UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE FÍSICA

CURSO DE GRADUAÇÃO EM FÍSICA

WAGNER COELHO NORMANDO FILHO

SOBRE A SEGURANÇA EM CANAIS QUÂNTICOS BIPARTIDOS VIA TAXA DE CHAVE

FORTALEZA

2022

WAGNER COELHO NORMANDO FILHO

SOBRE A SEGURANÇA EM CANAIS QUÂNTICOS BIPARTIDOS VIA TAXA DE CHAVE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Física do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Física.

Orientador: Prof. Dr. Raimundo Nogueira da Costa Filho

Coorientador: Prof. Dr. Valber da Silva Gomes

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

N765s Normando Filho, Wagner Coelho.
Sobre a segurança em canais quânticos bipartidos via taxa de chave / Wagner Coelho Normando Filho. – 2022.
60 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Centro de Ciências, Curso de Física, Fortaleza, 2022.
Orientação: Prof. Dr. Raimundo Nogueira da Costa Filho.
Coorientação: Prof. Dr. Valber da Silva Gomes.

1. Mecânica Quântica. 2. Teoria da Informação Quântica. 3. Distribuição de Chaves Quânticas. 4. Criptografia. I. Título.

CDD 530

WAGNER COELHO NORMANDO FILHO

SOBRE A SEGURANÇA EM CANAIS QUÂNTICOS BIPARTIDOS VIA TAXA DE CHAVE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Física do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Física.

Aprovada em 12/07/2022.

BANCA EXAMINADORA

Prof. Dr. Raimundo Nogueira da Costa Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Ramos Gonçalves
Universidade Federal do Ceará (UFC)

Profa. Dra. Hilma Helena Macedo de Vasconcelos
Universidade Federal do Ceará (UFC)

Aos dois zeros que eu tirei em física no colégio.

AGRADECIMENTOS

Gostaria de agradecer primeiramente aos meus pais, que nunca desistiriam de incentivar os meus estudos e de acreditar em mim. Sem o apoio deles eu não teria conseguido atingir meus objetivos.

A Bruna Lorena, minha namorada, por todo o amor, paciência e principalmente compreensão durante todo esse período da minha graduação.

Ao Prof. Dr. Raimundo Nogueira por ter aceitado ser meu orientador de TCC e pelas reuniões todas as terças feiras sobre Mecânica Quântica. Sem dúvidas, esses encontros me ajudaram a entender melhor a natureza da teoria e me incentivaram ainda mais a ser um pesquisador.

Ao Dr. Valber da Silva, por toda a paciência em responder minhas dúvidas durante a escrita desse trabalho e por ter me mostrado essa vasta área da ciência, que é a teoria da informação quântica.

Ao Prof. Dr. José Ramos pelos aprendizados em duas cadeiras de mecânica clássica e duas de mecânica quântica. Essas quatro disciplinas foram minha transição do mundo clássico para o mundo quântico.

A Prof. Dra. Hilma Helena por ter me aceitado como bolsista de iniciação científica mesmo eu ainda não sabendo nada de mecânica quântica. E principalmente por ter me acostumado a desenvolver o hábito de leitura de artigos científicos.

Ao aluno da matemática, e principalmente amigo, Thiago Lima. Cuja ajuda durante os primeiros semestres da minha graduação foram um suporte importante para o meu aprendizado.

Ao Genivaldo Vasconcelos, pela grande amizade cultivada durante a graduação. Nossas conversas divertidas e bem humoradas me ajudavam a aguentar o estresse da rotina.

Ao João Pedro, pelas tardes de estudo toda semana que fizemos esse semestre e principalmente pelos bons conselhos e apoio emocional em momentos dificeis.

Aos amigos Willian Wallace, amigo de laboratório, nossas conversas nos intervalos de estudo deixavam minha rotina mais leve e ao Bruno Jhonatan, pela amizade fiel cultivada desde o primeiro dia de aula da graduação.

Ao colega de bolsa e futuro amigo de pesquisa na área, Gabriel. Não tenho dúvidas que as nossas conversas sobre mecânica quântica durante todo o período da IC me ajudaram bastante.

A aluna do Doutorado em física, Bárbara Sales, pelos bons conselhos e por esclarecer minhas dúvidas acerca da graduação em física.

Aos professores Daniel Colares e Henrique Bezerra por me mostrarem que a matemática é sim divertida e ao professor Assis por me fazer apreciar buscar entender o funcionamento dos fenômenos naturais.

E por último, mas não menos importante, um agradecimento a Bianca Teixeira, minha teraupeuta e uma excelente profissional em psicologia. Nossos encontros toda semana tornam minha vida mais leve e me ensinam a apreciar a vista.

RESUMO

Este trabalho se propõe a estudar um método de verificar a segurança de um canal quântico compartilhado por dois usuários legítimos (Alice e Bob), definido em termos de um estado bipartido ρ_{AB}. Considerou-se um protocolo em que os usuários desejam compartilhar uma chave secreta para encriptar e decriptar mensagens onde a segurança do canal é garantida quantificando o valor da taxa de chave secreta (K). A mesma é definida em termos das informações mútuas dos usuários e da informação mútua que uma espiã (Eve) compartilha com um dos usuários, neste caso Alice, ao invadir o canal. A invasão de Eve é descrita por um operador B, que define a medição de um observável ao interceptar o estado que é enviado para Bob. Assim, devido a natureza não local da teoria quântica, a intervenção de Eve promove o colapso do estado, e os usuários recebem em seus laboratórios um estado definido pela ação de um mapa de medição projetiva. Dessa forma, buscou-se encontrar uma expressão geral para a taxa de chave secreta em termos das entropias de von Neumann e então promover um estudo do caso usando a matriz densidade para o estado de Werner, utilizando operadores gerais de spin como grandeza observável. Com o estudo do caso, encontrou-se uma equação em termo dos ângulos que determinam as medidas gerais de spin onde foi definido um parâmetro r, com r dado pelo produto escalar do vetor unitário que define as medidas de spin para Alice com o vetor unitário para as medidas de spin de Eve. Pelos resultados encontrados, conclui-se que o módulo de r pode ser interpretado como sendo o grau de interferência de Eve no canal, de modo que quanto maior o valor de r, menor é o valor do gráfico que se encontra ao plotar K em termos de μ. Dessa forma, verifica-se que a taxa de chave secreta pode ser uma forma de atestar a segurança de um canal, de modo que os usuários possam compartilhar, de maneira segura, uma chave.

Palavras-chave: mecânica quântica; teoria da informação quântica; distribuição de chaves quânticas; criptografia.

ABSTRACT

The purpose of this work is to study a method of attesting the security of a quantum channel shared by two legitimate users (Alice and Bob), defined in terms of a bipartite state ρ_{AB}. A protocol in which users want to share a secret key to encrypt and decrypt messages was considered where the channel security is guaranteed by quantifying the value of the secret key rate (K). It is defined in terms of the user's mutual information and the mutual information that a spy (Eve) shares with one of the users, in this case Alice, when invading the channel. Eve's invasion is described by an operator B, which defines the measurement of an observable by intercepting the state that is sent to Bob. Thus, due to the non-local nature of quantum theory, Eve's intervention promotes state collapse, and users receive in their labs a state defined by the action of a projective measurement map. Thus , we sought to find a general expression for the secret key rate in terms of entropies and then promote a case study using the density matrix for the Werner state using general spin operators as an observable quantity. With the study of the case, an equation was found in terms of the angles that determine the general measures of spin where a parameter r was defined, with r given by the dot product of the unit vector that defines the measures of spin for Alice with the unit vector for Eve spin measurements. From the results we found, it is concluded that the modulus of r can be interpreted as the degree of Eve interference in the channel, so that the higher the value of r, the lower the value of the graph that is found when plotting K in terms of μ. In this way, it is verified that the secret key rate can be a way of attesting the security of a channel, so that users can securely share a key.

Keywords: quantum mechanics; quantum information theory; quantum key distribution; cryptography.

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

$\mathscr{E}$	Quanta de energia
$\hbar$	Constante reduzida de Planck
f	frequência
K	Taxa de Chave Secreta
$\mathscr{H}$	Espaço de Hilbert
$\mathscr{H}^*$	Espaço de Hilbert Dual
δ_{ij}	Delta de Kronecker
$\otimes$	Produto Tensorial
ρ	Matriz Densidade
Tr	Traço da Matriz
Tr_A	Traço Parcial Sobre A
Tr_B	Traço Parcial Sobre B
E_p	Valor Esperado
H	Entropia de Shannon
S	Entropia de von Neumann
$H(.\|\|.)$	Entropia Relativa Clássica
$H(,)$	Entropia Conjunta Clássica
$H(\|)$	Entropia Condicional Clássica
$H(:)$	Informação Mútua Clássica
$S(.\|\|.)$	Entropia Relativa Quântica
$S(,)$	Entropia Conjunta Quântica
$S(\|)$	Entropia Condicional Quântica
$I(:)$	Informação Mútua Quântica
$\Phi_A^{a_i}$	Mapa de Medição Projetiva com Resultado Revelado (operador $\hat{A}$)
Φ_A	Mapa de Medição Projetiva com Resultado não Revelado (operador $\hat{A}$)
ρ_A	Matriz Reduzida do Sistema A

ρ_B	Matriz Reduzida do Sistema B
$\rho_{B\|A_i}$	Matriz Reduzida Condicionada a uma Medição do Operador $\hat{A}$

SUMÁRIO

1 INTRODUÇÃO

Por aproximadamente 200 anos, as leis do movimento de Newton foram o suficiente para descrever os fenômenos naturais. Contudo, a situação começou a mudar quando questões mais profundas acerca do funcionamento da natureza começaram a chamar a atenção dos físicos. O formalismo Newtoniano era usado para descrever corpos materiais e o Eletromagnetismo de Maxwell era suficiente para a descrição de fenômenos referentes às ondas eletromagneticas. A força de Lorentz conseguia prover um meio de estudar a ação dos campos sobre particulas em movimento. Todo o sucesso dessas teorias fez parecer que toda a descrição da natureza havia chegado ao fim.(ZETTILI, 2009)

Contudo, ao final do século 19, a teoria clássica começou a apresentar limitações. Um dos problemas mais famosos foi a castastrófe do ultravioleta. Em 1900, Max Planck (1858-1947) introduziu o conceito de *quanta* de energia com o objetivo de corrigir os resultados experimentais da radiação de corpo negro que falhavam sobre uma visão clássica. O postulado de Planck afirma que a troca de energia entre a radição e o meio ocorrem de forma discretas ou quantizadas. (ZETTILI, 2009). Essa energia quantizada era dada por:

$$\mathscr{E} = hf. \tag{1.1}$$

A limitação da mecânica clássica de prover uma explicação para o problema da radição do corpo negro e a consequente proposta de Planck para uma resolução desse problema são geralmente considerados os pontos de partidas do nascimento da área da física conhecida como Mecânica Quântica (MQ). (S.T.PIRES, 2011)

Atualmente, a MQ é uma das áreas mais bem sucedidas da física, visto sua concordância em todos os experimentos e previsões realizados até hoje (S.T.PIRES, 2011). É graças a ela que dispomos de todo esse aparato tecnologico que facilitam a vida cotidiana. Áreas como Física Atômica, Física Nuclear, Física do Estado Sólido e toda a Química moderna, tem seus alicerces na teoria quântica.

Mesmo após todo esse sucesso, existem questões mais fundamentais dentro dessa teoria que permanencem um mistério. As interpretações da mecânica sobre a realidade física ainda são tópicos de grandes debates no meio científico.

1.1 A Interpretação de Copenhague

A intepretação da teoria quântica mais aceita atualmente, devido a sua concordância com o experimento, é a interpretação proposta por Niels Bohr (1885-1962) e Werner Heisenberg (1901-1976). O cerne dessa teoria é de carater estatístico e contem um tipo de indeterminação referente ao ato de medir grandezas físicas (GRIFFITHS, 2018). Observar e medir sistemas físicos são atividades distintas. Medir está ligado com a aquisição de valores númericos e o observar está associado ao ato de olhar sem interferir ou adquirir qualquer resultado(S.T.PIRES, 2011). No meio macroscópico essas duas palavras apresentam significados bem distintos, porém quando se trata de partículas quânticas, observação e medição acabam tendo o mesmo sentido (S.T.PIRES, 2011).

Devido ao tamanho microscópico, não é possível exergar uma partícula. Assim, ela é observada com o auxílio de instrumentos de alta precisão que detectam sua presença. Assim ao usar desse meio para observar, por exemplo, a posição de uma partícula, acaba-se por se obter um resultado de medição, pois assim determinamos sua posição naquele momento da análise. Por outro lado, o ato de não observar a partícula em um certo ponto, também constitue uma medição, pois ganhamos a informação que partícula não estava naquele local. (S.T.PIRES, 2011).

Ainda dentro desse contexto de medição, uma propriedade muito importante que aparece em MQ é o principio da incerteza. Uma partícula quântica, como a descrita anteriormente, apresenta duas grandezas que se completam, que é a sua posição e o seu momento. O principio da incerteza em mecânica quântica estabelece que é impossível se ter a informação precisa, simultaneamente, da posição e do momento. (WILDE, 2013)

Sobre essa pespectiva, é possível concluir que é o ato de medir que força a partícula a assumir algum estado físico específico. Antes de haver a medição a partícula se encontrava em todos os estados acessíveis ao sistema, essa propriedade de sistemas quânticos é cocnhecido como superposição (GRIFFITHS, 2018). As palavras de S.T.Pires (2011) a seguir, resume muito bem o que foi discutido

> Essa característica da Mecânica Quântica nos leva a acreditar que, em geral, algumas grandezas não possuem um valor determinado antes de uma medição; medi-la não significa determinar um valor que ela possui, mas antes de tudo, força-la a tomar um valor.

Essa interpretação não-deterministica da MQ gira em torno da função de onda complexa, Ψ. De acordo com a interpretação de Copenhague, Ψ carrega toda a informação

necessária que se precisa saber acerca do sistema. Essa funçaõ de onda não representa algo real do mundo físico, mas é graças a ela que se encontra a probabilidade de se achar a partícula em alguma região do espaço. Max Born (1882-1970) postulou que a probabilidade de ter como resultado uma certa medição de posição estava associado ao módulo quadrado de Ψ, dado por (S.T.PIRES, 2011)

$$|\Psi|^2. \tag{1.2}$$

Erwin Schrodinger (1887-1961) estudou uma forma de considerar a evolução temporal dessa função de onda e estabelecer uma dinâmica para sistemas quânticos. Graças ao seus estudos, foi proposto que a evolução temporal dessa função complexa era determinada por meio de uma equação diferencial parcial que hoje leva o nome de Equação de Schrodinger. Muitos físicos como, Bohr, Heisenberg, Pascual Jordan (1902-1980) e Paul Dirac (1902-1984) foram importantes para fortalecer e completar a formulação da MQ em termos probabilisticos e ondulatorios. Qualquer outra tentativa de interpretação para a teoria quântica, gerava resultados contraditorios. (S.T.PIRES, 2011)

1.2 O Artigo EPR e o Teorema de Bell

Albert Eistein (1879-1955), Boris Podolsky (1896-1966) e Nathan Rosen (1909-1995) desenvolveram um trabalho de grande impacto no meio acadêmico. Esse trabalho foi publicado em forma de artigo e é amplamente conhecido no meio científico como artigo EPR (Einstein, Podolsky e Rosen) ou paradoxo EPR. Esse artigo com o título de, 'Pode a Descrição da Mecânica Quântica Sobre a Realidade Física ser Considerada Completa?', foi uma crítica direta a interpretação de Coponhague para a MQ.

De acordo com EPR, uma teoria ser dada como completa é preciso que exista um elemento na teoria associado a cada elemento da realidade física. (EINSTEIN *et al.*, 1935). Em outras palavras, para cada elemento previsto pela teoria física, deve existir um elemento de realidade associado. Somado a essa noção, os autores ainda definiram que era necessário, para que uma grandeza fosse considerada real, ser possível preve-la com certeza sem que nenhuma pertubação no sistema fosse feita. (EINSTEIN *et al.*, 1935). Em suas próprias palavras Einstein *et al.* (1935) concordavam que:

> If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

Assim,o trabalho desses autores tinha como objetivo colocar em prova a função de onda como uma descrição completa do sistema. Em MQ, quantidades físicas estão associadas a operadores (TANNOUDJI *et al.*, 2019a), assim para duas quantidades que são descritas por dois operadores que não comutam, o conhecimento de uma dessas quantidades exclui imediatamente o conhecimento da outra. Então, a descrição da realidade fornecida pela função de onda não era completa e grandezas físicas descritas por operadores que não comutam, não podem ter realidade física simultânea. (BALLENTINE, 1998). Além dessas questões não deterministicas de medições quânticas, outra propriedade da MQ que incomodava bastante Einstein era que a teoria não obedecia o principio da localidade. Esse principio afirmava que nenhuma influência poderia se propagar mais rápido que a velocidade da luz (GRIFFITHS, 2018). O experimento de David Bohm ilustra muito bem essa questão, onde ele conclui que existe uma correlação no resultado da medição de spin de uma partícula que se encontra no estado singleto (GRIFFITHS, 2018):

$$\frac{1}{\sqrt{2}}(|\uparrow_-\downarrow_+\rangle - |\downarrow_-\uparrow_+\rangle). \tag{1.3}$$

Assim, se duas partículas, 1 e 2, correlacionadas descritas por um estado como escrito acima fosse separada espacialmente, ao realizar a medição na partícula 1 saberíamos o resultado da medição de spin da partícula 2, sem que nenhuma medição fosse realizada e mesmo que a distância de separação fosse da ordem de anos-luz. (GRIFFITHS, 2018). E para Einstein isso era um problema, pois algum tipo de informação estava viajando mais rápido do que a luz e colapsando o estado do sistema após alguma de suas partições passarem por um processo de medição.

Para Einstein, Podolsky e Rosen, não era como se a MQ estivesse errada, eles apenas acreditavam que a função de onda por si so não era suficiente para uma descrição completa da natureza, eles defendiam que algo estava faltando. Einstein acreditava na ideia de que era necessário a existência de variáveis ocultas locais que deveriam entrar no formalismo para uma melhor descrição da teoria (GRIFFITHS, 2018). Para ele essas variáveis ocultas complementariam a função de onda de modo a remover a indeterminação da medição e além disso iriam reestabelecer a localidade.

Porém, em 1964, John Stewart Bell (1928-1990) mostrou que qualquer teoria de variável oculta local seria incompatível com a mecânica quântica. Ele chegou nesse resultado enunciando uma desigualdade que deveria ser obedecida por qualquer teoria de variável oculta

local.

$$|C(\mathbf{a},\mathbf{b}) - C(\mathbf{a},\mathbf{b'})| + |C(\mathbf{a'},\mathbf{b'}) - C(\mathbf{a'},\mathbf{b})| \leq 2. \tag{1.4}$$

A desigualdade acima faz parte do teorema de Bell e é deduzida sem fazer uso de nenhum princípio Quântico. Esse resultado tem como um dos principais alicerces para sua demonstração a consideração do principio da localidade de Einstein, onde ele afirma que nenhuma influência pode se propagar mais rápido que a luz (GRIFFITHS, 2018; BALLENTINE, 1998).

1.3 Teoria da Informação Quântica e Distribuição de Chaves Quânticas

Porém, foi fazendo uso das propriedades da teoria quântica que em 1984, Charles Henry Bennett e Gilles Brassard, deram um passo muito importante. Eles estabeleceram um método, usando a natureza estatística da MQ e principalmente o principio da incerteza, de garantir a segurança de um canal quântico de modo a ser possível detectar a presença de um invasor, codificando a informação dentro de variáveis complementares.(WILDE, 2013).

A teoria da informação quântica (TIQ) é um campo da ciência que busca generalizar os conceitos estudados na teoria da informação para um caso quântico. Dessa forma a TIQ procura descrever as propriedadades e a capacidade de sistemas quânticos para armazenar e transmitir informação, bem como a relação da informação quântica com os fenômenos quânticos (GYONGYOSI; IMRE, 2012). Uma das aplicações da TIQ é a sua capacidade de realizar tarefas de criptografia de modo a garantir a segurança no envio e recebimento de dados usando as leis da MQ.

Dentro dos mais variados contextos, sempre foi de grande importância para a civilização trocar informação de forma secreta. A criptografia é uma área da ciência que se dedica ao estudo de métodos de garantir a segurança de uma mensagem secreta de modo que só as partes involvidas tenham acesso a essa mensagem. Classicamente, os métodos de criptografia se baseam na divulgação pública do algoritimo capaz de encriptar e descriptar a mensagem trocada entre as partes envolvidas. Portanto, a segurança desse protocolo é baseada em uma grande sequência de números, conhecido como chave, que o emissor (Alice) e o recepetor (Bob), devem compartilhar de forma secreta. Pois é a garantia de que essa sequência de número vai permanecer secreta durante toda a troca de mensagens, que vai validar a segurança desse canal. (RIGOLIN;

RIEZNIK, 2005)

É graças ao princípio de teoria completa proposto por Bohr que é possível usar a MQ como uma forma de garantia de segurança total de um canal quântico, visto que graças a esse príncipio seria impossível burlar a segurança (RIGOLIN; RIEZNIK, 2005). Assim, a geração e o envio de chaves para encriptar e descriptar mensagens compartilhadas pelas partes que participam do canal seria totalmente livre de quebra de segurança;

A proposta de Bennett e Brassard foi o primeiro método que usava a mecânica quântica para estabelecer um meio de criptografia. (RIGOLIN; RIEZNIK, 2005). Esse protocolo é amplamente conhecido como BB84. O BB84 garante a segurança usando fótons não emaranhados que são preparados em quatro estados de polarização para que seja realizado o envio da chave. (NIELSEN; CHUANG, 2000). Em 1991, Arthur K. Ekert desenvolveu um outro protocolo de distribuição de chaves que ficou conhecido como E91. A grande inovação que Ekert propôs foi a utilização de um estado emaranhado que tem a mesma forma do estado mostrado em 1.3. A segurança desse protocolo era garantida pela impossibilidade da violoação do teorema de Bell anteriormente citado. (RIGOLIN; RIEZNIK, 2005)

A troca de informação entre Alice e Bob é feito com o auxílio de um canal quântico. Um canal quântico pode ser estabelecido por meio de um estado quântico definido em termos da sua matriz densidade (GYONGYOSI; IMRE, 2012), uma explicação mais detalhada acerca de matrizes densidades e mapas completamente positivo que preservam o traço, pode ser encontrada na fundamentação teorica. Assim, o objetivo de protocolos de segurança de distribuição de chaves é garantir a segurança desses canais, permitindo o recebimento e o envio de mensagens seja feita de forma segura.

Além das formas de garantir a segurança desses canais por meio do principio da não localidade e de estados emaranhados, uma outra forma de proteção contra invasores, também utilizada em protocolos de distribuição de chaves, é por meio do cálculo da taxa de chave secreta, definida da seguinte forma (BRAUNSTEIN; PIRANDOLA, 2012):

$$K = I(A:B) - I(A:E). \tag{1.5}$$

A equação acima é dada em termos da informação mútua das partes legítimas, $I(A:B)$ (Alice e Bob) e da informação mutua entre Alice e Eve $I(A:E)$, dado que Eve interferiu no canal. Uma discussão mais detalhada de K será feita mais na frente.

No presente trabalho será apresentada uma proposta de segurança de um canal quântico via cálculo da taxa de chave para um estado bipartido geral, avaliando um estudo de caso para o estado de Werner. No caítulo 2 será apresentado a fundamentação teorica necessária para a compreensão do trabalho, começando com uma rápida formulação matemática e depois partindo para conceitos importantes como operador densidade, quantificadores de entropia e mapas de medições projetivas, de modo que seja possível a construção da informação mutua de forma clara e concisa.

Ademais, no capítulo 3 voltaremos a comentar acerca de taxa de chave secreta e em como é possível obter uma expressão para K em termos das entropia de von Neumann onde será feito um estudo de caso usando o estado de Werner, para que seja possível avaliar a segurança do canal levando em consideração um ataque de Eve. E por último, no capítulo 4, será feito uma discussão dos resultados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Espaço de Hilbert e Notação de Dirac

Um espaço de Hilbert, denotado por $\mathscr{H}$, é um espaço vetorial complexo dotado de um produto interno $(\cdot,\cdot)$ (PETZ, 2008). Se u e v forem vetores de $\mathscr{H}$ então:

$$(u,v), \tag{2.1}$$

é o produto interno de u com v. Assim tomando $v = (v_1, v_2, ...v_i)$ e $u = (u_1, u_2, ...u_i)$ n-tuplas ordenadas $\in \mathbb{C}^n$, logo o produto interno entre u e v é definido como:

$$(u,v) = \sum_{i=1}^{n} u_i^* v_i = \begin{bmatrix} u_1^* & u_2^* \dots u_i^* \end{bmatrix} * \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_i \end{bmatrix}, \tag{2.2}$$

Onde z^* representa a operação de conjugado complexo de um número qualquer $z \in \mathbb{C}$ (ZETTILI, 2009).

Dentro da teoria quântica esses vetores do espaço de Hilbert apresentam uma notação específica para representá-los. Essa notação foi proposta por Dirac e sua grande funcionalidade é a sua facilidade operacional para representar operações matemáticas de algebra linear. A notação de Dirac é pautada na noção de bras e kets. Logo:

Definição 2.1.1 *Um elemento de um espaço de Hilbert $\mathscr{H}$ é chamado de vetor ket e denotado por $|\rangle$. Assim um vetor v é escrito como $|v\rangle$ e lê-se "ket v"*

Existe um outro espaço, associado ao espaço de Hilbert $\mathscr{H}$, que é chamado de espaço dual e denotado por $\mathscr{H}^*$. Os elementos do espaço dual são chamados de funcionais lineares, e é possível mostrar que o espaço dual formado de funcionais lineares é um espaço vetorial. Os funcionais lineares são operadores lineares, definido sobre os kets de $\mathscr{H}$, que associam cada ket do espaço $\mathscr{H}$ um número complexo. Com essa noção, é possível definir a ideia de bra (TANNOUDJI *et al.*, 2019a; ZETTILI, 2009)

Definição 2.1.2 *Qualquer elemento do espaço $\mathscr{H}^*$, é donotado por $\langle|$, e chamado de bra. Por exemplo, o elemento $\langle v| \in \mathscr{H}^*$ é um bra.*

2.2 Base De Um Espaço Vetorial

Um conjunto de vetores independentes de um espaço de Hilbert $\mathscr{H}$, denotados por:

$$\{|u_1\rangle, |u_2\rangle, \ldots |u_i\rangle\}, \tag{2.3}$$

É dito ser uma base do espaço $\mathscr{H}$ se qualquer vetor $|\psi\rangle \in \mathscr{H}$, pode ser escrito como (GRIFFITHS, 2018; NAKAHARA, 2008)

$$|\psi\rangle = \sum_{i=1}^{n} c_i |u_i\rangle. \tag{2.4}$$

O conjunto $\{c_1, c_2, \ldots, c_i\}$ de números complexos pertencentes a $\mathbb{C}$ são chamados de componentes do vetor $|\psi\rangle$ com respeito a base $\{|u_i\rangle\}_{i=1}^{n}$. (NAKAHARA, 2008). Se um conjunto de vetores de base obedecerem a seguinte relação:

$$\langle u_i | u_j \rangle = \delta_{ij}, \tag{2.5}$$

A base é dita ser ortornormal, ou seja, os vetores que geram $\mathscr{H}$ são unitários e ortogonais. (TANNOUDJI *et al.*, 2019a)

Com esse resultado, é possível concluir que se $|\psi\rangle$ for um vetor pertecente a um espaço de Hilbert $\mathscr{H}$ gerado pela base anteriormente definida, então

$$\langle u_j | \psi \rangle = \sum_{i=1}^{n} c_i \langle u_j | u_i \rangle = \sum_{i=1}^{n} c_i \delta_{ij} = c_j \rightarrow c_j = \langle u_j | \psi \rangle. \tag{2.6}$$

Substituindo o resultado acima em 2.4:

$$|\psi\rangle = \sum_{i=1}^{n} c_i |u_i\rangle = \sum_{i=1}^{n} \langle u_i | \psi \rangle |u_i\rangle = \sum_{i=1}^{n} |u_i\rangle \langle u_i | \psi \rangle = \Big(\sum_{i=1}^{n} |u_i\rangle \langle u_i| \Big) |\psi\rangle. \tag{2.7}$$

A relação acima só é válida, se e somente se:

$$\sum_{i=1}^{n} |u_i\rangle \langle u_i| = \mathbb{I}. \tag{2.8}$$

Esse resultado, conhecido como relação de completeza, deve ser obdecido por qualquer conjunto de vetores que formam um espaço e que são ortogonais (TANNOUDJI *et al.*, 2019a).

2.2.1 Espaço de Hilbert bipartido e multipartido

Como sera explorado melhor posteriormente, para cada estado quântico de um sistema físico em estudo, existe um vetor em um espaço de Hilbert $\mathscr{H}$ associado onde o

sistema é descrito. (HAYASHI, 2017). Dessa forma, pode ocorrer de existirem sistemas que são compostos por várias partes, e assim, existem vários subespaços de Hilbert para cada uma dessas partes. Sistemas físicos que apresentam essa caracteristica são chamados ditos compostos. Como exemplo de sistema composto, é possível citar o um sistema bipartido. Um sistema desse tipo, é formado por dois subespaços de Hilbert que caracterizam cada parte da descrição física do sistema todo, a definição mais precisa é a seguinte

Definição 2.2.1 *Um sistema físico cuja as partes são descritas em dois espaços de Hilbert, $\mathscr{H}_A$ e $\mathscr{H}_B$, é chamado de bipartido. A representação do espaço que descreve todo o sistema é dado pelo produto tensorial dos subespaços de Hilbert respectivo a cada parte. Se $\mathscr{H}$ é o espaço de Hilbert do sistema composto, então:*

$$\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B. \tag{2.9}$$

Dessa forma, se o conjunto $\{|e_1^A\rangle, |e_2^A\rangle, \ldots, |e_{i_A}^A\rangle\}$, $i_A = 1,2,3,...d_A$, for uma base ortonormal para $\mathscr{H}_A$ cuja dimensão é d_A e $\{|e_1^B\rangle, |e_2^B\rangle, \ldots, |e_{i_B}^B\rangle\}$, $i_B = 1,2,3,...d_B$, uma base ortonormal para $\mathscr{H}_B$, a base de vetores que vai gerar o espaço de Hilbert $\mathscr{H}_A \otimes \mathscr{H}_B$ é dada por:

$$\{|e_1^A\rangle \otimes |e_1^B\rangle, \ldots |e_1^A\rangle \otimes |e_{d_B}^B\rangle, |e_2^A\rangle \otimes |e_1^B\rangle, \ldots, |e_2^A\rangle \otimes |e_{d_B}^B\rangle, \ldots, |e_{d_A}^A\rangle \otimes |e_1^B\rangle, \ldots, |e_{d_A}^A\rangle \otimes |e_{d_B}^B\rangle\}. \tag{2.10}$$

A dimensão do espaço $\mathscr{H}$ é dada por $d_A \times d_B$ (TANNOUDJI *et al.*, 2019a). Então, se z_{ij} forem o total de números complexos correspondentes a dimensão de $\mathscr{H}$, logo qualquer vetor $|\tau\rangle$ desse espaço fica escrito por meio da seguinte combinação linear:

$$|\tau\rangle = \sum_{i,j}^{d_A,d_B} z_{ij} |e_i^A\rangle \otimes |e_j^B\rangle. \tag{2.11}$$

Para simplificar a notação, a expressão $|e_i^A\rangle \otimes |e_j^B\rangle$ será escrita como $|e_i^A, e_j^B\rangle$

O caso mais geral de sistema composto, é o caso de um sistema constituido de N partes. Assim, vai se fazer necessário a existência de N espaços de Hilbert e o sistema vai ser descrito em um espaço de Hilbert chamado de multipartido (HAYASHI, 2017).

Definição 2.2.2 *Um sistema físico cuja as N partes são descritas por N subespaços de Hilbert; $\mathscr{H}_1, \mathscr{H}_2, \ldots, \mathscr{H}_{\mathscr{N}}$, é chamado de multipartido. A representação do espaço que descreve todo o sistema é dada por:*

$$\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2 \ldots \otimes \mathscr{H}_N. \tag{2.12}$$

2.3 Operadores e a Equação do Autovalor

Operadores representam um papel central dentro do contexto da teoria da mecânica quântica. Uma definição de operador que vai servir para os propositos desse trabalho é a seguinte (ZETTILI, 2009):

Definição 2.3.1 *Um operador, denotado por $\hat{A}$, é uma operação matemática que quando atua em um ket $|\lambda\rangle \in \mathscr{H}$ transforma em um outro ket $|\lambda'\rangle$ do mesmo espaço . O mesmo é válido para ação de $\hat{A}$ em um bra $\langle\pi|$.*

$$\begin{aligned} \hat{A}|\lambda\rangle &= |\lambda'\rangle, \\ \langle\pi|\hat{A} &= \langle'\pi|. \end{aligned} \tag{2.13}$$

Um dado operador $\hat{A}$, é dito ser linear, se a sua ação em um vetor expresso por $|\theta\rangle = \theta_1|u_1\rangle + \theta_2|u_2\rangle$ obedece a seguinte propriedade

$$\hat{A}|\theta\rangle = \theta_1\hat{A}|u_1\rangle + \theta_2\hat{A}|u_2\rangle. \tag{2.14}$$

Para o contexto do presente trabalho, a definição de mapa como um operador linear é de grande valia e será utilizada mais na frente, assim:

Definição 2.3.2 *Um mapa A: $\mathscr{H} \to \mathscr{H}$ é um operador linear se obedecer a relação acima para qualquer $|u_i\rangle \in \mathscr{H}$ e qualquer escalar $\theta_i \in \mathbb{C}$.*

Um ket $|\xi\rangle$ qualquer é dito ser autovetor de um operador $\hat{A}$, se e somente se:

$$\hat{A}|\xi\rangle = \lambda|\xi\rangle. \tag{2.15}$$

Onde o número λ é o autovalor associado ao autovetor $|\xi\rangle$. A equação acima é conhhecida como equação do autovalor ou problema do autovalor para o operador $\hat{A}$.(TANNOUDJI *et al.*, 2019a), o conjunto de todos os autovalores do operador $\hat{A}$ é chamado de espectro. Para que seja possível encontrar os autovetores $|\xi\rangle$ é preciso resolver o sistema que se obtém a partir da multiplicação matricial na equação acima, é necesssário primeiro encontrar a expressão anterior em termos de suas componentes.

Seja então $\{|e_k\rangle\}_{k=1}^{N}$ uma base ortonormal em $\mathscr{H}$. Se $a_{ij} = \langle e_i|\hat{A}|e_j\rangle$ for os elementos da matriz do operador $\hat{A}$ e $\xi_i = \langle e_i|\xi\rangle$ as componentes de $|\xi\rangle$, a equação 2.15 pode ser reescrita como:

$$\hat{A}|\xi\rangle = \sum_{ij}|e_i\rangle\langle e_i|\hat{A}|e_j\rangle\langle e_j|\xi\rangle = \sum_{ij}a_{ij}\xi_j|e_i\rangle.$$

Então:

$$\sum_j a_{ij}\xi_j = \lambda\xi_i. \tag{2.16}$$

Agora é necessário encontrar os autovalores da equação. É possível reescrever a equação acima de uma maneira mais sugestiva, logo:

$$\sum_j (\hat{A} - \lambda\mathbb{I})_{ij}\xi_j = 0. \tag{2.17}$$

Essa relação em ξ_i tem soluções não triviais se e semomente se a matriz $(A - \lambda\mathbb{I})$ não apresenta inversa (NAKAHARA, 2008). Assim:

$$D(\lambda) = det(\hat{A} - \lambda\mathbb{I}) = 0. \tag{2.18}$$

A expressão acima é chamada de equação caracteristica.

2.4 A Matriz densidade

O operador (ou matriz) densidade é uma forma de descrever o comportamento de sistemas quânticos completamente análoga a descrição usando vetores de estado no espaço de Hilbert. Sabe-se que, se o estado do sistema quântico em estudo for completamente conhecido, então o ket $|\psi\rangle$ de um espaço de Hilbert caracteriza completamente esse sistema. Assim, sistemas com essa caracteristica são conhecidos como estados puros, visto que tudo que se precisa saber acerca do sistema pode ser obtido com a utilização de $|\psi\rangle$. (NIELSEN; CHUANG, 2000; NAKAHARA, 2008). Porém, pode acontecer que para um dado sistema quântico não se tenha todas as informações sobre o seu estado ou até mesmo em que estado esse sistema foi preparado pelo experimentador.

Dito isso, se não for possível obter todas as informações sobre os estados de um sistema quântico, é dito que esse sistema se encontra em um estado misto. Sistemas com esssa característica são descritos por meio de dois conjuntos, um conjunto correspondente a todos os estados (puros) acessíveis desse sistema e outro conjunto contendo as probabilidades associadas a cada um desses estados. Como não se sabe em que estado o sistema se encontra, uma abordagem estatística para a descrição de problemas desse tipo é necessária. Portanto, uma forma conveniente de descrever um sistema de estados mistos é por meio da matriz densidade definida da seguinte forma:

Definição 2.4.1 *Se* $\{|\psi_i\rangle\}_{i=1}^{N}$ *for um conjunto de estados puros para um certo sistema e* $\{p_i\}_{i=1}^{N}$ *as probabilidades associadas a cada estado possível que o sistema pode se encontrar, o ensemble estatístico* $\{p_i, |\psi_i\rangle\}_{i=1}^{n}$ *do sistema, pode ser descrito com o auxílio da matriz densidade denotada por* $\hat{\rho}$ *e expressa por:*

$$\hat{\rho} = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|, \tag{2.19}$$

Com $\hat{\rho} : \mathscr{H} \to \mathscr{H}$*, atuando nos vetores do espaço de hilbert.*

A matriz densidade é também conhecida como operador densidade. Um operador $\hat{\rho}$ é a matriz densidade de algum ensemble estatístico $\{p_i, |\psi_i\rangle\}_{i=1}^{n}$, se e somente se, as seguintes propriedades forem satisfeitas:

1. O traço (soma dos elementos da diagonal principal da matriz) for igual a 1

$$tr(\hat{\rho}) = 1. \tag{2.20}$$

2. $\hat{\rho}$ deve ser um operador definido positivo. (todos os seus autovalores são maiores que zero)

Supondo que $\hat{\rho}$ seja um operador que satisfaça as condições acima, dessa forma esse operador é definido positivo então, pelo teorema espectral demonstrado no apêndice A , ele admite uma decomposição da seguinte forma (NIELSEN; CHUANG, 2000):

$$\hat{\rho} = \sum_{k=1} \sigma_k |\phi_k\rangle\langle\phi_k|. \tag{2.21}$$

Os vetores $\{|\phi_k\rangle\}_{k=1}^{N}$ determinam um conjunto de autovetores ortogonais associados aos autovalores $\{\sigma_k\}_{k=1}^{N}$ reais e não negativos de $\hat{\rho}$. A partir da primeira condição do traço, tem-se $\sum_k \sigma_k = 1$. Dessa forma, se o sistema estiver em um estado $|\phi_k\rangle$ com probabilidade σ_k, esse sistema vai ter uma matriz densidade. Ou seja, essa matriz densidade vai ser definida pelo ensemble estatístico formado pelos autovetores e autovalores da matriz densidade, $\{\sigma_k, |\phi_k\rangle\}$.

2.5 Os Postulados da Mecânica Quântica

Nosso objetivo agora é descrever detalhadamente os postulados da mecânica quântica. Esse postulados vão estabelecer a conexão da matemática anteriormente descrita com o mundo físico real e fornecer meios de trabalhar com sistemas quânticos. Como os resultados mais importantes desse trabalho fazem uso da descrição da mecânica quântica via matriz densidade, os postulados aqui enunciados serão explicitados encima desse formalismo. É importante ter em

mente que os postulados da mecânica quântica enunciados em termos da matriz densidade não diferem em nada dos postulados pelo vetor de estado, é apenas um resultado mais geral e mais completo (NIELSEN; CHUANG, 2000)

Postulado 1 *: **Espaço de Estados***

Cada sistema quântico isolado é associado a um espaço de Hilbert $(\mathscr{H})$ *chamado de espaço de estados.*

Postulado 2 *: **Estado do Sistema***

O estado físico de um sistema quântico é descrito por operadores estatísticos $(\hat{\rho})$ *, também conhecidos como matriz densidade, que agem no espaço de Hilbert do sistema. A matriz* $\hat{\rho}$ *é um operador definido positivo com traço unitário. Se por acaso um sistema quântico encontra-se em um estado* $\hat{\rho}_i$ *com probabilidade associada* p_i*, a matriz densidade que descreve esse sistema vai ser dada por:*

$$\sum_{i=1}^{N} p_i \hat{\rho}_i. \tag{2.22}$$

Postulado 3 *: **O Processo de Medição***

O processo de medição em mecânica quântica é definido por um conjunto $\{\hat{M}_i\}$ *de operadores de medição que agem no espaço* $\mathscr{H}$*. Esses operadores obedecem a seguinte relação:*

$$\sum_{i=1}^{N} M_i M_i^{\dagger} = \mathbb{I}. \tag{2.23}$$

Para um dado operador autoadjunto $\hat{A}$ do espaço de estados, o teorema espectral garante que:

$$\hat{A} = \sum_{i}^{N} a_i P_i, \tag{2.24}$$

Onde $\{a_i\}$ é o conjunto de autovalores reais e distintos do operador $\hat{A}$ e $\{P_i = |v_i\rangle\langle v_i|\}$ o conjunto de projetores ortogonais definidos em termos dos autovetores de $\hat{A}$, com $P_i P_j = \delta_{ij} P_j$. O conjunto $\{P_i\}$ define um processo medição, com valor associado a cada elemento de $\{a_i\}$. O operador $\hat{A}$ é um observável e o processo de medição dado dessa forma é conhecido como medição projetiva. (LIMA *et al.*, 2004).

Para caso de medições em sistemas compostos, como por exemplo sistemas quanticos definidos em um espaço de Hilbert $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$, é possível realizar medições locais em apenas uma das partes do sistema. Assim, o processo de medição fica definido da seguinte forma (LIMA *et al.*, 2004):

Definição 2.5.1 *Se $\{M_i\}$ for um conjuto que determina um processo de medição sobre o espaço $\mathscr{H}_A$, os operadores $\{M_i \otimes \mathbb{I}^B\}$ atuando em $\mathscr{H}_{AB}$ definem um processo de medição local na parte A do sistema.*

Postulado 4 *: O Colapso do Estado*

Seja $\{\hat{M}_i\}$ um conjunto de operadores de medição. Se (a_i) representar um resultado qualquer de uma medição feita no estado $\hat{\rho} \in \mathscr{H}$, o estado do sistema imediatamente após a medição vai ser expresso por:

$$\hat{\rho}^{(a_i)} = \frac{M_i \hat{\rho} M_i^\dagger}{Tr[M_i M_i^\dagger \hat{\rho}]}. \tag{2.25}$$

O denominador na expressão acima é a probabilidade $p(a_i)$ do resultado (a_i) ser encontrado (NIELSEN; CHUANG, 2000).

$$p(a_i) = Tr[M_i M_i^\dagger \hat{\rho}]. \tag{2.26}$$

A equação 2.25 pode ser reescrita para um caso de medição em uma matriz densidade ρ_{AB} que define um sistema composto. Assim, se realizarmos um processo de medição projetiva local definido como em 2.5.1, com valor a_i, o postulado do colapso garante que (VALBER, 2018)

$$\hat{\rho}_{AB}^{(a_i)} = \frac{(M_i \otimes \mathbb{I}^B)\rho_{AB}(M_i \otimes \mathbb{I}^B)}{Tr[(M_i \otimes \mathbb{I}^B)\rho_{AB}(M_i \otimes \mathbb{I}^B)]}. \tag{2.27}$$

Postulado 5 ***Evolução Temporal***

Para um sistema quântico fechado, isto é, um sistema cuja a energia é conservada a medida que o tempo passa, a evolução temporal é descrita por meio da operação unitária $\hat{U}$. Se $\hat{\rho}_{t_1}$ for a matriz densidade de um estado em dado tempo t_1 e $\hat{\rho}_{t_2}$ em um tempo posterior t_2, logo:

$$\hat{\rho}_{t_2} = \hat{U}\hat{\rho}_{t_1}\hat{U}^\dagger. \tag{2.28}$$

2.5.1 Operações Quânticas e os Operadores de Kraus

As operações quânticas são formulações matemáticas que servem para a descrição da dinâmica de sistemas quânticos. (NIELSEN; CHUANG, 2000). De maneira geral, se um dado sistema quântico é descrito por uma matriz densidade $\hat{\rho} \in \mathscr{H}$, então sua transformação pode ser escrita como:

$$\Theta(\hat{\rho}) = \hat{\rho}'. \tag{2.29}$$

Na equação acima, $\Theta : \mathscr{H} \to \mathscr{H}$ é a matriz de um mapa linear e $\hat{\rho}'$ o estado após a aplicação da transformação. Um exemplo direto de uma operação quântica é a equação 2.28 que pode ser reescrita como $\Theta(\hat{\rho}) = \hat{U}\hat{\rho}\hat{U}^{\dagger}$. Operações quânticas descrevem a dinâmica do sistema para um estado que é consequência de algum processo físico, o estado antes desse processo é dado por $\hat{\rho}$ e o estado após o processo é expresso pela operação do mapa e denotado por $\Theta(\hat{\rho})$ (NIELSEN; CHUANG, 2000).

Com isso, o processo de medição realizado em 2.27 define uma operação quântica onde a matriz ρ^{i}_{AB} é o resultado da ação de um mapa de medição projetiva local com resultado a_i dado por $\Phi^{(i)}_{A} : \mathscr{H}_{AB} \to \mathscr{H}_{AB}$. De modo que: (VALBER, 2018)

$$\Phi^{(a_i)}_{A}(\hat{\rho}_{AB}) = \hat{\rho}^{(a_i)}_{AB} = \frac{(M_i \otimes \mathbb{I}^B)\rho_{AB}(M_i \otimes \mathbb{I}^B)}{Tr[(M_i \otimes \mathbb{I}^B)\rho_{AB}(M_i \otimes \mathbb{I}^B)]}. \tag{2.30}$$

O processo de medição dado pela expressão acima, define uma medição com resultado revelado, já que sabemos que o resultado é a_i. Assim, o resultado da operação quântica fornece um estado normalizado, que é condicionado ao valor da probabilidade $p(a_i)$.

Por outro lado, pode acontecer do processo de medição não ser totalmente conhecido e assim não ser possível obter o resultado da medição. Posto isso, não sabemos em qual estado o sistema se econtra, sendo necessário ponderar sobre a probabilidade de cada resultado (PRESKILL, 2018).

$$\Phi_A(\rho_{AB}) = \sum_{i=1}^{n} p(a_i)\Phi^{(a_i)}_{A}(\hat{\rho}_{AB}) = \sum_{i=1}^{n}(M_i \otimes \mathbb{I}^B)\rho_{AB}(M_i \otimes \mathbb{I}^B). \tag{2.31}$$

O mapa linear acima, onde os termos $\{M_i\}$ obedecem a relação de completeza, é chamado de canal quântico. Algumas vezes, a palavra superoperador é usada ao invés de canal quântico, já que o mapa definide anteriormente leva matrizes em matrizes ao invés de vetores em vetores. (PRESKILL, 2018). Matematicamente esses operadores recebem o nome de mapas completamente positivo que preservam o traço. A equação 2.31 é conhecida como formalismo do operador soma que determina a transformação da matriz $\hat{\rho}_{AB}$, os termos $\{M_i \otimes \mathbb{I}^B\}$ são os chamados operadores de Kraus.

2.6 Entropia & Informação

O objetivo agora é construir um meio de quantificar informação em estados quânticos, para tanto é necessário a utilização do conceito de entropia, visto que existe uma relação íntima

entre a entropia e a informação. (NESS, 1969). Para trilhar esse caminho, é necessário começar com a noção de quantificação de informação clássica encima de variáveis aleatórias, por meio da entropia de Shannon. Feito isso, e levando em considerações algumas propriedades matemáticas importantes do operador densidade, é possível generalizar a entropia de Shannon para o caso quântico por meio da matriz densidade do sistema em questão, essa generalização da entropia de Shannon recebe o nome de entropia de von Neumann (PETZ, 2008).

2.6.1 Entropia de Shannon

Seja X uma certa variável aleatória de valor real, $\{p_x\}_{x\in\Omega}$ o conjunto que representa a distribuição de probabilidade associada a X e Ω um espaço de probabilidades. Com isso, o valor esperado $E_p(X)$, fica definido como:

$$E_p(X) = \sum_{x\in\Omega} xp_x \tag{2.32}$$

Então, se o número $-ln(p_x)$, é considerado como uma variável aleatória de valor real, a entropia de Shannon é definida como o valor esperado da variável aleatória sobre o conjunto de distribuição de probabilidade. Então, se H denotar a entropia de Shannon(HAYASHI, 2017), logo:

$$H(p_1, p_2 \dots p_x) = -\sum_{x\in\Omega} p_x \ln(p_x) \tag{2.33}$$

$H(p_1, p_2 \dots p_x)$ pode ser simplesmente substituido por $H(X)$. E assim $H(X)$ é a entropia de Shannon de alguma variável aleatória X. O que o cálculo da entropia de Shannon fornece, é o quanto de informação se ganha ao se obter o valor de X. De maneira equivalente, $H(X)$ fornece o quanto de incerteza se tem encima de algum evento associado a X, antes que ele ocorra.

2.6.2 Entropia de von Neumann

Como a teoria quântica é em sua essência probabilistica, é possível englobar o conceito de quantificação de informação para o contexto quântico. O caminho para se fazer isso é tomando uma generalização da entropia de Shannon. Lembrando que a descrição quântica é feita em espaços de Hilbert, onde observáveis são descritos por matrizes autoadjuntas e operadores estatísticos representam estados do sistema em estudo, a grande ideia de von Neumann foi

associar uma medida de entropia à um operador que descreve um estado misto de um sistema quântico, a própria matriz densidade.

Já que operadores densidades são hermitianos e positivos semidefinidos, então pelas condições já citadas, seus autovalores são reais e maiores que zero. Além disso, a soma dos elementos de sua diagonal principal, traço, é um. Dessa forma, se $\hat{\rho}$ for uma matriz densidade para um sistema quântico misto, que obedece a essas propriedades, é possível escreve-la como (MAZIERO, 2015):

$$\hat{\rho} = \sum_{j=1}^{m} p_j |\psi_j\rangle\langle\psi_j| = \sum_{i=1}^{n} \lambda_i |\lambda_i\rangle\langle\lambda_i|, \tag{2.34}$$

Onde o conjunto $\{\lambda\}_{i=1}^{n}$ é o espectro da matriz densidade que contém seus autovalores e $\{|\lambda_i\rangle\}_{i=1}^{n}$ são os autovetores associados a cada autovalor. Então, como $\hat{\rho}$ é hermitiana e positiva semidefinida, tem-se:

- $\sum_{i=1}^{n} \lambda_i = 1$, $\lambda_i \in \mathbb{R}$ e $\lambda_i \geq 0$.
- $\langle\lambda_i|\lambda_i\rangle = \delta_{ij}$.

Assim, o espectro de autovalores da matriz densidade pode ser tratado como uma distribuição de probabilidade e os operadores densidades vistos como casos gerais de variáveis aleatórias que descrevem situações probabilisticas, que no contexto físico de estados mistos, consiste na probabilidade do sistema se encontrar em algum dos estados puros $|\psi_j\rangle$ que faz parte do ensemble estatístico do sistema. Assim, a entropia de von Neumann pode ser naturalmente tomando como uma generalização da entropia de Shannon, logo:

$$S(\hat{\rho}) = -Tr(\hat{\rho} log_2(\hat{\rho})) = -\sum_{i=1}^{n} \lambda_i ln(\lambda_i). \tag{2.35}$$

$S(\hat{\rho})$ denota a entropia de von Neumann para o operador densidade e Tr representa a função traço. Então, a entropia von neumann é a entropia de Shannon calculada sobre a distribuição de probabilidade constituida pelos autovalores da matriz densidade.

2.6.3 Entropia Relativa, Entropia Condicional & Informação Mútua

A entropia relativa é uma medida estatística de distância. Ou seja, é um quantificador que vai determinar o quão proximo duas distribuições de probabilidade se encontram uma da outra. Suponha que existam duas distribuições de probabilidades denotadas por p e q. Ambas definidas sobre o mesmo espaço de probabilidade Ω. De modo que $p = \{p_i\}_{i\in\Omega}$ e $q = \{q_i\}_{i\in\Omega}$.

Logo se $H(p_i||q_i)$ denotar a entropia relativa para essas distribuições de probabilidade, então:

$$H(p_i||q_i) = \sum_{i\in\Omega} p_i log\frac{p_i}{q_i} = -H(p_i) - \sum_{i\in\Omega} p_i log q_i. \tag{2.36}$$

A quantidade acima é dita ser uma medida de informação porque o ganho de informação se relaciona com a diferença entre as duas distribuições de probabilidade. Assim, a entropia relativa mede o quanto de informação é perdida quando p é usado para aproximar q (HAYASHI, 2017). Essa quantidade é útil pois outras entropias podem ser definidas como um caso particular da entropia relativa.

Uma outra relação de entropia que vai ser usada para definir quantificadores importantes, é a entropia conjunta de um par de variáveis aleatórias. Se X e Y forem variáveis aleatórias, então:

$$H(X,Y) = -\sum_{x,y} p(x,y)\log(p(x,y)). \tag{2.37}$$

Essa relação fornece o valor da incerteza referente ao par (X,Y). (NIELSEN; CHUANG, 2000)

Dessa forma, em certos casos físicos, como vai ser mostrado mais na frente, é importante se perguntar o quanto do conteúdo referente a informação de X se relaciona ao conteúdo da informação de Y? Para tanto, é necessário introduzir dois quantificadores muito importantes; a entropia condicional e a informação mútua.

A entropia condicional é intuitivamente construida considerando que se sabe o valor de Y, assim por meio de 2.33, é possível calcular uma quantidade de informação, $H(Y)$, referente ao par (X,Y). O resto de incerteza acerca de (X,Y), é calculada via a incerteza referente a X considerando que se sabe ainda o valor de Y. Logo, se H(X|Y) denotar a entropia condicional, então:

$$H(X|Y) = H(X,Y) - H(Y). \tag{2.38}$$

Para a construção da informação mutua, seja $P_{X,Y}$ a distribuição de probabilidade conjunta de X e Y, a distribuição marginal sobre cada uma das variáveis X e Y, é expressa da seguinte forma (HAYASHI, 2017):

$$P_X(x) = \sum_y P_{X,Y}(x,y), P_Y(y) = \sum_x P_{X,Y}(x,y) \tag{2.39}$$

A distribuição condicional fica dada de acordo com:

$$P_{X|Y}(x|y) = \frac{P_{X,Y}(x,y)}{P_Y(y)}. \tag{2.40}$$

Para o caso em que $P_X(x)P_Y(y) = P_{X|Y}(x,y)$ as duas variáveis aleatórias são independentes. Dessa forma, pela equação 2.36, $H(P_{X,Y}(x,y)||P_XP_Y) = 0$. Ou seja, a entropia relativa para uma situação de variáveis independentes é 0. Com essas noções, é possível agora introduzir a noção de informação mutual, que no contexto quântico tem um papel muito importante na quantificação de informação ao realizar medidas projetivas em subsistemas de um sistema constituido de duas ou mais partes.

A informação mútua vai ser denotada por H(X:Y), e sua função vai ser quantificar o quão distinta é a distribuição conjunta $P_{X,Y}(x,y)$ do produto das distribuições marginais $P_X(x)P_Y(y)$. Logo:

$$H(X:Y) = H(P_{X,Y}||P_XP_Y) = \sum_{x,y} P_{X,Y}(x,y) log(\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)}) =$$

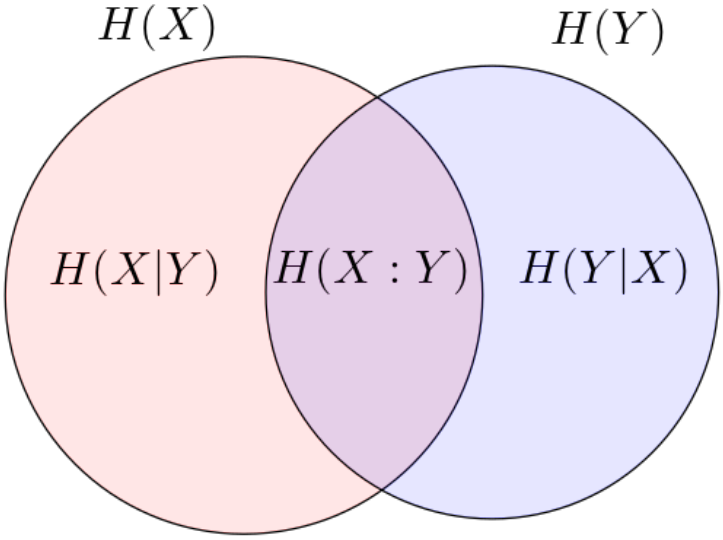
$$= H(X) - H(X|Y) = H(Y) - H(X|Y)$$

De modo que a informação mútua, $H(X:Y)$, fica definida por:

$$H(X:Y) = H(X) + H(Y) - H(X,Y) \tag{2.41}$$

De maneira esquematica, a relação entre essas quantidades de entropia pode ser esquematizada com o auxílio do diagrama mostrado na figura 1.

Figura 1 – Diagrama dos quantificadores de informação.



Fonte: elaborado pelo autor (2022).

É importante mencionar que como a matriz densidade se comporta como uma distribuição de probabilidade, todos esses quantificadores de informação são validos para a

entropia de von Neumann anteriormente definida. Então, se $\hat{\rho}$ e $\hat{\sigma}$ forem duas matrizes densidades que descrevem dois sistemas físicos, a entropia relativa de $\hat{\rho}$ para $\hat{\sigma}$ é expressa como (NIELSEN; CHUANG, 2000):

$$S(\hat{\rho}||\hat{\sigma}) = Tr(\hat{\rho}\ln\hat{\rho}) - Tr(\hat{\sigma}\ln\hat{\sigma}) \tag{2.42}$$

A equação acima é chamada de entropia relativa quântica. Da mesma forma que a entropia clássica, o valor da entropia quântica pode, em certas ocasiões assumir valores infinitos. Por exemplo, o valor de $S(\hat{\rho}||\hat{\sigma})$ tende para $+\infty$ se o núcleo de $\hat{\sigma}$ (o espaço vetorial gerado pelos autovetores de $\hat{\sigma}$ com autovalores iguais a 0) apresentar intersecção que seja diferente de 0 com o suporte de $\hat{\rho}$ (o espaço vetorial gerado pelos autovetores de $\hat{\rho}$ com autovalores que sejam diferentes de 0). Um resultado muito importante, é que a entropia relativa quântica é sempre maior do que ou igual a zero(NIELSEN; CHUANG, 2000). Essa afirmação fica bem enunciada no seguinte teorema, conhecido como teorema de Klein.

Teorema 2.6.1 *(Desigualdade de Klein) A entropia relativa quântica é não negativa,*

$$S(\hat{\rho}||\hat{\sigma}) \geq 0, \tag{2.43}$$

A igualdade só é garantida se e somente se $\hat{\rho} = \hat{\sigma}$

A demonstração da desigualdade de Klein foi colocada no apêndice B

Ainda dentro do contexto da entropia quântica, é importante mencionar algumas propriedades elementares para a relação 2.35 , que podem ser bem sumarizadas no seguinte teorema (NIELSEN; CHUANG, 2000).

Teorema 2.6.2 *Propriedades da entropia de von Neumann*

1. *A entropia é não negativa. O valor da entropia vai ser zero, se e somente se, o estado do sistema quântico é puro.*
2. *Em um espaço de Hilbert com N dimensões, a entropia de von Neumann assume o valor máximo de* $\ln(N)$. *O valor só é, exatamente, igual a* $\ln(N)$, *se e somente se, se o sistema quântico é completamente misto.*
3. *Se existe um sistema composto AB, que encontra-se em um estado puro então, S(A) = S(B).*
4. *Suponha o conjunto* $\{p_i\}$ *de probabilidades associadas a cada estado do conjunto* $\{\hat{\rho}_i\}$. *Se o os estados desse conjunto apresentarem o suporte em espaços ortogonais, logo:*

$$S(\sum_i p_i\hat{\rho}_i) = H(p_i) + \sum_i p_i S(\hat{\rho}_i) \tag{2.44}$$

5. *(Entropia Conjunta) Sendo $\{p_i\}$ um conjunto de probabilidades, $\{|e_i\rangle\}_{i=1}^{N}$ um conjunto ortogonal de estados para o espaço $\mathscr{H}_A$, e $\{\hat{\rho}_i\}$ for um conjunto qualquer de matrizes densidades para um sistema de um espaço $\mathscr{H}_B$, logo:*

$$S(\sum_i p_i|e_i\rangle\langle e_i| \otimes \hat{\rho}_i) = H(p_i) + \sum_i p_i S(\hat{\rho}_i) \tag{2.45}$$

É possível consultar a demonstração desse resultado no apêndice C

Vamos agora definir a informação mútua quântica, para isso considere um sistema quântico constituido por dois espaços de Hilbert, $\mathscr{H}_A$ e $\mathscr{H}_B$, cuja o operador densidade pode ser expresso como $\hat{\rho}^{AB}$. Assim, a entropia conjunta de um sistema composto, fica expressa por (NIELSEN; CHUANG, 2000).

$$S(A,B) = -tr[\hat{\rho}^{AB}\ln(\hat{\rho}^{AB})] \tag{2.46}$$

Para definir a entropia condicional e a informação mutua em um contexto quântica, basta reescrever as expressões clássicas construidas via entropia de Shannon, pela entropia de von Neumann. Assim, se S(A|B) for a entropia condicional, então:

$$S(A|B) = S(A,B) - S(B) \tag{2.47}$$

Assim

$$S(A:B) = S(A) - S(A|B) \tag{2.48}$$

Onde $S(A:B)$ é a informação mutua quântica.

2.7 Medições Quânticas e Entropia

A entropia de sistemas quânticos é modificada quando se é realizado medições no sistema em estudo. Essa mudança depende do tipo de medição que é feita, podendo ocorrer um aumento ou diminuição da entropia. Como o presente trabalho utiliza medições projetivas, será avaliado então o comportamento da entropia após uma medição projetiva descrita por um conjunto de projetores $\{P_i\}$ ser realizada em um sistema quântico com nenhuma informação acerca do resultado sendo revelada.(NIELSEN; CHUANG, 2000; PRESKILL, 2018)

Assim, para um sistema qualquer, o estado antes e depois de uma medição projetiva ser realizada pode ser expresso, respectivamente, por $\hat{\rho}$ e $\hat{\rho}'$. Com $\hat{\rho}'$ sendo:

$$\hat{\rho}' = \sum_i P_i \hat{\rho} P_i \tag{2.49}$$

Se a entropia do sistema após a medição for calculada, sera encontrado que o seu valor nunca diminui após uma medição projetiva ser realizada. A entropia permanece constante se e somente se o estado do sistema não colapsar com a medição. (NIELSEN; CHUANG, 2000). Esse resultado pode ser melhor colocado com o seguinte teorema:

Teorema 2.7.1 *(Medições projetivas aumentam a entropia) Seja $\{P_i\}$ um conjunto completo e ortogonal de projetores e $\hat{\rho}$ uma matriz densidade para uma sistema quântico qualquer. Se $\hat{\rho}'$, dado por 2.49, for o estado do sistema após uma medição, então:*

$$S(\hat{\rho}') \geq S(\hat{\rho}) \tag{2.50}$$

A igualdade é garantida, se e somente se, $\hat{\rho} = \hat{\rho}'$.

Prova:

Fazendo uso do teorema de Klein:

$$0 \leq S\left(\rho \| \rho'\right) = -S(\rho) - \operatorname{Tr}\left(\rho \ln \rho'\right). \tag{2.51}$$

Como $\sum_{i=1}^{n} P_i = \mathbb{I}$ e $P_i^2 = P_i$. Pela propriedade cíclica da operação traço, tem-se:

$$\begin{aligned} -\operatorname{Tr}\left(\rho \ln \rho'\right) &= -\operatorname{Tr}\left(\sum_i P_i \rho \ln \rho'\right) \\ &= -\operatorname{Tr}\left(\sum_i P_i \rho \ln \rho' P_i\right). \end{aligned} \tag{2.52}$$

Visto que $\rho' P_i = P_i \rho P_i = P_i \rho', P_i$ comuta com $\log \rho'$, concluimos então:

$$\begin{aligned} -\operatorname{Tr}\left(\rho \ln \rho'\right) &= -\operatorname{Tr}\left(\sum_i P_i \rho P_i \ln \rho'\right) \\ &= -\operatorname{Tr}\left(\rho' \ln \rho'\right) = S\left(\rho'\right). \end{aligned} \tag{2.53}$$

Substituindo o último resultado acima na equação 2.51, é possível chegar no resultado do teorema e assim concluir a prova.

3 CÁLCULO DA TAXA DE CHAVE QUÂNTICA

Para que se estabeleça um protocolo de distribuição de chaves, é necessário garantir a segurança da transmissão da chave entre as partes legítimas do canal. Classicamente esse método é estabelecido criando um número aleatório muito grande, a qualidade da segurança da troca de informação reside em manter esse número secreto durante todo o processo de envio e recebimento das informações que se deseja transmitir.

Em métodos de distribuição de chaves quânticas (DCQ), a segurança da chave é mantida pelas leis da Mecânica Quântica (NIELSEN; CHUANG, 2000). Assim, visto que o ato de medir um sistema quântico causa uma modificação do estado, se um invasor tentar invadir um canal realizando algum tipo de medição com o intuito de roubar alguma informação, o sistema imediatamente vai colapsar de acordo com o postulado 4, e as partes legítimas envolvidas na transmissão da mensagem poderam perceber que a segurança do canal foi quebrada.

Existe muitos métodos para revelar a presença de um espião em um canal, o primeiro protocolo de distribuição de chaves quânticas foi o BB84 (WILDE, 2013). Esse método era baseado em um sistemas quânticos de dois níveis. Assim, se os estados $|v_1\rangle$ e $|v_2\rangle$ representassem fotons linearmente polarizados, as partes legítimas desse canal escolhem antecipadamente a base que seria usada para medir esses estados, e assim um invasor usando uma base distinta para interceptar o foton, provocaria um colapso do estado o que avisaria aos usuários que a segurança foi comprometida. (RIGOLIN; RIEZNIK, 2005).

Outro protocolo de DCQ bastante conhecido, é o proposto por Ekert em 1991 e conhecido como E91 (WILDE, 2013). Aqui a segurança do canal é garantida devido a forte correlação existente em estados emaranhados e a impossibilidade da violação da desigualdade de bell.

Dentre as formas de garantia de segurançae em processos de DCQ, existe um método recente que propõe a obtenção de uma taxa de chave secreta dada por (GROSSHANS *et al.*, 2003):

$$K = I(A:B) - I(E:A). \tag{3.1}$$

A equação acima é definida em termos da subtração de duas informações mútuas. A primeira, $I(A:B)$, é referente a informação compartilhada entre as partes legítimas do canal e a segunda, $I(E:A)$, é a informação mútua que um dos usuários compartilha com o invansor. Essa última advem devido a medições locais que o invasor faz no canal, de modo a alterar o estado

para Alice e Bob. Assim, o termo $I(A:B)$ quantifica o tanto de informação que os usuários compartilham, considerando o estado ρ_{AB}, e $I(E:A)$ mensura a informação mutua que um dos usuários, nesse caso Alice, compartilha com o invasor (Eve), considerando um novo estado que advem do colapso de ρ_{AB} devido a medição local de Eve. Dessa forma, a subtração que define a taxa de chave K, representa um vazamento de informação devido a invervenção que Eve faz modificando o canal que os usuários legítimos compartilham. A equação para K deve ser necessáriamente não negativa $(K > 0)$, isso vem do fato de que Eve não é capaz de obter mais informação do que as próprias partes legítimas que participam do canal (GROSSHANS *et al.*, 2003). Com isso em mente, objetivo da taxa de chave secreta é atestar se o canal é seguro para que seja possível o compartilhamento de uma chave secreta entre os usários (GROSSHANS *et al.*, 2003).

Braunstein e Pirandola (2012) verificaram a segurança de um canal quântico definido por um estado bipartido ρ_{AB} usando a taxa de chave. Os autores computaram a taxa de chave secreta levando em consideração um possível ataque de um invasor. Uma outra utilização da taxa de chave secreta foi feita por Su (2013). Nesse trabalho o processo de distribuição de chaves foi em variáveis contínuas, utilizando como canal quântico um estado gaussiano com discordia quântica. Foi concluido que a função dada pela expressão de K cresce a medida que ocorre o aumento da discordia quântica.

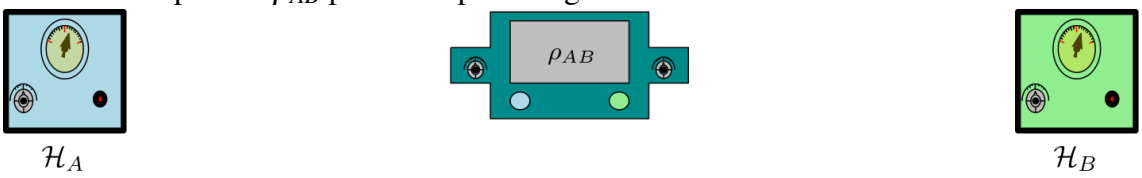
O presente trabalho pretende calcular uma medida de taxa de chave secreta para o protocolo recentemente proposto por Gomes *et al.* (2022). Os autores usaram um canal quântico correlacionado, onde foi quantificado uma medida de não-localidade para atestar a segurança do canal considerando que Eve intercepta o estado realizando uma medição de um observável B. (Para mais informações, consultar (GOMES *et al.*, 2022).

3.1 Obtenção da Equação Geral Para a Taxa de Chave Secreta

Antes de verificarmos a eficiência da taxa de chave secreta, será mostrado como se obtém, de maneira geral para um estado bipartido qualquer, a equação para K em termos da entropia de von Neumann. Assim, considera o esquema abaixo:

A imagem 2 representa um canal quântico definido por uma fonte que envia para dois usuários, Alice e Bob, um estado bipartido ρ_{AB}. $\mathscr{H}_A$ define o laboratório onde Alice faz medições locais, que é espacialmente separada do laboratório $\mathscr{H}_B$, onde Bob realiza suas medições locais. Assim, Alice realiza medição local de alguma grandeza definida por um operador autoadjunto $\hat{A}$,

Figura 2 – Esquema de um canal quântico estabelecido por uma fonte que envia um estado bipartido ρ_{AB} para duas partes legítimas.



Fonte: Elaborado pelo autor (2022).

dado por:

$$\hat{A} = \sum_{i=1}^{n} a_i A_i, \tag{3.2}$$

Onde $\{A_i\}$ são operadores de medições projetivas definidos em termos dos próprios autoestados de $\hat{A}$ e $\{a_i\}$ o conjunto de possíveis resultados. Dessa forma é possível computar a informação mutua entre Alice e Bob, dada por;

$$I(A:B) = S(B) - S(B|A) \tag{3.3}$$

$S(B)$ representa a entropia do estado $\rho_B = Tr_A(\rho_{AB})$ e $S(B|A)$, denota a entropia condicional do estado ρ_B dado uma medição projetiva feita por Alice no estado ρ_{AB} que ela recebeu em seu laboratório. Aqui, temos de forma implicita, a caracteristica não local da MQ, visto que uma medida no laboratório de Alice, afeta o estado ρ_{AB} que Bob recebeu em seu laboratório. Assim, a entropia condicional $S(B|A)$ é dada pelas entropias dos estados ρ_B, após o colapso causado por cada medição do observável $\hat{A}$, ponderadas pelas respectivas probabilidades $p(a_i)$. Isto é,

$$S(B|A) = \sum_{i=1} p(a_i) S(\rho_{B|A_i}). \tag{3.4}$$

Portanto, pelo resultado acima a equação 3.3 toma a seguinte forma:

$$I(A:B) = S(\rho_B) - \sum_{i=1}^{n} p(a_i) S(\rho_{B|A_i}). \tag{3.5}$$

Do ponto de vista operacional, é vatajoso encontrar uma forma mais simples de escreve a relação acima. Assim, usando a equação 2.27 tomando $M_i = A_i$, temos que o estado ρ_B após uma medição do operador $\hat{A}$, colapsa para:

$$\hat{\rho}_{AB}^{(a_i)} = \frac{(A_i \otimes \mathbb{I}^B)\rho_{AB}(A_i \otimes \mathbb{I}^B)}{Tr[(A_i \otimes \mathbb{I}^B)\rho_{AB}]}, \tag{3.6}$$

onde $Tr[(A_i \otimes \mathbb{I}^B)] = p(a_i)$

E assim, tomando a operação $Tr_A[\hat{\rho}_{AB}^{(a_i)}]$ é possível encontrar $\rho_{B|A_i}$, logo

$$\rho_{B|A_i} = \sum_{i'} \langle v_{i'}^A | \left[\frac{(A_i \otimes \mathbb{I}^B)\rho_{AB}(A_i \otimes \mathbb{I}^B)}{p(a_i)} \right] |v_{i'}^A\rangle. \tag{3.7}$$

Com $\{|v_i^A\rangle\}$ autoestados do operador $\hat{A}$. Se os projetores são dados por $A_i = |v_i^A\rangle\langle v_i^A|$, então:

$$\begin{aligned}\rho_{B|A_i} &= \frac{1}{p(a_i)} \sum_{i'=1}^{n} \langle v_{i'}^A | \Big(|v_i^A\rangle\langle v_i^A| \otimes \mathbb{I}^B)\rho_{AB}(|v_i^A\rangle\langle v_i^A| \otimes \mathbb{I}^B \Big) |v_{i'}^A\rangle \\ &= \frac{1}{p(a_i)} \sum_{i'=1} \langle v_{i'}^A | v_i^A\rangle\langle v_i^A | \rho_{ab} | v_i^A\rangle\langle v_i^A | v_{i'}^A\rangle.\end{aligned}$$

Dessa forma chega-se em:

$$\rho_{B|A_i} = \frac{1}{p(a_i)} \langle v_i^A | \rho_{AB} | v_i^A\rangle. \tag{3.8}$$

Como foi mostrado anteriormente, é possível representar medições projetivas usando o mapa definido em termos dos operadores de Kraus, de acordo com a equação 2.31. Sendo $M_i = A_i$, logo:

$$\Phi_A(\rho_{AB}) = \sum_{i=1}^{n} (A_i \otimes \mathbb{I}^B)\rho_{AB}(A_i \otimes \mathbb{I}^B) = \sum_{i=1}^{n} A_i \otimes \langle v_i^A | \rho_{AB} | v_i^A\rangle. \tag{3.9}$$

Usando o resultado 3.8 na equação acima, encontra-se que:

$$\Phi_A(\rho_{AB}) = \sum_{i}^{n} p(a_i) A_i \otimes \rho_{B|A_i}. \tag{3.10}$$

Pelo o teorema da entropia conjunta, ponto 5 do teorema 2.6.2, a equação acima pode ser reescrita da seguinte forma:

$$S(\Phi_A(\rho_{AB})) = S(\sum_{i}^{n} p(a_i) A_i \otimes \rho_{B|A_i}) = H(A) + \sum_{i=1}^{n} p(a_i) S(A_i \otimes \rho_{B|A_i}), \tag{3.11}$$

Se β for uma matriz densidade qualquer dada por $\beta = \rho \otimes \sigma$ onde ρ e σ são matrizes densidades, então a entropia $S(\beta) = S(\rho \otimes \sigma)$ é dada por (NIELSEN; CHUANG, 2000)

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma). \tag{3.12}$$

Com esse resultado podemos desenvolver a equação 3.11 como segue abaixo

$$S(\Phi_A(\rho_{AB})) = H(A) + \sum_{i=1}^{n} p(a_i)[S(A_i) + S(\rho_{B|A_i})] = H(A) + \sum_{i=1}^{n} p(a_i) S(\rho_{B|A_i}). \tag{3.13}$$

Onde o termo $S(A_i)$ é zero. Isso decorre do fato de que a entropia de von Neumann para estados puros é nula, visto que não existe incerteza associada. Dessa forma, para o projetor A_i vale o mesmo.

Podemos mostrar que o termo $H(A)$ encontrado na equação acima, que denota a entropia de Shannon, é igual a entropia de von Neumann $S(\Phi_A(\rho_A))$. Para tanto, tomemos o traço parcial sobre $\mathscr{H}_B$ no estado $\Phi_A(\rho_{AB})$, logo:

$$Tr_B[\Phi_A(\rho_{AB})] = Tr_B\Big[\sum_{i=1} p(a_i)A_i \otimes \rho_{B|A_i}\Big] = \sum_{i=1} p(a_i)A_i \otimes Tr_B[\rho_{B|A_i}], \tag{3.14}$$

como $\rho_{B|A_i}$ é normalizado, o traço é igual a 1. Dessa forma a equação se resume em;

$$Tr_B[\Phi_A(\rho_{AB})] = \sum_{i=1} p(a_i)|v_i^A\rangle\langle v_i^A| = \Phi_A(\rho_A), \tag{3.15}$$

Assim, como a entropia de von Neumann é a entropia de Shannon calculada sobre a distribuição de probabilidade constituida pelos autovalores da matriz densidade, então a equação 3.13 torna-se:

$$S(\Phi_A(\rho_{AB})) = S(\Phi_A(\rho_A)) + \sum_{i=1}^{n} p(a_i)S(\rho_{B|A_i}), \tag{3.16}$$

Substituindo esse resultado na equação para a informação mutua entre Alice e Bob:

$$I(A:B) = S(\rho_B) - S(\Phi_A(\rho_{AB})) + S(\Phi_A(\rho_A)). \tag{3.17}$$

A equação acima é uma forma completamente analítica para a obtenção da informação mutua entre as partes legítimas do protocolo.

Suponha agora que Eve, uma espião, tente roubar as informações do canal quântico. Eve atua em $\mathscr{H}_B$, fazendo medições projetivas com um operador definido no subespaço de Bob, expresso por:

$$\hat{B} = \sum_{j=1} b_i B_j. \tag{3.18}$$

Dessa forma, com a intervação de Eve, o estado quântico que os usários recebem em seus laboratórios é modificado. Tanto Alice quanto Bob não recebem mais o estado ρ_{AB}, mas sim o estado definido pelo mapa $\Xi_B : \mathscr{H}_{AB} \to \mathscr{H}_{AB}$, que atua no estado ρ_{AB}. Visto que Eve realiza uma medição não revelada, é possível usar a equação da transformação em termos dos operadores de Kraus para descrever a ação de Eve nesse canal, logo:

$$\Xi_B(\rho_{AB}) = \sum_{i=1}^{n} (\mathbb{I}^A \otimes B_i)\rho_{AB}(\mathbb{I}^A \otimes B_i). \tag{3.19}$$

Para simplificar a notação, tomemos $\Xi_B(\rho_{AB}) = \sigma_{AB}$. Assim, o estado que Alice e Bob recebem é a matriz densidade σ_{AB}. O procedimento para encontrar uma expressão para

$I(A,E)$ vai ser exatamente como foi feito para o caso de Alice e Bob, contudo não sera mais utilizado o estado ρ_{AB} mas sim o mapa anteriormente definido, visto que Bob recebe um estado que foi modificado por um agente externo. Então:

$$I(A:E) = S(E) - S(E|A). \tag{3.20}$$

Como Eve atua na partição de Bob, realizando medições locais com o operador $\hat{B}$ definido em $\mathscr{H}_B$, logo:

$$I(A:E) = S(\sigma_B) - S(\sigma_B|A). \tag{3.21}$$

Onde $S(\sigma_B)$ representa a entropia do estado σ_B da partição de Bob e $S(\sigma_B|A)$ é a entropia do estado σ_B condicionado a uma medição projetiva realizada por Alice. Assim, depois de uma serie de medições com saidas a_i:

$$I(A:E) = S(\sigma_B) - \sum_{i=1}^{n} p(a_i) S(\sigma_{B|A_i}). \tag{3.22}$$

Assim, para encontrar o estado $\sigma_{B|A_i}$ é necessário fazer o traço parcial sobre o estado colapsado de σ_{AB} obtido imediatamente após uma medição projetiva de Alice. Então:

$$\sigma_{AB}^{(a_i)} = \frac{(A_i \otimes \mathbb{I}^B)\sigma_{AB}(A_i \otimes \mathbb{I}^B)}{p(a_i)}. \tag{3.23}$$

Portanto, realizando a operação traço parcial sobre $\mathscr{H}_A$:

$$\sigma_{B|A_i} = Tr_A[\sigma_{AB}^{(a_i)}] = \sigma_{B|A_i} = \sum_{i'=1} \langle v_{i'}^A | \left[\frac{(\mathbb{I}^A \otimes A_i)\sigma_{AB}(\mathbb{I}^A \otimes A_i)}{p(a_i)} \right] | v_{i'}^A \rangle. \tag{3.24}$$

Que se reduz na seguinte expressão

$$\sigma_{B|A_i} = \frac{\langle v_i^A | \sigma_{AB} | v_i^A \rangle}{p(a_i)}. \tag{3.25}$$

Usando novamente a representação de Kraus para expressar as medidas projetivas de Alice sobre σ_{AB}, encontramos que:

$$\Phi_A(\sigma_{AB}) = \sum_{i=1} (\mathbb{I}^B \otimes A_i)\sigma_{AB}(\mathbb{I}^B \otimes A_i) = \sum_{i=1} A_i \otimes \langle v_i^A | \sigma_{AB} | v_i^A \rangle. \tag{3.26}$$

Substituindo o resultado 3.25 na última igualdade da equação acima, chega-se em:

$$\Phi_A(\sigma_{AB}) = \sum_{i=1} p(a_i) A_i \otimes \sigma_{B|A_i}, \tag{3.27}$$

Que ao aplicar o teorema da entropia conjunta fica:

$$S(\Phi_A(\sigma_{AB})) = \sum_{i=1} p(a_i) S(\sigma_{B|A_i}) + S(\Phi_A(\sigma_A)). \tag{3.28}$$

O procedimento feito para chegar na equação acima segue os mesmos passos feitos para a obtenção da expressão 3.16 após a aplicação do teorema da entropia conjunta na equação 3.11.

Substituindo esse resultado em 3.21 encontramos uma equação analítica para a informação mutua compartilhada entre Alice e Eve:

$$I(A:E) = S(\sigma_B) - S(\Phi_A(\sigma_{AB})) + S(\Phi_A(\sigma_A)). \tag{3.29}$$

Finalmente, podemos usar a expressão acima junto da equação encontrada para informação mutua entre Alice e Bob e substituir na equação definida para K e assim obter que:

$$K = S(\rho_B) - S(\Phi_A(\rho_{AB})) + S(\Phi_A(\rho_A)) - S(\sigma_B) + S(\Phi_A(\sigma_{AB})) - S(\Phi_A(\sigma_A)). \tag{3.30}$$

Que consiste na equação da taxa de chave secreta escrita em termos da entropia de von Neumann.

3.2 Um Estudo de Caso: O Estado de Werner

Para analisar a eficiência da equação da taxa de chave secreta encontrada anteriormente, é possível fazer um estudo de caso usando o estado de Werner, cuja expressão é dada por:

$$\rho_{AB} = \rho_\mu = (1-\mu)\frac{\mathbb{I}^A \otimes \mathbb{I}^B}{4} + \mu |s\rangle\langle s|. \tag{3.31}$$

μ é um parâmetro de ruído pertecente ao intervalo fechado $[0,1]$ e $|s\rangle$ o estado singleto definido em termos da base ortonormal $\{|+\rangle, |-\rangle\}$ de autoestados do operador σ_z e expresso por (TANNOUDJI *et al.*, 2019b)

$$|s\rangle = \frac{|+_A -_B\rangle - |-_A +_B\rangle}{\sqrt{2}}. \tag{3.32}$$

Em sistemas descritos por estado de Werner, é vantajoso definir os observáveis gerais de medida de spin $\hat{A}$ e $\hat{B}$. Para essa análise, o operador $\hat{A}$ vai representar o observável de medição local de spin na partição da Alice, dado por:

$$\hat{A} = \sum_{i=1} \vec{\sigma} \cdot \hat{\mathbf{a}} = \sum_{i=1} \sigma_i a_i \tag{3.33}$$

Onde $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ são as matrizes de Pauli e $\hat{\mathbf{a}} = (a_1, a_2, a_3)$ é um vetor unitário em coordenadas esféricas que vai generalizar as medições projetivas de spin em qualquer direção.

$$\hat{\mathbf{a}} = sen(\theta_A)cos(\phi_A)\hat{\mathbf{x}} + sin(\theta_A)sen(\phi_A)\hat{\mathbf{y}} + cos(\theta_A)\hat{\mathbf{z}}. \tag{3.34}$$

E o operador $\hat{B}$, atuando em $\mathscr{H}_B$, vai ser o operador de medições locais que representa a invasão de Eve no canal, que pode ser escrito como:

$$\hat{B} = \sum_{j=1} \vec{\sigma} \cdot \hat{e} = \sum_{i=1} \sigma_i e_i. \tag{3.35}$$

Como anteriormente, $\hat{e}$ representa um vetor em coordenadas esféricas que vai generalizar as medições de spin em qualquer direção. Porém, a diferença agora é que esses ângulos são referentes as medições de Eve. Então:

$$\hat{\mathbf{e}} = sen(\theta_e)cos(\phi_e)\hat{\mathbf{x}} + sin(\theta_e)sen(\phi_e)\hat{\mathbf{y}} + cos(\theta_e)\hat{\mathbf{z}}. \tag{3.36}$$

Dado que $\hat{A}$ e $\hat{B}$ são matrizes Hermitianas que definem observáveis em espaços de Hilbert, a decomposição espectral garante que (NIELSEN; CHUANG, 2000):

$$\begin{aligned} \hat{A} &= \sum_{i=1} a_i A_i, \\ \hat{B} &= \sum_{i=1} b_j B_j. \end{aligned} \tag{3.37}$$

Pelas equações de $\hat{A}$ e $\hat{B}$ em termos das matrizes de Dirac, é possível achar a forma matricial dos operadores de spin, bem como seus autovetores. Assim, a forma matricial de $\hat{A}$ é:

$$\hat{A} = \sum_{i=1} \sigma_i a_i = \sigma_1 a_1 + \sigma_2 a_2 + \sigma_3 a_3 = \begin{bmatrix} cos(\theta_A) & sin(\theta_A)e^{-i\phi_A} \\ sen(\theta_A)e^{i\phi_A} & -cos(\theta_A) \end{bmatrix}. \tag{3.38}$$

Os autovalores da matriz acima são $\{+1, -1\}$ associados respectivamente aos autovetores $|\psi_A^+\rangle$ e $|\psi_A^-\rangle$, cuja a forma em vetor coluna é:

$$|\psi_A^+\rangle = \begin{bmatrix} cos(\frac{\theta_A}{2}) \\ sen(\frac{\theta_A}{2})e^{i\phi_A} \end{bmatrix}. \tag{3.39}$$

e para $|\psi_A^-\rangle$

$$|\psi_A^-\rangle = \begin{bmatrix} -e^{-i\phi_A} sen(\frac{\theta_A}{2}) \\ cos(\frac{\theta_A}{2}) \end{bmatrix}. \tag{3.40}$$

Além disso, os dois autoestados acima podem ser escritos em termos da base de autoestados do operador σ_z, logo:

$$|\psi_A^+\rangle = cos(\frac{\theta_A}{2})|+\rangle + sen(\frac{\theta_A}{2})e^{i\phi_A}|-\rangle, \tag{3.41}$$

$$|\psi_A^-\rangle = -sen(\frac{\theta_A}{2})e^{-i\phi_A}|+\rangle + cos(\frac{\theta_A}{2})|-\rangle. \tag{3.42}$$

Como a analise do caso é feita usando medidas de spin, a matriz de $\hat{B}$ de Eve tem exatamente a mesma forma que a matriz $\hat{A}$, sendo apenas diferente em seu indice do ângulo. Assim:

$$\hat{B} = \begin{bmatrix} cos(\theta_e) & sin(\theta_e)e^{-i\phi_e} \\ sen(\theta_e)e^{i\phi_e} & -cos(\theta_e) \end{bmatrix}. \tag{3.43}$$

Apresentando os mesmos autovalores e os mesmos autovetores, mudando apenas o indíce para o ângulo de Eve. Então, em termos da base gerada por σ_z, tem-se:

$$|\psi_B^+\rangle = cos(\frac{\theta_e}{2})|+\rangle + sen(\frac{\theta_e}{2})e^{i\phi_e}|-\rangle. \tag{3.44}$$

$$|\psi_B^-\rangle = -sen(\frac{\theta_e}{2})e^{-i\phi_e}|+\rangle + cos(\frac{\theta_e}{2})|-\rangle. \tag{3.45}$$

Com as expressões acima, somos capazes de cálcular todas as equações dos mapas necessários que nos permite encontrar uma equação para K em termos das informações mútuas. Porém, devido aos elementos de algumas matrizes serem muito grandes, nem todas os mapas foram representados na forma matricial linhas e colunas. Para começar, busquemos a informação mútua entre Alice e Bob, cuja expressão, encontrada anteriormente, é:

$$I(A:B) = S(\rho_B) - S(\Phi_{AB}(\rho_{AB})) + S(\Phi_A(\rho_A)). \tag{3.46}$$

Cálculemos agora a entropia de von Neumann para as matrizes $\rho_B, \Phi_A(\rho_{AB})$ e $\Phi_A(\rho_A)$. Assim, começando com $S(\rho_B)$, é necessário encontrar a forma matricial de ρ_B e seus

autovalores de modo que seja possível aplicar a definição da entropia de von Neumann mostrada em 2.35.

A matriz reduzida ρ_B, obtida a partir do estado de Werner, pode ser encontrada usando a relação do traço parcial dada no apêndice D. Então:

$$\rho_B = Tr_A(\rho_\mu) = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}. \tag{3.47}$$

Como os autovalores da matriz acima são 1/2 e 1/2, a entropia de von Neumann fica:

$$S(\rho_B) = -\frac{1}{2}\ln(\frac{1}{2}) - \frac{1}{2}\ln(\frac{1}{2}) = \ln(2). \tag{3.48}$$

Para calcular $\Phi_A(\rho_{AB})$ é necessário usar equação para o mapa em termos dos operadores de Kraus mostrado na equação 3.9. Portanto:

$$\begin{aligned} \Phi_A(\rho_\mu) = (|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B)\rho_\mu(|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B) \\ +(|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B)\rho_\mu(|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B). \end{aligned} \tag{3.49}$$

Os termos $|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B$ e $|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B$ são matrizes 4x4 obtidas usando os projetores do operador $\hat{A}$ mostrados em 3.39 e 3.40. Os elementos do conjunto abaixo são os autovalores do mapa da equação acima, obtidos com o auxílio do software Mathematica 11.2.

$$\left\{\frac{1-\mu}{4}, \frac{1-\mu}{4}, \frac{1+\mu}{4}, \frac{1+\mu}{4}\right\}. \tag{3.50}$$

Com isso, é possível calcular $S(\Phi_A(\rho_\mu))$. Assim, aplicando as propriedades do logarítimos para simplificar a equação, encontra-se que:

$$S(\Phi_A(\rho_{AB})) = \frac{1}{2}(\ln(16) + (\mu-1)\ln(1-\mu) - (1+\mu)\ln(1+\mu)). \tag{3.51}$$

Por último é necessário encontrar o mapa $\Phi_A(\rho_A)$. Aqui, a operação de Kraus é feita sobre uma matriz 2x2, de modo que não é mais necessário o produto tensorial com as matrizes identidades na equação 3.26. Assim, o resultado do cálculo da entropia para o estado acima vai ter como resultado o mesmo obtido em $S(\rho_B)$, já que as matrizes são iguais. Dessa forma:

$$S(\Phi_A(\rho_A)) = log(2). \tag{3.52}$$

Com esse último resultado, somos capazes de encontrar a informação mútua entre Alice e Bob substituindo todas essas relações de entropia na equação $I(A:B)$, assim:

$$I(A:B) = 2\ln(2) - \frac{1}{2}(\ln(16) + (\mu-1)\ln(1-\mu) - (1+\mu)\ln(1+\mu)) \tag{3.53}$$

Para encontrar a taxa de chave secreta adequada ao estado de Werner, é necessário agora buscar a entropia de Alice e Eve, cuja equação é:

$$I(A:E) = S(\sigma_B) - S(\Phi_A(\sigma_{AB})) + S(\Phi_A(\sigma_A)). \tag{3.54}$$

Mais uma vez precisamos calcular cada mapa que aparece na equação acima e depois aplicar a entropia de von Neumann. A diferença para esse procedimento vai ser no fato de que a matriz ρ_{AB} é interceptada por Eve e uma medição projetiva do operador $\hat{B}$ é realizada em $\mathscr{H}$. Dessa forma é preciso obter a expressão do mapa $\Xi_B(\rho_{AB}) = \sigma_{AB}$ que define o ataque de Eve no canal. Usando a equação 3.19:

$$\sigma_{AB} = (\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|) + (\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|). \tag{3.55}$$

Como os operadores $\hat{A}$ e $\hat{B}$ denotam os mesmos operadores gerais de spin, tendo como única diferença o indice do ângulo, a forma da matricial da equação acima teria a mesma forma da matriz do mapa $\Phi_A(\rho_\mu)$, mudando apenas o indice de ângulo ($a \to e$). Como a intervenção de Eve modifica o estado para os dois usuários do canal, Alice vai receber o estado σ_{AB} assim como Bob. Dito isso, quando Alice realizar sua medição projetiva local em $\mathscr{H}$, o mapa que define essa ação vai ser dadao por:

$$\begin{aligned}\Phi_A(\sigma_{AB}) = (|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B)\sigma_{AB}(|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B) + \\ (|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B)\sigma_{AB}(|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B).\end{aligned} \tag{3.56}$$

Substituindo a expressão para σ_{AB} na equação acima:

$$\begin{aligned}\Phi_A(\sigma_{AB}) = (|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B)\Big[(\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|) \\ +(\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|)\Big](|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B) + \\ (|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B)\Big[(\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+|) \\ +(\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|)\rho_\mu(\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-|)\Big](|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B).\end{aligned} \tag{3.57}$$

Para melhor visualizar a equação acima, podemos definir:

$$|\psi_A^+\rangle\langle\psi_A^+| \otimes \mathbb{I}^B \equiv \tilde{A}_+, \tag{3.58}$$

$$|\psi_A^-\rangle\langle\psi_A^-| \otimes \mathbb{I}^B \equiv \tilde{A}_- \tag{3.59}$$

Como também:

$$\mathbb{I}^A \otimes |\psi_B^+\rangle\langle\psi_B^+| \equiv \tilde{B}_+, \tag{3.60}$$

$$\mathbb{I}^A \otimes |\psi_B^-\rangle\langle\psi_B^-| \equiv \tilde{B}_- \tag{3.61}$$

Logo a equação para $\Phi_A(\sigma_{AB})$, torna-se:

$$\Phi_A(\sigma_{AB}) = \tilde{A}_+\tilde{B}_+\rho_\mu\tilde{A}_+\tilde{B}_+ + \tilde{A}_+\tilde{B}_-\rho_\mu\tilde{B}_-\tilde{A}_+ + \tilde{A}_-\tilde{B}_+\rho_\mu\tilde{B}_+\tilde{A}_- + \tilde{A}_-\tilde{B}_-\rho_\mu\tilde{B}_-\tilde{A}_-. \tag{3.62}$$

Assim, para proceder com o cálculo é necessário obter os autovalores do mapa $\Phi_A(\sigma_{AB})$, para isso foi usado o software Mathematica 11.3, e os autovalores foram listados no conjunto abaixo.

$$\begin{aligned}\Big\{&\frac{1}{4}(\ln(1+\mu cos(\theta_a)cos(\theta_e)+\mu cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e)),\\ &\frac{1}{4}(\ln(1+\mu cos(\theta_a)cos(\theta_e)+\mu cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e)),\\ &\frac{1}{4}(\ln(1-\mu cos(\theta_a)cos(\theta_e)+\mu cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e)),\\ &\frac{1}{4}(\ln(1+\mu cos(\theta_a)cos(\theta_e)+\mu cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e))\Big\}.\end{aligned} \tag{3.63}$$

Com os autovalores é possível usar a expressão para a entropia de von Neumann e obter que:

$$\begin{aligned}S(\Phi_A(\sigma_{AB})) = \frac{1}{2}(&\ln(16) - \ln(1+\mu cos(\theta_a)cos(\theta_e)\mu cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e) -\\ &\ln(1-\mu(cos(\theta_a)cos(\theta_e)+cos(\phi_a-\phi_e)sin(\theta_a)sen(\theta_e)) -\\ &2\mu arctanh[\mu(cos(\theta_a)cos(\theta_e)+\\ &cos(\phi_a-\phi_e)sen(\theta_a)sen(\theta_e)](cos(\theta_a)cos(\theta_e)+cos(\phi_a-\phi_e)sin(\theta_a)sen(\theta_e)).\end{aligned} \tag{3.64}$$

Calculemos agora a entropia $S(\sigma_B)$ referente ao reduzido σ_B obtido da matriz densidade σ_{AB}. Para encontrar os autovalores da matriz σ_B tomou-se a operação tração parcial sobre o subespaço $\mathscr{H}_A$ na equação 3.55. O conjunto abaixo representa os autovalores do mapa σ_B, obtido com o auxílio do software Mathematica 11.3.

$$\Big\{\frac{1}{2},\frac{1}{2}\Big\}. \tag{3.65}$$

Então:

$$S(\sigma_B) = \ln(2). \tag{3.66}$$

Portanto, para obter $\Phi_A(\sigma_A)$ é preciso utilizar os operadores de Kraus. Aqui não é mais necessário fazer o produto tensorial com as matrizes unitárias visto que a matriz que vai passar pela transformação é 2x2. Assim:

$$\Phi_A(\sigma_A) = (|\psi_A^+\rangle\langle\psi_A^+|)\sigma_A(|\psi_A^+\rangle\langle\psi_A^+|) + (|\psi_A^-\rangle\langle\psi_A^-|)\sigma_A(|\psi_A^-\rangle\langle\psi_A^-|). \tag{3.67}$$

A operação de obtenção e simplificação do mapa definido acima foi feito com o auxílio do software matemática 11.3. A matriz encontrada tem a seguinte forma:

$$\Phi_A(\sigma_A) = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}. \tag{3.68}$$

E assim a entropia é:

$$S(\Phi_A(\sigma_A)) = \ln(2). \tag{3.69}$$

Com esse último resultado tem-se tudo em mãos para encontrar a taxa de chave secreta para um canal dado por um estado de Werner. Como a relação encontrada anteriormente para K, é dada por:

$$K = S(\rho_B) - S(\Phi_A(\rho_{AB})) + S(\Phi_A(\rho_A)) - S(\sigma_B) + S(\Phi_A(\sigma_{AB})) - S(\Phi_A(\sigma_A)). \tag{3.70}$$

Primeiramente, substituindo apenas $S(\rho_B)$, $S(\Phi_A(\rho_A))$, $S(\sigma_B)$ e $S(\Phi_A(\sigma_A))$, temos:

$$K = \ln(2) - S(\Phi_A(\rho_{AB})) + \ln(2) - \ln(2) + S(\Phi_A(\sigma_{AB})) - \ln(2). \tag{3.71}$$

Os termos de $\ln(2)$ se anulam aos pares visto que representam a entropia de um estado maximamente misturado, cuja a matriz é proporcional a identidade. A equação então se reduz à:

$$K = -S(\Phi_A(\rho_{AB})) + S(\Phi_A(\sigma_{AB})). \tag{3.72}$$

Antes de substituirmos as duas entropias restantes na equação acima, avaliemos a equação 3.64 mais uma vez. É possível perceber que existe um termo presente na equação dado por:

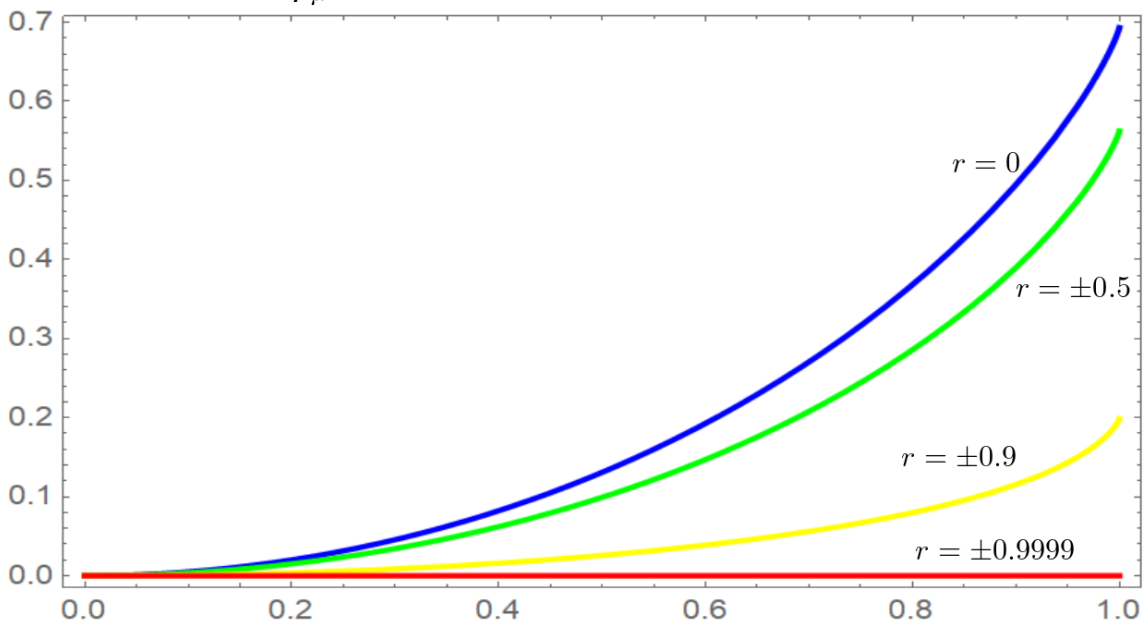
$$cos(\theta_a)cos(\theta_e) + cos(\phi_a - \phi_e)sen(\theta_a)sen(\theta_e), \tag{3.73}$$

Que consiste em uma função expressa em termos dos ângulos que determinam as medições dos observáveis $\hat{A}$ e $\hat{B}$. Essa função corresponde ao produto interno dos vetores unitários $\hat{a}$ e $\hat{e}$. Assim, seja $r = \hat{a} \cdot \hat{e}$, com r definido no intervalo fechado [-1,1]. Dessa forma substituindo na equação para K a entropia $S(\Phi_A(\rho_{AB}))$ encontrada em 3.51 junto da equação de $S(\Phi_A(\sigma_{AB}))$ em termos desse parâmetro r, encontra-se que:

$$\begin{aligned} K = \frac{1}{2}(&\ln(1-\mu) + \ln(\mu+1) + 2\mu arctanh(\mu) \\ &- \ln(1-\mu r) - \ln(\mu r+1) - 2\mu r arctanh(\mu r)) \end{aligned} \tag{3.74}$$

Que consiste na equação para a taxa de chave secreta usando o estado de Werner. O resultado de K pode ser mostrado no gráfico da figura 3, a seguir:

Figura 3 – Gráfico da taxa de chave, representada para alguns valores de r, usando o estado de Werner ρ_μ.



Fonte: elaborado pelo autor (2022).

Para mostrar que a equação obtida acima é monótona com respeito a μ (pois Eve não pode conseguir mais informação que os usuários legítimos), considere a sua derivada primeira

com respeito a μ mantendo r constante:

$$K' = arctanh(\mu) + r[arctanh(r\mu)]. \tag{3.75}$$

Pelo teste da derivada primeira, a função K vai ser crescente se, e somente se, $K' \geq 0$ (GUIDORIZZI, 2016). Já que μ é definido apenas no intervalo fechado [0,1], então a função $arctanh(\mu)$ é crescente em μ. Assim é necessário avaliar apenas o estudo do sinal para o termo $r[arctanh(r\mu)] \geq 0$. Portanto, $r[arctanh(r\mu)] \geq 0$ vai ser igual a 0 se, e somente se, $r = 0$ ou $\mu = 0$. Se $r < 0$ o termo entre colchetes vai ser negativo, e a multiplicação por r vai fornecer que $r[arctanh(r\mu)] > 0$. Se $r > 0$, por trivialidade, temos que $r[arctanh(r\mu)] > 0$. Assim concluimos que dado um valor de r dentro do intervalo fechado $[-1, 1]$, a derivada K' é positiva. Uma vez que a derivada é sempre positiva, então a função K é monótona com respeito a μ.

O resultado da figura 3 mostra o gráfico de K para a linha azul (r = 0), linha verde (r = $\pm$0.5), linha amarela (r = $\pm$0.9) e linha vermelha (r = $\pm$0.9999). Em todos esses casos é possível constatar que a taxa de chave secreta K, cresce de forma monotóna com μ. K atinge seu máximo para o estado puro singleto, que consiste em um dos estados de Bell (NIELSEN; CHUANG, 2000). Então, o parâmetro r pode ser visto como o grau de atuação de Eve nesse canal quântico compartilhado por Alice e Bob. Se $r = 0$ o canal está livre da invasão ou Eve atinge a mesma quantidade de informação mutua entre Alice e Bob, de modo que $I(A : B) = I(A : E)$ o que implica em $K = 0$, informando aos usuários legítimos que o canal não é mais seguro.

Assim, existe uma quantidade de informação mútua entre Alice e Eve denotada por $I(A : E)$, devido a medição que Eve faz ao invadir o canal. Assim sendo, o que a equação 3.1 para a taxa de chave secreta faz é mensurar o vazamento de informação compartilhada entre Alice e Bob devido a Eve. Pois como a medida de Eve muda o estado para os dois usuários, graças a natureza não local da mecânica quântica (BALLENTINE, 1998), vai então existir uma quantidade de informação mutua entre Alice e Eve, visto que Alice segue o protocolo normalmente realizando sua medição projetiva local. Posto isso, se $I(A : B) - I(A : E) > 0$, que consiste em uma condição suficiente para que esse canal quântico seja seguro, então é possível os usuários desses canal compartilhem uma chave secreta para o envio e recebimento de mensagens com a garantia de que nenhuma informação vai ser vazada (GROSSHANS *et al.*, 2003).

Portanto, conclui-se que a medida que o valor de r cresce em módulo, o gráfico de K diminui mostrando que quanto mais intenso for a atuação de Eve no roubo de informação menor é a capacidade do canal compartilhar uma chave secreta de forma segura.

4 CONCLUSÕES

A natureza não-local da mecânica quântica é foco de estudo até hoje, dado a estranheza da ação a distância que aparece em fenômenos quânticos. Assim, aplicações da não-localidade e da incerteza de Heisenberg, que são conceitos intrínseco da MQ, são de extrema valia para tarefas em computação quântica e teoria da informação quântica, como por exemplo na distribuição de chaves quânticas (DCQ).

Esse trabalho, sustentado na não localidade quântica e no conceito de informação mutua, procurou fazer uma analise da segurança de um canal quântico definido por um estado bipartido ρ_{AB} compartilhado por dois usuários legítimos Alice e Bob. Dessa forma, exploramos rapidamento os princípios matemáticos que modelam a teoria quântica, como a noção de espaço de Hilbert e operadores. Depois, partimos para o estudo da MQ e seus postulados, onde o conceito de mapa de medição projetiva local foi apresentado.

Vimos como a noção de entropia se relaciona com a informação por meio dos quantificadores apresentados. Dentro desse contexto, foi mostrado como a entropia de Shannon pode ser generalizada para um caso quântico por meio da matriz densidade, obtendo a entropia de von Neumann, que quantifica a informação quântica do sistema. Feito isso, foi construido a noção de informação compartilhada para um estado bipartido, por meio do quantificador de informação mutua definido em termos das entropias de von Neumann.

Com o conceito de informação mutua apresentado, foi introduzido então a noção da taxa de chave secreta (K), que consiste em uma relação para atestar a segurança de um canal quântico, dado a existência de um invasor (Eve) que realiza uma medição local, modificando o estado que os usuários legítimos recebem. Dessa forma, Eve compartilha um valor de informação com um dos usuários legítimos.

Assim, foi encontrado uma relação geral para a taxa de chave secreto em termos das entropias. Essa taxa de chave deve se comportar de modo que $K > 0$, visto que é impossível para Eve compartilhar mais informação que os usuários legítimos. Com a equação geral encontrada, foi usado o estado de Werner para atestar a segurança, busando encontrar o valor de K em termos dos autovalores para os mapas das transformações. Após encontrar a equação para K, verificou-se o estudo do sinal para concluir que a expressão encontrada era crescente em termos de um valor fixo de r dentro do intervalo $[-1,1]$ ao variar o valor de $\mu : [0,1]$.

Feito isso, os resultados plotados na figura 3, mostram o que acontece com o comportamento da função K a medida que a intervenção de Eve é atenuada ou intensificada no

canal. Verificou-se que o parâmetro r designa a ação de Eve no canal, consequentemente quanto maior o valor de r, menor é o valor obtido para a função K. Esse resultado atesta para os usuários legítimos que o canal não é mais seguro e que a informação compartilhada está sendo vazada devido a invansão de Eve. Para r = 0.9999 afere-se que K é anulado, mostrando que Eve pode atingir o mesmo valor de informação mutua entre Alice e Bob e assim zerando a taxa de chave secreta.

REFERÊNCIAS

BALLENTINE, L. E. **Quantum Mechanics A Morden Development**. [S.l.]: World Scientific Publishing, 1998. ISBN 981-02-4105-4.

BRAUNSTEIN, S. L.; PIRANDOLA, S. Side-channel-free quantum key distribution. **Phys. Rev. Lett.**, American Physical Society, v. 108, p. 130502, Mar 2012. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.108.130502. Acesso em: 1 maio 2022.

EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physics reality be considered complete? **Physical Review**, Nova Jersey, v. 47, n. 1, p. 777–779, 1935.

GOMES, V.; DIEGUEZ, P.; VASCONCELOS, H. Realism-based nonlocality: Invariance under local unitary operations and asymptotic decay for thermal correlated states. **Physica A:** statical mechanics and its applications, v. 601, p. 127568, 2022. ISSN 0378-4371. Disponível em: https://www.sciencedirect.com/science/article/pii/S0378437122003958. Acesso em: 8 março 2022.

GRIFFITHS, D. J. **Introduction to Quantum Mechanics**. [S.l.]: Cambridge University Press, 2018. ISBN 978-1107189638.

GROSSHANS, F.; CERF, N. J.; WENGER, J.; TUALLE-BROURI, R.; GRANGIER, P. **Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables**. arXiv, 2003. Disponível em: https://arxiv.org/abs/quant-ph/0306141. Acesso em: 18 jun. 2022.

GUIDORIZZI, H. L. **Um Curso de Cálculo**. [S.l.]: LTC,2016. v. 1. ISBN 978-85-216-3056-2.

GYONGYOSI, L.; IMRE, S. Properties of the quantum channel. **ArXiv**, abs/1208.1270, 2012.

HAYASHI, M. **Quantum Information Theory**: Mathematical foundation. [S.l.]: Springer, 2017. ISBN 978-3-662-49725-8.

LIMA, B. N. B.; LEANDRO; CIOLETTI, M.; CUNHA, M. de O. T.; BRAGA, G. A. **Entropia: ıntrodução à Teoria Matemática da (Des)Informação**. 2004. Minicurso apresentado na II Bienal da SBM - UFBa - Salvador - 25 a 29/10/2004. Disponível em: http://www.bienasbm.ufba.br/M40.pdf. Acesso em: 22 maio 2022.

MAZIERO, J. Entendendo a entropia de von neumann. **Revista Brasileira de Ensino de Física**, Brasil, v. 37, n. 1, p. 1314, 2015.

NAKAHARA, M. **Quantum Computing From Linear Algebra to Physics Realizations**. [S.l.]: CRC Press, 2008. ISBN 9780429146510.

NESS, H. V. **Understanding Thermodynamics**. [S.l.]: Dover Publications,Inc. Newfurk, 1969. ISBN 9780486632773.

NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. [S.l.]: Cambridge University Press, 2000. ISBN 978-1-107-00217-3.

PETZ, D. **Quantum Information Theory and Quantum Statistics**. Berlin Heidelberg: Springer, 2008. ISBN 978-3-540-74634-8.

PRESKILL, J. **Lecture Notes for Ph219/CS219 Quantum Information Chapter 3**. 2018. Updated October 2018. Disponível em: http://theory.caltech.edu/~preskill/ph219/chap3_15.pdf. Acesso em: 23 maio 2022.

RIGOLIN, G.; RIEZNIK, A. A. **Introduction to quantum cryptography**. arXiv, 2005. Disponível em: https://arxiv.org/abs/physics/051112

S.T.PIRES, A. **Evolução das Ideias da Física**. São Paulo: Livraria da Física, 2011. ISBN 978-85-7861-103-3.

SU, X. **Applying gaussian quantum discord to quantum key distribution**. arXiv, 2013. Disponível em: https://arxiv.org/abs/1310.4253. Acesso em: 8 maio 2022.

TANNOUDJI, C. C.; DIU, B.; LALOE, F. **Quantum Mechanics**: basic concepts, tools, and applications. [S.l.]: Wiley-Vch, 2019. v. 1. ISBN 978-3527345533.

TANNOUDJI, C. C.; DIU, B.; LALOE, F. **Quantum Mechanics**: angular momentum, spin, and approximation methods. [S.l.]: Wiley-Vch, 2019. v. 2. ISBN 978-3527345540.

VALBER. **Não Localidade Baseada em Realismo**. Tese (Doutorado) - Universidade do Paraná, Setor de Ciências Exatas, Programa de Pós-graduação em física, 2018, Curitiba, 2018.

WILDE, M. M. **Quantum Information Theory**. [S.l.]: Cambridge University Press, 2013. ISBN 978-1-107-03425-9.

ZETTILI, N. **Quantum Mechanics:** concepts and applications. [S.l.]: Wiley, 2009.

APÊNDICE A – TEOREMA ESPECTRAL

Teorema A.0.1 *Considera A uma matriz normal cuja os autovalores são os elementos do conjunto* $\beta = \{\lambda_1, \lambda_2, \ldots, \lambda_i\}$ *associados a cada autovetor do conjunto* $\gamma = \{|v_1\rangle, |v_2\rangle, \ldots, |v_i\rangle\}$. *Tomando os elementos de* γ *como sendo ortogonais, então a matriz A pode ser decomposta da seguinte forma:*

$$A = \sum_{i=1}^{n} \lambda_i A_i = \sum_{i=1}^{n} \lambda_i |v_i\rangle\langle v_i| \tag{A.1}$$

Prova:

Pela relação de completeza para os autovetores de A, temos:

$$\sum_{i=1}^{n} |v_i\rangle\langle v_i| = \mathbb{I}. \tag{A.2}$$

Se aplicarmos a matriz de A na equação acima, chegamos em:

$$A\mathbb{I} = A\Big(\sum_{i=1}^{n} |v_i\rangle\langle v_i|\Big) = \sum_{i=1}^{n} A|v_i\rangle\langle v_i|, \tag{A.3}$$

Porém como $|v_i\rangle$ é um autovetor de A associado ao autovalor λ_i, a equação do autovalor garante que:

$$A|v_i\rangle = \lambda_i|v_i\rangle \tag{A.4}$$

Substituindo o resultado acima na equação A.3:

$$A\mathbb{I} = \sum_{i=1}^{n} A|v_i\rangle\langle v_i| = \sum_{i=1}^{n} \lambda_i|v_i\rangle\langle v_i|. \tag{A.5}$$

Finalmente:

$$\sum_{i=1}^{n} \lambda_i|v_i\rangle\langle v_i| \tag{A.6}$$

Como queriamos demonstrar.

APÊNDICE B – DEMONSTRAÇÃO DA DESIGUALDADE DE KLEIN

Teorema B.0.1 *(Desigualdade de Klein) A entropia relativa quântica é não negativa,*

$$S(\hat{\rho}||\hat{\sigma}) \geq 0, \tag{B.1}$$

A igualdade só é garantida se e somente se $\hat{\rho} = \hat{\sigma}$

Prova:

Sejam $\rho = \sum_{i=1}^{n} p_i |v_i\rangle\langle v_i|$ e $\sigma = \sum_{j=1}^{n} q_j |u_j\rangle\langle u_j|$ decomposições espectrais. Assim, fazendo uso da expressão para entropia relativa:

$$S(\rho||\sigma) = \sum_{i=1}^{n} p_i \ln p_i - \sum_{i=1}^{n} \langle v_i|\rho \ln \sigma|v_i\rangle. \tag{B.2}$$

Sendo $|v_i\rangle$ autovetor de ρ, então:

$$\langle v_i|\rho = p_i\langle v_i| \tag{B.3}$$

Substituindo o resultado acima na última termo em B.2,

$$\sum_{i=1}^{n} \langle v_i|\rho \ln \sigma|v_i\rangle = \sum_{i=1}^{n} \left(\langle v_i|\{p_i\langle v_i|\} \ln \Big[\sum_{j=1}^{n} q_j |u_j\rangle\langle u_j| \Big] |v_i\rangle \right) = \sum_{i,j=1}^{n} \ln q_j P_{ij}, \tag{B.4}$$

Com $P_{ij} = \langle v_i|u_j\rangle\langle u_j|v_i\rangle \geq 0$.

Reescrevendo a equação B.2 da seguinte forma:

$$S(\rho||\sigma) = \sum_i p_i \left(\ln p_i - \sum_j P_{ij} \ln q_j \right) \tag{B.5}$$

P_{ij} satisfaz $P_{ij} \geq 0, \sum_i P_{ij} = 1$ e $\sum_j P_{ij} = 1$. Usando o fato de que o logaritmo é uma função estritamente côncava, então , $\sum_j P_{ij} \ln q_j \leq \ln r_i$, onde $r_i \equiv \sum_j P_{ij} q_j$. A igualdade [e resgatada se, e somente se, existe um valor j tal que $P_{ij} = 1$

APÊNDICE C – PROPRIEDADES DA ENTROPIA DE VON NEUMANN

Teorema C.0.1 *Propriedades da entropia de von Neumann*

1. *A entropia é não negativa. O valor da entropia vai ser zero, se e somente se, o estado do sistema quântico é puro.*
2. *Em um espaço de Hilbert com N dimensões, a entropia de von Neumann assume o valor máximo de* $\ln(N)$. *O valor só é, exatamente, igual a* $\ln(N)$, *se e somente se, se o sistema quântico é completamente misto.*
3. *Se existe um sistema composto AB, que encontra-se em um estado puro então, S(A) = S(B).*
4. *Suponha o conjunto* $\{p_i\}$ *de probabilidades associadas a cada estado do conjunto* $\{\hat{\rho}_i\}$. *Se o os estados desse conjunto apresentarem o suporte em espaços ortogonais, logo:*

$$S(\sum_i p_i\hat{\rho}_i) = H(p_i) + \sum_i p_i S(\hat{\rho}_i) \tag{C.1}$$

5. *(Entropia Conjunta) Sendo* $\{p_i\}$ *um conjunto de probabilidades,* $\{|e_i\rangle\}_{i=1}^N$ *um conjunto ortogonal de estados para o espaço* $\mathscr{H}_A$, *e* $\{\hat{\rho}_i\}$ *for um conjunto qualquer de matrizes densidades para um sistema de um espaço* $\mathscr{H}_B$, *logo:*

$$S(\sum_i p_i|e_i\rangle\langle e_i| \otimes \hat{\rho}_i) = H(p_i) + \sum_i p_i S(\hat{\rho}_i) \tag{C.2}$$

Prova:

1. Segue da definição
2. Pela desigualdade de Klein, temos:

$$0 \leq S(\rho||\mathbb{I}/d) = -S(\rho) + \ln(d). \tag{C.3}$$

3. Pela decomposição de Schmidt os autovalores das matrizes que definem A e B são os mesmo. Assim, obtem-se a igualdade ao usar entropia de von Neumann.
4. Considere o conjunto de matrizes $\{\rho_j\}_{j=1}$. Seja também $\{\lambda_i^{\,j}\}_{i=1}^n$ autovalores correspondendo, respectivamente, a cada um dos autovetores $\{|e_i^j\rangle\}$ para cada uma das j-ésimas matrizes. Como $p_i\lambda_i^{\,j}$ são autovalores e $|e_i^j\rangle$ autovetores para a matriz $\sum_{j=1}^n p_j\rho_j$. Dessa forma:

$$S(\sum_{j=1}^n p_j\rho_j) = -\sum_{ij} p_i\lambda_i^{\,j}\ln(p_i\lambda_i^{\,j}) = -\sum_{i=1} p_i\ln(p_i) - \sum_i^n p_i\sum_{j=1}^n \lambda_i^{\,j}\ln(\lambda_i^{\,j}). \tag{C.4}$$

Então:

$$S(\sum_{j=1}^n p_j\rho_j) = H(p_i) + \sum_{i=1}^n S(\rho_i) \tag{C.5}$$

5. Segue imediatamente da equação anterior.

APÊNDICE D – OPERAÇÃO PARA O TRAÇO PARCIAL DE UMA MATRIZ 4X4.

Considere um vetor de estado $|\psi\rangle$ qualquer dado em termos da base produto $\{|0_A, 1_B\rangle\}$. Logo:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle.$$

Com a,b,c e d $\in \mathbb{C}$. O vetor bra associado ao ket acima é dada por:

$$\langle\psi| = \langle 00|a^* + \langle 01|b^* + \langle 10|c^* + \langle 11|d^* \tag{D.1}$$

Assim, podemos calcular a matriz densidade $\rho_{Ab} = |\psi\rangle\langle\psi|$. Então:

$$\begin{aligned}
\rho_{AB} &= (a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)(\langle 00|a^* + \langle 01|b^* + \langle 10|c^* + \langle 11|d^*) \\
&= |a|^2|00\rangle\langle 00| + ab^*|00\rangle\langle 01| + ac^*|00\rangle\langle 10| + ad^*|00\rangle\langle 11| + ba^*|01\rangle\langle 00| \\
&+ |b|^2|01\rangle\langle 01| + bc^*|01\rangle\langle 10| + bd^*|01\rangle\langle 11| + ca^*|10\rangle\langle 00| + cb^*10\rangle\langle 10| \\
&+ |c|^2|10\rangle\langle 10| + cd^*|10\rangle\langle 11|da^*|11\rangle\langle 00| + db^*|11\rangle\langle 01| + dc^*|11\rangle\langle 10| \\
&+ |d|^2|11\rangle\langle 11|.
\end{aligned} \tag{D.2}$$

o elemento ρ_{11} da matriz ρ é definido em termos da operação do elemento de matriz via notação de dirac dado por $\rho_{11} = \langle 00|\rho|00\rangle$. Assim o elemento $\rho_{12} = \langle 00|\rho|10\rangle$, de modo que continuando para todos os elementos, obtemos a seguinte matriz

$$\rho_{AB} = \begin{bmatrix} |a|^2 & ab^* & ac^* & ad^* \\ ba^* & |b|^2 & bc^* & bd^* \\ ca^* & cb^* & |c|^2 & cd^* \\ da^* & db^* & dc^* & |d|^2 \end{bmatrix}. \tag{D.3}$$

Para obter a matriz reduzida ρ_B, fazemos o traço parcial sobre B, de modo que:

$$Tr_A(\rho_{\rho_{AB}}) = \rho_B = \langle 0|\rho_{AB}|0\rangle + \langle 1|\rho_{AB}|1\rangle. \tag{D.4}$$

Logo:

$$\langle 0|\rho_{AB}|0\rangle = |a|^2|0\rangle\langle 0| + ac^*|0\rangle\langle 1| + ba^*|1\rangle\langle 0| + |b|^2|1\rangle\langle 1|. \tag{D.5}$$

Da mesma forma:

$$\langle 1|\rho_{AB}|1\rangle = |c|^2|1\rangle\langle 1| + cd^*|0\rangle\langle 1| + dc^*|1\rangle\langle 0| + |d|^2|1\rangle\langle 1|. \tag{D.6}$$

Substituindo as expressões acima em D.4:

$$\rho_A = (|a|^2 + |b|^2)|1\rangle\langle 1| + (ac^* + cd^*)|0\rangle\langle 1| + (ba^* + dc^*)|1\rangle\langle 0| + (|b|^2 + |d|^2)|1\rangle\langle 1|. \quad \text{(D.7)}$$

Finalmente:

$$\rho_B = \begin{bmatrix} |a|^2 + |b|^2 & ac^* + cd^* \\ ba^* + dc^* & |b|^2 + |d|^2 \end{bmatrix} = \begin{bmatrix} \rho_{11} + \rho_{33} & \rho_{12} + \rho_{34} \\ \rho_{21} + \rho_{45} & \rho_{22} + \rho_{44} \end{bmatrix}. \quad \text{(D.8)}$$

É possível também obter a matriz densidade reduzida da parte A operando $Tr_B(\rho_{AB})$. O procedimento é exatamente como feito anteriormente para ρ_B, assim:

$$\rho_A = \langle 0|\rho_{AB}|0\rangle + \langle 1|\rho_{AB}|1\rangle. \quad \text{(D.9)}$$

Então:

$$\rho_A = (|a|^2 + |b|^2)|0\rangle\langle 0| + (ac^* + bd^*)|0\rangle\langle 1| + (ca^* + db^*)|1\rangle\langle 0| + (|c|^2 + |d|^2)|1\rangle\langle 1|. \quad \text{(D.10)}$$

A forma matricial fica então:

$$\rho_A = \begin{bmatrix} |a|^2 + |b|^2 & ac^* + bd^* \\ ca^* + db^* & |c|^2 + |d|^2 \end{bmatrix} = \begin{bmatrix} \rho_{11} + \rho_{22} & \rho_{13} + \rho_{34} \\ \rho_{31} + \rho_{41} & \rho_{33} + \rho_{44} \end{bmatrix}. \quad \text{(D.11)}$$