Rodrigo Lopes

QUANTIFICADOR DE INDISTINGUIBILIDADE PARA UM ENSEMBLE DE ESTADOS QUÂNTICOS

Dissertação submetida ao Programa de Pós-Graduação em Física da Universidade Federal de Santa Catarina para a obtenção do Grau de mestre em Física.
Orientador: Prof. Dr Eduardo Inacio Duzzioni.

Florianópolis
2015

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Lopes, Rodrigo Lopes
Quantificador de Indistinguibilidade Para um Ensemble de Estados Quânticos / Rodrigo Lopes Lopes ; orientador, Eduardo Inacio Duzzioni Duzzioni - Florianópolis, SC, 2015.
68 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas. Programa de Pós-Graduação em Física.

Inclui referências

1. Física. 2. Indistinguibilidade de estados quânticos. 3. Informação Quântica. 4. Mecânica Quântica. 5. Física Teórica. I. Duzzioni, Eduardo Inacio Duzzioni. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Física. III. Título.

QUANTIFICADOR DE INDISTINGUIBILIDADE PARA UM ENSEMBLE DE ESTADOS QUÂNTICOS

Rodrigo Lopes

Esta Dissertação foi julgada adequada para a obtenção do título de **MESTRE EM FÍSICA**, na área de concentração de **Física Atômica e Molecular** e aprovada em sua forma final pelo Programa de Pós-Graduação em Física.

Prof. Dr. Eduardo Inacio Duzzioni
(UFSC - orientador)

Prof. Dr. Ivan Helmuth Bechtold
(FSC/UFSC - Coordenador do Programa)

Prof. Dr. Eduardo Inacio Duzzioni
(UFSC - presidente)

Prof. Dr. Renato Moreira Angelo
(membro externo) - UFPR/FSC

Profª. Drª. Paula Borges Monteiro
(membro externo) - IFSC/Florianópolis

Prof. Dr. Gerson Gregorio Gomes
(membro externo) - IFSC/Florianópolis

Prof. Dr. Eduardo Cerutti Mattei
(membro suplente) - UFSC/FSC

AGRADECIMENTOS

A minha esposa Sylvia, filhos, Artur e Ana Paula, e pais, Domingos e Vicentina, por todo apoio, motivação, torcida e paciência.

Ao meu orientador, Prof. Eduardo Inacio Duzzioni, pela orientação e confiança.

Aos professores de Física do IFSC, por seu incentivo e amizade.

Aos professores com os quais cursei disciplinas, pela competência e entusiasmo.

Ao servidor Antonio Marcos Machado, pela atenção e incentivo.

Aos colegas do curso de pós-graduação, sem os quais não seria possível acompanhar as disciplinas cursadas.

Ao Instituto Federal de Santa Catarina, por oportunizar a minha volta a pesquisa.

Por fim, a todas as pessoas que de alguma forma torceram e torcem pelo meu sucesso.

RESUMO

Os estados $|\phi\rangle$ e $|\theta\rangle$ são distintos na mecânica quântica, entretanto, se $\langle\phi|\theta\rangle \neq 0$, é impossível definir medidores que consigam distinguir entre estes dois estados de forma conclusiva e sem erro. Quão distinguíveis são dois ou mais estados quânticos e como discriminá-los da melhor forma possível, são perguntas importantes que precisam ser respondidas no contexto da Teoria da Informação Quântica. A distinguibilidade de um ensemble de estados quânticos está relacionada com a quantidade de informação que ele pode transmitir. Um ensemble possui estados quânticos puros distinguíveis apenas se todos os seus elementos são ortogonais dois a dois e, neste caso, a quantidade de informação transmitida é igual a de um conjunto de mensagens clássicas distintas. Neste trabalho, propomos um quantificador de indistinguibilidade associado com o quanto falta de informação para que um ensemble de estados quânticos se comporte como um conjunto de mensagens clássicas distintas, ou seja, o quanto falta de informação para que os elementos do ensemble sejam distinguíveis. Esta ideia é generalizada para um ensemble de estados quânticos mistos.

Palavras chaves: Indistinguibilidade, distinguibilidade, quantidade de informação, informação quântica.

ABSTRACT

$|\phi\rangle$ and $|\theta\rangle$ are distinct states in quantum mechanics, however, if $\langle\phi|\theta\rangle \neq 0$, it is impossible to have meters in a laboratory that can distinguish between these two states conclusively and without error. How distinguishable are two or more quantum states and how to discriminate among them in the best way are important questions to be answered in the field of Quantum Information. The distinguishability of an ensemble of quantum states is related to the amount of information that it can transmit. One ensemble has distinguishable pure quantum states only if all elements are orthogonal two by two, so that, the amount of transmitted information is equal to a set of classical information. In this work, we propose a quantifier of indistinguishability associated to the amount of information that is missing for an ensemble of quantum states behaves as a set of classical information, i.e., how much information is missing for the ensemble of elements to be distinguishable. This idea is generalized for an ensemble of mixed states.
Keywords: Indistinguishability, distinguishability, amount of information, quantum information.

Lista de Figuras

Nomenclatura

MQ	Mecânica quântica
I	Quantidade de informação
$H(p_i)$	Entropia de Shannon
$S(\rho)$	Entropia de von Neumann
$Ind(\rho)$	Quantificador de indistinguibilidade
$Ind_M(\rho)$	Quantificador de indistinguibilidade para estados mistos
ρ	Operador densidade ou matriz densidade
Em	Erro mínimo de Helstrom
SMO	*String* médio ótimo
SMO_{CC}	*String* médio ótimo que permite distinguir perfeitamente conjuntos de informações clássicas
SMO_{QM}	*String* médio ótimo que permite distinguir perfeitamente estados quânticos mistos

Conteúdo

Capítulo 1

Introdução

A rapidez do processamento e a transmissão de informações estão "emaranhados" com a sociedade moderna, onde o colapso de uma implica no colapso da outra. A popularização do computador pessoal, o desenvolvimento da internet e o aumento da capacidade de processamento dos grandes computadores, são alguns dos responsáveis por esta dependência do mundo moderno.

Atualmente conhecemos melhor o universo que vivemos através de simulações realizadas em super computadores. Entretanto, à medida que aprofundamos o nosso conhecimento sobre a natureza, novos problemas surgem, normalmente exigindo simulações mais complexas para serem resolvidos, levando à busca de algorítmos mais eficientes e computadores mais velozes. Porém, qual o limite dos computadores tradicionais ou clássicos e, se possível, como superar este limite?

Na década de 1980, dois fatos aumentaram o *status* da computação quântica como candidata a superar os limites da computação clássica. Em 1981, Richard Feynman, na primeira Conferência de Computação Física do MIT, propôs a utilização de fenômenos quânticos em uma rotina computacional para simular experimentos em física quântica [1]. Quatro anos depois, David Deutsch [2], descreve o primeiro computador quântico universal. Entretanto, só na década seguinte, com a criação de algorítmos quânticos [3, 4] demonstrando que a computação quântica resolve determinados problemas de forma mais eficiente do que a computação clássica, intensificaram-se os estudos nessa área de conhecimento.

O desenvolvimento da computação quântica está relacionado com a criação de uma nova área de conhecimento, a Teoria da Informação

Quântica, que surge para resolver o problema da quantificação e processamento de informação quântica.

Apenas na década de 1940 a informação classica é tratada com rigor matemático [1]. Claude Shannon, em 1937 na sua dissertação de mestrado[1], desenvolveu a teoria moderna da informação clássica, quantificando os recursos físicos necessários para se transmitir ou armazenar certa quantidade de informação num canal livre de ruídos em termos de ocorrência de *bits* (simplificação para dígito binário, *"Binary digit"* em inglês), através de um quantificador chamado de entropia de Shanonn $H(p_i)$ [5].

Em 1995, Ben Schumacher descobre uma maneira de interpretar estados quânticos como informação [6], descobrindo um análogo quântico para o *bit* que recebeu o nome de *bit quântico* ou *qbit*. Assim como $H(p_i)$ mede a quantidade de informação clássica, Schumacher[2] propôs que a entropia de von Neumann $S(\rho)$ é a forma mais apropriada para medir a quantidade de informação quântica [7].

Enquanto *bit*, menor unidade de informação clássica, é codificado somente em 0 ou 1, o *qbit* é codificado por um estado quântico, que obedece as leis da mecânica quântica (MQ) , representado de forma geral por

$$|qbit\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

sendo $|\alpha|^2 + |\beta|^2 = 1$, $\alpha\ e\ \beta \in \mathbb{C}$, $\langle 0|0\rangle = \langle 1|1\rangle = 1$ e $\langle 0|1\rangle = 0$.

É possível demonstrar que duas informações quânticas, codificadas por *qbits*, ocupam menos espaço na transmissão em um canal sem ruído do que duas informações clássicas, com as mesmas probabilidades de ocorrer [6]. Isto significa que economizamos espaço utilizando *qbits*, mas apenas quando os estados não são ortogonais e consequentemente não distinguíveis.

Estados quânticos não-ortogonais e sua indistinguibilidade são considerados recursos na criptografia quântica. Exemplo disso, é o protocolo de criptografia BB84 [8], onde é extremamente improvável que uma mensagem criptografada seja decifrada por um espião, pois este não consegue distinguir as mensagens enviadas por *qbits* não-ortogonais. Entretando, esta mesma indistinguibilidade pode ser um problema na comunicação quântica, quando estados quânticos são utilizados para enviar informações e estas devem ser discriminadas sem um canal de

[1] Os resultados obtidos na dissertação de mestrado de Shannon foram publicados apenas mais tarde na ref. [5]

[2] Schumacher cita no artigo sua própria tese e a de Everett quando usa o conceito de entropia de von Neumann para o operador densidade, entendido como uma medida teórica da informação do nível de emaranhamento.

comunicação auxiliar. Há na literatura propostas de protocolos para discriminar da melhor forma possível dois *qbits* não-ortogonais [9–11], porém estes sempre levam em conta uma possibilidade de erro ou resultado inconclusivo.

A impossibilidade de distinguir perfeitamente dois estados quânticos não-ortogonais é uma limitação imposta pela natureza e não uma limitação tecnológica [12]. Discriminar perfeitamente dois estados não ortogonais permitiria criar uma cópia perfeita de um estado quântico desconhecido arbitrário, o que é proibido pelo teorema da não clonagem [13], ou , até, comunicação por sinais viajando com velocidade superior a da luz no vácuo c, violando um dos princípios da teoria da relatividade de Einstein.

Pode-se criar um protocolo para superar $\vec{c}$ distinguindo estados não-ortogonais.

i. Alice e Bob compartilham um dos estados emaranhado de Bell, que pode ser escrito na base $\{|0\rangle, |1\rangle\}$, que vamos chamar de base I, ou pode ser escrito na base $\{|+\rangle, |-\rangle\}$, base II, por,

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \text{ou} \quad |\phi^+\rangle = \frac{|++\rangle + |--\rangle}{\sqrt{2}}, \tag{1.2}$$

sendo I e II bases ortonormais e,

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{1.3}$$

ii. Alice pode executar medidas no estado que está em sua posse utilizando projetores nas bases I ou II.

iii. Utilizando projetores na base I o estado em posse de Bob colapsa para $|0\rangle$ ou $|1\rangle$, já utilizando projetores na base II, o estado em posse de Bob colapsa para $|+\rangle$ ou $|-\rangle$.

iv. Bob mede os estados em sua posse com a tarefa de determinar a base utilizada por Alice para efetuar a medida. Para isso ele deve distinguir perfeitamente os estados que compõe a base I dos estados que compõe a base II.

Conseguindo distinguir perfeitamente os estados, Bob sempre saberia qual foi a base de medida escolhida por Alice. Combinando previamente, os dois definem que projetores na base I representam o *bit* 0 e na base II representam o *bit* 1. Desta forma podem utilizar o protocolo para transmitir informações de forma instantânea, ou seja, com

velocidade maior do que $\vec{c}$, o que é teoricamente impossível. Perceba que os estados da base I não são ortogonais aos estados da base II, já que

$$|\langle 0|-\rangle| = |\langle 0|+\rangle| = |\langle 1|-\rangle| = |\langle 1|+\rangle| = 1/\sqrt{2}, \tag{1.4}$$

que torna impossível a discriminação perfeita entre os estados quânticos das duas bases.

Portanto, sempre que um ensemble de *qbits* não-ortogonais é utilizado em algum tipo de processo, existe uma indistinguibilidade média mínima entre os estados quânticos que o formam, que não está relacionada a uma limitação tecnológica e por isso não pode ser ultrapassada. Porém, dado um ensemble de estados quânticos puros ou mistos conhecidos, em média quão indistinguíveis entre si são os estados?

A pergunta pode ser exemplificada da seguinte forma. Alice possui o ensemble de estados quânticos A, cada um deles com uma probabilidade p_i de ocorrer, sorteia um dos estados e envia um deles para Bob executar um determinado protocolo. Conhecendo o ensemble que Alice possui, em média, quão difícil é para Bob discriminar o estado que está recebendo?

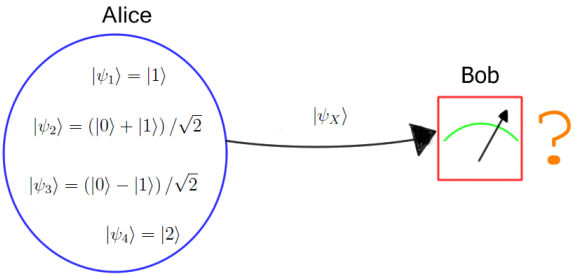

Figura 1.1: Ensemble de estados quânticos de Alice, do qual um é enviado para Bob e deve ser discriminado por uma única medida.

Analisando a figura 1.1, onde $\{|0\rangle, |1\rangle, |2\rangle\}$ é uma base ortonormal, é fácil perceber que o único estado que Bob pode distinguir com uma única medida perfeitamente dos demais é o $|\psi_4\rangle$, para todos os outros é impossível uma discriminação perfeita.

Neste trabalho vamos propor um quantificador para indistinguibilidade média $Ind(\rho)$ dos estados quânticos de um ensemble de N ($N \geq 2$) estados quânticos diferentes conhecidos a priori. É importante enfatizar que este quantificador foi definido por construção e não de um dedução formal. O $Ind(\rho)$ quantifica o quão difícil é, em média, distinguir um

estado quântico dentro de um ensemble conhecido. Esperamos que no futuro o valor do $Ind(\rho)$ seja um parâmetro para os protocolos que trabalhem com conjuntos de $N > 2$ estados quânticos, já que para $N = 2$ os erros esperados já são bem conhecidos na literatura, sendo proporcionais ao produto interno (*overlap*) entre os dois estados ou à distância entre dois operadores ρ [16–18].

Descrevemos brevemente a seguir o conteúdo desta dissertação: No capítulo 2 faremos uma revisão de indistinguibilidade, entropia de Shanon $H(p_i)$, entropia de von Neumann $S(\rho)$, limite de Holevo χ e a relação entre medida de informação e indistinguibilidade. O principal objetivo é mostrar a impossibilidade de distinguir dois estados não-ortogonais e dar uma interpretação para as entropias de Shannon e von Neumann que estejam de acordo com a proposta do trabalho. Partindo da proposta que $S(\rho)$ pode assinalar distinguibilidade, no capítulo 3, vamos propor um parâmetro para subtrair $S(\rho)$ e criar um quantificador $Ind(\rho)$ para um ensemble de estados puros. No capítulo 4, vamos generalizar o $Ind(\rho)$ do capítulo 3 para um ensemble de estados mistos, demonstrando que $Ind(\rho)$ pode ser utilizado para medir a indistinguibilidade de qualquer tipo de ensemble com $N \geq 2$ estados quânticos. Aqui também, vamos aplicar o quantificador no estado de Werner e analisar seu comportamento para um ensemble de estados mistos bipartidos. No capítulo 5 , por fim, apresentamos as conclusões e perspectivas.

Capítulo 2

Indistinguibilidade e Entropias

O quantificador de indistinguibilidade média entre os estados de um ensemble $Ind(\rho)$, proposto neste trabalho, está relacionado com uma falta de informação média que o ensemble carrega. Neste capítulo vamos fazer uma revisão sobre quantidades de informação clássica e quântica, sempre com unidade em *bits*. Assumiremos que o leitor tenha conhecimento prévio sobre princípios da mecânica quântica, medidas projetivas, POVM (da sigla em inglês *Positive Operator-Valued Measure*) e operador densidade ρ. Para uma revisão desses tópicos sugerimos os livros clássicos de mecânica quântica [19] e, para a informação quântica com um enfoque à física, os livros de Nielsen e Chuang [1] ou Barnett [20] são boas sugestões.

2.1 Distinguibilidade entre dois estados não-ortogonais.

A interpretação e o significado físico da não ortogonalidade entre dois estados quânticos é um enigma fundamental na formulação da MQ [21]. Existem trabalhos que tentam determinar o quão distinguíveis são dois estados quânticos [22, 23], já que eles são distinguíveis apenas quando são ortogonais.

Considerando dois estados $|\psi\rangle$ e $|\phi\rangle$, sendo que

$$|\psi\rangle = \left(|\phi\rangle + |\phi^{\perp}\rangle\right)/\sqrt{2}, \tag{2.1}$$

onde $\langle\phi|\phi^{\perp}\rangle = 0$, temos que $\langle\psi|\phi\rangle \neq 0$. Este resultado é o principal ingrediente para a não distinguibilidade entre $|\psi\rangle$ e $|\phi\rangle$. Apesar de $|\psi\rangle$ e $|\phi\rangle$ serem estados diferentes na MQ, não há nenhum processo físico que possa distinguir com exatidão em uma única medida $|\psi\rangle$ e $|\phi\rangle$, ou seja, é impossível ter-se nos laboratórios medidores que consigam distinguir entre estes dois estados de forma conclusiva e sem erro. Em [1, 10] encontramos uma prova desta afirmação. Vamos supor que existam dois medidores Π_1 e Π_2, que consigam distinguir com exatidão e de forma conclusiva $|\psi\rangle$ e $|\phi\rangle$. Para isso cada medidor tem que apresentar valor diferente de zero na sua medida (dar um clique no laboratório) apenas para um dos estados. Além disso, os dois devem gerar o espaço de Hilbert que engloba os estados que estão sendo medidos, ou seja:

$$\Pi_1|\phi\rangle = 0 \ , \ \Pi_2|\psi\rangle = 0 \ \text{ e } \ \Pi_1 + \Pi_2 = \hat{\mathbb{1}}, \tag{2.2}$$

sendo Π_1 e Π_2 POVM hermitianos. Se estes medidores existem, então,

$$\begin{aligned} &\langle\psi|\,\Pi_1\,|\phi\rangle + \langle\psi|\,\Pi_2\,|\phi\rangle = 0; \\ &\langle\psi|\,\underbrace{\Pi_1 + \Pi_2}_{\hat{\mathbb{1}}}\,|\phi\rangle = 0; \\ &\langle\psi|\phi\rangle = 0, \end{aligned} \tag{2.3}$$

demonstrando que só é possível distinguir estados quânticos arbitrários de forma confiável se eles forem ortogonais. Estados não-ortogonais possuem informações inacessíveis à medição. Qualquer protocolo que tente discriminá-los com apenas uma medição deve aceitar erro ou resultados inconclusivos. Por exemplo, Alice possui o seguinte ensemble[1],

$$\epsilon = \{\{1/2, |0\rangle\}, \{1/2, |+\rangle\}\},$$

com

$$\rho = \sum_i |\psi_i\rangle\langle\psi_i|,$$

onde $|\pm\rangle$ é dado pela equação 1.3 e $\{|0\rangle, |1\rangle\}$ é uma base ortogonal completa. Ela envia um dos estados quânticos para Bob, que deve descobrir qual recebeu com apenas uma medida. Bob tenta executar esta tarefa através de dois protocolos:

I. Com medidas de von Neumann, utilizando os projetores,

$$\Pi_0 = |0\rangle\langle 0| \quad \text{e} \quad \Pi_1 = |1\rangle\langle 1| \ .$$

[1] A notação utilizada para ensemble é $\{p_i, |\psi_i\rangle\}$, sendo p_i a probabilidade de ocorrência de $|\psi_i\rangle$ no conjunto.

Quando Π_1 der um clique, Bob saberá com certeza que recebeu o estado $|+\rangle$, mas quando o clique for do Π_0 ele poderá no máximo tentar adivinhar qual estado recebeu sabendo que existe uma probabilidade não nula de cometer um erro. Podemos calcular facilmente a probabilidade de resultados que podem apresentar erro:

$$p^e = \frac{1}{2}\left(\langle 0|\Pi_0|0\rangle + \langle +|\Pi_0|+\rangle\right) = 0,75 \tag{2.4}$$

II. Utilizando medidas generalizadas POVM, onde

$$\Pi_1 = |1\rangle\langle 1| \quad , \quad \Pi_- = |-\rangle\langle -| \quad \text{e} \quad \Pi = \hat{\mathbb{1}} - (\Pi_1 + \Pi_-) \quad ,$$

Quando Π_1 der um clique, Bob saberá com certeza que recebeu o estado $|+\rangle$, quando o clique for do Π_- saberá que está com o estado $|0\rangle$, porém quando o clique for em Π ele terá um resultado inconclusivo. Podemos calcular também a probabilidade de um resultado inconclusivo,

$$p^e = Tr(\Pi\rho) = 0,5 \ , \tag{2.5}$$

onde $\rho = \frac{1}{2}\left(|+\rangle\langle +| + |0\rangle\langle 0|\right)$.

Comparando os resultado das equações 2.4 e 2.5, podemos notar que, independente da estratégia adotada por Bob, sempre existirá uma possibilidade de erro ou inconclusão em sua medida. Considerando que Bob escolher aleatoriamente os estados do ensemble, de acordo com o protocolo I ele erraria em média $37,5\%$ ao tentar adivinhar o estado. Por outro lado, usando o protocolo II erraria 25% das vezes. Ainda, para o protocolo I, podemos encontrar projetores que minimizam este erro, entretanto ele nunca chegará a zero.

2.2 Erro mínimo de Helstrom

Em 1976, Helstrom [16] estabelece qual o erro mínimo Em na discriminação de dois estados não ortogonais. O Em é igual a 1 menos a probabilidade de sucesso máxima utilizando medidores de von Neumann para distinguir dois estados quânticos. Para demonstrar este resultado vamos escolher dois projetores Π_α e Π_β que discriminam da melhor forma possível dois estados equiprováveis, $|\alpha\rangle$ e $|\beta\rangle$. A probabilidade de sucesso p_s é dada por,

$$p_s = \frac{1}{2}\left(\langle\alpha|\,\Pi_\alpha\,|\alpha\rangle + \langle\beta|\,\Pi_\beta\,|\beta\rangle\right). \tag{2.6}$$

Utilizando a relação de completeza dos projetores,

$$\begin{aligned} p_s &= \frac{1}{2}\left(\langle\alpha|\Pi_\alpha|\alpha\rangle + \langle\beta|\mathbb{1} - \Pi_\alpha|\beta\rangle\right) \\ &= \frac{1}{2}\left[1 + \mathrm{Tr}\left(\Pi_\alpha\left(|\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|\right)\right)\right]. \end{aligned} \tag{2.7}$$

Por fim, temos que maximizar o traço de $\Pi_\alpha\Gamma$, sendo

$$\Gamma = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|, \tag{2.8}$$

para obter a p_s máxima. Para isso, devemos encontrar os autovetores de Γ, sendo Π_α uma projeção no autovetor com o maior autovalor de Γ. Os autovalores de Γ são

$$\lambda_\pm = \pm\sqrt{1 - |\langle\alpha|\beta\rangle|^2}. \tag{2.9}$$

Substituindo a equação 2.9 em 2.7, determinamos a probabilidade de sucesso máximo,

$$p_s^{\text{máx}} = \frac{1}{2}\sqrt{1 - |\langle\alpha|\beta\rangle|^2}. \tag{2.10}$$

Com isso temos o Em dado por,

$$Em = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\alpha|\beta\rangle|^2}\right). \tag{2.11}$$

Considerando um caso geral em que os estados $|\alpha\rangle$ e $|\beta\rangle$ ocorrem com probabilidades p_1 e p_2, o Em é dado por,

$$Em = \frac{1}{2}\left[1 - \sqrt{1 - 4p_1p_2\,|\langle\alpha|\beta\rangle|^2}\right]. \tag{2.12}$$

O erro mínimo de Helstrom não é um quantificador de indistinguibilidade, porém ele deve variar monotonicamente com esta quantidade, já que avaliando a equação 2.12 observamos que o erro mínimo depende do *ovelap* entre os estados $|\alpha\rangle$ e $|\beta\rangle$. Apenas quando $\langle\alpha|\beta\rangle = 0$ a probabilidade de sucesso é de 100%.

2.3 Entropia de Shannon

Medir informação é fundamental para enviar e armazenar dados de forma controlada e eficiente. Se quisermos armazenar informações sobre um número n de eventos que ocorrem com probabilidade p_i, devemos

definir quantos bits cada informação deve ter para minimizar o espaço, este espaço recebe o nome de *string*[2], utilizado quando elas são gravadas em um dispositivo. Shannon resolve esse problema para informações clássicas, definindo a menor razão de compressão de dados que admite um sistema de compressão confiável, ou seja, um sistema em que as informações podem ser recuperadas e são distinguíveis.

Segundo Shannon o significado da informação é irrelevante para o problema da engenharia. Tratar a codificação da informação e não seu significado é o que permite que ela seja codificada [24]. Neste contexto é fácil perceber que a quantidade de informação está associada à probabilidade com que ela ocorre. Se o objetivo é minimizar o espaço utilizado para armazenar as informações, as muito prováveis devem ter um número de bits menor, já que serão armazenadas um número maior de vezes, e as pouco prováveis terão um número de bits maior. Então, uma função que quantifique a quantidade de informação I deve variar com o inverso da probabilidade com que ela ocorre, isto é, $f(1/p)$. Esta função deve ser aditiva, já que o espaço utilizado por duas informações é o espaço utilizado pela primeira mais o espaço utilizado pela segunda [25]. Em 1928 Hartley [26] propõe uma medida para quantificar a informação de determinado evento como sendo

$$I\left(p_i\right) = \log_2\left(1/p_i\right) = -\log_2\left(p_i\right), \tag{2.13}$$

onde p_i é a probabilidade de ocorrência do evento. É fácil mostrar que a função logarítmica satisfaz a exigência da informação ser aditiva, já que a probabilidade de ocorrer dois eventos descorrelacionados, A e B, é dada por $p_A p_B$ e a quantidade de informação neste caso seria igual a,

$$\begin{aligned} I\left(p_A p_B\right) &= -log_2\left(p_A p_B\right) \\ &= -\log_2 p_A - \log_2 p_B. \end{aligned} \tag{2.14}$$

Por exemplo, um evento que tenha probabilidade $1/2^{100}$ de ocorrer deve ser codificado com 100 *bits* $\left(-\log_2\left(1/2^{100}\right) = 100\right)$ enquanto um com probabilidade $1/2$ deve ser codificado com 1 *bit* $\left(-\log_2(1/2) = 1\right)$. Note que esta é uma ótima maneira de economizar espaço, pois eventos com muitos *bits* são armazenados poucas vezes e os eventos com poucos *bits* são armazenados muitas vezes.

Em 1948 Shanonn propõe a medida abaixo para quantificar o string médio ótimo SMO para enviar um conjunto de informações por um canal sem ruído [5, 27]:

$$H\left(X\right) \equiv -\sum_x p_x \log_2 p_x, \tag{2.15}$$

[2] É uma sequência de caracteres, dada por uma sequência de bits.

onde p_x é a probabilidade que um evento X ocorra e $-\log_2 p_x$ é a informação de Hartley. O quantificador proposto por Shannon é uma média da quantidade de informção de Hartley. Por definição, se $p_i = 0$, $H(0) = -0\log_2 0 \equiv 0$. Este quantificador é conhecido atualmente como entropia de Shannon $H(p_i)$. Embora, inicialmente Shanon não tenha chamado de entropia, o nome foi sugerido por von Neumann, que lhe disse: "Em primeiro lugar, um desenvolvimento matemático muito próximo já existe na mecânica estatística de Boltzmann e, em segundo lugar, ninguém entende muito bem o que é entropia, então, em qualquer discussão, você estará em posição de vantagem." [27]

Não existe uma relação estrita entre entropia de informação e a entropia termodinâmica. O sentido preferencial dos processos e a diminuição da energia disponível, por exemplo, que são princípios e hipóteses decorrentes da entropia termodinâmica, não estão presentes na teoria de informação. Na teoria da informação a entropia quantifica o tamanho médio do menor *string* necessário para enviar determinada mensagem por um canal sem ruído [27]. A conexão entre as duas pode ser feita a um nível estatístico, já que as duas estão relacionadas com a incerteza sobre o sistema. Segundo Jaynes (1957) [28], a entropia de Shannon pode ser vista como proporcional à quantidade de informação necessária para definir o estado microscópico detalhado do sistema, assim um sistema com maior número de estados acessíveis necessita de uma maior quantidade de informação para ser descrito. Ou seja, a quantidade de informação necessária para descrever um sistema é proporcional a sua entropia definida por Boltzmann. Não é o objetivo deste trabalho estabelecer a relação citada, porém, é interessante fazer uma breve análise. Imagine dois livros, A e B, o primeiro com 2 folhas e o segundo com 4, onde estas são colocadas em uma sequência aleatória. Queremos armazenar em um dispositivo todas as sequências possíveis de folhas para os dois livros. Sendo as sequências equiprováveis e sabendo que existem 2 possibilidades de ordem para A e 24 para B, podemos determinar $H(p_i)$ para os dois livros. Para A temos,

$$H(1/2) = 2\left[-\frac{1}{2}log_2\frac{1}{2}\right] = 1, \tag{2.16}$$

para B,

$$H(1/24) = 24\left[-\frac{1}{24}log_2\frac{1}{24}\right] = 4,58. \tag{2.17}$$

É fácil verificar que um sistema com maior número de estados acessíveis necessita de uma quantidade maior de informação para ser descrito

completamente. É desta forma que podemos relacionar $H(p_i)$ com a entropia estatística do sistema.

Podemos utilizar o exemplo anterior para tentar quantificar a quantidade de informação que carrega uma notícia. Suponha que seja feita a medida da ordem das páginas dos dois livros, onde estes simplesmente são abertos e a ordem das páginas anotada. No livro A tínhamos 2 estados possíveis e agora apenas 1, enquanto no B tínhamos 24 e agora 1. Assim, o fato de conhecermos a informação de B diminui muito mais a entropia do sistema do que a de A. Neste contexto a notícia da ordem do livro B carrega mais informação do que a do livro A, ou seja, quanto mais improvável é uma notícia mais informação ela carrega. Note que não estamos preocupados com a utilidade da notícia e sim com o quanto ela é improvável.

Cabe reforçar que $H(p_i)$ fornece o SMO para enviar ou armazenar informações, de forma que elas possam ser recuperadas e sejam distinguíveis. Este é o aspecto da entropia de Shanonn que é importante para o nosso trabalho.

2.4 Entropia de von Neumann

A entropia de von Neumann é considerada uma generalização da entropia de Shannon para um conjunto de estados quânticos em que a distribuição de probabilidade é obtida a partir do operador densidade [1]. A entropia de von Neumann é definida como,

$$S(\rho) \equiv -Tr(\rho \log_2 \rho) = -\sum_i p_i \log_2(p_i), \tag{2.18}$$

sendo

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \;\; ; \;\; \langle\psi_i|\psi_j\rangle = \delta_{ij} \;\; e \;\; \sum_i p_i = 1. \tag{2.19}$$

Propriedades de $S(\rho)$:

i. Positividade: $S(\rho) \geq 0$, já que $0 \leq p_i \leq 1$, onde p_i são os autovalores de ρ.

ii. $S(\rho) = 0$ para um estado puro, pois neste caso existe um único autovalor igual a 1 para um autovetor, sendo que $\log_2 1 = 0$.

iii. Independência da base: $S(\rho) = S(U\rho U^\dagger)$, onde U é uma transformação unitária, já que os autovalores não são afetados por mudança na base.

Em 1932, von Neumann propõe esta medida para descrever a entropia de um ensemble de estados quânticos. Entretanto, apenas em 1995, Ben Schumacher começa a utilizá-la para medir quantidade de informação quântica [6]. Novamente não estamos interessados na relação da medida com a entropia estatística do sistema e sim na sua utilização como quantificador de informação. Por isso, é importante estabelecer a relação entre $H(p_i)$ e $S(\rho)$. Para isso vamos pensar na entropia de Shannon como a forma ótima de armazenar informações, ou seja, como o SMO para informações clássicas, e a entropia de von Neumann como uma forma ótima de armazenar estados quânticos. Na equação 2.18, podemos observar que para um ensemble de estados quânticos ortogonais $S(\rho) = H(p_i)$. Neste contexto, um ensemble com estados quânticos ortogonais equivale a um conjunto de informações clássicas, uma vez que todos os estados podem ser perfeitamente distinguíveis entre si.

A relação que estamos interessados pode ser explicada através de um exemplo que construímos: queremos enviar o ensemble de estados quânticos, representado abaixo, por um canal clássico sem ruído:

$$\epsilon = \{1/4, |0\rangle, 1/4, |1\rangle, 1/4, |+\rangle, 1/4, |-\rangle\}, \tag{2.20}$$

sendo $|\pm\rangle$ dado pela equação 1.3. Queremos determinar qual o SMO para enviar ϵ. Quanticamente podemos escrever este conjunto utilizando o operador densidade $\rho \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i|$, onde agora, p_i e $|\psi_i\rangle$ são obtidos a partir do ensemble ϵ. Na base dos estados enviados podemos escrevê-lo,

$$\rho = \frac{1}{4}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|\right). \tag{2.21}$$

Existe a liberdade de escrever ρ em qualquer base. Podemos escrevê-lo na forma diagonal, em que os elementos da diagonal principal são seus autovalores e sua base seus autovetores,

$$\rho_{Diag} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}. \tag{2.22}$$

Então, para enviar ϵ, basta mandar duas informações que correspondem aos elementos da diagonal principal da matriz densidade, onde as probabilidades de ocorrerem as informações são os autovalores do operador densidade. O SMO neste caso é obtido por

$$H(p_i) = -\sum_i p_i \log_2(p_i) = -2\frac{1}{2}\log_2\left(\frac{1}{2}\right) = 1. \tag{2.23}$$

Perceba que se estivermos analisando uma situação em que todos os elementos deste ensemble são enviados de Alice para Bob, que tem o objetivo de distingui-los, utilizando medidas projetivas na base dos autovetores de ρ, o resultado obtido será exatamente a matriz densidade na forma diagonal. Neste sentido, ler um ensemble de estados quânticos em um dispositivo clássico, como uma memória de computador, que foi armazenado de forma ótima, equivale a medi-los utilizando projetores na base dos autovetores do operador densidade. Então, segundo Schumacher, $S(\rho)$ será interpretado como a SMO para enviar um conjunto de estados quânticos e desta forma estabelecer uma relação entre ela e $H(p_i)$ [6]. Entretanto, uma diferença importante é que não existe uma garantia de recuperarmos os estados quânticos enviados com um *string* dado por $S(\rho)$, esta garantia só ocorre se todos os estados quânticos forem ortogonais entre si. Enquanto que, ao enviar de forma ótima um conjunto de notícias clássicas por um canal sem ruído, podemos sempre recuperar e diferenciar as informações. Geralmente o SMO quântico fornece uma quantidade de informação menor do que o necessário para diferenciar os *q-bits* armazenados ou enviados.

2.5 Entropia de von Neumann e Indistinguibilidade

Jozsa e Schlienz (2000) em seu artigo [21], mostram que a entropia de von Neumann varia monotonicamente com a distinguibilidade para um ensemble com dois estados puros. Vamos refazer o exemplo mostrado no artigo para que o leitor entenda a motivação que levou ao quantificador de indistinguibilidade que será proposto no capítulo 3.

Considere o ensemble

$$\epsilon = \{\{1/2, |\psi_1\rangle\}, \{1/2, |\psi_2\rangle\}\}, \tag{2.24}$$

representado pelo operador densidade

$$\rho = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|),$$

sendo

$$|\psi_1\rangle = |0\rangle \;\text{ e }\; |\psi_2\rangle = \alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle; \;\; (0 \leq \alpha \leq 1).$$

Utilizando a equação 2.12 determinamos o erro mínimo de Helstrom ao tentar discriminar os dois estados do sistema,

$$Em = \frac{1}{2}\left(1 - \sqrt{1-\alpha^2}\right), \tag{2.25}$$

e, utilizando a equação 2.18 podemos determinar $S(\rho)$. Para isso basta escrever ρ na forma diagonal,

$$\rho = \begin{pmatrix} \frac{1+\alpha}{2} & 0 \\ 0 & \frac{1-\alpha}{2} \end{pmatrix}. \tag{2.26}$$

Fornecendo o seguinte resultado para $S(\rho)$

$$S(\rho) = -\frac{1+\alpha}{2}\log_2\left(\frac{1+\alpha}{2}\right) - \frac{1-\alpha}{2}\log_2\left(\frac{1-\alpha}{2}\right). \tag{2.27}$$

Os resultados obtidos nas equações 2.25 e 2.27 estão representados na Fig. 2.1.

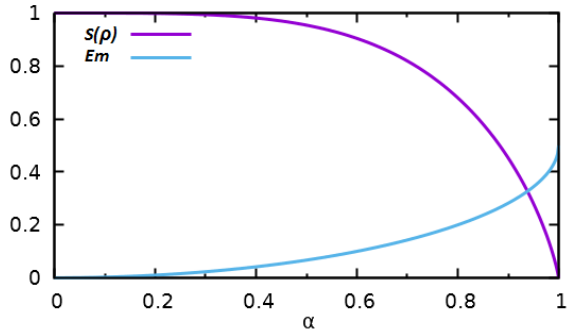

Figura 2.1: Relação entre o erro mínimo de Helstrom Em e a entropia de von Neumann $S(\rho)$ em função de α.

Analisando o gráfico 2.1 verificamos que maior $S(\rho)$ implica em um menor erro para discriminar os dois estados do ensemble e vice-versa. Lembrando que o erro mínimo depende do *overlap* entre os dois estados, observamos que quanto maior o *overlap*, menor a distinguibilidade e menor $S(\rho)$ para $N = 2$ estados quânticos diferentes. Esta relação é coerente, pois menor $S(\rho)$ significa que precisamos enviar menos informação pelo canal, porém teremos mais dificuldade de discriminar os elementos do ensemble.

Do ponto de vista da informação quântica, quanto mais distinguíveis os estados quânticos de um ensemble, mais informações clássicas eles podem comunicar. Neste sentido, Jozsa e Schlienz [21] propõe que $S(\rho)$ pode ser usado para quantificar a distinguibilidade de um conjunto de estados puros. Aparentemente é equivalente utilizar *overlap* ou $S(\rho)$

para assinalar distinguibilidade. Entretanto, os autores afirmam que isto é uma falha de nossa intuição, demonstrando que não existe uma relação monotônica entre as duas grandezas para um ensemble com $N > 2$ estados quânticos. É possível, para $N > 2$ estados quânticos, aumentar o *overlap* entre os estados tomados dois a dois e aumentar o $S(\rho)$ do ensemble, ou seja, é possível aumentar a distinguibilidade do ensemble tornando os estados dois a dois mais indistinguíveis. Segundo os autores, a distinguibilidade medida por $S(\rho)$ é uma propriedade global de um conjunto de estados puros e não uma propriedade local, acumulativo de pares dos estados quânticos constituintes.

Uma generalização de $S(\rho)$, como medida de distinguibilidade, para um ensemble de estados mistos é dado pelo limite de Holevo [29], que veremos a seguir

2.6 Limite de Holevo

Holevo, em 1973, define, através de um teorema, qual é a quantidade máxima de informação clássica que pode ser transmitida por um canal quântico [30], onde informação clássica é definida como informação acessível e recuperável.

Teorema. *Alice prepara um estado ρ_x, no qual $X = 0, \cdots, n$ com probabilidades $p_0, \cdots, p_n$, e envia para Bob. Bob realiza medidas generalizadas POVM no estado, sendo Y o resultado da medida. O limite de Holevo estabelece o máximo que Bob pode conhecer de X sabendo Y*[3]*:*

$$H(X : Y) \leq \chi, \tag{2.28}$$

em que

$$\chi = S(\rho) - \sum_x p_x S(\rho_x) \quad \text{é a quantidade } \chi \text{ de Holevo,} \tag{2.29}$$

$H(X : Y)$ é a informação mútua ou comum entre X e Y e $\rho = \sum_x p_x \rho_x$ [1].

Para um ensemble de estados puros, o χ de Holevo é simplesmente $S(\rho)$, já que

$$S(\rho_x) = 0. \tag{2.30}$$

Como citado anteriormente, o χ de Holevo pode ser visto como uma generalização da $S(\rho)$ para um ensemble de estados mistos. Desta

[3] No capítulo 12 do livro do Nielsen e Chuang, o leitor pode encontrar a dedução deste limite de forma mais didática do que no artigo original.

forma podemos interpretar o χ de Holevo, o limite da quantidade de informação transmitida em um canal quântico, como uma medida da distinguibilidade de um ensemble de estados quânticos [31–34]. A quantidade de informação média enviada por um ensemble de estados quânticos é geralmente inferior à necessária para distingui-los perfeitamente, exceto para o caso em que todos os estados são ortogonais.

Por exemplo, para o ensemble descrito pela equação 2.20, cuja matriz densidade é dada pela equação 2.21, o $\chi = S(\rho) = 1$. Portanto, existem 4 estados equiprováveis, que vamos chamar de 4 informações quânticas, que possuem em média apenas 1 *bit* de informação. Tratando os 4 estados do ensemble como 4 informações clássicas, distinguíveis, concluímos que em média são necessários 2 *bits* para armazenar tal informação. Neste caso garantimos que a informação sobre os 4 estados poderá ser inteiramente recuperada. Com 1 *bit*, utilizando ainda a equação 2.15, podemos distinguir apenas 2 informações clássicas equiprováveis. Podemos afirmar então que falta 1 *bit* para distinguir perfeitamente as quatro informações, ou, de forma equivalente, que podemos a princípio distinguir apenas 2 informações.

Pode-se mostrar então que o χ de Holevo determina o máximo de informação distinguível em um ensemble de estados quânticos e, por isso, podemos utilizá-lo como quantificador de distinguibilidade. Nos próximos capítulos vamos utilizar esta interpretação para criar um quantificador de indistinguibilidade.

Capítulo 3

Indistinguibilidade em ensemble de estados puros

Neste capítulo propomos um quantificador para indistinguibilidade de um ensemble de estados quânticos puros conhecidos. O problema que queremos resolver pode ser exemplificado da seguinte forma: existe um sistema que envia estados quânticos conhecidos com certa probabilidade; apesar de conhecermos todos os estados e suas probabilidades de ocorrer, nunca sabemos qual estado foi enviado. Queremos determinar o quão difícil é distinguir entre os estados quânticos do ensemble.

Como já foi visto, a entropia de von Neumann está relacionada com a distinguibilidade de um ensemble ϵ de N estados quânticos puros. Quanto mais fácil de discriminar os estados quânticos, maior o SMO necessário para armazená-los ou enviá-los, onde o $SMO = S(\rho)$ para informações quânticas. Vale lembrar que, para um ensemble de estados quânticos puros, $S(\rho)$ é exatamente o χ de Holevo, ou seja, o limite máximo de informação que podemos obter de um estado do sistema a partir do resultado de uma medida. Como $S(\rho)$ está relacionada com a distinguibilidade, podemos propor sua utilização em um quantificador de indistinguibilidade. Porém, falta uma referência da qual será subtraída $S(\rho)$ para que esta medida represente realmente um quantificador de indistinguibilidade. Por exemplo, os dois ensembles,

$$\epsilon_1 = \{\{1/2, |0\rangle\}, \{1/2, |1\rangle\}\} \quad \text{e} \tag{3.1}$$

$$\epsilon_2 = \{\{1/4, |0\rangle\}, \{1/4, |1\rangle\}, \{1/4\,|+\rangle\}, \{1/4, |-\rangle\}\}, \tag{3.2}$$

sendo,

$$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2},$$

podem ser representados pela mesma matriz densidade,

$$\rho_{Diag} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix},$$

e possuem a mesma entropia de von Neuman, $S(\rho) = 1$, e consequentemente a mesma distinguibilidade. Entretanto, é fácil verificar, que os dois ensembles apresentam indistinguibilidades muito diferentes; enquanto em ϵ_1 podemos distinguir perfeitamente os estados $|0\rangle$ e $|1\rangle$, que são ortogonais, o mesmo não ocorre para ϵ_2, onde não podemos diferenciar o $|0\rangle$ do $|+\rangle$, por exemplo.

Nesse sentido, o problema da indistinguibilidade de estados é mais difícil do que o da distinguibilidade de estados. O exemplo dos ensembles ϵ_1 e ϵ_2 serve para mostrar que existe muitos ensembles com a mesma distinguibilidade, porém com indistinguibilidades diferentes. Para associar $S(\rho)$ com um quantificador de indistinguibilidade $Ind(\rho)$, precisamos de uma referência, da qual subtraímos o seu valor e obtemos a indistinguibilidade.

3.1 *String* médio ótimo para distinguir perfeitamente estados quânticos puros

Nesta seção vamos propor uma referência para subtrair $S(\rho)$ e determinar $Ind(\rho)$. Para isto, o $S(\rho)$ será interpretado como o SMO para armazenar um ensemble de estados quânticos ϵ em um dispositivo ou enviá-lo através de um canal clássico de comunicação. É importante lembrar que dois estados quânticos ortogonais são classificados como estados clássicos, já que o SMO utilizado para que ele seja enviado ou armazenado coincide com o valor da entropia de Shannon para a distribuição de probabilidades de informações clássicas.

Para que fique clara a escolha deste parâmetro, inicialmente trataremos do caso mais simples, um ensemble com dois elementos que são equiprováveis. O exemplo a seguir demonstra o raciocínio utilizado para criar o quantificador de indistinguibilidade. Comparando,

$$\epsilon = \{\{1/2, |0\rangle\}, \{1/2, |1\rangle\}\}$$

com

$$\epsilon' = \{\{1/2, |0\rangle\}, \{1/2, |+\rangle\}\},$$

observamos que o SMO, dado por $S(\rho)$ 2.18, do primeiro ensemble é 1 *bit* (conjunto de estados clássicos) e do segundo $0,6$ *bit*. Portanto, os dois ensembles possuem o mesmo número de informações, mas o segundo pode ser armazenado ou enviado com um *string* menor. O problema é que existe um preço a pagar por essa compressão, se tentarmos a partir da informação armazenada recuperar os elementos de ϵ teremos garantia de sucesso, mas não para ϵ'.

No capítulo 2 mostramos que o SMO necessário para, por exemplo, armazenar um ensemble de estados quânticos puros é dado pela entropia de von Neumann, que é equivalente a guardar apenas as probabilidades do operador densidade diagonalizado. O que significa que, para um ϵ qualquer com dois estados puros, recuperar as informações armazenadas com o SMO nos fornece apenas o operador densidade diagonal, o mesmo obtido caso fizéssemos medidas projetivas sobre os elementos de ϵ, cujos projetores são obtidos a partir dos autoestados do operador densidade. É fácil perceber que, mesmo conhecendo os estados que formavam o ensemble antes da informação ser armazenada, não podemos recuperá-los caso os estados não sejam ortogonais. Para deixar mais claro montamos as seguintes matrizes densidade nas bases dos seus autoestados,

$$\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

e

$$\rho'_{Diag} = \begin{pmatrix} 0,85 & 0 \\ 0 & 0,15 \end{pmatrix}.$$

Como conhecemos os elementos que formavam o conjunto podemos afirmar exatamente a probabilidade de cada estado quântico no ensemble ϵ. Observe que as informações recuperadas são exatamente as probabilidades de cada estado quântico do conjunto, mas isso não é possível sem erro para ϵ'. Portanto, fica faltando informação para que possamos montar ϵ'. Vamos propor que esta falta de informação para distinguir perfeitamente os estados que compõe ϵ' é proporcional a sua indistinguibilidade. Neste caso o nosso *string* médio ótimo para distinguir perfeitamente estados quânticos puros é 1 *bit*, que é o SMO necessário para distinguir sem erro dois estados quânticos equiprováveis.

Vamos testar essa proposta comparando a falta de informação, $1 - SMO$, com o erro mínimo de Helstrom Em. No cápitulo 2 mostramos que o erro mínimo Em aumenta à medida que aumenta o overlap entre os estados quânticos, ou seja, é proporcional à indistinguibilidade do

conjunto, sendo um bom quantificador para indistinguibilidade entre dois estados quânticos com probabilidades p_1 e p_2. Portanto, vamos considerar Em uma referência para analisarmos o comportamento da nossa proposta de quantificador.

Comparando os ensembles citados acima, temos para ϵ,

$$S(\rho) = 1, \quad 1 - S(\rho) = 0 \quad \text{e} \quad Em = 0 \tag{3.3}$$

para ϵ',

$$S(\rho') \approx 0,60, \quad 1 - S(\rho) \approx 0,40 \quad \text{e} \quad Em \approx 15\% \tag{3.4}$$

e, analisando um novo ensemble em que os estados são mais paralelos,

$$\epsilon'' = \left\{ \{1/2, |0\rangle\}, \left\{ 1/2, \left(\frac{\sqrt{5}}{\sqrt{6}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle \right) \right\} \right\}$$

$$S(\rho'') \approx 0,26, \quad 1 - S(\rho) \approx 0,74 \quad \text{e} \quad Em = 0,29\%. \tag{3.5}$$

Vamos enfatizar estas medidas através da tabela 3.1.

Ensemble	SMO	Erro mínimo	$1 - SMO$
ϵ	1	0	0
ϵ'	0,60	15%	0,40
ϵ''	0,26	29%	0,74

Tabela 3.1: Relação entre SMO e erro mínimo Em.

É possível observar uma proporção entre o erro mínimo de Helstrom e a falta de informação ($1 - SMO$), mostrando que esta é aparentemente uma boa medida de indistinguibilidade.

Tomando o exemplo da seção 2.5, cujo ensemble é dado pela equação 2.24, podemos observar mais claramente a proporção entre Em e $1 - SMO$ à medida que os estados ficam mais paralelos. Neste exemplo o SMO é dado pela equação 2.27. À medida que α varia partimos de um ensemble em que os dois estados são ortogonais ($\alpha = 0$), quando podemos diferenciá-los sem erros ou resultados inconclusivos, para um em que os estados são praticamente iguais ($\alpha \approx 1$) em que a indistinguibilidade dos estados é máxima. Não vamos considerar a situação em que ($\alpha = 1$), pois neste caso os estados são iguais e podemos considerar que o ensemble é composto por um único estado e não tem sentido falar

sobre indistinguibilidade. O gráfico da Fig. 3.1 mostra a relação entre $1 - SMO$ e o erro mínimo de Helstrom Em.

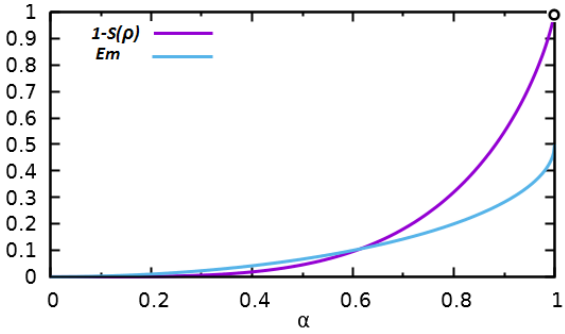

Figura 3.1: Relação entre o erro mínimo de Helstrom Em e a falta de informação $1 - S(\rho)$ para distinguir os estados conlusivamente.

Observando o gráfico da Fig. 3.1 concluímos que a falta de informação para distinguir os estados conlusivamente $1 - SMO$ possui o comportamento esperado para um quantificador de indistinguibilidade entre dois estados quânticos puros equiprováveis, indo de zero, quando os estados são ortogonais, até próximo de 1, quando os estados ficam praticamente iguais. Observamos ainda que $1 - S(\rho)$ varia monotonicamente com Em.

O leitor pode se perguntar por que não utilizar simplesmente o Em como quantificador de indistinguibilidade, mas cabe lembrar que ele é útil apenas quando o ensemble é constituido de dois estados puros. Para um número $N \geq 2$ de estados quânticos, puros ou mistos, com probabilidades p_i de ocorrerem, o Em não se aplica, tornando necessário um novo quantificador.

Para que a falta de informação que discrimina perfeitamente os estados seja um candidato para o $Ind(\rho)$ é necessário generalizar o *String* médio ótimo para distinguir perfeitamente estados quânticos puros para qualquer ensemble de estados quânticos.

3.2 Generalização do *string* médio ótimo para distinguir perfeitamente estados quânticos puros

Vimos na seção anterior que $1 - SMO$, onde SMO é a entropia de von Neumann, é um bom quantificador para indistinguibilidade de um ensemble com dois estados quânticos puros equiprováveis. Para generalizar esta medida vamos nos concentrar no 1 *bit* que aparece em $1 - SMO$. O 1 *bit* é exatamente o valor de $S(\rho)$ quando os dois estados são ortogonais e possuem a mesma probabilidade p_i de ocorrer. Neste caso, como sabemos, $S(\rho) = H(p_i)$. Então, podemos substituir 1 *bit* por $H(p_i)$ e propor $H(p_i)$ como referência da qual temos que diminuir $S(\rho)$ para quantificar a indistinguibilidade de N estados quânticos puros. O que estamos propondo é que cada estado puro do ensemble, mesmo não sendo ortogonais aos demais, seja tratado como se fosse classicamente distintos. Desta forma calculamos $H(p_i)$ usando as probabilidades de ocorrência de $|\psi_i\rangle$ no ensemble. O quantificador de indistinguibilidade $Ind(\rho)$ é dado por

$$Ind(\rho) = H(p_i) - S(\rho), \tag{3.6}$$

onde ρ é o operador densidade que representa o ensemble e p_i é a probabilidade de cada estado no ensemble. Interpretando cada termo da equação temos:

- $H(p_i)$ é o SMO necessário para que todos os estados quânticos que compõe o ensemble sejam distinguíveis (para determinar esse valor temos que considerar que todos os estados são clássicos ou ortogonais entre si);
- $S(\rho)$ é o SMO para armazenar ou enviar o ensemble de estados quânticos;
- $Ind(\rho)$ é o quantificador de indistinguibilidade em *bits*, que está relacionado ao quanto falta de informação em média para que os estados sejam distinguíveis perfeitamente.

Podemos testar essa medida para o exemplo citado inicialmente no capítulo 2. Para

$$\epsilon_1 = \{\{1/2, |0\rangle\}, \{1/2, |1\rangle\}\},$$

temos:

$$H(p_i) = 1 \quad , \quad S(\rho) = 1\ bit \quad \text{e} \quad Ind(\rho) = 0,$$

que assinala que os estados são distinguíveis, como era esperado. Para,

$$\epsilon_2 = \left\{ \{1/4, |0\rangle\}, \{1/4, |1\rangle\}, \{1/4, |+\rangle\}, \{1/4, |-\rangle\} \right\},$$

já conhecemos $S(\rho) = 1$, pois esse é representado pela mesma matriz densidade de ϵ_1. Falta apenas calcular $H(p_i)$ para determinar qual seria o SMO para que todos os elementos sejam distintiguíveis, lembrando que eles seriam realmente distinguíveis se fossem ortogonais entre si. Temos:

$$H(p_i) = -4\frac{1}{4}\log_2\left(\frac{1}{4}\right) = 2.$$

Ou seja, é necessário no mínimo um *string* de 2 bits para que quatro estados quânticos com a mesma probabilidade de ocorrer sejam distinguíveis. Calculando o $Ind(\rho)$ temos:

$$Ind(\rho) = H(p_i) - S(\rho) = 1.$$

Indicando que não podemos determinar com precisão todos os estados do ensemble. Podemos interpretar que falta em média $1bit$ de informação para que os estados sejam diferenciados.

Estritamente falando: $H(p_i)$ é o SMO para armazenar uma mensagem clássica e $S(\rho)$ é o SMO para armazenar uma mensagem quântica. Portanto, $Ind(\rho)$ mede a indistinguibilidade média mínima entre os estados do ensemble.

Propriedades de $Ind(\rho)$:

i. Positividade: $Ind(\rho)$ é sempre maior ou igual a zero, já que $S(\rho) \leq H(p_i)$.

ii. Independência da base: $Ind(\rho)$ é independente da base utilizada para medida, pois $H(p_i)$ depende apenas de p_i dos elementos que formam o ensemble e a entropia de von Neumann não depende da base. Esta propriedade evita processos de minimização ou maximização.

Como $Ind(\rho)$ não é definido a partir da dedução de princípios gerais da mecânica quântica, uma forma de verificar sua validade é através de exemplos em que a medida é aplicada. O primeiro exemplo pode ser visto na primeira seção deste capítulo, para isso basta lembrar que $1bit$ é o $H(p_i)$ do ensemble proposto. A seguir vamos analisar novos exemplos em que determinamos $Ind(\rho)$.

3.2.1 Exemplo 1

Neste primeiro exemplo vamos analisar o que ocorre quando colocamos mais um elemento em,

$$\epsilon = \{\{1/2, |0\rangle\}, \{1/2, |+\rangle\}\},$$

que possui $H(p_i)$ e $S(\rho)$ já conhecidos e iguais à $1,00$ e $0,60$, respectivamente, tendo $Ind(\rho) = 0,40$.

Vamos inicialmente acrescentar o estado $|1\rangle$, de forma que as novas probabilidades dos estados que compõem o ensemble são todas iguais e valem $1/3$. É esperado que a indistinguibilidade do novo conjuto ϵ' aumente, já que não podemos distinguir perfeitamente o $|1\rangle$ do $|+\rangle$. Para determinar $Ind(\rho)$ temos que primeiro determinar $H(p_i)$:

$$H(p_i') = -3\frac{1}{3}\log_2\frac{1}{3} = 1,58; \tag{3.7}$$

segundo, escrever a matriz densidade diagonal:

$$\rho'_{Diag} = \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}; \tag{3.8}$$

terceiro determinar $S(\rho')$,

$$S(\rho') = -\frac{2}{3}\log_2\frac{2}{3} - \frac{1}{3}\log_2\frac{1}{3} = 0,92; \tag{3.9}$$

por fim, utilizando os resultados das equações 3.7 e 3.9, encontramos,

$$Ind(\rho') = H(p_i') - S(\rho') = 0,66. \tag{3.10}$$

Como era esperado $Ind(\rho') > Ind(\rho)$, ou seja, em média é mais difícil distinguir os elementos dos ensemble ϵ' do que os de ϵ.

Vamos agora acrescentar o estado $|2\rangle$ à ϵ. Como $|2\rangle$ é ortogonal a todos os elementos de ϵ, é esperado que a indistinguibilidade do ensemble diminua. O novo ϵ'' também possui todos os elementos com probabilidades iguais a $1/3$. Repetindo as etapas do caso anterior temos,

$$Ind(\rho'') = H(p_i'') - S(\rho'') = 0,26. \tag{3.11}$$

Como era esperado $Ind(\rho'') < Ind(\rho)$, ou seja, em média é mais fácil distinguir os elementos do ensemble ϵ'' do que os de ϵ.

Analisando os resultados obtidos em 3.10 e 3.11, podemos ver que o quantificador $Ind(\rho)$ pode ser interpretado como uma média da indistinguibilidade dos estados quânticos que compõe o ensemble. Essa interpretação é coerente se lembrarmos que $Ind(\rho)$ representa uma média da falta de informação necessária para distinguir todos os estados do ensemble.

3.2.2 Exemplo 2

Agora vamos analisar a relação entre Em e $Ind(\rho)$ quando apenas as probabilidades clássicas do ensemble são mudadas. Dado o ensemble,

$$\epsilon = \{\{p, |0\rangle\}, \{(1-p)\,|+\rangle\}\},$$

sendo,

$$\rho = p\,|0\rangle\langle 0| + (1-p)\,|+\rangle\langle +| \quad , \quad (0 \leq p_i \leq 1),$$

cuja forma diagonal é

$$\rho_{Diag} = \begin{pmatrix} 0,5\left(1-\sqrt{2p^2-2p+1}\right) & 0 \\ 0 & 0,5\left(1+\sqrt{2p^2-2p+1}\right); \end{pmatrix},$$

para calcular $Ind(\rho)$, temos

$$H(p_i) = -p\log_2 p - (1-p)\log_2(1-p), \tag{3.12}$$

e:

$$\begin{aligned} S(\rho) = &-0,5\left(1-\sqrt{2p^2-2p+1}\right)\log_2\left(0,5\left(1-\sqrt{2p^2-2p+1}\right)\right) \\ &-0,5\left(1+\sqrt{2p^2-2p+1}\right)\log_2\left(0,5\left(1+\sqrt{2p^2-2p+1}\right)\right), \end{aligned} \tag{3.13}$$

sendo $Ind(\rho)$ dado pela subtração entre a equações 3.12 e 3.13.

Em, dado pela equação 2.12, é igual a,

$$Em = \frac{1}{2}\left(1-\sqrt{1+2p^2-2p}\right). \tag{3.14}$$

A comparação de $Ind(\rho)$ com o resultado da equação 3.14 pode ser feita pelo gráfico da Fig. 3.2.

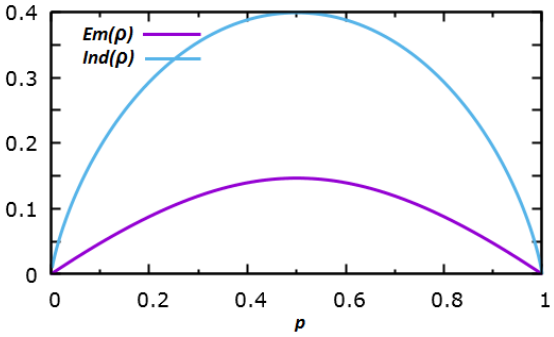

Figura 3.2: Relação entre o erro mínimo Em e a indistinguibilidade do ensemble $Ind(\rho)$ em função de p, onde p e $(1-p)$ representam as probabilidade clássicas dos estados no ensemble.

Analisando o gráfico 3.2 observamos novamente uma relação monotônica entre Em e $Ind(\rho)$. Quando $p = 0 \;\; ou \;\; 1$ temos apenas um estado quântico no ensemble e a indistinguibilidade neste caso é zero. À medida que p vai de 0 a 1/2 a mistura entre os estados aumenta e também deve aumentar $Ind(\rho)$ e, a medida que p vai de 1/2 a 1, a mistura entre os estados diminui e $Ind(\rho)$ deve diminuir, exatamente o que é mostrado no gráfico.

3.2.3 Exemplo 3

No capítulo 2 discutimos a ref. [21] que serviu de motivação para criação do quantificador $Ind(\rho)$. Vamos analisar o valor de $Ind(\rho)$ para os ensembles de estados quânticos citados como exemplo no artigo, a saber,

$$\epsilon = \{\{1/3, |\psi_1\rangle\}, \{1/3, |\psi_2\rangle\}, \{1/3, |\psi_3\rangle\}\}$$

que gera um estado ρ e,

$$\widetilde{\epsilon} = \left\{\left\{1/3, \left|\widetilde{\psi}_1\right\rangle\right\}, \left\{1/3, \left|\widetilde{\psi}_2\right\rangle\right\}, \left\{1/3, \left|\widetilde{\psi}_3\right\rangle\right\}\right\}$$

que gera um estado $\widetilde{\rho}$. Sendo,

$|\psi_1\rangle = \left|\widetilde{\psi}_1\right\rangle = |0\rangle,$

$|\psi_2\rangle = \left|\widetilde{\psi}_2\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$

$|\psi_3\rangle = \frac{\sqrt{2}-1}{\sqrt{6}}|0\rangle + \frac{\sqrt{2}+1}{\sqrt{6}}|1\rangle,$

$\left|\widetilde{\psi}_3\right\rangle = \frac{2}{3\sqrt{3}}\,|0\rangle + \frac{4}{3\sqrt{3}}\,|1\rangle + \frac{\sqrt{7}}{3\sqrt{3}}\,|2\rangle$.

É possível verificar que os overlaps $\langle\psi_i|\psi_j\rangle \leq \langle\widetilde{\psi}_i|\widetilde{\psi}_j\rangle$, porém o $S(\rho) < S(\widetilde{\rho})$. Para os dois ensembles o $H(p_i)$ é facilmente calculado e vale $1,58$. Os valores de $S(\rho)$ dos dois exemplos podem ser encontrados no artigo e valem $S(\rho) = 0,85$ e $S(\widetilde{\rho}) = 0,91$. Portanto, os valores de indistinguibilidade são: $Ind(\rho) = 0,73$ e $Ind(\widetilde{\rho}) = 0,67$.

Fica claro neste exemplo que o quantificador proposto não está relacionado diretamente com os overlaps dois a dois. Lembrando que para um ensemble de estados puros o χ de Holevo é igual a $S(\rho)$, observamos novamente um maior valor de $Ind(\rho)$ para um menor valor de χ de Holevo.

3.2.4 Exemplo 4

Para finalizar vamos propor um ensemble com 3 estados puros em que podemos variar as probabilidades quânticas de dois estados, tornando o sistema distinguível para $\alpha = \beta = 0$. Temos,

$$\rho = \frac{1}{3}\left(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3|\right),$$

sendo

$$\begin{aligned}
|\psi_1\rangle &= |0\rangle, \\
|\psi_2\rangle &= \left(\alpha|0\rangle + \sqrt{1-\alpha^2}|1\rangle\right), \ \text{com} \ 0 \leq \alpha \leq 1, \\
|\psi_3\rangle &= \left(\beta|1\rangle + \sqrt{1-\beta^2}|2\rangle\right), \ \text{com} \ 0 \leq \beta \leq 1.
\end{aligned}$$

Utilizando o suporte dos autovetores de ρ, podemos escrevê-lo na sua forma diagonal,

$$\rho_{Diag} = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1-\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2} & 0 \\ 0 & 0 & 1+\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2} \end{pmatrix} \tag{3.15}$$

A entropia de von Neumann, equação 2.18, é dada por:

$$\begin{aligned} S(\rho) = 0,53 &- \frac{1}{3}\left(1-\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right) \\ &\times \log_2\left[\frac{1}{3}\left(1-\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right)\right] + \\ &- \frac{1}{3}\left(1+\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right) \\ &\times \log_2\left[\frac{1}{3}\left(1+\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right)\right], \end{aligned} \tag{3.16}$$

$H(p_i)$ é facilmente calculado e vale $1,58$, que subtraído de 3.16 fornece

$$\begin{aligned} Ind(\rho) = 1,05 &+ \frac{1}{3}\left(1-\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right) \\ &\times \log_2\left[\frac{1}{3}\left(1-\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right)\right] + \\ &+ \frac{1}{3}\left(1+\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right) \\ &\times \log_2\left[\frac{1}{3}\left(1+\sqrt{\alpha^2+\beta^2-\alpha^2\beta^2}\right)\right], \end{aligned} \tag{3.17}$$

O resultado obtido na equação 3.17 em função de α e β é mostrado na Fig. 3.3.

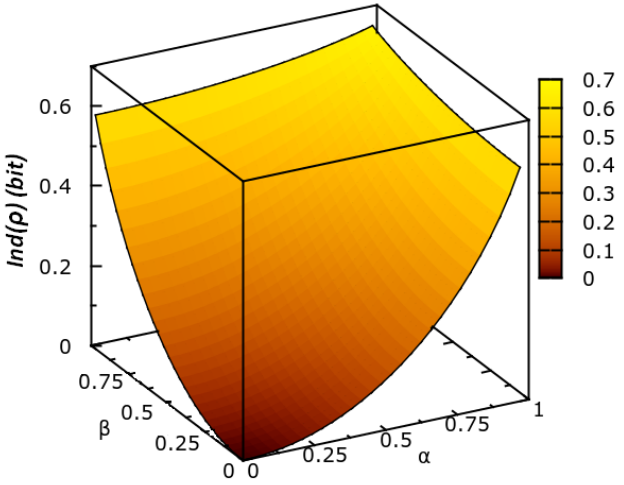

Figura 3.3: Variação de $Ind(\rho)$ em função de α e β.

O resultado apresentado no gráfico da figura 3.3 é coerente com o esperado. Para $\alpha = 0$ e $\beta = 0$ a $Ind(\rho) = 0$, o que é esperado já que neste caso os três estados se tornam ortogonais e são perfeitamente distinguíveis . Fixando $\alpha = 0$, tornando o $|\psi_1\rangle$ ortogonal ao $|\psi_2\rangle$ e ao $|\psi_3\rangle$, e aumentando β obsevamos um crescimento de $Ind(\rho)$, isto deve ocorrer pois os estados $|\psi_2\rangle$ e $|\psi_3\rangle$ se tornam mais paralelos, aumentando a indistinguibilidade média do conjunto. O mesmo ocorre quando fixamos $\beta = 0$ e aumentamos o α, neste caso estamos tornando $|\psi_1\rangle$ e $|\psi_2$ mais paralelos. Por fim, é possível verificar também que $Ind(\rho)$ cresce à medida que aumentamos α e β, isto deve ocorrer pois os estados se tornam mais paralelos o que geralmente torna o conjunto em média mais indistinguível.

T

Capítulo 4

Indistinguibilidade em ensemble de estados mistos

Até o momento analisamos situações em que o ensemble é formado por estados puros e observamos que $Ind(\rho)$ se comportou da forma esperada. Neste capítulo vamos propor um quantificador de indistinguibilidade para um ensemble ϵ de estados quânticos mistos $Ind_M(\rho)$. O ensemble de estados mistos é definido como

$$\rho = \sum_i p_i \rho_i, \tag{4.1}$$

onde existe uma incerteza clássica em cada estado quântico que compõe ϵ.

Continuaremos associando a indistinguibilidade à falta de informação para distinguir completamente os estados do ensemble, sendo $S(\rho)$ o SMO para enviar um ensemble de estados quânticos, ou seja, a máxima informação que pode ser distinguível em um ensemble de estados quânticos. Porém, teremos que buscar uma nova referência para subtrair $S(\rho)$, já que, como veremos a seguir, o $H(p_i)$ não é mais uma quantidade de informação suficiente para garantir a distinguibilidade dos elementos que formam um ensemble de estados mistos. No capítulo 3, utilizamos o erro mínimo de Helstrom e o limite de Holevo para justificar a validade de nosso quantificador. Para um ensemble de estados mistos o erro mínimo Helstrom não é valido, já que este é proporcional ao *overlap* de estados quânticos puros, e vamos substituí-lo pela

fidelidade quântica $F(\rho|\rho')$. A qual pode ser escrita como

$$F(\rho|\rho') = \left[Tr\left(\sqrt{\sqrt{\rho'}\rho\sqrt{\rho'}}\right)\right]^2. \tag{4.2}$$

Essa é uma medida de distância geométrica para estados mistos, a qual se reduz ao overlap quando os estados são puros, ou seja, ela é zero quando os estados são distinguíveis e 1 quando são iguais. $F(\rho|\rho')$ pode ser utilizada para indicar a indistinguibilidade entre ρ e ρ'. Então, para um ensemble formado por ρ e ρ', $Ind_M(\rho)$ deve ser proporcional a $F(\rho|\rho')$.

4.1 Distinguibilidade de conjuntos de informações clássicas

Para definir $Ind_M(\rho)$ é necessário determinar o SMO para distinguir sem erro todos os estados quânticos mistos que compõem o ensemble. No capítulo 3 determinamos o SMO para distinguir perfeitamente estados puros considerando que todos os estados quânticos que compõe o ensemble são clássicos, ou seja, equivalem a informações clássicas e por isso distinguíveis. O caminho natural seria propor que os estados quânticos mistos equivalem a conjuntos de informações clássicas, entretanto encontramos um problema: apesar de informações clássicas serem sempre distinguíveis, o mesmo não se pode afirmar para conjuntos de informações clássicas, ou seja, é possível que não possamos distinguir perfeitamente dois ou mais conjuntos de informações clássicas quando é permitido olhar apenas uma informação[1]. Vamos analisar o exemplo abaixo para que isto fique mais claro.

Imagine um jogo entre duas pessoas, Maria e João, que consiste em determinar a que país pertence cada informação anotada em papéis que são escolhidos de forma aleatória. Inicialmente Maria fornece uma lista para João de características de dois países, A e B, cada um contendo três informações, população, clima e área. João memoriza esta lista perfeitamente. Em seguida, Maria anota apenas as informações sobre cada país em papéis coloridos, país A em papel azul e B em papel vermelho, sendo que apenas ela conhece a relação entre a cor e o país, para poder determinar se João ganhou ou não o jogo. Em uma caixa as

[1] É importante lembrar que sempre estamos relacionando o conjunto de informações clássicas com ensemble de estados quânticos e, neste caso, olhar uma única informação clássica equivale a fazer uma única medida.

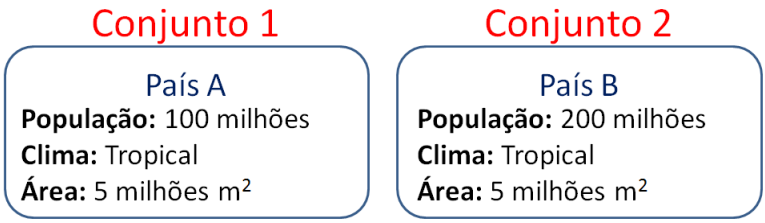

Figura 4.1: Conjunto de informações sobre os países A e B

seis informações são misturadas e João pode pegar apenas uma, falando a que país aquela informação está associada.

João pode distinguir os países utilizando apenas as informações contidas em cada papel. Portanto, João não é capaz de estabelecer relação entre a cor dos papéis e o país. Ao pegar o papel com a informação população igual a 100 milhões, João sabe que se trata do país A. Por outro lado, se as informações forem clima ou área, então, João não terá como distinguir entre os conjuntos 1 e 2, e terá uma chance de erro de 50% na adivinhação do país. O que Maria está fazendo ao usar cores distintas é adicionar uma sistema auxiliar, o que permite responder com certeza de qual país trata as características escritas no papel.

Como estamos interessados em um SMO necessário para distinguir perfeitamente os estados quânticos de um ensemble de estados mistos, precisamos responder a seguinte pergunta. Qual o SMO que permite distinguir perfeitamente dois ou mais conjuntos de informações clássicas SMO_{CC}?

No exemplo anterior vimos que para distinguir conjuntos de informações clássicas sem erro, tendo acesso a apenas uma informação, é necessário que todas as informações de um conjunto sejam diferentes da do outro. Vamos analisar um novo jogo entre Maria e João para determinar o SMO_{CC}.

Neste novo jogo Maria possui duas moedas, 1 e 2, como mostra a Fig. 4.2. A moeda 1 possui cara e coroa que, quando atirada para cima, possui probabilidades $p_1^1 = p_2^1 = 1/2$ de ficar com o lado cara ou coroa voltado para cima. A moeda 2 possui cara nos dois lados e apresenta sempre o mesmo resultado quando lançada para cima. João conhece as moedas e com os olhos vendados pega uma delas, joga para cima girando, tira a venda quando a moeda está sobre o solo e pode ver apenas a face que está virada para cima. De posse desta informação ele deve dizer se pegou a moeda 1 ou 2.

Figura 4.2: Moeda 1 com um lado coroa e outro cara e moeda 2 com os dois lados cara.

Novamente, nesse jogo não é possível garantir que João determine corretamente a moeda lançada, já que as duas moedas apresentam uma informação possível em comum. Repetindo o jogo um grande número de vezes, teríamos o seguinte conjunto de informações C_I, considerando que $p_1 = p_2 = 1/2$ sejam as probabilidades de Maria pegar as moedas 1 e 2:

$$C_I = \frac{3}{4}Cara + \frac{1}{4}Coroa. \tag{4.3}$$

Podemos separar o conjunto de informações dado pela equação 4.3 em duas partes,

$$C_I = \frac{1}{2}\underbrace{\left(\frac{1}{2}Cara + \frac{1}{2}Coroa\right)}_{Moeda\ 1 = Conjunto\ 1} + \frac{1}{2}\underbrace{Cara}_{Moeda\ 2 = Conjunto\ 2}. \tag{4.4}$$

Perceba que os conjuntos 1 e 2 possuem a informação cara em comum, tornando a indistinguibilidade entre os dois diferente de zero.

Queremos agora encontrar uma forma de João distinguir perfeitamente as moedas 1 e 2. A estratégia para distinguir os elementos de um conjunto dos elementos do outro conjunto depende do protocolo. Precisamos encontrar a melhor estratégia, ou seja, a que possui o SMO_{CC}.

Estratégia: Colocar uma marca vermelha no lado cara da moeda 1 conforme Fig. 4.3, vamos chamar esse lado de cara*.

Figura 4.3: Moeda 1 com um lado coroa e outro cara marcado e moeda 2 com os dois lados cara.

Repetindo todo o processo é fácil perceber que João pode discrimar perfeitamente as duas moedas, já que as duas fornecem conjuntos de informações diferentes uma da outra. Vamos montar o conjunto de informações C_I' para muitos jogos,

$$C_I' = \frac{1}{4}Cara^* + \frac{1}{4}Coroa + \frac{1}{2}Cara. \tag{4.5}$$

Separar os conjuntos de informações dado pela equação 4.5 em duas partes,

$$C_I' = \frac{1}{2}\underbrace{\left(\frac{1}{2}Cara^* + \frac{1}{2}Coroa\right)}_{Moeda\ 1 = Conjunto\ 1} + \frac{1}{2}\underbrace{Cara}_{Moeda\ 2 = Conjunto\ 2}. \tag{4.6}$$

Perceba que agora não existem informações coincidentes entre os dois conjuntos e por isso eles são perfeitamente distinguíveis. Vamos utilizar C_I' da equação 4.5 para determinar o SMO_{CC} através da entropia de Shanonn.

$$H(C_I') = -\frac{1}{2}\log_2\frac{1}{2} - 2\frac{1}{4}\log_2\frac{1}{4} = 1,5. \tag{4.7}$$

Isto significa que precisamos de pelo menos $1,5$ *bit* em média para distinguir o conjunto 1 do conjunto 2.

Se calcularmos o SMO para armazenar C_I, dado pela equação 4.3, encontramos

$$H(C_I) = -\frac{3}{4}\log_2\frac{3}{4} - \frac{1}{4}\log_2\frac{1}{4} = 0,81. \tag{4.8}$$

Note que $H(C_I') > H(C_I)$ o que implica que $H(C_I)$ é menor do que o SMO_{CC} que permite discriminar perfeitamente os conjuntos de informações $C1$ e $C2$. Isto ocorre por que os dois conjuntos de C_I possuem

informações iguais e estas são somadas quando montamos a equação 4.3. O fato de somarmos os elementos iguais permite que as informações sejam armazenadas em SMO menor $-\frac{3}{4}\log_2\frac{3}{4} < -\frac{1}{4}\log_2\frac{1}{4} - \frac{1}{2}\log_2\frac{1}{2}$, entretanto, não permite que os conjuntos de informações sejam sempre diferenciados.

Podemos concluir então que conjuntos de informações clássicas são distinguíveis quando as informações de um conjunto são diferentes das dos demais. Este será o análogo que vamos utilizar para determinar a SMO para que dois ou mais estados quânticos mistos sejam distinguíveis.

4.2 *String* médio ótimos para distinguir perfeitamente conjuntos de informações clássicas

Nesta seção vamos definir o SMO_{CC} considerando que todas as informações que constituem os conjuntos são diferentes. Podemos escrever um conjunto de conjuntos de informação clássica da seguinte forma,

$$C_I = \sum_i p_i C_{I_i} \quad (0 \leq p_i \leq 1 \;\; e \;\; \sum_i p_i = 1), \tag{4.9}$$

onde

$$C_{I_i} = \sum_{i,j} p_j^i I_j^i \;\; (0 \leq p_j^i \leq 1 \;\; e \;\; \sum_j p_j^i = 1) \tag{4.10}$$

I_j^i representam informações do conjunto C_{I_i} com probabilidades p_j^i de ocorrer. Sendo $I_j^i \neq I_l^k$ para todos $i \neq k$, condição necessária para determinar o SMO_{CC}, e $p_i p_j^i$ é a probabilidade de obter o elemento j do conjunto i no ensemble total.

Substituindo a equação 4.10 na equação 4.9, temos

$$C_I = \sum_i p_i p_j^{i,j} I_j^i, \tag{4.11}$$

Sendo que SMO_{CC} será dado por $H(C_I)$,

$$\begin{aligned} H(C_I) &= -\sum_{i,j} p_i p_j^i \log_2 p_i p_j^i \\ &= -\left(\sum_{i,j} p_i p_j^i \log_2 p_i + \sum_{i,j} p_i p_j^i \log_2 p_j^i \right) \\ &= -\left(\underbrace{\sum_j p_j^i}_{1} \sum_i p_i \log_2 p_i + \sum_{i,j} p_i p_j^i \log_2 p_j^i \right) \\ &= -\left(\sum_i p_i \log_2 p_i + \sum_{i,j} p_i p_j^i \log_2 p_j \right) \end{aligned} \tag{4.12}$$

$$H(C_I) = -\left(\sum_i p_i \log_2 p_i + \sum_i p_i \sum_{i,j} p_j^i \log_2 p_j^i \right). \tag{4.13}$$

Para interpretar a equação 4.13 vamos reescrevê-la da seguinte forma

$$H(C_I) = \underbrace{-\sum_i p_i \log_2 p_i}_{ParteI} \underbrace{-\sum_i p_i H(C_{I_i})}_{ParteII}. \tag{4.14}$$

SMO_{CC} pode ser dividido em duas partes:

i. Parte I, relacionada com a quantidade de informação associada ao número de C_{I_i} que formam C_I e suas respectivas probabilidades p_i.

ii. Parte II, uma média da quantidade de informações que cada C_{I_i} possui.

Então, para determinar o SMO_{CC} devemos conhecer o número de conjuntos que formam o C_I, com suas respectivas probabilidades, e todas as informações que formam os C_{I_i} também com suas respectivas probabilidades.

4.3 Distinguibilidade de estados quânticos mistos

No capítulo 3 mostramos que estados quânticos puros são distinguíveis quando são ortogonais e, neste caso, são classificados como estados clássicos, já que informações clássicas são distinguíveis, apesar de conjuntos de informações clássicas poderem ser indistinguíveis. Esse resultado foi utilizado para determinar o SMO que distingue perfeitamente estados puros do ensemble, dado por $H(p_i)$. Nesta seção vamos propor de forma equivalente um SMO que distingue perfeitamente estados mistos $\rho = \sum_i p_i \rho_i$ de um ensemble. Entretanto, não podemos simplesmente propor que os estados mistos que compõe o ensemble equivalem a conjuntos de conjuntos de informações clássicas, pois já vimos que conjuntos de informações clássicas podem ter indistinguibilidade diferente de zero. Por isso, vamos propor que os estados mistos equivalem a conjuntos de informações clássicas distinguíveis para determinar o SMO que distingue perfeitamente estados mistos de um ensemble SMO_{QM}. SMO_{QM} é o *string* médio ótimo necessário para distinguir perfeitamente um ensemble de estados quânticos mistos. Podemos entender melhor a proposta analisando o exemplo abaixo.

Neste exemplo vamos criar um análogo quântico para o jogo de João e Maria com a moeda. Jogos quânticos serão jogados por Alice e Bob. Neste novo jogo, no lugar de moedas, Alice vai enviar informações para Bob através de duas fontes de fótons, 1 e 2. A fonte 1 emite sempre fótons com polarização vertical $|0\rangle$, equivalente a moeda que possui apenas cara, e a fonte 2 emite fótons com polarização vertical $|0\rangle$ e horizontal $|1\rangle$, sendo $\langle 0|1\rangle = 0$, com probabilidades $p_1^2 = p_2^2 = 1/2$, equivalente "'a moeda com cara e coroa. Como já foi visto anteriormente, $|0\rangle$ e $|1\rangle$ são estados quânticos classificados como clássicos, já que podem ser distinguidos perfeitamente, então estamos trabalhando apenas com ρ_i de estados clássicos, ou seja, ortogonais. As duas fontes possuem a mesma probabilidade de emitir fótons. Bob recebe um fóton e com uma única medida deve distinguir de que fonte ele veio. Podemos representar o ensemble de estados quânticos enviados por Alice por

$$\rho = \frac{1}{2}(\rho_1 + \rho_2) \ ,$$

sendo

$$\rho_1 = |0\rangle \langle 0| \tag{4.15}$$

o estado quântico enviado pela fonte 1 e

$$\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{4.16}$$

o estado quântico enviado pela fonte 2. A $F(\rho_1|\rho_2) = 1/2$, o que significa que os dois estados não são distinguíveis perfeitamente.

Tanto Alice quanto Bob conhecem os ensembles que formam ρ_1 e ρ_2. Então, Alice envia um fóton para Bob e ele utiliza medidas projetivas na base $|0\rangle, |1\rangle$ para determinar de que fonte de fótons ele foi emitido. É importante enfatizar que o máximo que Bob pode fazer é tentar determinar qual estado do fóton que ele está recebendo e assim descobrir de qual ρ_i ele faz parte. Os resultados possíveis de Bob são:

i. Mede $|0\rangle$ e conclui que faz parte de estado ρ_1.

ii. Mede $|0\rangle$ e conclui que faz parte de estado ρ_2.

iii. Mede $|1\rangle$ e conclui que faz parte de estado ρ_2.

Fazendo apenas uma análise qualitativa, vamos supor que Bob nunca opte por escolher ρ_2 quando o resultado for $|0\rangle$, já que ele sabe que é duas vezes mais provável que ele pertença ao estado ρ_1, e sempre opte por ρ_2 quando o resultado for $|1\rangle$. Desta forma ele erra em média 25% das vezes. Este erro surge por uma falta de conhecimento, ou incerteza clássica, do estado enviado pela fonte de fótons 2, equivalente à moeda que possui os lados cara e coroa. Perceba que neste exemplo não existe uma superposição quântica entre os estados medidos por Bob; é importante lembrar que esta superposição era a responsável pela indistinguibilidade do capítulo 3. Aqui Bob nunca tem dúvida sobre sua medida, ou seja, se está medindo o $|0\rangle$ ou $|1\rangle$, entretanto os estados ρ_1 e ρ_2 não podem ser distinguidos perfeitamente por possuírem estados quânticos iguais.

Para que Bob sempre distinguisse perfeitamente o estado enviado por Alice, ela poderia colocar uma marca nos estados enviados pela fonte de fótons 2, equivalente a marca da moeda do jogo de João e Maria. Vamos supor que esta marca é equivalente a Alice utilizar outro parâmetro quântico para os fótons que tivesse autoestados $|0\rangle$, $|1\rangle$ e $|2\rangle$, sendo

$$\rho_1 = |0\rangle\langle 0| \quad \text{e}$$

$$\rho_2 = \frac{1}{2}(|1\rangle\langle 1| + |2\rangle\langle 2|).$$

Neste caso a $F(\rho_1|\rho_2) = 0$ e Bob poderia distinguir perfeitamente o estado que ele recebe, bastava para isso utilizar medidas projetivas na base $\{|0\rangle, |1\rangle, |2\rangle\}$.

Podemos estabelecer então que para distinguir perfeitamente dois estados mistos ρ_i não basta que os estados que compõem cada ρ_i sejam clássicos; é necessário que todos os estados que compõe ρ_1 sejam perfeitamente distinguíveis dos estados que compõem ρ_2, para isso os estados que compõem ρ_1 devem ser ortogonais aos de ρ_2. Essa condição de distinguibilidade nos permite estabelecer SMO_{QM}.

4.4 *String* médio ótimo para distinguir perfeitamente estados quânticos mistos

Nesta seção vamos discutir que forma deve assumir o SMO_{QM}, o qual será utilizado na primeira versão da equação do $Ind_M(\rho)$. O leitor pode pular para a próxima seção e ver diretamente a equação $Ind_M(\rho)$ na sua versão final 4.33, entretanto acreditamos que esta seção é importante para a compreensão do raciocínio que levou a equação final.

Para propor a primeira versão do SMO_{QM}, do qual deve ser subtraído o $S(\rho)$ para determinar a $Ind_M(\rho)$, vamos assumir um ensemble de estados mistos dado por

$$\rho = \sum_i p_i \rho_i, \tag{4.17}$$

sendo

$$\rho_i = \sum_j p_j^i |\psi_j^i\rangle\langle\psi_j^i|, \tag{4.18}$$

onde conhecemos todos estados quânticos puros que compõe ρ_i. Tal conhecimento nos permite executar o seguinte protocolo para determinar SMO_{QM}:

i. Considerar que os estados quânticos puros que compõem os ρ_i são classificados como clássicos e que os estados que compõem ρ_i são ortogonais aos que compõem ρ_j para todo $i \neq j$, condição que permite distinguir perfeitamente os ρ_i.

ii. Reescrever o ρ na base dos estados puros $|\psi_j^i\rangle$ que fazem parte de todos ρ_i, considerando-os estados clássicos, ou seja,$\langle\psi_k^l|\psi_j^m\rangle =$

$\delta_{kj}\delta_{lm}$. Vamos chamar esse novo ρ de operador densidade distinguível ρ_D,

$$\rho_D = \sum_{i,j} p_i p_j^i |\psi_j^i\rangle\langle\psi_j^i|. \tag{4.19}$$

iii. Considerar que os ρ_i são conjuntos de informações clássicas completamente distinguíveis, desta forma vamos inicialmente propor que SMO_{QM} será dado pelo SMO_{CC} através da equação 4.13. A partir de agora vamos chamar $H(C_I)$, fornecido pela equação 4.13, de $H(\rho_D)$.

Temos assim a primeira versão da equação $Ind_M(\rho)$,

$$Ind_M(\rho) = H(\rho_D) - S(\rho). \tag{4.20}$$

Vamos aplicar a primeira versão do quantificador dado pela equação 4.20 para o exemplo abaixo e analisar os resultados. O ensemble de estados mistos é dado por

$$\rho = \frac{1}{2}\left(\rho_1 + \rho_2\right), \tag{4.21}$$

em que

$$\rho_1 = |\psi_1\rangle\langle\psi_1| \quad e \tag{4.22}$$

$$\rho_2 = p|\psi_2\rangle\langle\psi_2| + (1-p)|\psi_3\rangle\langle\psi_3|, \quad (0 \leq p \leq 1), \tag{4.23}$$

sendo

$$|\psi_1\rangle = |0\rangle \quad , \quad |\psi_2\rangle = |1\rangle \quad \text{e} \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

O primeiro passo é determinar $H(\rho_D)$. Para isso $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ são considerados ortogonais.

$$H(\rho_D) = 1 + \frac{1}{2}\left[-p\log_2 p - (1-p)\log_2(1-p)\right]. \tag{4.24}$$

Em seguida, para determinar $Ind_M(\rho)$ é necessário determinar o SMO para o ensemble, dado por $S(\rho)$. Vamos escrever ρ na sua forma diagonal,

$$\rho_{Diag} = \begin{pmatrix} \frac{1}{4}\left(2-(1-p)\sqrt{2}\right) & 0 \\ 0 & \frac{1}{4}\left(2+(1-p)\sqrt{2}\right) \end{pmatrix}. \tag{4.25}$$

Com os termos da diagonal de 4.25 determinamos $S(\rho)$,

$$\begin{aligned} S\left(\rho\right) = &-\frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\log_2\left(\frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\right) + \\ &-\frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\log_2\left(\frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\right). \end{aligned} \tag{4.26}$$

A $Ind_M(\rho)$ será dada pela subtração dos resultados das equações 4.24 e 4.26.

$$\begin{aligned} Ind_M(\rho) = 1 &+ \frac{1}{2}\left[-p\log_2 p - (1-p)\log_2(1-p)\right] + \\ &+ \frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\log_2\left(\frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\right) + \\ &+ \frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\log_2\left(\frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\right). \end{aligned} \tag{4.27}$$

Uma primeira análise do nosso novo quantificador $Ind_M(\rho)$ pode ser feita comparando o resultado da equação 4.27 com o limite de Holevo. Para isso vamos determinar o χ de Holevo 2.29. É necessário antes calcular $S(\rho_1)$ e $S(\rho_2)$.

Como $S(\rho_1)$ vale zero, já que ρ_1 é um estado puro, determinamos apenas $S(\rho_2)$, onde ρ_2 está escrito na forma diagonal,

$$\rho_{2_{Diag}} = \begin{pmatrix} \frac{1}{2}\left(1-\sqrt{2p^2-2p+1}\right) & 0 \\ 0 & \frac{1}{2}\left(1+\sqrt{2p^2-2p+1}\right) \end{pmatrix}.$$

Portanto,

$$\begin{aligned} S(\rho_2) = &-\frac{1}{2}\left(1-\sqrt{2p^2-2p+1}\right)\log_2\left(\frac{1}{2}\left(1-\sqrt{2p^2-2p+1}\right)\right) + \\ &-\frac{1}{2}\left(1+\sqrt{2p^2-2p+1}\right)\log_2\left(\frac{1}{2}\left(1+\sqrt{2p^2-2p+1}\right)\right). \end{aligned} \tag{4.28}$$

O χ de Holevo é dado por

$$\begin{aligned} \chi(\rho) = &-\frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\log_2\left[\frac{1}{4}\left(2-(1-p)\sqrt{2}\right)\right] + \\ &-\frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\log_2\left[\frac{1}{4}\left(2+(1-p)\sqrt{2}\right)\right] + \\ &+\frac{1}{2}\left(1-\sqrt{2p^2-2p+1}\right)\log_2\left[\frac{1}{2}\left(1-\sqrt{2p^2-2p+1}\right)\right] \\ &+\frac{1}{2}\left(1+\sqrt{2p^2-2p+1}\right)\log_2\left[\frac{1}{2}\left(1+\sqrt{2p^2-2p+1}\right)\right]. \end{aligned} \tag{4.29}$$

O gráfico abaixo fornece a relação entre a indistinguibilidade $Ind_M(\rho)$ e o χ de Holevo, dados pelas equações 4.27 e 4.29, como função de p.

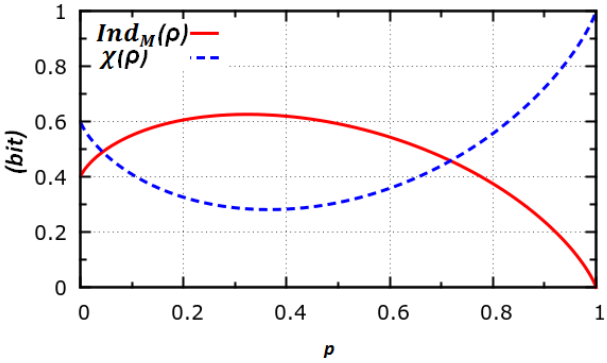

Figura 4.4: Relação entre $Ind_M(\rho)$ e χ de Holevo em função de p.

O comportamento de $Ind_M(\rho)$ é o esperado, já que o valor de $Ind_M(\rho)$ varia inversamente com o χ, que representa a máxima informação acessível dos elementos de um conjunto através de uma medida. Essa mesma relação foi encontrada para conjuntos de estados puros vistos anteriormente no capítulo 3 em que o SMO para distinguir sem erros os estados de um ensemble era $H(p_i)$. Ainda neste exemplo é interessante analisar o valor de $Ind_M(\rho)$ para $p = 0$ e $p = 1$, em que o conjunto volta a ter apenas estados puros e $Ind_M(\rho)$ apresenta os mesmo valores do $Ind(\rho)$ proposto no capítulo 3. Com $p = 1$ os dois estados são ortogonais e $Ind_M(\rho) = 0$, já com $p = 0$ retornamos ao exemplo 3.4, proposto no início do capítulo 03, com $\alpha = \frac{\sqrt{2}}{2}$, onde $Ind_M(\rho) = Ind(\rho) \approx 0,40$.

Até o momento conseguimos encontrar uma equação para um novo quantificador de indistinguibilidade $Ind_M(\rho)$ de um ensemble com estados mistos. Este novo quantificador é baseado em um protocolo que define a informação necessária para distinguir os estados do ensemble $H(\rho_D)$. O problema deste protocolo é que fica condicionado ao conhecimento dos estados quânticos puros que formam os estados mistos ρ_i e isso nem sempre é possível. Na maioria das vezes o máximo que podemos ter de informação é a matriz densidade que representa o ensemble que é o estado misto. Lembrando que existe a liberdade do ensemble [1], em que ensembles diferentes podem ser representados pelos mesmo operador densidade, muitas vezes é impossível conhecer os estados quânticos que formam o ensemble a partir da matriz densidade, muito menos garantir que os estados quânticos mistos são formados

por estados puros. Um exemplo disso foi visto no capítulo 3, em que os dois ensembles 3.1 e 3.2 são representados pela mesma matriz densidade. Portanto, apesar de aparentemente ter um bom comportamento, o $Ind_M(\rho)$ proposto até o momento, tem sua aplicação limitada. Para que o quantificador proposto não seja restrito, desejamos construir um $Ind_M(\rho)$ que dependa apenas do conhecimento da matriz densidade ρ_i que representa cada estado quântico misto que compõe o ensemble ϵ, dado por ρ.

4.5 Quantificador de indistinguibilidade para um ensemble de estados mistos

Se analisarmos a equação 4.20 para quantificar indistinguibilidade de um ensemble de estados mistos, podemos percerber que apenas o termo $p_i H(p_j^i)$ de $H(\rho_D)$, necessita do conhecimento dos estados que compõe o ρ_i para ser calculado. Devemos então propor um substituto para $p_i H(p_j^i)$ que dependa apenas do conhecimento da matriz densidade que representa ρ_i para que $Ind_M(\rho)$ se torne mais geral.

A hipótese para o substituto de $p_i H(p_j^i)$ surge da análise do gráfico da figura 4.4. Na figura nota-se que $Ind_M(\rho)$é proporcional à $H(p_i)$ menos o χ de Holevo. Desta forma $H(p_i) + \sum_i p_i H(p_j^i)$ deve ter o mesmo comportamento de $H(p_i) + \sum_i p_i S(\rho_i)$, para ρ da equação 4.21. Podemos comparar estes resultados com o gráfico 4.5.

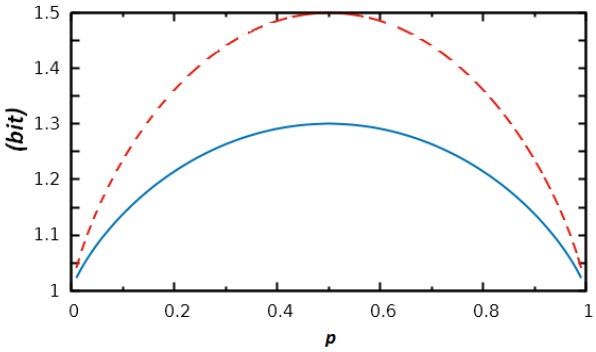

Figura 4.5: Linha laranja tracejada $H(p_i) + \sum_i p_i H(p_j^i)$ e a contínua representa $H(p_i) + \sum_i p_i S(\rho_i)$

Na figura 4.5 observamos que o nosso parâmetro $H(\rho_D)$ possui mais informação do que $H(p_i) + \sum_i p_i S(\rho_i)$, embora as duas quantidades tenham o mesmo comportamento. A nossa hipótese é que $H(\rho_D)$ contenha mais informação do que o necessário para distinguir todos os ρ_i de ρ. Reavaliando o protocolo utilizado para criar $H(\rho_D)$, estabelecemos que para distinguir perfeitamente os estados mistos exigimos que todos os estados puros que compõe ρ_i fossem ortogonais entre si. Entretanto, isto obviamente é mais do que o necessário. Podemos verificar isso com um exemplo simples.

Alice novamente lança fótons para Bob provenientes de duas fontes. Agora a fonte 1 emite apenas fótons no estado $|2\rangle$ e a fonte 2 fótons nos estados $|0\rangle$ e $|+\rangle$, dado pela equação 1.3. Sendo $\langle 0|1\rangle = \langle 0|2\rangle = \langle 1|2\rangle = 0$, é facil perceber que Bob pode distinguir a fonte da qual foi emitida o fóton apenas fazendo medidas projetivas na base $\{|0\rangle, |1\rangle, |2\rangle\}$. Sempre que o resultado for $|2\rangle$ o fóton foi emitido pela fonte 1 e para qualquer outro resultado o fóton foi emitido pela fonte 2. Portanto, para distinguir perfeitamente estados mistos, não precisamos que os estados quânticos que formam ρ_i sejam ortogonais entre si, mas apenas que os estados que formam ρ_i sejam ortogonais aos que formam ρ_j, para todo $i \neq j$. Tal propriedade é garantida fazendo-se $F(\rho_i|\rho_j) = 0$ para $i \neq j$,

Podemos propor então que o SMO_{QM} é dado por:

$$H(\rho_D) = H(p_i) + \sum_i p_i S(\rho_i). \tag{4.30}$$

Note que a informação média sobre os elementos de ρ_i é dada por $\sum_i p_i S(\rho_i)$, é geralmente menor do que $\sum_i p_i H(p_j^i)$. Isto implica em um resultado curioso, geralmente é necessário menos informação para distinguir perfeitamente dois estados quânticos mistos formados por estados puros, dado pelo SMO_{QM}, do que dois conjuntos de informações clássicas com os mesmo números de elementos e suas respectivas probabilidades, dado por SMO_{CC}. Este resultado não aparece quando tratamos a indistinguibilidade de N estados puros com probabilidades p_i, para eles o SMO para distingui-los perfeitamente é igual ao SMO de N informações clássicas com as respectivas probabilidades.

Se substituirmos a equação 4.30 na equação 4.20, chegamos a uma nova equação de $Ind(\rho)$,

$$Ind_M(\rho) = \left[H(p_i) + \sum_i p_i S(\rho_i) \right] - S(\rho). \tag{4.31}$$

Podemos reescrever $Ind(\rho)$ rearranjando os termos da equação 4.31,

$$Ind_M(\rho) = H(p_i) - \left[S(\rho) - \sum_i p_i S(\rho_i) \right]. \tag{4.32}$$

Substituindo na equação 4.32 a equação 2.29 chegamos a equação final para indistinguibilidade de estados mistos,

$$Ind_M(\rho) = H(\rho) - \chi(\rho). \tag{4.33}$$

Sendo,

$$\rho = \sum_i p_i \rho_i \;\; e \;\; H(\rho) = H(p_i).$$

Observe que a equação 4.33 depende apenas do conhecimento das matrizes densidade que representam os estados mistos e dos p_i. Este resultado é fundamental para este tipo de quantificador, permitindo generalizar sua aplicação.

É fácil perceber que para um ensemble de estados puros o $\chi(\rho)$ será apenas $S(\rho)$, voltando ao quantificador proposto no capítulo 3, equação 3.6. Esse resultado é importante para viabilizar $Ind_M(\rho)$, da equação 4.33, como quantificador de indistinguibilidade global para qualquer ensemble de $N \geq 2$ estados quânticos puros ou mistos, e por isso $Ind_M(\rho)$ será a partir de agora apenas chamado de $Ind(\rho)$. Entretanto, fica a tarefa de interpretar os termos da equação 4.33 da mesma forma que foi interpretada a equação 3.6.

Podemos de interpretar o $Ind(\rho)$ a partir da equação 4.31. Para isso vamos dividir a equação em duas partes,

$$Ind(\rho) = \underbrace{\left[H(p_i) + \sum_i p_i S(\rho_i) \right]}_{I} - \underbrace{S(\rho)}_{II}. \tag{4.34}$$

A parte I quantifica a informação mínima necessária para distinguir os estados quânticos do ensemble, podendo ser dividida ainda em mais duas partes.

i. $H(p_i)$ é o SMO para representar os conjuntos que existem no ensemble, desde que cada um seja tratado como estado perfeitamente distinguível.

ii. $\sum_i p_i S(\rho_i)$ é a média da informação mínima necessária de cada estado misto. Este termo da equação é zero quando o ensemble possui apenas estados puros.

iii. Abrindo a expressão da parte I de $Ind(\rho)$, dada pela equação 4.34, encontramos o termo $p_i[-log_2 p_i + S(\rho_i)]$, este termo pode ser interpretado como a quantidade de informação mínima de cada ρ_i para eles sejam distinguíveis no ensemble.

A parte II, em que temos apenas $S(\rho)$, continua sendo interpretada como SMO ótimo para enviar um ensemble de estados quânticos. Esta forma de interpretar $Ind(\rho)$ está diretamente relacionada com a interpretação do χ de Holevo, onde o termo $\sum_i p_i S(\rho_i)$ representa uma falta de informação que diminui a capacidade de um canal quântico.

4.6 Relação entre as equações para distinguibilidade de um ensemble de estados mistos

A equação para $Ind(\rho)$ dado pela equação 4.33, proposta na seção anterior, se mostrou mais geral do que aquela dada pela equação 4.20. Agora vamos demonstrar que a equação dada por 4.33 é a forma correta de determinar a indistinguibilidade média de um ensemble de estados quânticos mistos.

Para isso vamos retornar ao exemplo em que Alice vai enviar informações para Bob através de duas fontes de fótons, 1 e 2. A fonte 1 emite sempre fótons com polarização vertical $|0\rangle$ e a fonte 2 emite fótons com polarização $|+\rangle$ e horizontal $|1\rangle$, sendo $\langle 0|1\rangle = 0$ e o estado $|+\rangle$ dado pela equação 1.3. Bob deve distinguir de que fonte é o fóton que está recebendo. A única diferença para o exemplo citado anteriormente é que agora a fonte 1 emite fótons com probabilidade p e a fonte 2 com probabilidade $(1-p)$. Temos que

$$\rho = p\ \rho_1 + (1-p)\rho_2\ \ , (0 \leq p \leq 1)\ \ , \tag{4.35}$$

sendo

$$\rho_1 = |0\rangle\langle 0| \tag{4.36}$$

o estado quântico enviado pela fonte 1 e

$$\rho_2 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|1\rangle\langle 1| \tag{4.37}$$

o estado quântico enviado pela fonte 2.

Estamos interessados apenas nos valores de p iguais a 0 e 1, para esses dois valores $Ind(\rho)$ deve ser igual a zero, já que temos apenas um estado no ensemble.

Para $p = 1$ temos $H(p_i) = 0$, $S(\rho) = 0$, $H(p_j^1) = H(p_j^2) = 0$ e $S(\rho_1) = S(\rho_2) = 0$, então a $Ind(\rho)$ dada pelas equações 4.20 e 4.33 vale zero, que é o resultado esperado.

Para $p = 0$ temos $H(p_i) = 0$, $S(\rho) = 0,6$, $H(p_j^1) = 0$, $H(p_j^2) = 1$, $S(\rho_1) = 0$ e $S(\rho_2) = 0,60$, neste caso o $Ind(\rho)$ dado pela equação 4.20 será

$$Ind(\rho) = H(p_i) + \sum_{i,j} p_i H(p_j^i) - S(\rho) = 0,4, \tag{4.38}$$

demonstrando que a equação 4.20 não pode ser utilizada para quantificar indistinguibilidade. Já para equação 4.33

$$Ind(\rho) = H(p_i) + \sum_{i} p_i S(\rho_i) - S(\rho) = 0, \tag{4.39}$$

que é o resultado esperado para indistinguibilidade neste caso.

4.7 Indistinguibilidade do Estado de Werner

Para finalizar este capítulo vamos encontrar a indistinguibilidade do estado de Werner com a equação 4.33. O propósito aqui é apenas didático. O estado de Werner é um ensemble de dois estados mistos bipartidos AB,

$$\rho_W = (1-p)\underbrace{\frac{\hat{\mathbb{1}}_{AB}}{4}}_{\rho_1} + p\underbrace{\left|\psi_{AB}^-\right\rangle\left\langle\psi_{AB}^-\right|}_{\rho_2} \ (0 \leq p \leq 1), \tag{4.40}$$

sendo

$$\left|\psi_{AB}^-\right\rangle = \frac{|01\rangle - |01\rangle}{\sqrt{2}}. \tag{4.41}$$

Este estado é um exemplo interessante, pois viola o critério de Peres-Horodecki [35,36] para $p \geq 1/3$, ou seja, para $p \geq 1/3$ é não separável e por isso emaranhado. Não existe o objetivo de $Ind(\rho)$ assinalar emaranhamento, apenas estamos curiosos sobre o comportamento do quantificador para esse estado.

Para determinar $Ind(\rho)$ vamos inicialmente determinar o $H(p_i)$. Como ele depende apenas das probabilidades de aparecem ρ_1 e ρ_2 no ensemble, temos

$$H(\rho_W) = -(1-p)\log_2(1-p) - p\log_2 p. \tag{4.42}$$

O próximo passo é diagonalizar ρ_W e encontrar $S(\rho_W)$, ou seja,

$$\rho_{W_{Diag}} = \begin{pmatrix} \frac{3p+1}{4} & 0 & 0 & 0 \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ 0 & 0 & 0 & \frac{1-p}{4} \end{pmatrix}, \tag{4.43}$$

o que fornece

$$S(\rho_W) = -\frac{3p+1}{4}\log_2(\frac{3p+1}{4}) - 3\frac{1-p}{4}\log_2(\frac{1-p}{4}). \tag{4.44}$$

Como o estado de Werner é um ensemble de estados mistos, é necessário determinar o $S(\rho_i)$. Para ρ_2 $S(\rho_2) = 0$, pois este é um estado puro. Já para o ρ_1, com quatro autovalores iguais a $1/4$, $S(\rho_1) = 2$.
Podemos agora determinar o $Ind(\rho_W)$ utilizando a equação 4.33, como

$$\begin{aligned} Ind(\rho_W) &= H(\rho_W) - \chi(\rho_W) \\ &= H(\rho_W) - \left\{ S(\rho_W) - \left[(1-p)S(\rho_1) + p\overbrace{S(\rho_2)}^{0} \right] \right\} \\ &= -p\log_2 p - (1-p)\log_2(1-p) \\ &\quad - \left[-3\frac{1-p}{4}\log_2\left(\frac{1-p}{4}\right) - \frac{3p+1}{4}\log_2(\frac{3p+1}{4}) - 2(1-p) \right]. \end{aligned} \tag{4.45}$$

O gráfico abaixo fornece o valor de $Ind(\rho)$ em função de p.

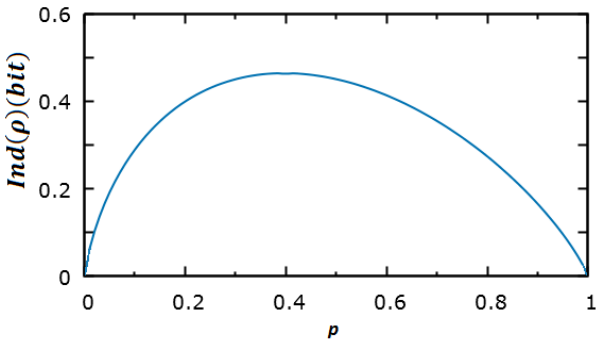

Figura 4.6: $Ind(\rho)$ para o estado de Werner como função de p.

Analisando o gráfico 4.6 observamos que a indistinguibilidade parte de zero, quando $p = 0$, onde existe um único estado, aumenta até $p = 0,4$ e volta a diminuir até chegar a zero, quando $p = 1$, onde novamente existe um único estado.

Este exemplo mostra que o quantificador para indistinguibilidade global, proposto nesta dissertação, pode ser aplicado em casos com ensemble de estados emaranhados. Entretanto fica faltando um entendimento de como aplicar esse quantificador para uma indistinguibilidade local, que seria mais interessante para esse tipo de problema.

Capítulo 5

Conclusões e perspectivas futuras

Neste trabalho construímos um quantificador de indistinguibilidade representado por $Ind(\rho)$. Tal quantificador é uma medida entrópica que determina a quantidade de informação média que falta para distinguir perfeitamente os estados quânticos de um ensemble. Nesse sentido, para saber quão indistinguíveis são os estados de um ensemble entre si, é necessário primeiramente conhecer o quanto eles são distinguíveis, dado pelo χ de Holevo, e o string média ótima que descreve o ensemble tratando os seus estados como completamente distinguíveis entre si.

Demonstramos que a $Ind(\rho)$ variou monotonicamente com erro mínimo de Helstrom em ensembles com dois estados quânticos e com o χ de Holevo, sendo este último utilizado para medir distinguibilidade de um sistema quântico. O quantificador se mostrou uma ferramenta prática, já que ele não necessita de extremização ou minimização, o que diminui significativamente a complexidade de sua aplicação em problemas envolvendo ensembles com muitos estados quânticos.

Generalizamos a equação $Ind(\rho)$ permitindo que ela fosse válida para ensembles de estados puros ou mistos. Observamos que o termo $S(\rho_i)$, que aparece no χ de Holevo, pode ser interpretado como o mínimo de informação necessário de cada ρ_i, em um ensemble de estados mistos, que deve ser somado a $H(\rho)$ para distingui-los perfeitamente um dos outros. Isso permite interpretar $\sum_i p_i S(\rho_i)$ como uma falta de informação média dos estados, que diminui o acesso a informação sobre o ensemble.

Uma forma de ver isto é lembrar o cálculo da indistinguibilidade

para estados puros. Neste caso o χ de Holevo se reduz a $S(\rho)$, sendo esta a quantidade subtraída de $H(p_i)$ para determinar o quanto falta de informação para que possamos distinguir completamente os elementos do ensemble. Para estados mistos, o $\sum_i p_i S(\rho_i)$ é subtraído de $S(\rho)$, e só então o restante é subtraído do $H(p_i)$ para determinar o quanto falta de informação para distinguir perfeitamente os estados. Nos dois casos $S(\rho)$ é o SMO necessário para enviar um ensemble de estados quânticos, entretanto, para um ensemble de estados mistos, o $S(\rho_i)$ representa uma informação a mais que está escondida dentro de cada ρ_i, que dificulta ainda mais a discriminação perfeita do estados do sistema.

Um resultado curioso, que não nos parece intuitivo, é que a quantidade de informação média mínima necessária para discriminar perfeitamente dois ensembles de estados quânticos[1] é sempre menor que ou igual à quantidade de informação média mínima necessária para discriminar perfeitamente dois conjuntos clássicos. Porém, até o momento, não encontrarmos uma aplicação prática para envios de mensagens através de estados quânticos mistos.

É importante salientar que o quantificador proposto não foi obtido através de uma dedução matemática rigorosa, embora satisfizesse bem os critérios desejados.

Como perspectivas futuras desse trabalho, propomos: descobrir protocolos de computação e comunicação quântica que utilizem os quantificadores de indistinguibilidade propostos como algum tipo de parâmetro; comparar os quantificadores de indistinguibilidade com quantificadores de correlações quânticas que funcionam como recurso computacional; criar uma versão do $Ind(\rho)$ para indistinguibilidade local.

[1] Estados mistos.

Bibliografia

[1] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 10th ed, **ISBN**: 9781107002173 (2011).

[2] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society A **400**, 1818 (1985).

[3] P. W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring in Proceedings of 35th Annual Symposium of Foundations of Computer Science*, IEEE Press, Los Alamitos, CA, (1994).

[4] L. K. Grover, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, Phys. Rev. Lett. **79**, 325 (1997).

[5] C. E. Shannon, *A mathematical theory of communications*, Bell Systems Technical Journal **27**, 379-423, 623-656 (1948).

[6] B. Schumacher, *Quantum coding*, Phys. Rev. A **51**, 2738 (1995).

[7] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, **ISBN** 978-0691028934, Princeton University Press (1996).

[8] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, In Proceedings of IEEE International Conference on Computers, Systems and Signal Precessing, 175-179, IEEE, New York, (1984).

[9] J. A. Bergou, U. Futschik, E. Feldman. *Optimal Unambiguous Discrimination of Pure Quantum States*, Phys. Rev. Lett. **108**, 250502 (2012).

[10] C. M. R. Ruiz, *O papel das correlações não clássicas e interações coerentes no protocolo de discriminação não ambígua de estados quânticos*, Universidade Federal do ABC, Dissertação (Mestrado em Física), (2014).

[11] W. R. M. Rabelo, *Algoritmos para a Informação Quântica: Discriminação de Estados Quânticos e Modelo Híbrido*, Universidade Federal de Minas Gerais, Tese (Doutorado em Física), (2006).

[12] J. Bergou, U. Herzog, M. Hillery, *Discrimination of Quantum States* Lect. Notes Phys. pp 417, **ISBN** 978-3-540-44481-7, Springer (2004).

[13] W. Wootters, W. Zurek, *A Single Quantum Cannot be Cloned*, Nature **299**, 802 (1982).

[14] M. Gross, S. Haroche, *Superradiance: An Essay on the Theory of Collective Spontaneous Emission*, Phys. Rev. Lett **93**, 301–396 (1982).

[15] P. H. Moryia, *Manipulação do Pulso Superradiante Via Interações Atômicas*, Universidade Federal de São Carlos, Dissertação (Mestrado em Física), (2012).

[16] C. W. Helstrom, *Quantum Detection and Estimation Theory*, **ISBN** 978-0124110113, Academic Press (1976).

[17] G. Jaeger, A. Shimony, *Optimal distinction between two non-orthogonal quantum states*, Phys. Lett. A **197**, 83 (1995).

[18] A. Chefles, *Quantum state discrimination*, Contemporary Physics **41**, Issue 6, 401-424 (2000).

[19] J. J. Sakurai and Jim J. Napolitano, *Modern Quantum Mechanics* 2nd edition, **ISBN** 978-0805382914, Addison-Wesley (2010).

[20] S. Barnett. *Quantum Information*, **ISBN** 978-0198527633, Oxford Master Series in Physics (2009).

[21] R. Jozsa, J. Schlienz. *Distinguishability of states and von Neumann entropy*, Phys. Rev. A **62**, 012301 (2000).

[22] A. Peres, *How to Differentiate Between Non-Orthogonal States*, Phys. Lett. A **128**, 19 (1988).

[23] I.D. Ivanovic, *How to Differentiate Between Non-Orthogonal States*, Phys. Lett. A **123** 257 (1987).

[24] J. O. C. Pineda, *A entropia segundo Claude Shannon: o desenvolvimento do conceito fundamental da teoria da informação*, Pontifícia Universidade Católica, Dissertação (Mestrado em Física), (2006).

[25] J. Maziero, *Entendendo a entropia de von Neumann*, Rev. Bras. Ens. Fis. **37**, 1806 (2015).

[26] R. V. L. Hartley, *Transmission of Information*, Bell System Technical Journal **7**, 535 (1928).

[27] A. R. Artuso, *Entropias de Shanonn e Rényi Aplicadas ao Reconhecimento de Padrões*, Revista CIATEC-UPF **3**, 56 (2011).

[28] E. T. Jaynes, *Information Theory and Statistical Mechanics*, Physical Review **106**, 620 (1957).

[29] D. Yang, *Distinguishability, classical information of quantum operations*, arXiv:quant-ph/0504073v1 (2005).

[30] A. S. Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel*, Probl. Peredachi Inf. **9**, 177 (1973).

[31] A. S. Holevo. *Reliability Function of General Classical-Quantum Channel* arXiv:quant-ph/9907087v2 (2000).

[32] J. Tyson, *Two-sided estimates of minimum-error distinguishability of mixed quantum states via generalized Holevo-Curlander bounds*, J. Math. Phys. **50**, 032106 (2009).

[33] M. Dall'Arno, *A Hierarchy of Bounds on Accessible Information and Informational Power* arXiv:1504.04429 (2015).

[34] N. D. Pozza, G. Pierobon, *On the Optimality of Square Root Measurements in Quantum State Discrimination*, Phys. Rev. A **91**, 042334 (2015).

[35] A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett. **77**, 19113 (1996).

[36] M. Horodecki, P. Horodecki e R. Horodecki, *Separability of mixed states: Necessary and sufficient conditions*, Phys. Lett. A **223**, 1 (1996).

[37] M. Paris , J. Rehacek, *Quantum State Estimation*, **ISBN** 978-3-540-22329-0, Springer (2004).

[38] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, *Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels*, Phys. Rev. Lett **70**, 1895–1899 (1993).

[39] Michał Horodecki, Aditi Sen(De), Ujjwal Sen, and Karol Horodecki, *Local Indistinguishability: More Nonlocality with Less Entanglement*, Phys. Rev. Lett **90**, 4 301–396 (1982).

[40] Teng Ma, Ming-Jing Zhao, Yao-Kun Wang, Shao-Ming Fei *Non-commutativity and Local Indistinguishability of Quantum States*, Scientific Reports **4**, 6336 (2003).