19}$$

Sabemos que cada $\lambda_i \geq 0$ e verificamos se os conjuntos $\{|i_A\rangle\}, \{|i_B\rangle\}$ são ortonormais.

De fato, note que:

$$\langle i'_A|i_A\rangle = \sum_{j'} u^*_{j'i'} \langle j'| \sum_j u_{ji} |j\rangle = \sum_{j'j} u^*_{j'i'} u_{ji} \langle j'|j\rangle = \sum_j u^*_{ji'} u_{ji} = \delta_{i'i}, \tag{4.20}$$

onde a última igualdade segue da ortonormalidade das colunas de U.

Similarmente, vemos que $\{|i_B\rangle\}$ é ortonormal.

Como estamos inicialmente supondo que o estado $|\psi\rangle$ é normalizado, segue que $\langle\psi|\psi\rangle = 1$, de forma que:

$$1 = \langle\psi|\psi\rangle = \sum_{i',i} \lambda^*_{i'} \lambda_i \langle i'_A| \langle i'_B|i_B\rangle |i_A\rangle = \sum_i |\lambda_i|^2, \tag{4.21}$$

como queríamos.

Vejamos agora como fica o operador densidade associado ao estado $|\psi\rangle$:

$$\hat{\rho} = |\psi\rangle \langle\psi| = \sum_{i,i'} \lambda_i \lambda^*_{i'} |i_A\rangle |i_B\rangle \langle i'_A| \langle i'_B| . \tag{4.22}$$

Sendo assim, o operador densidade reduzido sobre a segunda variável se torna:

$$\begin{aligned} \hat{\rho}_A = \mathrm{tr}_B(\hat{\rho}) &= \sum_j \langle j_B|\hat{\rho}|j_B\rangle \\ &= \sum_{j,i,i'} \lambda_i \lambda^*_{i'} \langle j_B|i_A\rangle |i_B\rangle \langle i'_A| \langle i'_B|j_B\rangle \\ &= \sum_i |\lambda_i|^2 |i_A\rangle \langle i_A| . \end{aligned} \tag{4.23}$$

Da mesma forma,

$$\begin{aligned} \hat{\rho}_B = \mathrm{tr}_A(\hat{\rho}) &= \sum_j \langle j_A|\hat{\rho}|j_A\rangle \\ &= \sum_{j,i,i'} \lambda_i \lambda^*_{i'} \langle j_A|i_A\rangle |i_B\rangle \langle i'_A|j_A\rangle |i'_B\rangle \\ &= \sum_i |\lambda_i|^2 |i_B\rangle \langle i_B| . \end{aligned} \tag{4.24}$$

Utilizando a ortonormalidade dos conjuntos $|i_A\rangle$ e $|i_B\rangle$, nota-se que:

$$\hat{\rho}_A^2 = \sum_i |\lambda_i|^4 |i_A\rangle \langle i_A| \quad \text{e} \quad \hat{\rho}_B^2 = \sum_i |\lambda_i|^4 |i_B\rangle \langle i_B| . \tag{4.25}$$

Daí, verifica-se que os autovalores de $\hat{\rho}_B^2$ e $\hat{\rho}_A^2$ são reais e iguais. Além disso, como o traço de uma matriz é a soma de seus autovalores, segue que $\mathrm{tr}(\hat{\rho}_A^2) = \mathrm{tr}(\hat{\rho}_B^2)$.

Voltando ao nosso problema, como o traço de cada um dos estados reduzidos é o mesmo, vejamos as condições necessárias e suficientes para que a sua entropia linear seja 0, ou seja, para que $S_{\mathsf{lin}}(\hat{\rho}_{\mathsf{red}}) = 0$.

Estamos supondo que o estado $|\psi\rangle$ é normalizado, ou seja, que $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$, independentemente se o estado é separável ou não. Dessa forma, segue que:

$$\begin{aligned}
\mathrm{tr}(\hat{\rho}_1^2) &= (|a|^2 + |b|^2)^2 + 2(ac^* + bd^*)(a^*c + b^*d) + (|c|^2 + |d|^2)^2 \\
&= (|a|^2 + |b|^2)^2 + (|c|^2 + |d|^2)^2 + 2(|a|^2|c|^2 + ab^*c^*d + a^*bcd^* + |b|^2|d|^2) \\
&= (|a|^2 + |b|^2)^2 + (|c|^2 + |d|^2)^2 + 2(|a|^2|c|^2 + |b|^2|c|^2 + |a|^2|d|^2 + |b|^2|d|^2) \\
&\quad + 2(ab^*c^*d + a^*bcd^* - |b|^2|c|^2 - |a|^2|d|^2) \\
&= [(|a|^2 + |b|^2) + (|c|^2 + |d|^2)]^2 + 2(ab^*c^*d + a^*bcd^* - |b|^2|c|^2 - |a|^2|d|^2) \\
&= 1 + 2(ab^*c^*d + a^*bcd^* - |b|^2|c|^2 - |a|^2|d|^2).
\end{aligned} \tag{4.26}$$

Das relações acima, segue que $\mathrm{tr}(\hat{\rho}_1^2) = 1$ se, e somente se $ab^*c^*d + a^*bcd^* - |b|^2|c|^2 - |a||d|^2 = 0$. Mas isso implica que:

$$\begin{aligned}
&ab^*c^*d + a^*bcd^* - |b|^2|c|^2 - |a|^2|d|^2 = 0 \Leftrightarrow \\
&(ad)(bc)^* + (ad)^*(bc) - (bc)(bc)^* - (ad)^*(ad) = 0 \Leftrightarrow \\
&(ad)[(bc)^* - (ad)^*] + (bc)[(ad)^* - (bc)^*] = 0 \Leftrightarrow \\
&[(bc)^* - (ad)^*](ad - bc) = 0 \Leftrightarrow \\
&ad = bc.
\end{aligned} \tag{4.27}$$

Mas a expressão acima é justamente a obtida em (2.6), a condição necessária e suficiente para um estado bipartido quadridimensional ser separável.

Concluímos então que estados reduzidos de um sistema são sensíveis ao emaranhamento entre as partes do estado puro total, pois, dessa forma, a entropia linear desses estados será 0 se, e somente se, o estado é separável. Esta conclusão qualifica a entropia linear do estado reduzido a um sensor de emaranhamento de estados puros e bipartidos.

4.2 DINÂMICA DE EMARANHAMENTO

A partir de agora, vamos considerar que o vetor de estado $|\psi\rangle$ carrega dependência temporal. Assumimos que o sistema descrito está sujeito a um hamiltoniano $\hat{H}$,

responsável por sua dinâmica, e leva em consideração as interações, tanto internas quanto externas ao sistema. Para simplificar o problema, consideramos que o operador $\hat{H}$ é independente do tempo. Além disso, no instante inicial, o estado é representado por $|\psi_0\rangle$. Podemos escrever $|\psi(t)\rangle$ como:

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar}\hat{H}t} |\psi_0\rangle . \tag{4.28}$$

Para entender melhor como se dá essa dinâmica, vejamos o significado do operador $e^{-\frac{i}{\hbar}\hat{H}t}$. Utilizando série de Taylor, podemos escrever:

$$e^{-\frac{i}{\hbar}\hat{H}t} = \sum_{n=0}^{\infty} \frac{1}{n!} \left(-\frac{i}{\hbar}\hat{H}t \right)^n . \tag{4.29}$$

Segue que o comportamento temporal do sistema está diretamente relacionado com $\hat{H}$.

Assim como vimos nas seções anteriores, podemos associar $|\psi(t)\rangle$ ao operador densidade $\hat{\rho}(t)$, dado por:

$$\hat{\rho}(t) = |\psi(t)\rangle \langle\psi(t)| . \tag{4.30}$$

Escrevendo $U \equiv e^{-\frac{i}{\hbar}\hat{H}t}$ e notando que $\langle\psi(t)| = \langle\psi_0| U^\dagger$, segue que:

$$\hat{\rho}(t) = U |\psi_0\rangle \langle\psi_0| U^\dagger. \tag{4.31}$$

Na seção anterior, definimos a entropia linear associada a um operador $\hat{\rho}$ e aos operadores reduzidos. Podemos fazer a mesma análise na dinâmica temporal, mas agora a entropia também será uma função do tempo, digamos $S(t)$. Estamos interessados, em particular, em estados inicialmente separáveis, mas que tornam-se emaranhados no decorrer do tempo, devido à interação entre as duas partes estudadas. Vejamos como se dá esse comportamento na seção seguinte, para um hamiltoniano específico.

4.3 ENTROPIA LINEAR E A FATORAÇÃO DE INTEIROS

Considere um sistema consistindo de duas partes, A e B, sujeitas ao hamiltoniano $\hat{H} = \hat{H}_A + \hat{H}_B + \hat{H}_{AB}$. Definimos que os autoestados do observável $\hat{H}_A$ constitui uma base $\{|n_A\rangle\}$ com autovalores ϵ_{n_A}. De maneira análoga, consideramos o mesmo para os autoestados de $\hat{H}_B$.

Então, para o espaço de Hilbert total, definimos a base $\{|n_A, n_B\rangle\}$, para a qual o termo de interação $\hat{H}_{AB}$ será assumido como:

$$\hat{H}_{AB} |n_A, n_B\rangle = \lambda \hat{H}_A \otimes \hat{H}_B |n_A, n_B\rangle = \lambda \epsilon_{n_A} \epsilon_{n_B} |n_A, n_B\rangle . \tag{4.32}$$

Aqui, vamos considerar o caso específico em que $\hat{H}_A$ e $\hat{H}_B$ se referem ao hamiltoniano do oscilador harmônico, isto é $\epsilon_{n_i} = \hbar\omega_0(n_i + \frac{1}{2})$, para $i = A, B$.

Conforme descrito na subseção anterior, estamos estudando o caso dinâmico $|\psi(t)\rangle = e^{-\frac{i}{\hbar}\hat{H}t}\,|\psi_0\rangle$, uma vez que $\hat{H}$ é independente do tempo. O nosso objetivo agora é calcular a entropia linear dos estados reduzidos em função do tempo. Para isso, vejamos qual é a forma do estado reduzido associado a $\hat{\rho}(t) \equiv |\psi(t)\rangle\,\langle\psi(t)|$, tomando o traço parcial sobre a segunda variável. Por simplicidade, vamos denotar $|\psi_T\rangle \equiv |\psi(t)\rangle$ e $\hat{\rho}_T \equiv \hat{\rho}(t)$, de modo que:

$$\hat{\rho}_{T_A} = \sum_{n_B} \langle n_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\,. \tag{4.33}$$

Porém, no cálculo da entropia linear, precisamos da pureza de ρ_{T_A}, a qual será denotada por $\gamma(t) \equiv \mathrm{tr}(\hat{\rho}^2_{T_A})$. Assim, obtemos:

$$\begin{aligned}\hat{\rho}^2_{T_A} &= \left[\sum_{n_B} \langle n_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\right]\left[\sum_{m_B} \langle m_B|\psi_T\rangle\,\langle\psi_T|m_B\rangle\right] \\ &= \sum_{n_B,m_B} \langle n_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\,\langle m_B|\psi_T\rangle\,\langle\psi_T|m_B\rangle\,.\end{aligned} \tag{4.34}$$

Resta tomar o traço de $\hat{\rho}^2_{T_A}$, que pode ser calculado como

$$\begin{aligned}\gamma(t) \equiv \mathrm{tr}(\hat{\rho}^2_{T_A}) &= \sum_{n_A} \langle n_A|\,\hat{\rho}^2_{T_A}\,|n_A\rangle \\ &= \sum_{n_A} \langle n_A|\left[\sum_{n_B,m_B} \langle n_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\,\langle m_B|\psi_T\rangle\,\langle\psi_T|m_B\rangle\right]|n_A\rangle \\ &= \sum_{n_A,n_B,m_B} \langle n_An_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\,\hat{I}_A\,\langle m_B|\psi_T\rangle\,\langle\psi_T|n_Am_B\rangle \\ &= \sum_{n_A,n_B,m_B} \langle n_An_B|\psi_T\rangle\,\langle\psi_T|n_B\rangle\left[\sum_{m_A} |m_A\rangle\,\langle m_A|\right]\langle m_B|\psi_T\rangle\,\langle\psi_T|n_Am_B\rangle \\ &= \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_T\rangle\,\langle\psi_T|m_An_B\rangle\,\langle m_Am_B|\psi_T\rangle\,\langle\psi_T|n_Am_B\rangle\,.\end{aligned} \tag{4.35}$$

Agora lembramos que $|\psi_T\rangle = e^{-\frac{i}{\hbar}\hat{H}t}\,|\psi_0\rangle$, para encontrar:

$$\begin{aligned}\langle n_An_B|\psi_T\rangle &= \langle n_An_B|\,e^{-\frac{i}{\hbar}\hat{H}t}\,|\psi_0\rangle \qquad (4.36)\\ &= \sum_{n=0}^{\infty} \frac{1}{n!}\,\langle n_An_B|\left(-\frac{i}{\hbar}\hat{H}t\right)^n|\psi_0\rangle \\ &= \sum_{n=0}^{\infty} \frac{1}{n!}\,\langle n_An_B|\left(-\frac{i\epsilon_{n_An_B}}{\hbar}t\right)^n|\psi_0\rangle \\ &= \langle n_An_B|\exp\left\{-\frac{i\epsilon_{n_An_B}t}{\hbar}\right\}|\psi_0\rangle \qquad (4.37)\\ &= \langle n_An_B|\psi_0\rangle\exp\left\{-\frac{i\epsilon_{n_An_B}t}{\hbar}\right\}, \qquad (4.38)\end{aligned}$$

com $\epsilon_{n_An_B} = \epsilon_{n_A} + \epsilon_{n_B} + \lambda\epsilon_{n_A}\epsilon_{n_B}$. De forma análoga, verificamos que $\langle\psi_T|n_An_B\rangle = \langle\psi_0|n_An_B\rangle \exp\left\{\frac{+i\epsilon_{n_An_B}t}{\hbar}\right\}$.

Dito isso, podemos escrever $\gamma(t)$ da seguinte maneira:

$$\gamma(t) = \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_0\rangle \langle\psi_0|m_An_B\rangle \langle m_Am_B|\psi_0\rangle \langle\psi_0|n_Am_B\rangle \exp\left\{ -\frac{i\lambda t}{\hbar}[\epsilon_{n_A}\epsilon_{n_B} - \epsilon_{m_A}\epsilon_{n_B} + \epsilon_{m_A}\epsilon_{m_B} - \epsilon_{m_B}\epsilon_{n_A}]\right\}. \tag{4.39}$$

Recordando que estamos considerando (para o caso que os dois têm a mesma frequência angular ω_0) $\epsilon_{n_A} = \hbar\omega_0(n_A + \frac{1}{2})$, e o mesmo para ϵ_{nb}, obtemos:

$$\begin{aligned}
\gamma(t) &= \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_0\rangle \langle\psi_0|m_An_B\rangle \langle m_Am_B|\psi_0\rangle \langle\psi_0|n_Am_B\rangle \\
&\exp\left\{ -i\lambda\hbar\omega_0^2 t\left[\left(n_A + \frac{1}{2}\right)(n_B - m_B) + \left(m_A + \frac{1}{2}\right)(m_B - n_B)\right]\right\} \\
&= \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_0\rangle \langle\psi_0|m_An_B\rangle \langle m_Am_B|\psi_0\rangle \langle\psi_0|n_Am_B\rangle \\
&\exp\left\{ -i\lambda\hbar\omega_0^2 t\left[(n_B - m_B)\left(n_A + \frac{1}{2} - m_A - \frac{1}{2}\right)\right]\right\} \\
&= \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_0\rangle \langle\psi_0|m_An_B\rangle \langle m_Am_B|\psi_0\rangle \langle\psi_0|n_Am_B\rangle \\
&\exp\left\{ -i\lambda\hbar\omega_0^2 t[(n_B - m_B)(n_A - m_A)]\right\}.
\end{aligned} \tag{4.40}$$

Por fim, reescrevendo a exponencial acima e nomeando $\omega \equiv \lambda\hbar\omega_0^2$, obtemos a seguinte expressão para a pureza de $\hat{\rho}_{T_A}$:

$$\gamma(t) = \sum_{m_A,n_A,m_B,n_B} \langle n_An_B|\psi_0\rangle \langle\psi_0|m_An_B\rangle \langle m_Am_B|\psi_0\rangle \langle\psi_0|n_Am_B\rangle\, e^{-i\omega t(n_B-m_B)(n_A-m_A)}. \tag{4.41}$$

Esta expressão deve ser inserida na fórmula da entropia linear, fornecendo uma maneira de quantificar dinamicamente o emaranhamento do sistema em questão. Note que, dado o estado inicial, todo o comportamento do emaranhamento em função do tempo está definido. Para realizar a conexão deste problema com a Teoria de Números, em particular com a fatoração de inteiros, precisaremos introduzir os modos de Fourier para esta dinâmica. Para isso, a seguir, tomaremos a transformada de Fourier de (4.41).

4.3.1 Transformada de Fourier

Inicialmente vamos considerar uma função $f_t \equiv e^{-i\overline{\omega}t}$ e tomar sua transformada de Fourier, a qual será denotada por $\tilde{f}_\Omega$.

Para uma função real $g : \mathbb{R} \to \mathbb{R}$, dentro de certas condições de convergência, a sua transformada de Fourier é definida como [16, p. 260–276]:

$$\tilde{g}(\Omega) = \Omega_0 \int_{-\infty}^{+\infty} g(t) e^{i\Omega t} dt, \tag{4.42}$$

onde Ω_0 é uma constante dimensional. Dessa forma, a função $\tilde{f}$ é dada por :

$$\begin{aligned}
\tilde{f}_\Omega &= \Omega_0 \int_{-\infty}^{+\infty} e^{-i\overline{\omega}t} e^{i\Omega t} dt = \Omega_0 \int_{-\infty}^{0} e^{-i\overline{\omega}t} e^{i\Omega t} dt + \Omega_0 \int_{0}^{+\infty} e^{-i\overline{\omega}t} e^{i\Omega t} dt \\
&= \lim_{\epsilon\to 0} \Omega_0 \int_{-\infty}^{0} e^{-i(\overline{\omega}+i\epsilon)t} e^{i\Omega t} dt + \lim_{\epsilon\to 0} \Omega_0 \int_{0}^{+\infty} e^{-i(\overline{\omega}-i\epsilon)t} e^{i\Omega t} dt \\
&= \lim_{\epsilon\to 0} \Omega_0 \int_{-\infty}^{0} e^{-i(\overline{\omega}+i\epsilon-\Omega)t} dt + \lim_{\epsilon\to 0} \Omega_0 \int_{0}^{+\infty} e^{-i(\overline{\omega}-i\epsilon-\Omega)t} dt \\
&= \lim_{\epsilon\to 0} \frac{\Omega_0 e^{-i(\overline{\omega}-\Omega)t} e^{\epsilon t}}{-i(\overline{\omega}+i\epsilon-\Omega)}\bigg|_{-\infty}^{0} + \lim_{\epsilon\to 0} \frac{\Omega_0 e^{-i(\overline{\omega}-\Omega)t} e^{-\epsilon t}}{-i(\overline{\omega}-i\epsilon-\Omega)}\bigg|_{0}^{+\infty} \\
&= \lim_{\epsilon\to 0} \frac{i\Omega_0}{(\overline{\omega}+i\epsilon-\Omega)} - \lim_{\epsilon\to 0} \frac{i\Omega_0}{(\overline{\omega}-i\epsilon-\Omega)},
\end{aligned} \tag{4.43}$$

em que a operação envolvendo o número $\epsilon \to 0$, para $\epsilon > 0$, foi inserida por uma questão de especificação da técnica de integração, que garanta a sua convergência.

Para os próximos passos, usaremos quatro identidades:

i)

$$\frac{1}{\overline{\omega}-\Omega\pm i\epsilon} = \frac{1}{\overline{\omega}-\Omega\pm i\epsilon}\frac{\overline{\omega}-\Omega\mp i\epsilon}{\overline{\omega}-\Omega\mp i\epsilon} = \frac{\overline{\omega}-\Omega}{(\overline{\omega}-\Omega)^2+\epsilon^2} \mp \frac{i\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2}; \tag{4.44}$$

ii)

$$\lim_{\epsilon\to 0} \frac{\overline{\omega}-\Omega}{(\overline{\omega}-\Omega)^2+\epsilon^2} = \begin{cases} \frac{1}{\overline{\omega}-\Omega}, \text{ se } \overline{\omega} \neq \Omega \\ 0, \text{ se } \overline{\omega} = \Omega \end{cases}; \tag{4.45}$$

iii)

$$\lim_{\epsilon\to 0} \frac{\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2} = \begin{cases} 0, \text{ se } \overline{\omega} \neq \Omega \\ \lim_{\epsilon\to 0} \frac{1}{\epsilon}, \text{ se } \overline{\omega} = \Omega \end{cases}; \tag{4.46}$$

iv)

$$\begin{aligned}
\lim_{\epsilon\to 0} \int_{-\infty}^{+\infty} \frac{\epsilon d\Omega}{(\overline{\omega}-\Omega)^2+\epsilon^2} &= \lim_{\epsilon\to 0} \int_{-\infty}^{+\infty} \frac{\epsilon^2 dy}{(\epsilon y)^2+\epsilon^2} = \lim_{\epsilon\to 0} \int_{-\infty}^{+\infty} \frac{dy}{y^2+1} \\
&= 2\lim_{\epsilon\to 0} \int_{0}^{+\infty} \frac{dy}{y^2+1} = 2\int_{0}^{\pi/2} d\theta = \pi,
\end{aligned} \tag{4.47}$$

em que consideramos as mudanças de variáveis: $y = \frac{\Omega-\overline{\omega}}{\epsilon}$ e $y = \tan\theta$.

Usando a identidade i) obtemos:

$$\begin{aligned}\tilde{f}_\Omega &= \lim_{\epsilon\to 0}\left[\frac{i\Omega_0}{(\overline{\omega}+i\epsilon-\Omega)}-\frac{i\Omega_0}{(\overline{\omega}-i\epsilon-\Omega)}\right]\\ &= \lim_{\epsilon\to 0} i\Omega_0\left[\frac{\overline{\omega}-\Omega}{(\overline{\omega}-\Omega)^2+\epsilon^2}-\frac{i\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2}-\frac{\overline{\omega}-\Omega}{(\overline{\omega}-\Omega)^2+\epsilon^2}-\frac{i\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2}\right]\\ &= \lim_{\epsilon\to 0}\frac{2\Omega_0\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2}. \end{aligned} \tag{4.48}$$

Usando a notação δ para a distribuição *delta de Dirac*, podemos escrever a última igualdade da seguinte maneira, devido a igualdade iii):

$$\tilde{f}_\Omega = \lim_{\epsilon\to 0} 2\Omega_0\left(\frac{\epsilon}{(\overline{\omega}-\Omega)^2+\epsilon^2}\right) \propto \delta(\overline{\omega}-\Omega) = \alpha\delta(\overline{\omega}-\Omega). \tag{4.49}$$

Pela definição da delta de Dirac [16, p. 221-231], sabemos que:

$$\int_{-\infty}^{\infty}\delta(\overline{\omega}-\Omega)d\Omega = 1, \tag{4.50}$$

Segue que, através da identidade iv):

$$2\Omega_0\pi = \alpha\int_{-\infty}^{\infty}\delta(\overline{\omega}-\Omega)d\Omega = \alpha. \tag{4.51}$$

Portanto, a transformada de Fourier $\tilde{f}_\Omega$ assume a forma:

$$\tilde{f}_\Omega = 2\pi\Omega_0\delta(\overline{\omega}-\Omega). \tag{4.52}$$

4.3.2 Modos de Fourier e a fatoração de inteiros

Agora, aplicaremos a transformada de Fourier da entropia linear de $\hat{\rho}_{T_A}$, dada por $S_{\text{lin}}(t) = 1-\gamma(t)$. Note que, pela equação (4.52) fazendo $\overline{\omega}=1$, segue que a transformada de Fourier da função constante igual a 1 é $2\pi\Omega_0\delta(-\Omega)$. Por [16, p. 221-231], tem-se que $\delta(-\Omega)=\delta(\Omega)$. Sendo assim:

$$\tilde{S}_{\text{lin}}(\Omega) = \Omega_0\int_{-\infty}^{+\infty} S_{\text{lin}}(t)e^{i\Omega t}dt = \Omega_0\int_{-\infty}^{+\infty}(1-\gamma(t))e^{i\Omega t}dt. \tag{4.53}$$

Utilizando a pureza do estado $\hat{\rho}_{T_A}$ em (4.41) e a transformada de Fourier obtida em (4.52), segue que:

$$\begin{aligned}\tilde{S}_{\text{lin}}(\Omega) = 2\pi\Omega_0\Big\{&\delta(\Omega)-\\ &\sum_{m_A,\ldots,n_B}\langle n_An_B|\psi_0\rangle\langle\psi_0|m_An_B\rangle\langle m_Am_B|\psi_0\rangle\langle\psi_0|n_Am_B\rangle\,\delta[\omega(n_B-m_B)(n_A-m_A)-\Omega]\Big\}.\end{aligned} \tag{4.54}$$

Para simplificar, assumiremos uma escala de tempo tal que $\omega = 1$, de forma que a transformada de Fourier acima pode ser escrita como:

$$\tilde{S}_{\text{lin}}(\Omega) = 2\pi\Omega_0\Big\{\delta(\Omega) - \sum_{m_A,n_A,m_B,n_B} \langle n_A n_B|\psi_0\rangle \langle\psi_0|m_A n_B\rangle \langle m_A m_B|\psi_0\rangle \langle\psi_0|n_A m_B\rangle \delta[(n_B - m_B)(n_A - m_A) - \Omega]\Big\}. \tag{4.55}$$

Para continuar a análise do problema, suponha que o estado inicial $|\psi_0\rangle$ é da forma $|\psi_0\rangle = |n_{A_0} n_{B_0}\rangle$. Sendo assim, a expressão do somatório acima assume a forma:

$$\begin{aligned}&\langle n_A n_B|n_{A_0} n_{B_0}\rangle \langle n_{A_0} n_{B_0}|m_A n_B\rangle \langle m_A m_B|n_{A_0} n_{B_0}\rangle \langle n_{A_0} n_{B_0}|n_A m_B\rangle = \\ &\overline{\delta}(n_A - n_{A_0})\overline{\delta}(n_B - n_{B_0})\overline{\delta}(n_{A_0} - m_A)\overline{\delta}(n_{B_0} - m_B),\end{aligned} \tag{4.56}$$

onde a notação $\overline{\delta}$ foi utilizada para a função delta de Kronecker. Desta forma, segue que a expressão acima só é diferente de zero se $n_A = m_A$ e $n_B = m_B$, o que implica que:

$$\tilde{S}_{\text{lin}}(\Omega) = 2\pi\Omega_0\delta(\Omega)(\delta(\Omega) - \delta(\Omega)) = 0. \tag{4.57}$$

Esta expressão é entendida quando verificamos que este estado inicial é separável, e que sua a entropia linear é independente do tempo, de acordo com a equação (4.41). Como este resultado não nos interessa, pelo excesso de simplicidade, vamos passar a a considerar que o estado inicial $|\psi_0\rangle$ é o *estado coerente*, o qual é escrito como:

$$|\psi_0\rangle \equiv |z_{A_0} z_{B_0}\rangle = e^{-\frac{1}{2}|z_{A_0}|^2 - \frac{1}{2}|z_{B_0}|^2} \sum_{n_{A_0}=0, n_{B_0}=0}^{\infty} \frac{z_{A_0}^{n_{A_0}}}{\sqrt{n_{A_0}!}} \frac{z_{B_0}^{n_{B_0}}}{\sqrt{n_{B_0}!}} |n_{A_0} n_{B_0}\rangle, \tag{4.58}$$

em que z_{A_0} e z_{B_0} são parâmetros complexos. Estados como estes estão presentes em uma vasta literatura especializada (veja [17], por exemplo). Dentre os seus usos mais marcantes, ressaltamos suas aplicações ao estudo do limite semiclássico da Mecânica Quântica. De fato, sua indicação para este tipo de problema é justificada pois trata-se dos estados quânticos mais próximos da descrição quântica. Eles possuem a menor incerteza possível no espaço de fases, segundo o Princípio de Incerteza de Heisenberg, e, quando sujeitos a um hamiltoniano apropriado, desenvolvem uma dinâmica que segue, com boa precisão, a trajetória do problema clássico análogo. Infelizmente, no entanto, por falta de tempo, não conseguiremos discuti-los neste trabalho mais detalhadamente. Note que o estado inicial $|\psi_0\rangle$ em (4.58) satisfaz a

seguinte relação:

$$\begin{aligned}
&\langle n_A n_B|\psi_0\rangle \langle\psi_0|m_A n_B\rangle \langle m_A m_B|\psi_0\rangle \langle\psi_0|n_A m_B\rangle \\
&= e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \frac{z_{A_0}^{n_A}}{\sqrt{n_A!}} \frac{z_{B_0}^{n_B}}{\sqrt{n_B!}} \frac{z_{A_0}^{*m_A}}{\sqrt{m_A!}} \frac{z_{B_0}^{*n_B}}{\sqrt{n_B!}} \frac{z_{A_0}^{m_A}}{\sqrt{m_A!}} \frac{z_{B_0}^{m_B}}{\sqrt{m_B!}} \frac{z_{A_0}^{*n_A}}{\sqrt{n_A!}} \frac{z_{B_0}^{*m_B}}{\sqrt{m_B!}} \\
&= e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \frac{|z_{A_0}|^{2n_A}}{n_A!} \frac{|z_{B_0}|^{2n_B}}{n_B!} \frac{|z_{A_0}|^{2m_A}}{m_A!} \frac{|z_{B_0}|^{2m_B}}{m_B!} \\
&= e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \frac{|z_{A_0}|^{2(n_A+m_A)}}{n_A!m_A!} \frac{|z_{B_0}|^{2(n_B+m_B)}}{n_B!m_B!}.
\end{aligned} \tag{4.59}$$

Assim, $\tilde{S}_{\text{lin}}(\Omega)$ para tal cenário pode ser escrita como:

$$\begin{aligned}
\tilde{S}_{\text{lin}}(\Omega) = 2\pi\Omega_0 \Big\{ &\delta(\Omega) \\
&- e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \sum_{m_A,n_A,m_B,n_B} \frac{|z_{A_0}|^{2(n_A+m_A)}}{n_A!m_A!} \frac{|z_{B_0}|^{2(n_B+m_B)}}{n_B!m_B!} \delta[(n_B-m_B)(n_A-m_A)-\Omega] \Big\}.
\end{aligned} \tag{4.60}$$

Neste ponto, devemos notar, através de uma simples inspeção nesta equação, que $\tilde{S}_{\text{lin}}(\Omega)$ pode assumir valores não nulos somente quando a sua variável Ω for um número inteiro. Pensando na transformada inversa de Fourier, em que a função original $S_{\text{lin}}(t)$ é escrita como uma integral sobre $\tilde{S}_{\text{lin}}(\Omega)$, verificamos que apenas os modos de oscilação para frequências Ω inteiras devem ser considerados. Mostraremos agora que o cálculo da amplitude destes modos (ou termos) de Fourier envolve estratégias extraídas dos estudos sobre a fatoração de números inteiros.

Para uma primeira ilustração, considere, em particular, o cálculo de $\tilde{S}_{\text{lin}}$ para valores $\Omega = P_1 \times P_2 > 0$ em que $P_1 < P_2$ são primos distintos. Sendo assim, temos que $\delta(\Omega) = 0$ e $\delta((n_B - m_B)(n_A - m_A) - \Omega) \neq 0$ se $(n_B - m_B)(n_A - m_A) = P_1 \times P_2$, donde consideramos $n_B = P_1 + m_B$ e $n_A = P_2 + m_A$. Então a expressão anterior torna-se:

$$-2\pi\Omega_0 e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \sum_{m_A,m_B} \frac{|z_{A_0}|^{2(P_2+2m_A)}}{(P_2+m_A)!m_A!} \frac{|z_{B_0}|^{2(P_1+2m_B)}}{(P_1+m_B)!m_B!}. \tag{4.61}$$

Em (4.60), também poderíamos ter assumido que $n_B = P_2 + m_B$ e $n_A = P_1 + m_A$, o que resulta em:

$$-2\pi\Omega_0 e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \sum_{m_A,m_B} \frac{|z_{A_0}|^{2(P_1+2m_A)}}{(P_1+m_A)!m_A!} \frac{|z_{B_0}|^{2(P_2+2m_B)}}{(P_2+m_B)!m_B!}. \tag{4.62}$$

A partir das expressões (4.61) e (4.62), segue que $\tilde{S}_{\text{lin}}(\Omega = P_1 \times P_2)$ está bem definido:

$$\begin{aligned}
\tilde{S}_{lin}(\Omega) = &-2\pi\Omega_0 e^{-2|z_{A_0}|^2-2|z_{B_0}|^2} \\
&\sum_{m_A,m_B} \left[\frac{|z_{A_0}|^{2(P_2+2m_A)}}{(P_2+m_A)!m_A!} \frac{|z_{B_0}|^{2(P_1+2m_B)}}{(P_1+m_B)!m_B!} + \frac{|z_{A_0}|^{2(P_1+2m_A)}}{(P_1+m_A)!m_A!} \frac{|z_{B_0}|^{2(P_2+2m_B)}}{(P_2+m_B)!m_B!} \right].
\end{aligned} \tag{4.63}$$

No caso geral, um número inteiro Ω pode ser fatorado como $\Omega = P_1^{\alpha_1} \times P_2^{\alpha_2} \times \cdots \times P_n^{\alpha_n}$, onde cada α_i é um número natural e $\{P_i\}$ é um conjunto finito de primos distintos. Nesse caso, é um simples problema de combinatória rearranjar os fatores de Ω de modo a escrevê-lo como produto de dois números inteiros e o valor de $\tilde{S}_{\text{lin}}(\Omega)$ assume uma forma semelhante à apresentada em (4.63). Por exemplo, para $\Omega = 16 = 2^4$, temos as seguintes combinações:

$$\begin{aligned} \Omega &= 2^4 \cdot 1 \\ &= 2^3 \cdot 2^1 \\ &= 2^2 \cdot 2^2. \end{aligned} \tag{4.64}$$

Nesse caso, o tratamento para $\tilde{S}_{\text{lin}}(\Omega)$ é similar, mas não idêntico, ao cálculo realizado acima para $\Omega = P_1 \times P_2$.

$\tilde{S}_{\text{lin}}(\Omega)$ depende de quantas maneiras o número inteiro Ω pode ser fatorado no produto de outros dois números inteiros, a partir da fatoração em números primos. O questionamento que surge aqui é: será que este resultado, que poderia ser, inclusive, obtido experimentalmente ajustando apropriadamente os parâmetros envolvidos, poderia trazer novos elementos para o tema? Apesar de ser apenas uma especulação, nosso trabalho aponta para uma aplicação da fatoração de números inteiros na caracterização dos modos de Fourier da entropia linear de um sistema específico.

A reposta para a pergunta feita anteriormente não é dada nesse trabalho, mas discorremos sobre o assunto no próximo capítulo, onde também discutimos trabalhos similares, em que quantidades quânticas conectam-se, não com a fatoração, mas com a partição de inteiros.

5 PARTIÇÃO E FATORAÇÃO DE INTEIROS APLICADOS À MECÂNICA QUÂNTICA

Neste capítulo, veremos qual é a relação entre partição de números inteiros e a densidade de estados para um caso específico de gás de bósons. Então comentaremos sobre as possíveis conexões entre a Mecânica Quântica e a fatoração de inteiros, tema deste trabalho.

5.1 PARTIÇÃO DE INTEIROS NA MECÂNICA QUÂNTICA

A *partição* de um número inteiro n é uma representação de n através de somas de números inteiros. Por exemplo, o número 4 pode ser representado por 5 partições:

$$\begin{aligned} 4 &= 4 && \text{(partição 1)} \\ 4 &= 3+1 && \text{(partição 2)} \\ 4 &= 2+2 && \text{(partição 3)} \\ 4 &= 2+1+1 && \text{(partição 4)} \\ 4 &= 1+1+1+1 && \text{(partição 5).} \end{aligned} \tag{5.1}$$

Dizemos que a partição de 4, denotada por $p(4)$, é 5. Para $n = 1, \cdots, 9$, veja o gráfico da função $p(n)$ na Figura 1. Ressaltamos que o comportamento do gráfico para valores maiores de n não é tão simples como visto na figura. Por exemplo, $p(100) = 190.569.292$ e $p(1000) = 24.061.467.864.032.622.473.692.149.727.991$.

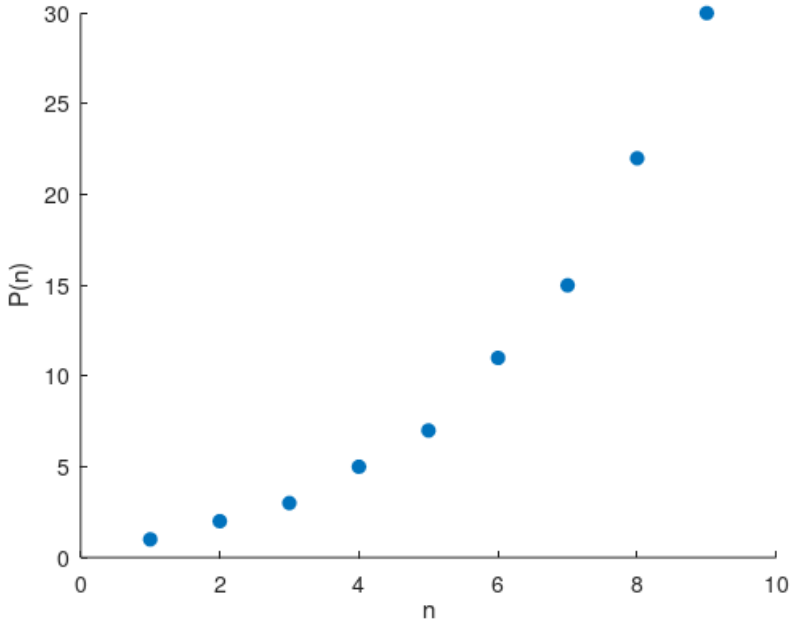
Em 1918, foi demonstrada uma fórmula assintótica para a quantidade de partições de um número inteiro arbitrariamente grande [18]. A saber:

$$p(n) \approx \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right), \quad \text{para } n \to \infty. \tag{5.2}$$

Esse resultado volta a aparecer na Mecânica Quântica numa via totalmente distinta da original. Ele surge, por exemplo, na descrição da densidade de energia de um gás de bósons [19] e de um gás de férmions [20]. Aqui, vamos abordar um caso simplificado para ilustrar a relação entre os dois trabalhos.

Considere um gás rarefeito de N bósons, para o qual podemos ignorar a interação entre partículas. O macroestado e o microestados do sistema são determinados, essencialmente, pela energia total e pelas configurações de energias individuais de cada partícula que constitui o gás, respectivamente. A quantidade possível de microestados de um sistema, para um dado macroestado, é dita *densidade de estado*. Sabemos que para o caso quântico, a energia é quantizada. Perceba a analogia da densidade

FIGURA 1 – Gráfico da função partição para $n = 1, \cdots, 9$.



Fonte: O autor (2021).

de níveis com o problema da partição de inteiros: O número de microestado para uma energia macroscópica E é o número de possibilidades de distribuir as partículas em cada nível individual, restringindo a soma destas energias a E. Consideremos uma escala de energia para qual a energia do estado fundamental é 0, os demais níveis são $1, 2, 3, \ldots$ e que a energia total do sistema seja de 4. Como descrito anteriormente, podemos particionar o número 4 de 5 maneiras distintas e, considerando que o gás seja constituído de pelo menos 5 partículas, as 4 maneiras são possíveis. Por exemplo, uma partícula do gás poderia estar no nível de energia 4 e as restantes no nível 0; 2 partículas poderiam estar no nível de energia 2 e as outras no nível 0; poderia haver 4 partículas no nível de energia 1 e as demais no nível zero; e assim sucessivamente. Aqui, ressalta-se a importância de estarmos analisando um gás de bósons, pois, se o gás fosse de férmions, haveria restrições para a distribuição em níveis de energia individuais, pelo *Princípio de exclusão de Pauli*, e a conexão estudada não seria tão direta. Além disso, considera-se o princípio da indistinguibilidade, para que a escolha de qual partícula em um determinado nível de energia seja irrelevante [21].

Para fechar nosso argumento sobre a equação (5.2), considere agora que a energia total do sistema seja um inteiro E, onde E é um número arbitrariamente grande e que a quantidade de partículas no gás também seja grande o suficiente, desde que possamos desprezar as interações entre elas. Como dito anteriormente, há uma expressão assintótica para a partição de inteiros grandes (5.2), de modo que, a partir dela, podemos saber qual é o número de microestados do sistema. Note que isso está

relacionado com o conceito de entropia. Por outro lado, as condições consideradas são apropriadas para a aplicação de aproximações semiclássicas ao problema quântico. De fato, abordagens semiclássicas para a densidade de estados de um sistema de muitos bósons não interagentes, distribuídos em níveis de energia equidistantes, existem e produzem resultados concordantes com a Teoria de Números. Em alguns casos, inclusive, resultados quânticos aproximados em problemas similares, mas distintos, deste que discutimos, também encontram suporte nesta área de conhecimento da matemática pura [22, 23]. Além disso, note que a aplicação da expressão assintótica para a partição na mecânica quântica ocorre para sistemas com altas energias, ou seja, no regime de validade do limite semiclássico.

5.2 DA MECÂNICA QUÂNTICA À FATORAÇÃO DE INTEIROS

De maneira similar à partição, o número 16 pode ser fatorado, como produto de dois números inteiros, da seguinte maneira:

$$\begin{aligned} 16 &= 2^4 \\ &= 2^4 \cdot 1 \\ &= 2^3 \cdot 2^1 \\ &= 2^2 \cdot 2^2. \end{aligned} \tag{5.3}$$

Sendo f a função que toma um número inteiro positivo e retorna a quantidade de maneiras que podemos fatorá-lo no produto de dois números inteiros, temos que $f(16) = 3$. Assim como as partições de um número N por $N = a + b$ e $N = b + a$ são as mesmas, aqui também consideramos que as fatorações de $N = c \cdot d$ e $N = d \cdot c$ são as mesmas. Dessa forma $f(p) = 1$ sempre que p é um número primo e, como há infinitos números primos, é impossível encontrar uma fórmula assintótica para $f(n)$ quando $n \to \infty$, assim como disposto em (5.2). Portanto, ainda não estabelecemos uma relação entre a fatoração de inteiros e emaranhamento com a mesma nitidez que existe entre a partição de inteiros e a densidade de estados, como discutimos na seção anterior. No entanto, especulamos que tal ligação possa existir, trazendo vantagens para qualquer um dos lados.

Com o exemplo simples visto na seção anterior, já é possível verificar que o estudo da partição de inteiros está relacionado com a densidade de estado de sistemas quânticos. Apesar de existir uma expressão assintótica para a partição de números inteiros, não há uma resposta para o problema de fatoração de inteiros [24]. Um problema relativamente conhecido da fatoração de inteiros diz sobre a eficiência de algoritmos desenvolvidos para realizar tal tarefa. Em particular, dado um inteiro N, não se conhece um “algoritmo de tempo polinomial” para calcular a fatoração. A saber, um algoritmo de tempo polinomial T é tal que seu tempo de execução é limitado

por uma expressão polinomial da variável do input, ou seja, sendo N o input, segue que $T(N) = \mathscr{O}(N^k)$, onde $\mathscr{O}$ é a ordem de grandeza do polinômio. Para os algoritmos conhecidos, este tempo é significativamente maior, crescendo exponencialmente com o tempo. Esta limitação operacional está envolvida com, por exemplo, técnicas de criptografia, que, por isso, permanecem em contínua discussão. Seria possível que um sistema quântico como o estudado no capítulo anterior venha a ser útil nesta discussão?

Assim como a Mecânica Quântica mostrou uma aplicação da Teoria de Números ao fornecer a expressão assintótica mencionada anteriormente, encontramos nesse trabalho uma aplicação da Mecânica Quântica que se relaciona com a fatoração de números inteiros, mesmo que de maneira ainda fraca. Se essa relação pode ser utilizada para resolver ou trazer uma aplicação ao problema de fatoração de inteiros, não há como concluir a partir deste trabalho, mas espera-se que os tópicos levantados apontem para um caminho que possa contribuir para esse fim.

6 CONSIDERAÇÕES FINAIS

Uma hipótese que contradiz uma determinada teoria pode ter duas consequências: ou a hipótese é falha, ou a teoria é falsa ou incompleta. A abordagem apresentada por Bell para a discussão levantada por EPR mostrou que até então não se tinham conhecimentos necessários para que a hipótese levantada pelos autores fosse falseada. Porém, a discussão levou a uma série de indagações pela comunidade científica que culminaram no desenvolvimento do estudo do emaranhamento, uma importante área da Física que é fundamental, entre outras aplicações, na Computação Quântica.

Através de uma bela formulação matemática, partindo da definição de vetores em um espaço de Hilbert, podemos dizer que o estudo do emaranhamento em sistemas quânticos puros ajuda a entender a noção de entropia, em particular, a entropia linear. Para isso, define-se uma operação que modifica um operador e reduz sua dimensão, semelhante ao traço, mas não tão amplamente conhecida: o traço parcial. Com essa operação são obtidos os chamados operadores densidade reduzidos. A entropia linear desse operador é interpretada como uma medida de emaranhamento. Ainda que neste trabalho tenham sido abordados sistemas quânticos simples, como os puros e bipartidos, o bom entendimento destes é de considerável importância para a compreensão de sistemas quânticos mais complexos.

Assim como é possível aplicar a teoria da partição de números inteiros na Mecânica Quântica, ao estudar a densidade de estados de um gás de bósons ou férmions, espera-se que esse trabalho contribua analogamente à fatoração de números inteiros, em especial a problemas da área que ainda não foram solucionados. Ao que tange as aplicações já existentes na literatura apresentadas nesse trabalho, é fundamental considerar o limite semiclássico. Da mesma maneira, o exemplo apresentado nesse trabalho pode ser um caminho para a aplicação da fatoração de inteiros na Mecânica Quântica. A exemplo do debate EPR, o que pode ser necessário para o próximo passo do avanço da Ciência não é uma resposta nova para um problema, mas sim uma pergunta sobre aquilo que se conhece.

Ressaltamos aqui que esse trabalho foi realizado durante a pandemia da COVID-19, a qual trouxe alterações para o calendário da universidade. Uma das consequências dessas alterações foi o tempo reduzido de cada período acadêmico, menor que cada semestre letivo até o ano de 2019. Isso fez com que o tempo total disponível para a realização das disciplinas *TCC A* e *TCC B* se reduzisse de aproximadamente 9 meses para 5 meses. Consequentemente, o aprofundamento de alguns tópicos relevantes para o desenvolvimento desse trabalho não pôde ser realizado.

REFERÊNCIAS

[1] EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? **Physical Review**, APS, v. 47, n. 10, p. 777, 1935. Citado 1 vez na página 10.

[2] BILOBRAN, A. L. O. **Uma Medida da Realidade Física**. Dissetação (Mestrado em Física) - Setor de Ciências Exatas, Universidade Federal do Paraná, Curitiba, 2015. Citado 1 vez na página 10.

[3] BELL, J. S. On the einstein podolsky rosen paradox. **Physics**, APS, v. 1, n. 3, p. 195, 1964. Citado 1 vez na página 10.

[4] SILVEIRA, L. S. **Modelo de variáveis ocultas para descrição de emaranhamento e não localidade de Bell no contexto de estados puros**. Dissetação (Mestrado em Física) - Setor de Ciências Exatas, Universidade Federal do Paraná, Curitiba, 2017. Citado 2 vez na página 10.

[5] ASPECT, A.; GRANGIER, P.; ROGER, G. Experimental tests of realistic local theories via Bell's theorem. **Physical Review Letters**, APS, v. 47, n. 7, p. 460, 1981. Citado 1 vez na página 10.

[6] SHALM, L. K. et al. Strong loophole-free test of local realism. **Physical Review Letters**, APS, v. 115, n. 25, p. 250402, 2015. Citado 1 vez na página 10.

[7] GISIN, N. Bell's inequality holds for all non-product states. **Physics Letters A**, Elsevier, v. 154, n. 5-6, p. 201–202, 1991. Citado 1 vez na página 10.

[8] YU, S.; CHEN, Q.; ZHANG, C.; LAI, C. H.; OH, C. H. All entangled pure states violate a single Bell's inequality. **Physical Review Letters**, APS, v. 109, n. 12, p. 120402, 2012. Citado 1 vez na página 10.

[9] PADE, J. **Quantum Mechanics for Pedestrians 2 Applications and Extensions Second Edition**. New York: Springer, 2018. Citado 4 vezes nas páginas 11, 13, 14, 16.

[10] NIELSEN, M. A.; CHUANG, I. **Quantum computation and quantum information**. New York: American Association of Physics Teachers, 2002. Citado 4 vezes nas páginas 11, 20, 28.

[11] ERDÖS, P.; LEHNER, J. et al. The distribution of the number of summands in the partitions of a positive integer. **Duke Mathematical Journal**, Duke University Press, v. 8, n. 2, p. 335–345, 1941. Citado 1 vez na página 12.

[12] OVERMARS, A.; VENKATRAMAN, S. New Semi-Prime Factorization and Application in Large RSA Key Attacks. **Journal of Cybersecurity and Privacy**, Multidisciplinary Digital Publishing Institute, v. 1, n. 4, p. 660–674, 2021. Citado 1 vez na página 12.

[13] WEHRL, A. General properties of entropy. **Reviews of Modern Physics**, APS, v. 50, n. 2, p. 221, 1978. Citado 1 vez na página 20.

[14] HIGHAM, N. J. **Functions of matrices: theory and computation**. [S.l.]: SIAM, 2008. Citado 1 vez na página 22.

[15] MIT. **28. Similar Matrices and Jordan Form**. Youtube. 2018. Disponível em: youtube.com/watch?v=TSdXJw83kyA. Acesso em: 17 dez. 2021. Citado 1 vez na página 22.

[16] BUTKOV, N. **Mathematical Physics**. New York: Addison-Wesley Publishing Company, 1973. Citado 3 vezes nas páginas 34, 35.

[17] GAZEAU, J.-P. **Coherent States in Quantum Physics**. Berlin: WILEY-VCH, 2009. Citado 1 vez na página 36.

[18] HARDY, G. H.; RAMANUJAN, S. Asymptotic formulaæ in combinatory analysis. **Proceedings of the London Mathematical Society**, Wiley Online Library, v. 2, n. 1, p. 75–115, 1918. Citado 1 vez na página 39.

[19] GROSSMANN, S.; HOLTHAUS, M. Microcanonical fluctuations of a Bose system's ground state occupation number. **Physical Review E**, APS, v. 54, n. 4, p. 3495, 1996. Citado 1 vez na página 39.

[20] LEBOEUF, P.; MONASTRA, A.; RELANO, A. Fluctuations in the level density of a Fermi gas. **Physical Review Letters**, APS, v. 94, n. 10, p. 102502, 2005. Citado 1 vez na página 39.

[21] MASSIMI, M. **Pauli's exclusion principle: The origin and validation of a scientific principle**. [S.l.]: Cambridge University Press, 2005. Citado 1 vez na página 40.

[22] TRAN, M. N.; MURTHY, M.; BHADURI, R. K. On the quantum density of states and partitioning an integer. **Annals of Physics**, Elsevier, v. 311, n. 1, p. 204–219, 2004. Citado 1 vez na página 41.

[23] RIBEIRO, A. D. Level density of a Bose gas: Beyond the saddle point approximation. **Journal of Mathematical Physics**, AIP Publishing LLC, v. 56, n. 4, p. 042104, 2015. Citado 1 vez na página 41.

[24] ARORA, S.; BARAK, B. **Computational complexity: a modern approach**. [S.l.]: Cambridge University Press, p. 438, 2009. Citado 1 vez na página 41.