

---

Universidade Federal de Campina Grande  
Centro de Engenharia Elétrica e Informática  
Coordenação de Pós-Graduação em Ciência da Computação

Capacidade Quântica de Sigilo Erro-Zero e  
Informação Acessível Erro-Zero de Fontes Quânticas

Elloá Barreto Guedes da Costa

Tese submetida à Coordenação do Curso de Pós-Graduação em  
Ciência da Computação da Universidade Federal de Campina  
Grande (Campus I) como parte dos requisitos necessários para ob-  
tenção do grau de Doutor em Ciência da Computação.

Área de Concentração: Ciência da Computação  
Linhas de Pesquisa: Metodologia e Técnicas da Computação

Francisco Marcos de Assis  
(Orientador)

Campina Grande – Paraíba – Brasil  
© Elloá Barreto Guedes da Costa, 2013

---

Elloá Barreto Guedes da Costa

Capacidade Quântica de Sigilo Erro-Zero e Informação  
Acessível Erro-Zero de Fontes Quânticas

Tese submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Campina Grande (Campus I) como parte dos requisitos necessários para obtenção do grau de Doutor em Ciência da Computação.

Orientador: Francisco Marcos de Assis

Universidade Federal de Campina Grande  
Centro de Engenharia Elétrica e Informática  
Programa de Pós-Graduação em Ciência da Computação

Campina Grande, Paraíba, Brasil

2013



**DIGITALIZAÇÃO:**  
**SISTEMOTECA - UFCG**

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL DA UFCG**

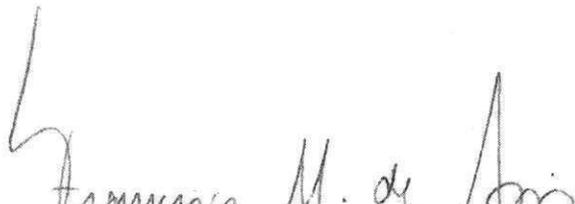
- C837c Costa, Elloá Barreto Guedes da.  
Capacidade quântica de sigilo erro-zero e informação acessível erro-zero de fontes quânticas / Elloá Barreto Guedes da Costa. – Campina Grande, 2013.  
196 f. : il.
- Tese (Doutorado em Ciência da Computação) - Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática.
- "Orientação: Prof. Dr. Francisco Marcos de Assis".  
Referências.
1. Capacidade Quântica de Sigilo Erro-Zero. 2. Informação Acessível Erro-Zero de Fontes Quânticas. 3. Teoria da Informação. 4. Teoria da Informação Quântica Erro-Zero. I. Assis, Francisco Marcos de. II. Título.

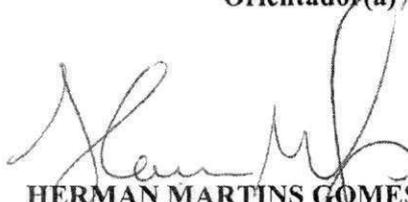
CDU 004.4(043)

**" CAPACIDADE QUÂNTICA DE SIGILO ERRO-ZERO E INFORMAÇÃO ACESSÍVEL  
ERRO-ZERO DE FONTES QUÂNTICAS"**

**ELLOÁ BARRETO GUEDES DA COSTA**

**TESE APROVADA EM 13/11/2013**

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

  
**HERMAN MARTINS GOMES, Ph.D, UFCG**  
Examinador(a)

**TIAGO LIMA MASSONI, Dr., UFCG**  
Examinador(a)

  
**MARCELO DE OLIVEIRA TERRA CUNHA, Dr., UFMG**  
Examinador(a)

  
**RENATO PORTUGAL, Dr., LNCC**  
Examinador(a)

**CAMPINA GRANDE - PB**

*Aos que amo.*

# Agradecimentos

Agradeço primeiramente a Deus pela iluminação, pelas oportunidades, pela proteção e por todas as dádivas concedidas em todos os momentos da minha vida. Agradeço também pela oportunidade de conviver e aprender diariamente com pessoas incríveis, algumas das quais cito a seguir.

Agradeço à minha família, pelo apoio constante e amor incondicional. Meu sincero agradecimento pelo privilégio de ter nascido nesse lar, por ter podido aprender valores que sempre me ajudaram em toda a minha vida e pelos momentos de alegria e de dificuldade que sempre compartilhamos e superamos juntos.

Agradeço ao meu orientador Prof. Francisco Marcos de Assis pela paciência, pelo tempo disponibilizado, pelo conhecimento compartilhado, pela confiança e pelo apoio em momentos difíceis e de superação. Carrego comigo o seu exemplo de pesquisador, de honestidade e de dedicação. Obrigada por ter me ajudado a trilhar mais essa etapa em minha vida acadêmica. Estendo meu agradecimento aos seus familiares, em especial à Dona Aída e a Juliana, que sempre se fizeram presentes e torceram por mim.

Agradeço à Andréa Mendonça, pelo apoio, pela companhia e pelas palavras de conforto e sabedoria compartilhadas em todos os momentos. Obrigada por me ajudar a acreditar que o mar há de se acalmar depois de qualquer tempestade.

Agradeço a Gilson Oliveira, por todas as discussões proveitosas, sugestões de melhoria, críticas construtivas e pelas incontáveis caronas no dia a dia. Seu exemplo de perseverança e bondade genuína são valores nos quais me inspiro a me tornar uma pessoa melhor.

Agradeço aos meus familiares maternos e paternos que me apoiaram em vários momentos da minha vida pessoal e da minha vida acadêmica. Agradeço à minha avó Josefa Ribeiro, à minha avó Maria Águida (*in memoriam*), aos meus tios Graça, Jaime, Sandra, José Leite, Consuelo, Jazette, Edson e Edna. Agradeço às minhas primas Rachel e Nara que nunca deixaram de se fazer presentes. Agradeço ao meu sobrinho Rafael por enriquecer nossas vidas todos os dias com a sua inocência e sua alegria de viver.

Agradeço a todos os professores que contribuíram para minha formação. Em especial, agradeço aos professores Aécio F. de Lima, Bernardo Lula Jr., Camilo Lélis (*in memorian*), Damião Gonçalves, Joseana Fachine e Valdiélio Menezes que acreditaram e investiram no meu potencial.

Agradeço aos meus amigos pelos inúmeros momentos de descontração e de companheirismo. Em especial a Adriana Carla, Camilla Falconi, Débora Magalhães, Débora Prazeres, Diego Tavares, Eline Alves, Francisco Neto, Georgina Serres, Irlene Matias, Larissa Lucena, Lorena Lira, Mariana Fragoso, Mariana Romão, Mikaela Maia, Paula Pérez e Renato Sobrinho. Certamente a vida seria bem menos divertida sem vocês.

Agradeço ao Instituto de Estudos em Computação e Informação Quânticas por me ter aberto as portas para a pesquisa e ter me ajudado a descobrir uma área científica pela qual me tornei completamente fascinada. Agradeço aos professores do instituto e aos colegas com os quais sempre pude aprender mais e encontrar apoio nos momentos difíceis. Meu agradecimento especial a Bruno Albert, Christiane Lima, Edmar Candeia, Francisco Revson Pereira, Marcus Vinícius Rodrigues, Rubem Medeiros e Washington César.

Agradeço aos professores e funcionários da Universidade Federal de Campina Grande pelas aulas ministradas e por toda a dedicação na prestação dos serviços e no cumprimento de suas atribuições com qualidade. Agradeço aos professores e funcionários do Programa de Pós-Graduação em Ciência da Computação, em especial ao prof. Hyggo Almeida, prof. Nazareno Andrade, Rebeqa Lemos, Vera Oliveira e Fábio Pimenta.

Aos professores e colegas de trabalho da Escola Superior de Tecnologia da Universidade do Estado do Amazonas pelo apoio na etapa de conclusão deste trabalho de tese.

Aos que contribuíram direta e indiretamente para a realização deste trabalho e que não foram mencionados aqui, meu muito obrigada.

Agradeço ao povo e ao governo brasileiro, por intermédio do CNPq, pelo apoio financeiro fornecido para execução das atividades deste doutorado.

*“A coragem surge na medida em que reconhecemos o quanto algo realmente é importante para tornar a nossa vida mais significativa. Pois, quando temos a meta de nos desenvolver interiormente, passamos a confiar que o nosso potencial de realizá-la é maior que as interferências que estão à nossa frente.”*

(Michel Rinkpoche)

*“Omnia Vincit Amor”*

(Virgílio)

# Resumo

A Teoria da Informação Quântica é uma área de pesquisa a qual considera o estudo dos limites máximos possíveis para o processamento e transmissão da informação, considerando que esta última encontra-se representada de acordo com as leis da Mecânica Quântica. Uma das maneiras de contribuir com esta área de pesquisa é no desenvolvimento de contrapartidas quânticas para os conceitos da Teoria da Informação Clássica. Graças a esta abordagem é que foi proposta a Teoria da Informação Quântica Erro-Zero, a qual considera o uso e as condições para que canais quânticos ruidosos possam transmitir informação clássica sem erros de decodificação. Apesar da proposição desta teoria e dos progressos recentes, foi identificado que o conhecimento das potencialidades, limitações e aplicações desta teoria ainda é incipiente. Na tentativa de minimizar este problema, esta tese apresenta dois novos conceitos ligados à Teoria da Informação Quântica Erro-Zero: (i) a capacidade quântica de sigilo erro-zero; e a (ii) informação acessível erro-zero de fontes quânticas. Em relação à primeira contribuição, tem-se o estabelecimento das condições necessárias para enviar informação por canais quânticos ruidosos sem que haja erros de decodificação e com sigilo absoluto, identificando uma nova capacidade de canais quânticos, estabelecendo a relação desta capacidade com a Teoria dos Grafos e identificando as situações em que esta possui caracterização de letra isolada. A segunda contribuição trata da proposição de uma medida de informação sobre fontes quânticas, a qual mensura o potencial de decodificar, sem erros, estados quânticos emitidos por estas fontes. Obter esta medida é um problema análogo ao de calcular a capacidade erro-zero de canais clássicos equivalentes e não há medida equivalente na Teoria da Informação Erro-Zero Clássica. Os conceitos propostos colaboram para o desenvolvimento da Teoria da Informação Quântica Erro-Zero em termos teóricos e práticos, uma vez que é possível considerar implementações de ambas contribuições com tecnologia existente atualmente. Além disto, intersecções da Teoria da Informação Quântica Erro-Zero junto à Criptografia, Teoria dos Grafos e Ciência da Computação são identificadas. O estabelecimento de tais contribuições colabora diretamente para a resolução de um dos desafios da Teoria da Informação Quântica, o qual trata da determinação de limites para a classe de tarefas de processamento de informação que são possíveis considerando a utilização da Mecânica Quântica.

**Palavras-chaves:** Capacidade Quântica de Sigilo Erro-Zero; Informação Acessível Erro-Zero de Fontes Quânticas; Teoria da Informação; Teoria da Informação Quântica Erro-Zero.

# Abstract

Quantum Information Theory is a research area that investigates the limits of information processing and transmission considering the laws of Quantum Mechanics. The translation of concepts from Classical Information Theory is a widely known approach to contribute to Quantum Information Theory. Thanks to that, the Quantum Zero-Error Information Theory was proposed. This theory investigates the use and the conditions for classical information exchange through noisy quantum channels without decoding errors. Despite the recent developments, it was identified that the knowledge about its potentialities, limitations and applications is still incipient. In the attempt to minimize this problem, this thesis presents two new concepts related to the Quantum Zero-Error Information Theory: *(i)* the quantum zero-error secrecy capacity; and the *(ii)* zero-error quantum accessible information. Regarding the first contribution, there is the establishment of the required conditions to send information through quantum channels without decoding errors and with perfect secrecy. This proposal identifies a new capacity of quantum channels, enlightens its relation with Graph Theory, and shows the situations where this capacity has single-letter characterization. Regarding the second contribution, there is the proposal of a quantum information measurement which quantifies the error-free decoding ability of a quantum source. Obtaining such measurement is a problem equivalent to the one of determining the zero-error capacity of an equivalent classical channel and for which there is no counterpart in Classical Zero-Error Information Theory. The concepts proposed collaborate to Quantum Zero-Error Information Theory in theoretical and practical ways, since it is possible to implement both of them using current technology. Moreover, intersections with Cryptography, Graph Theory and Computer Science were identified. These concepts contribute straightforwardly to the resolution of a challenge of Quantum Information Theory which is the determination of the limits for the tasks of information processing that can be accomplished considering the use of Quantum Mechanics.

**Keywords:** Quantum Zero-Error Secrecy Capacity; Zero-Error Quantum Accessible Information; Information Theory; Quantum Zero-Error Information Theory.

# Lista de Figuras

Figura 1	– Modelo de um canal clássico de comunicações. . . . .	30
Figura 2	– Duas seqüências distinguíveis $\mathbf{x}'$ e $\mathbf{x}''$ – para pelo menos um $i$ , $1 \leq i \leq n$ , os símbolos $x'_i$ e $x''_i$ devem ser não-adjacentes. . . . .	32
Figura 3	– Grafos correspondentes ao canal DMC $W_1$ . . . . .	34
Figura 4	– Representação de um sistema de comunicações quântico erro-zero. . . . .	35
Figura 5	– Dois estados quânticos $\rho_i$ e $\rho_j$ são distinguíveis na saída de um canal $\mathcal{E}$ caso exista pelo menos um $\rho_{i,k} \perp_{\mathcal{E}} \rho_{j,k}$ , $1 \leq k \leq n$ . . . . .	37
Figura 6	– Canal quântico de despolarização. . . . .	38
Figura 7	– Grafo representando as transições efetuadas pelo canal quântico $\mathcal{E}$ sobre a entrada. . . . .	39
Figura 8	– Grafo característico para o canal $\mathcal{E}$ do Exemplo 2.3. . . . .	41
Figura 9	– Canal quântico cuja obtenção da capacidade erro-zero é não-trivial. . . . .	41
Figura 10	– Exemplo de grafo característico de um canal quântico e de grafo não-comutativo correspondente. . . . .	44
Figura 11	– Idéia geral do canal de <i>wiretap</i> quântico. . . . .	57
Figura 12	– Modelo de um sistema de comunicações quântico em que há apenas uma fonte e um receptor. . . . .	61
Figura 13	– Valor da quantidade de Holevo para o exemplo em questão, exibido em função da relação $\theta/\pi$ (NIELSEN; CHUANG, 2010, pp. 535). . . . .	63
Figura 14	– Cenário de comunicações considerado. . . . .	66
Figura 15	– Representação das transições do canal $\mathcal{E}_1$ para os estados de entrada dos pares ótimos $(\mathcal{S}_1, \mathcal{M}_1)$ e $(\mathcal{S}'_1, \mathcal{M}'_1)$ . . . . .	75
Figura 16	– Grafos característicos para $(\mathcal{S}_1, \mathcal{M}_1)$ e $(\mathcal{S}'_1, \mathcal{M}'_1)$ . . . . .	75
Figura 17	– Resultados da simulação realizada na tentativa de maximizar o valor de $\chi^{\text{Bob}}$ nas Eqs. (3.27)-(3.28) sobre os pares $(p_0, p_1)$ . . . . .	76
Figura 18	– Representação das transições provocadas pelo canal $\mathcal{E}_2$ sobre as entradas dos pares ótimos $(\mathcal{S}_2, \mathcal{M}_2)$ e $(\mathcal{S}'_2, \mathcal{M}'_2)$ . . . . .	77
Figura 19	– Grafos característicos de $(\mathcal{S}_2, \mathcal{M}_2)$ e $(\mathcal{S}'_2, \mathcal{M}'_2)$ . . . . .	77

Figura 20	- Duas diferentes perspectivas para o gráfico obtido da busca exaustiva sobre as triplas $(p_1, p_2, p_3)$ na tentativa de maximizar a Eq. (3.35) . . .	78
Figura 21	- Representação da atuação do canal $\mathcal{E}_3$ sob as entradas do par ótimo $(\mathcal{S}_3, \mathcal{M}_3)$ e do DFS existente. . . . .	79
Figura 22	- Canal $\mathcal{E}_4$ e seu respectivo grafo característico. . . . .	80
Figura 23	- Modelo de um sistema de comunicações quântico em que há apenas uma fonte e um receptor. . . . .	85
Figura 24	- Grafo característicos da fonte quântica $F_2$ . . . . .	89
Figura 25	- Grafo característico da fonte quântica $F_3$ . . . . .	90
Figura 26	- Relações entre entropia e informação mútua. . . . .	125
Figura 27	- Modelo simplificado de um sistema de comunicações digitais ponto-a-ponto. . . . .	125

# Lista de Tabelas

Tabela 1 – Sumário de outras definições de capacidade erro-zero para canais quânticos. . . . .	46
--	----

# Lista de Símbolos e Terminologia

$\mathcal{B}(\cdot)$	Conjunto de operadores de um espaço de Hilbert
$C(\cdot)$	Capacidade ordinária de um canal clássico
$C_0(\cdot)$	Capacidade erro-zero de um canal clássico
$C_{1,\infty}(\cdot)$	Capacidade ordinária de um canal quântico
$C^{(0)}(\cdot)$	Capacidade erro-zero de um canal quântico
$C_S(\cdot)$	Capacidade de sigilo de um canal quântico
$C_S^{(0)}(\cdot)$	Capacidade de sigilo erro-zero de um canal quântico
CSS	Códigos Calderbank-Shor-Steane
$\delta_{i,j}$	Delta de Kronecker
DFS	Subespaços e Subsistemas Livres de Descoerência
DSM	Canal Clássico Discreto e Sem Memória
$H(\cdot)$	Entropia de Shannon
$\mathcal{H}$	Espaço de Hilbert
$\tilde{\mathcal{H}}$	Subespaço livre de descoerência de um espaço de Hilbert
$\mathbb{H}$	Hamiltoniano
HSW	Capacidade Holevo-Schumacher-Westmoreland
$\mathbb{1}$	Matriz identidade
$I_{\text{acc}}^{(0)}(\cdot)$	Informação Acessível Erro-Zero de uma Fonte Quântica
$\mathcal{NP}$	Classe de complexidade de tempo não-deterministicamente polinomial
OSR	<i>Operator-Sum Representation</i>
POVM	<i>Positive Operator-Valued Measurement</i>
QEAC	<i>Quantum Error-Avoiding Code</i>
QECC	<i>Quantum Error-Correcting Code</i>
QMA	Classe de complexidade <i>Quantum Merlin Arthur</i>
QZEC	Capacidade Quântica Erro-Zero
QZESC	Capacidade Quântica de Sigilo Erro-Zero
$S(\cdot)$	Entropia de von Neumann
$\text{Tr}(\cdot)$	Traço parcial

$\chi(\cdot)$	Quantidade de Holevo
$\omega(\cdot)$	Clique de um grafo
$\vartheta(\cdot)$	Função de Lovász
ZEAI	Informação Acessível Erro-Zero

# Lista de Formalismos

## Caracterizações

3.1 Canal Quântico com Capacidade Erro-Zero Positiva . . . . .	66
--	----

## Definições

Definição 2.1 Código Clássico $(m, n)$ Livre de Erros . . . . .	30
Definição 2.2 Adjacência de Símbolos Clássicos . . . . .	31
Definição 2.3 Capacidade Clássica Erro-Zero (SHANNON, 1956) . . . . .	32
Definição 2.4 Grafo Característico de um DMC (KORNER; ORLITSKY, 1998) . .	33
Definição 2.5 Código Quântico $(m, n)$ Livre de Erros . . . . .	35
Definição 2.6 Capacidade Quântica Erro-Zero (MEDEIROS, 2008) . . . . .	36
Definição 2.7 Adjacência de Estados Quânticos . . . . .	37
Definição 2.8 Par Ótimo $(\mathcal{S}, \mathcal{M})$ . . . . .	37
Definição 2.9 Grafo Característico de um Canal Quântico . . . . .	40
Definição 2.10 Subespaços Livres de Descoerência (BACON, 2001) . . . . .	49
Definição 2.11 Subsistemas Livre de Descoerência . . . . .	50
Definição 2.12 Canal <i>Wiretap</i> Quântico . . . . .	57
Definição 2.13 Código <i>Wiretap</i> Quântico de Blocos . . . . .	58
Definição 2.14 Capacidade Quântica de Sigilo . . . . .	58
Definição 2.15 Fonte Quântica Sem Memória . . . . .	60
Definição 2.16 Informação Acessível . . . . .	61
Definição 2.17 Entropia de uma Fonte Quântica . . . . .	62

Definição 3.1	Capacidade Quântica de Sigilo Erro-Zero . . . . .	69
Definição 4.1	Informação Acessível Erro-Zero . . . . .	85
Definição 4.2	Ortogonalidade de Letras Quânticas . . . . .	87
Definição 4.3	Grafo Característico de uma Fonte Quântica . . . . .	87
Definição A.1	Qubit . . . . .	111
Definição A.2	Sistemas Multi-Qubit . . . . .	112
Definição A.3	Operador Quântico . . . . .	114
Definição A.4	Produto Tensorial de Operadores Quânticos . . . . .	115
Definição A.5	Medição Projetiva . . . . .	116
Definição A.6	Operador Densidade . . . . .	117
Definição B.1	Entropia de Shannon . . . . .	123
Definição B.2	Entropia Conjunta . . . . .	123
Definição B.3	Entropia Condicional . . . . .	123
Definição B.4	Entropia Relativa . . . . .	124
Definição B.5	Informação Mútua . . . . .	124
Definição B.6	Taxa Alcançável . . . . .	126
Definição B.7	Capacidade Ordinária de um Canal Clássico . . . . .	127
Definição B.8	Entropia de von Neumann . . . . .	128
Definição B.9	Entropia Conjunta de von Neumann . . . . .	129
Definição B.10	Entropia Condicional de von Neumann . . . . .	129
Definição B.11	Informação Mútua de von Neumann . . . . .	129

## Exemplos

Exemplo 2.1	Problema do Pentágono . . . . .	33
Exemplo 2.2	Canal Quântico com Capacidade Erro-Zero Igual a Zero . . . . .	38
Exemplo 2.3	Canal Quântico com Capacidade Erro-Zero Positiva . . . . .	38
Exemplo 2.4	Capacidade Erro-Zero Obtida por Meio de um Grafo . . . . .	40
Exemplo 2.5	Versão Quântica do Problema do Pentágono . . . . .	41

Exemplo 2.6	Grafo Não-Comutativo . . . . .	44
Exemplo 2.7	Canal Quântico de Defasamento Coletivo . . . . .	51
Exemplo 2.8	Identificação de um DFS em um Canal Quântico . . . . .	54
Exemplo 2.9	Limitante de Holevo . . . . .	62
Exemplo 2.10	Medições com Resultados Inconclusivos . . . . .	63
Exemplo 3.1	QZESC Estritamente Positiva . . . . .	75
Exemplo 3.2	QZESC é Não-Trivial . . . . .	76
Exemplo 3.3	Situação 2 do Teorema 3.1 . . . . .	79
Exemplo 3.4	Canal Quântico com QZESC Igual a Zero . . . . .	80
Exemplo 4.1	Fonte Quântica com ZEAI Igual a Zero . . . . .	89
Exemplo 4.2	ZEAI de uma Fonte Quântica Puramente Clássica . . . . .	89
Exemplo 4.3	ZEAI de uma Fonte Quântica Correspondente ao Pentágono . . . . .	90

## Lemas

Lema 3.1	Par Ótimo $(S', \mathcal{M}')$ Define um QEAC . . . . .	67
Lema 3.2	Par Ótimo $(S', \mathcal{M}')$ Define Código <i>Wiretap</i> . . . . .	68

## Postulados

Postulado A.1	Espaço de Estados de um Sistema Quântico Isolado . . . . .	118
Postulado A.2	Evolução de Sistemas Quânticos Isolados . . . . .	119
Postulado A.3	Medição de Sistemas Quânticos . . . . .	119
Postulado A.4	Sistemas Quânticos Compostos . . . . .	120

## Teoremas

Teorema 2.1	Capacidade Clássica Erro-Zero em Termos de Grafos . . . . .	33
Teorema 2.2	Capacidade Quântica Erro-Zero em Termos de Grafos . . . . .	40
Teorema 2.3	Condições para os Subespaços Livres de Descoerência . . . . .	50
Teorema 2.4	Choi e Kribs (CHOI; KRIBS, 2006) . . . . .	53

Teorema 2.5	Método para obtenção de DFS . . . . .	54
Teorema 2.6	Capacidade Quântica de Sigilo . . . . .	59
Teorema 2.7	Limitante de Holevo . . . . .	62
Teorema 3.1	Capacidade Quântica de Sigilo Erro-Zero . . . . .	70
Teorema 4.1	Expressão Numérica para a ZEAI . . . . .	86
Teorema 4.2	ZEAI em Termos da Teoria dos Grafos . . . . .	88
Teorema A.1	Operador Densidade . . . . .	117
Teorema B.1	Mapeamento Quântico . . . . .	131

# Sumário

<b>1</b>	<b>Introdução</b>	<b>22</b>
1.1	Organização da Tese	27
<b>2</b>	<b>Fundamentação Teórica</b>	<b>29</b>
2.1	Teoria da Informação Clássica Erro-Zero	29
2.2	Teoria da Informação Quântica Erro-Zero	34
2.3	Subespaços e Subsistemas Livres de Descoerência	49
2.4	Capacidade Quântica de Sigilo	56
2.5	Informação Acessível	60
<b>3</b>	<b>Capacidade Quântica de Sigilo Erro-Zero</b>	<b>65</b>
3.1	Caracterização e Formalização	66
3.2	Relação com a Teoria dos Grafos	72
3.3	Análise de Segurança	74
3.4	Exemplos	75
3.5	Trabalhos Relacionados	81
<b>4</b>	<b>Informação Acessível Erro-Zero de Fontes Quânticas</b>	<b>84</b>
4.1	Caracterização e Formalização	85
4.2	Relação com a Teoria dos Grafos	87
4.3	Exemplos	89
4.4	Trabalhos Relacionados	91
<b>5</b>	<b>Considerações Finais</b>	<b>94</b>
5.1	Contribuições	94
5.2	Perspectivas para Pesquisa	99
	<b>Referências Bibliográficas</b>	<b>102</b>
	<b>Apêndice A Noções Gerais da Mecânica Quântica</b>	<b>110</b>
A.1	Representação da Informação	111
A.2	Processamento da Informação	114
A.3	Medição da Informação	116
A.4	Operador Densidade	117
A.5	Postulados da Mecânica Quântica	118

A.6	Medição POVM . . . . .	120
<b>Apêndice B</b>	<b>Noções Gerais da Teoria da Informação . . . . .</b>	<b>121</b>
B.1	Teoria da Informação Clássica . . . . .	122
B.2	Teoria da Informação Quântica . . . . .	127
<b>Apêndice C</b>	<b>Artigos Publicados . . . . .</b>	<b>133</b>

# Capítulo 1

## Introdução

A *Teoria da Informação Quântica* pode ser definida como o estudo dos limites máximos possíveis para o processamento da informação, considerando que esta última encontra-se representada de acordo com as leis da Mecânica Quântica (NIELSEN; CHUANG, 2010). O desenvolvimento desta área teve início durante os anos 1960 e 1970, nos quais diversos pesquisadores e engenheiros se questionavam quais tarefas seriam possíveis de serem realizadas ao usar estados quânticos como recursos intermediários (HOLEVO, 1982). Alguns anos mais tarde, com a proposição de protocolos para distribuição quântica de chaves (BENNETT; BRASSARD, 1984) e a concepção de uma máquina de Turing quântica (DEUTSCH, 1985), foi possível vislumbrar e impulsionar a realização de determinadas tarefas consideradas impraticáveis na Teoria da Informação Clássica.

Há dois grandes desafios para a Teoria da Informação Quântica, sendo um deles de conotação teórica e o outro de conotação prática. O primeiro destes desafios consiste na determinação de limites para a classe de tarefas de processamento de informação que são possíveis considerando a utilização da Mecânica Quântica. Isto significa, inclusive, investigar se a Teoria da Informação Quântica é capaz de realizar tarefas que são inviáveis de acordo com os princípios da Teoria da Informação Clássica. O segundo desafio, por sua vez, consiste na determinação de meios para realizar as tarefas de processamento que forem possíveis, ou seja, desenvolver dispositivos e tecnologias que possam implementar as tarefas concebidas em nível teórico (NIELSEN, 1998).

Na tentativa de colaborar para a resolução do primeiro desafio da Teoria da Informação Quântica, um caminho natural consiste na tradução dos conceitos do paradigma clássico para o paradigma quântico. Um destes conceitos, em particular, é o da *Teoria da Informação Erro-Zero*, que diz respeito ao envio de informações por canais ruidosos com probabilidade nula de ocorrência de erros de decodificação (SHANNON, 1956). A tese de Medeiros (MEDEIROS, 2008) foi pioneira na caracterização da *Teoria da Informação*

*Quântica Erro-Zero*, pois definiu conceitos teóricos e as condições para o envio de mensagens clássicas por canais quânticos ruidosos com probabilidade de erro de decodificação igual a zero.

Após este trabalho seminal, outros autores propuseram aplicações e identificaram propriedades da capacidade erro-zero de canais quânticos. Beigi e Shor (BEIGI; SHOR, 2008), por exemplo, utilizaram o formalismo desenvolvido por Medeiros (MEDEIROS, 2008) para esclarecer a relação entre as classes de complexidade  $\mathcal{NP}$  e  $\mathcal{QMA}$ . Outros trabalhos exploraram cenários em que há superativação da capacidade erro-zero, ou seja, investigaram as condições em que dois ou mais canais quânticos que possuem capacidade erro-zero nula podem ser agrupados e utilizados de tal modo que o canal resultante possua capacidade erro-zero positiva (CUBITT; CHEN; HARROW, 2009; DUAN, 2009; CHEN et al., 2010; CUBITT; SMITH, 2012). Um trabalho mais recente nesta área é o de Duan et al. (DUAN; SEVERINI; WINTER, 2011; DUAN; SEVERINI; WINTER, 2013), que além de estudarem os grafos não-comutativos, propuseram uma versão quântica para a função  $\vartheta$  de Lovász, um limitante superior para a capacidade erro-zero de canais quânticos. Até mesmo implementações práticas destes canais foram propostas, tal como pode ser visto no trabalho de Gyongyosi e Imre (GYONGYOSI; IMRE, 2012).

Sabe-se que canais quânticos podem ser utilizados de maneiras mais versáteis que os canais clássicos, pois podem transmitir informação clássica e quântica, criar emaranhamento, e serem utilizados em conjunto com outros canais, sejam eles clássicos ou quânticos. Para cada uma destas configurações, há uma capacidade que quantifica o potencial do canal para comunicação (WILLIAMS, 2011). Em um *survey* sobre capacidades de canais quânticos, Smith (SMITH, 2010) elencou algumas destas medidas, incluindo também algumas discussões sobre aspectos teóricos e aplicações das mesmas. Apesar da proposição da capacidade erro-zero de canais quânticos ter sido feita alguns anos antes e dos trabalhos desenvolvidos em decorrência, conforme mencionado, esta capacidade não é mencionada no *survey* em questão.

Vale salientar que a maioria dos trabalhos sobre a capacidade erro-zero de canais quânticos encontrados na literatura concentram-se principalmente em dois aspectos: (i) buscar meios de promover a superativação desta capacidade (CUBITT; CHEN; HARROW, 2009; DUAN, 2009; CHEN et al., 2010; CUBITT; SMITH, 2012); e (ii) propor versões alternativas para a capacidade erro-zero de canais quânticos (DUAN; SEVERINI; WINTER, 2011; DUAN; SEVERINI; WINTER, 2013). Embora estes trabalhos colaborem para o progresso da Teoria da Informação Quântica Erro-Zero, são poucos os relatos de pesquisas que tenham por objetivo relacionar esta teoria com outros conceitos e outras áreas do conhecimento, propor aplicações de interesse prático, ou que expandam o caráter erro-zero para outras medidas de informação.

Os aspectos mencionados evidenciam que, embora progressos tenham sido realizados tendo como objetivo investigar o uso e as propriedades dos canais quânticos com capacidade erro-zero, há um *problema* que permanece em aberto:

*O conhecimento das potencialidades, limitações e aplicações da Teoria da Informação Quântica Erro-Zero ainda é incipiente.*

Levando em consideração o problema identificado e os aspectos mencionados, o objetivo deste trabalho de tese foi de endereçar o problema enunciado, com o intuito de minimizá-lo.

A resolução de problemas teóricos nesta área é não-trivial, pois além do formalismo matemático necessário, é comum a existência de intersecções com diferentes conceitos da Teoria da Informação, Ciência da Computação, Teoria dos Grafos, Criptografia, dentre outros. Para embasar esta afirmação, mesmo sem considerar o caso quântico, o problema da determinação da capacidade erro-zero para o grafo  $G_5$  (problema do pentágono) proposto por Shannon (SHANNON, 1956), por exemplo, permaneceu cerca de 20 anos em aberto, vindo a ser resolvido por Lovász (LOVÁSZ, 1979) com a utilização de técnicas de Combinatória.

Considerando as dificuldades de trabalhar em uma área multi-disciplinar e as diferentes maneiras de endereçar o problema-alvo deste trabalho de tese, duas linhas de investigação foram consideradas, as quais vieram a caracterizar os objetivos específicos deste trabalho de tese:

1. Caracterizar e definir as condições para a positividade da capacidade quântica de sigilo erro-zero;
2. Caracterizar a informação acessível erro-zero de fontes quânticas e suas propriedades.

Para alcançar cada objetivo específico, questões de pesquisa foram elencadas e respondidas ao longo do desenvolvimento desta tese.

A primeira linha de investigação partiu de resultados propostos por Schumacher e Westmoreland (SCHUMACHER; WESTMORELAND, 1998), os quais argumentavam sobre a forte relação entre sigilo em canais quânticos e coerência. Tendo isto em vista, o passo seguinte foi investigar o uso de canais com descoerência coletiva que possuem subespaços e subsistemas livres de descoerência. Utilizando o modelo dos canais *wiretap* quânticos (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005), um dos primeiros resultados alcançados neste trabalho de tese consistiu na prova de que subespaços livres de

descoerência caracterizam um meio seguro para troca de informações em canais quânticos espionados (GUEDES; DE ASSIS, 2012d; GUEDES; DE ASSIS, 2013b).

Um trabalho desenvolvido por Medeiros et al. (MEDEIROS et al., 2006b) explorou a relação entre os canais quânticos erro-zero com subespaços e subsistemas livres de descoerência, mostrando que estes últimos podem fazer parte da estrutura de alguns códigos quânticos livres de erros. Levando em consideração o trabalho de Medeiros et al. (MEDEIROS et al., 2006b) e os resultados sobre a segurança dos subespaços e subsistemas livres de descoerência para envio de informação clássica, foi possível identificar uma nova capacidade dos canais quânticos, a qual foi denominada *Capacidade Quântica de Sigilo Erro-Zero* (QZESC – *Quantum Zero-Error Secrecy Capacity*) (GUEDES; DE ASSIS, 2012b). Esta capacidade diz respeito ao envio de informação clássica por um canal quântico ruidoso sem a ocorrência de erros de decodificação e de vazamento de informação. Por meio do desenvolvimento de provas formais e de exemplos, foi possível verificar que a QZESC é não-trivial (maior que 1 bit por símbolo por uso do canal em alguns casos) e também mapear situações nas quais ela possui caracterização de letra isolada, ou seja, quando esta capacidade pode ser computável em tempo polinomial.

Os canais quânticos que possuem QZESC positiva podem ser utilizados para comunicações incondicionalmente seguras sem a necessidade de comunicação prévia entre as partes, pré-existência de emaranhamento ou uso de canais auxiliares. Isto significa que, sob determinadas condições, foi possível verificar que canais quânticos erro-zero podem ser utilizados para envio de informação sigilosa, demonstrando uma aplicação da Teoria da Informação Quântica Erro-Zero na Criptografia.

A segunda linha de investigação partiu do uso de fontes quânticas em sistemas de comunicação. A fonte é um componente responsável por gerar mensagens clássicas que são associadas a estados quânticos e enviadas por um canal quântico. O grande problema no uso de fontes quânticas reside em descobrir qual o melhor esquema de medições capaz de recuperar o máximo de informação enviada originalmente, ou seja, obter a informação acessível quântica da fonte (NIELSEN; CHUANG, 2010, Seção 12.1).

A maioria dos trabalhos identificados na literatura sobre informação acessível no cenário quântico trata do problema de determinar limitantes (HOLEVO, 1973; WOOTTERS, 1993; FUCHS, 1995) ou de propor heurísticas e métodos para determinar o melhor esquema de medições para as informações emitidas pela fonte (NASCIMENTO; DE ASSIS, 2006a; NASCIMENTO; DE ASSIS, 2006b; REHACEK; ENGLERT; KASZLIKOWSKI, 2005; SUZUKI; ASSAD; ENGLERT, 2007; LEE et al., 2011; SASAKI et al., 1999). Foi verificado também que nenhum trabalho apresentado na literatura considerou como o caráter erro-zero poderia ser inserido nesse contexto.

Assim, a segunda linha de investigação tratou da proposição de uma nova medida de informação, a chamada *Informação Acessível Erro-Zero* (ZEAI – *Zero-Error Accessible Information*), definida como sendo a maior quantidade de informação que pode ser recuperada de uma fonte quântica sem erros (GUEDES; DE ASSIS, 2013a). Na obtenção da informação acessível erro-zero quântica foi identificada uma equivalência entre a fonte quântica e canais clássicos com capacidade erro-zero. Graças à esta relação, o problema de obter a informação acessível erro-zero de uma fonte é equivalente ao de obter a capacidade clássica erro-zero de um canal clássico discreto e sem memória. Além de propor tal medida, foi também estabelecida a relação desta com a informação acessível e com a quantidade de Holevo.

Para apresentar a relevância deste trabalho de tese, é importante ressaltar que esta se dá em diferentes vertentes, uma vez que duas linhas de investigação distintas foram consideradas.

Em relação à proposição da capacidade quântica de sigilo de erro-zero, há uma colaboração para a implementação de um esquema de comunicações seguras utilizando a tecnologia atual. De acordo com Lidar e Whaley (LIDAR; WHALEY, 2003), a construção de canais quânticos completamente livres de erros é uma tarefa difícil e ainda distante dos dias atuais. Como o esquema de comunicações proposto é voltado para canais quânticos ruidosos, este pode ser implementado em canais existentes atualmente, tais como os que possuem ruído coletivo (JAEGER; SERGIENKO, 2008; XIA et al., 2010; DORNER; KLEIN; JAKSCH, 2008) e os que possuem capacidade erro-zero positiva (GYONGYOSI; IMRE, 2012), incluindo também uma implementação de um canal quântico por Xue (XUE, 2008), o qual tem seu uso voltado para longas distâncias. Isto representa uma vantagem sobre os esquemas de distribuição quântica de chaves, que são menos tolerantes ao ruído (LIDAR; WHALEY, 2003).

Uma das primeiras consequências identificadas em função do desenvolvimento deste trabalho diz respeito à simplificação de protocolos quânticos para comunicação segura existentes na literatura (GUEDES; DE ASSIS, 2012a).

Além de possuir uma importância prática, em nível teórico a caracterização das condições para a existência e positividade da capacidade quântica de sigilo erro-zero ampliam o conhecimento sobre os canais quânticos e as suas habilidades para transmissão de informação.

Em relação à segunda linha de investigação, há a proposição de uma nova medida de informação sobre fontes quânticas, desenvolvida com base na Teoria da Informação Quântica Erro-Zero. O cálculo desta medida baseia-se na identificação da capacidade erro-zero de um canal clássico, ou seja, há uma relação de redução entre calcular a in-

formação acessível erro-zero de uma fonte quântica e calcular a capacidade erro-zero de um canal clássico. Embora tenha uma conotação essencialmente teórica, esta medida de informação pode auxiliar na escolha ou verificação de adequação de uma fonte quântica para fins práticos de uma comunicação. Vale ressaltar que a informação acessível erro-zero de uma fonte quântica é uma medida intrinsecamente quântica, isto é, não possui uma contrapartida clássica. As contribuições resultantes da segunda linha de investigação têm como consequências imediatas a proposição de uma medida de informação e a identificação de uma relação entre fontes quânticas e canais clássicos por intermédio do caráter erro-zero. Ambas consequências possuem um papel relevante no desenvolvimento da Teoria da Informação Quântica Erro-Zero.

A proposição da QZESC e da ZEAI endereçam o problema que motivou a realização deste trabalho. Estes dois novos conceitos mostram aplicações da Teoria da Informação Quântica Erro-Zero junto a outras áreas do conhecimento, propõe novas maneiras de enviar informação por canais quânticos com capacidade erro-zero, apresenta uma nova medida de informação sobre fontes quânticas que agrega o caráter erro-zero e desvenda relações não-triviais entre diversos conceitos, tais como, subespaços e subsistemas livres de descoerência e segurança incondicional, informação acessível erro-zero de fontes quânticas e a capacidade erro-zero de canais clássicos, dentre outras. Tais contribuições também estão alinhadas com o desafio de caráter teórico da Teoria da Informação mencionado anteriormente, que diz respeito à determinação de limites para a classe de tarefas de processamento de informação que são possíveis considerando a utilização da Mecânica Quântica.

Além de colaborar para a resolução de um dos desafios da Teoria da Informação Quântica, o desenvolvimento de trabalhos científicos desta natureza é apoiado por comunidades científicas de grande respaldo. O *Institute of Electrical and Electronics Engineers* (IEEE) possui um comitê técnico voltado para tecnologias emergentes que apóia o desenvolvimento de iniciativas que formem novos cientistas nesta área (IEEE, 2012). Segundo a *Association for Computing Machinery* (ACM), por sua vez, a Teoria da Informação Quântica é uma área com muitos problemas fundamentais em aberto cuja resolução possui impacto direto na Ciência da Computação e na Criptografia (ACM SIGACT, 2000). O trabalho em questão colabora diretamente na resolução de problemas desta natureza.

## 1.1 Organização da Tese

Esta tese está organizada como segue. A fundamentação teórica necessária para apresentação dos resultados encontra-se no Capítulo 2, contemplando a Teoria da Informação Clássica Erro-Zero, a Teoria da Informação Quântica Erro-Zero, os subespaços e

subsistemas livres de descoerência, a capacidade quântica de sigilo e a informação acessível. A caracterização e a definição das condições para a positividade da capacidade quântica de sigilo erro-zero, contribuições resultantes da primeira linha de investigação desta tese, são apresentadas no Capítulo 3. Neste capítulo também encontram-se exemplos e as relações das contribuições propostas com outros trabalhos da literatura. A caracterização da informação acessível erro-zero de fontes quânticas e de suas propriedades, contribuições resultantes da segunda linha de investigação desta tese, são apresentadas no Capítulo 4. Neste capítulo também encontram-se exemplos desta medida de informação e da relação da mesma com outros trabalhos na literatura. As considerações finais são apresentadas no Capítulo 5, o qual contempla as conclusões, a lista de artigos produzidos e sugestões de trabalhos futuros. Noções gerais da Mecânica Quântica e da Teoria da Informação são apresentadas nos Apêndices A e B, respectivamente. Os trabalhos publicados no decorrer do desenvolvimento desta tese encontram-se listados no Apêndice C.

**Notação e Convenções** A notação de Dirac (DIRAC, 1982) foi utilizada como referência para a notação de estados quânticos e das operações sobre eles. A matriz identidade é denotada por  $\mathbb{1}$ . Os logaritmos são tomados na base 2. O operador  $\text{Tr}$  denota o traço parcial sobre um estado quântico. As demais notações e convenções adotadas são apresentadas ao longo do texto.

## Capítulo 2

# Fundamentação Teórica

Neste capítulo são apresentados os conteúdos que compõem a fundamentação teórica utilizada para o desenvolvimento desta tese. São abordados a Teoria da Informação Clássica Erro-Zero na Seção 2.1; a Teoria da Informação Quântica Erro-Zero na Seção 2.2; os subespaços e subsistemas livres de descoerência na Seção 2.3; a capacidade quântica de sigilo na Seção 2.4; e, por fim, a informação acessível na Seção 2.5.

Para que o leitor possa ter um amplo entendimento da fundamentação teórica é necessário que este conheça os conceitos elementares da Mecânica Quântica e da Teoria da Informação. Algumas das noções gerais dessas áreas foram compiladas nos Apêndices A e B, respectivamente. Além destes apêndices, as obras de Nielsen e Chuang (NIELSEN; CHUANG, 2010), Williams (WILLIAMS, 2011) e Kaye et al. (KAYE; LAFLAMME; MOSCA, 2007) são recomendadas como referência para o aprendizado dos conceitos ligados à Mecânica Quântica; e as obras de Cover e Thomas (COVER; THOMAS, 2006) e de Desurvire (DESURVIRE, 2009), bem como o artigo de Bennet e Shor (BENNETT; SHOR, 1998) são recomendadas como referência para o aprendizado dos conceitos ligados à Teoria da Informação.

### 2.1 Teoria da Informação Clássica Erro-Zero

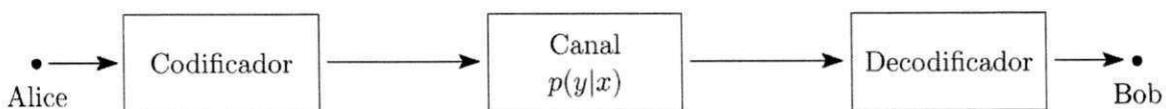
A *Teoria da Informação Clássica* pode ser vista como o estudo de padrões na informação e de maneiras de explorá-los para melhorar o envio da informação por canais ruidosos. Na codificação de fonte, padrões de dados são utilizados para representar sinais de maneira eficiente; enquanto na codificação do canal, padrões de ruído são utilizados para descobrir meios de transmitir a informação de maneira confiável. Frequentemente, estes objetivos são alcançados tolerando-se uma *pequena probabilidade de erro* (SHANNON, 1948). Porém, existem situações em que é necessário considerar a *ausência de erro*,

ainda que possa haver distorções, ruído ou interferências na Comunicação.

O estudo destes cenários em que é considerada a ausência de erros inaugurou a *Teoria da Informação Clássica Erro-Zero* (SHANNON, 1956). O estudo e a aplicação desta teoria são importantes por diversos motivos, a citar: (i) existem cenários em que erros não são tolerados; (ii) apenas um pequeno número de usos do canal ou de instâncias de fontes estão disponíveis; (iii) resultados que asseguram que a probabilidade de erro decai com o crescimento no número de usos ou de instâncias não podem ser considerados; (iv) resultados para a Teoria da Informação podem ser derivados dos resultados da Teoria da Informação Clássica Erro-Zero por meio de utilização de técnicas de combinatória; (v) funções e métodos usados na Teoria da Informação Clássica Erro-Zero são comumente aplicáveis a problemas da Matemática e da Ciência da Computação; e (vi) o problema e sua formulação simplificada levam a muitas soluções que são de interesse por si só (KORNER; ORLITSKY, 1998). Algumas aplicações que ressaltam a importância desta teoria residem na transmissão de informação, na Criptografia (WOLF; WULLSCHLEGER, 2004), na produção de chips VLSI (KORNER; ORLITSKY, 1998), na compressão de dados (COVER; THOMAS, 2006), dentre outras.

Para apresentar alguns conceitos ligados à Teoria da Informação Clássica Erro-Zero, é necessário efetuar a formulação de como são feitas as trocas de informações. Para tanto, será considerado o modelo de canal clássico estacionário discreto sem memória (DMC – *Discrete Memoryless Channel*) ilustrado na Figura 1.

Figura 1: Modelo de um canal clássico de comunicações.



Fonte: Cover e Thomas (COVER; THOMAS, 2006).

Um canal DMC  $W$  é caracterizado por uma matriz estocástica cujas linhas são indexadas pelos elementos de  $\mathcal{X} = \{x_1, \dots, x_n\}$  e cujas colunas são indexadas pelos elementos de  $\mathcal{Y} = \{y_1, \dots, y_m\}$ . O elemento  $(i, j)$  de  $W$  indica a probabilidade  $p(y_j|x_i)$ , ou seja, a probabilidade de obter a saída  $y_j$  quando  $x_i$  é enviado pelo canal. A partir dos DMC, é feita a definição de códigos clássicos  $(m, n)$  livres de erro.

**Definição 2.1 (Código Clássico  $(m, n)$  Livre de Erros)** *Um código clássico  $(m, n)$  livre de erros para um canal DMC  $W$  é composto por:*

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

## 2. Uma função de codificação

$$f_n : \{1, \dots, m\} \rightarrow \mathcal{X}^n \quad (2.1)$$

levando a palavras código  $f_n(1), \dots, f_n(n)$ .

## 3. Uma função de decodificação

$$g : \{1, \dots, k\} \rightarrow \{1, \dots, m\} \quad (2.2)$$

que deterministicamente associa uma mensagem com cada palavra recebida, com a seguinte propriedade:

$$\Pr[g(W(f_n(i))) \neq i] = 0 \quad \forall i \in \{1, \dots, m\} \quad (2.3)$$

A particularidade da definição destes códigos reside na Eq. (2.3), que restringe totalmente a existência de erros de decodificação. Neste contexto, há o interesse particular em símbolos que possam ser completamente distinguíveis na saída do canal clássico, os quais são chamados de símbolos *não-adjacentes*.

**Definição 2.2 (Adjacência de Símbolos Clássicos)** *Seja um DMC  $W$  e dois símbolos do alfabeto de entrada  $x_i, x_j \in \mathcal{X}$ . Os símbolos  $x_i$  e  $x_j$  são ditos serem adjacentes (ou indistinguíveis) se existe um símbolo de saída em  $\mathcal{Y}$  o qual pode ser causado por um destes dois símbolos, i.e., se existe um  $y \in \mathcal{Y}$  tais que  $p(y|x_i)$  e  $p(y|x_j)$  são ambos maiores que zero. Caso contrário, diz-se que estes símbolos são não-adjacentes (ou distinguíveis).*

Considerando o envio de uma seqüência  $\mathbf{x} = x_1x_2 \dots x_n$  pelo canal  $W$ , a saída será uma seqüência  $\mathbf{y} = y_1y_2 \dots y_n$  com a seguinte probabilidade

$$p^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n p(y_i|x_i) \quad (2.4)$$

O produtório reflete a falta de memória do canal bem como a estacionariedade do mesmo, pois as probabilidades são advindas de uma mesma matriz. Se duas seqüências  $\mathbf{x}'$  e  $\mathbf{x}''$  podem ambas resultar em uma mesma seqüência  $\mathbf{y}$  com probabilidade positiva, então não existe um decodificador capaz de decidir com probabilidade de erro igual a zero qual das duas seqüências foi originalmente enviada. Estas duas seqüências são ditas serem *indistinguíveis* ou *adjacentes* pelo receptor da saída do canal (KORNER; ORLITSKY, 1998).

É útil pensar na distribuição de probabilidades  $p(\cdot|x)$  e  $p^n(\cdot|\mathbf{x})$  como em vetores de dimensão  $|\mathcal{X}|$  e  $|\mathcal{X}^n|$ , respectivamente. Utilizando esta abordagem, pode-se afirmar que

duas seqüências  $\mathbf{x}', \mathbf{x}'' \in \mathcal{X}$  são distinguíveis na saída do DMC  $W$  se, e somente se, os vetores correspondentes  $p^n(\cdot|\mathbf{x}')$  e  $p^n(\cdot|\mathbf{x}'')$  são ortogonais. Isto é equivalente a afirmar que  $\mathbf{x}'$  e  $\mathbf{x}''$  são distinguíveis se, e somente se, existir pelo menos um  $i$ ,  $1 \leq i \leq n$ , tal que  $x'_i$  e  $x''_i$  sejam não-adjacentes, vide Figura 2.

Figura 2: Duas seqüências distinguíveis  $\mathbf{x}'$  e  $\mathbf{x}''$  – para pelo menos um  $i$ ,  $1 \leq i \leq n$ , os símbolos  $x'_i$  e  $x''_i$  devem ser não-adjacentes.

$$\begin{array}{l} \mathbf{x}' = x'_1 x'_2 \dots \left( x'_i \right) \dots x'_{n-1} x'_n \\ \mathbf{x}'' = x''_1 x''_2 \dots \left( x''_i \right) \dots x''_{n-1} x''_n \end{array}$$

Fonte: Elaborada por Medeiros (MEDEIROS, 2008).

Levando os conceitos apresentados em consideração, é possível definir a *capacidade clássica erro-zero*.

**Definição 2.3 (Capacidade Clássica Erro-Zero (SHANNON, 1956))** *Seja um DMC  $W$  e defina  $N(n)$  como sendo a cardinalidade máxima de um conjunto de vetores mutuamente ortogonais de  $p^n(\cdot|\mathbf{x})$ ,  $\mathbf{x} \in \mathcal{X}^n$ . A capacidade clássica erro-zero de  $W$  é dada por*

$$C_0(W) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log N(n) \quad (2.5)$$

Intuitivamente,  $C_0(W)$  é a maior taxa de transmissão de bits por símbolo livres de erro possível para o canal  $W$ . O número  $N(n)$  na Eq. (2.5) é super multiplicativo, i.e.,  $N(n+m) \geq N(n) \cdot N(m)$ .

Shannon mostrou que a capacidade clássica erro-zero de um DMC depende apenas dos símbolos do alfabeto da fonte  $\mathcal{X}$  que são adjacentes (SHANNON, 1956). Esta é uma diferença significativa em relação a capacidade ordinária de um canal DMC, pois esta última depende da escolha da distribuição de probabilidades sobre os símbolos de entrada.

### 2.1.1 Representação em Termos de Grafos

Shannon reformulou o problema de determinar a capacidade erro-zero de um canal em termos da Teoria dos Grafos (SHANNON, 1956). Associa-se a um DMC  $W$  um *grafo característico*, construído conforme Definição 2.4

**Definição 2.4 (Grafo Característico de um DMC (KORNER; ORLITSKY, 1998))**

Seja  $W$  um canal clássico discreto e sem memória. Associado a  $W$  está um grafo característico  $\mathcal{G}(W) = \langle V, E \rangle$  construído como segue:

1.  $V = \mathcal{X}$  é o conjunto de vértices do grafo;
2. Há uma aresta  $(i, j) \in E$  se os símbolos  $x_i, x_j \in \mathcal{X}$  são não-adjacentes na saída de  $W$  (conforme Definição 2.2).

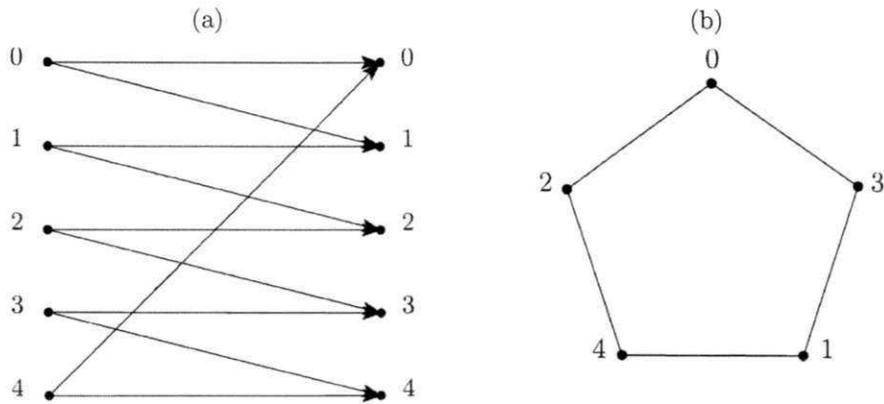
Esta noção de grafo característico também pode ser expandida para o  $n$ -produto  $\mathcal{G}^n(W)$ , no qual  $V^n = \mathcal{X}^n$  e existe uma aresta  $(\mathbf{x}', \mathbf{x}'') \in E$  se para pelo menos um  $i$ ,  $1 \leq i \leq n$ , os  $i$ -ésimos símbolos  $x'_i$  e  $x''_i$  são não-adjacentes na saída de  $W$ .

Na Teoria dos Grafos, a *ordem* de um grafo  $G$  é definida como sendo a cardinalidade do seu conjunto de vértices. O *clique* de um grafo é definido como sendo qualquer subgrafo completo de  $G$ ; e o *número de clique* de  $G$ , denotado por  $\omega(G)$ , denota a ordem de um clique maximal em  $G$ . Levando estes conceitos em consideração, é possível denotar a capacidade erro-zero de um DMC  $W$  utilizando a Teoria dos Grafos como segue (SHANNON, 1956).

**Teorema 2.1 (Capacidade Clássica Erro-Zero em Termos de Grafos)** *Seja  $W$  um canal clássico discreto e sem memória. Seja  $\mathcal{G}^n(W)$  o grafo característico correspondente a  $n$  usos do canal  $W$ , conforme descrito na Definição 2.4. A capacidade clássica erro-zero para um DMC  $W$  pode ser re-escrita como*

$$C_0(W) = \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n(W)). \quad (2.6)$$

**Exemplo 2.1 (Problema do Pentágono)** *Seja um DMC  $W_1$  cujo alfabeto de entrada consiste nos símbolos  $\{0, 1, 2, 3, 4\}$ . Em virtude do ruído do canal, estes símbolos podem se confundir na saída do mesmo, conforme grafo ilustrado na Figura 3a. O grafo característico de  $W_1$  encontra-se ilustrado na Figura 3b.*

Figura 3: Grafos correspondentes ao canal DMC  $W_1$ .

Fonte: Elaborado pela autora.

O problema de calcular a capacidade erro-zero do DMC  $W_1$ , denominado problema do pentágono, foi proposto por Shannon (SHANNON, 1956) e resolvido por Lovász (LOVÁSZ, 1979) por meio da utilização de técnicas de Combinatória. O valor desta capacidade considera o uso de um código clássico ( $m = 5, n = 2$ ) livre de erros em que são enviadas as mensagens  $\{00, 12, 24, 31, 43\}$ . A capacidade erro-zero deste DMC é dada por:

$$C_0(W_1) = \frac{1}{2} \log 5 \quad (2.7)$$

$$\approx 1,1609 \text{ bits por símbolo por uso do canal.} \quad (2.8)$$

É interessante notar que neste exemplo a capacidade clássica erro-zero de  $W_1$  é não-nula e não-trivial, visto que é maior que 1.

## 2.2 Teoria da Informação Quântica Erro-Zero

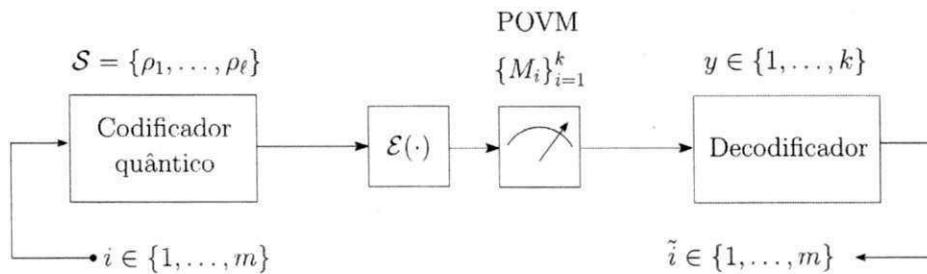
A Teoria da Informação Quântica Erro-Zero é uma sub-área da Teoria da Informação Quântica que tem por objetivo o estudo e a proposição de técnicas, protocolos e medidas para transmissão da informação por canais quânticos ruidosos sem a ocorrência de erros de decodificação. A proposição desta teoria é recente e foi feita por Medeiros (MEDEIROS, 2008) ao transpor conceitos da Teoria da Informação Erro-Zero Clássica, proposta por Shannon (SHANNON, 1956), para o cenário quântico.

Em sua tese de doutorado, Medeiros (MEDEIROS, 2008) tratou do estabelecimento das condições necessárias para realizar o envio de informação clássica por canais quânticos ruidosos sem ocorrência de erros de decodificação. Assim, dado um canal quântico, deseja-se saber qual o máximo de informação clássica que pode ser transmitida por este com uma

probabilidade nula de erro. Para tanto, considera-se um canal quântico  $d$ -dimensional  $\mathcal{E} \equiv \{E_a\}$  modelado por um mapeamento linear completamente positivo que preserva o traço. Seja  $\mathcal{S}$  um subconjunto de estados quânticos de dimensão  $d$  para  $\mathcal{E}$ . Estados  $\rho_i \in \mathcal{S}$  são referidos como *estados de entrada*.

Inicialmente, um emissor (Alice) escolhe uma mensagem de um conjunto  $\{1, \dots, m\}$  com  $m$  mensagens clássicas. O codificador mapeia estas mensagens em um produto  $n$ -tensorial de estados quânticos de  $\mathcal{S}$ . O estado  $d^n$ -dimensional é chamado *palavra código quântica*, a qual é enviada pelo canal quântico ruidoso  $\mathcal{E}$ . O receptor (Bob) realiza uma medição coletiva com um POVM (*Positive Operator-Valued Measurement*) no estado recebido. As saídas da medição são argumentos para a função de decodificação. O decodificador deve decidir qual mensagem foi enviada por Alice com a propriedade de que erros não são tolerados. A Figura 4 sintetiza a idéia deste protocolo de comunicação.

Figura 4: Representação de um sistema de comunicações quântico erro-zero.



Fonte: Elaborada por Medeiros (MEDEIROS, 2008).

O protocolo de comunicação livre de erros pode ser sumarizado como segue:

- O alfabeto da fonte é o conjunto  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$  de estados de entrada de dimensão  $d$ ;
- Para serem transmitidas pelo canal quântico, mensagens clássicas são mapeadas em produtos tensoriais dos estados quânticos em  $\mathcal{S}$ ;
- Embora as entradas não possam ser emaranhadas, medições coletivas com o POVM são permitidas na saída do canal. Estas medições são suficientes para atingir a capacidade quântica erro-zero, como será mostrado.

Levando em consideração estas colocações, é possível definir códigos quânticos livres de erro.

**Definição 2.5 (Código Quântico  $(m, n)$  Livre de Erros)** *Um código quântico  $(m, n)$  livre de erros para um canal quântico  $\mathcal{E}$  é composto de:*

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

2. Uma função de codificação

$$f_n : \{1, \dots, m\} \rightarrow \mathcal{S}^{\otimes n} \quad (2.9)$$

levando a palavras código  $f_n(1) = \bar{\rho}_1, \dots, f_n(m) = \bar{\rho}_m$ ;

3. Uma função de decodificação

$$g : \{1, \dots, k\} \rightarrow \{1, \dots, m\} \quad (2.10)$$

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

$$\Pr[g(\mathcal{E}(f_n(i))) \neq i] = 0 \quad \forall i \in \{1, \dots, m\} \quad (2.11)$$

A taxa deste código é igual a  $R_n = \frac{1}{n} \log m$  bits por uso do canal

Levando em consideração esta definição de códigos livres de erro, é possível definir a capacidade quântica de erro zero (QZEC – Quantum Zero-Error Capacity).

**Definição 2.6 (Capacidade Quântica Erro-Zero (MEDEIROS, 2008))** Seja  $\mathcal{E}(\cdot)$  um mapeamento quântico positivo, linear, que preserva o traço representando um canal quântico ruidoso. A capacidade erro-zero de  $\mathcal{E}(\cdot)$ , denotada por  $C^{(0)}(\mathcal{E})$ , é o maior limite superior das taxas alcançáveis com probabilidade de erro de decodificação igual a zero, isto é

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_n \frac{1}{n} \log m \quad (2.12)$$

em que  $m$  é o número máximo de mensagens clássicas que o sistema pode transmitir sem erro, quando um código quântico  $(m, n)$  livre de erros é utilizado com alfabeto de entrada igual a  $\mathcal{S}$ .

Há o interesse nas situações em que a capacidade erro-zero de um canal quântico  $\mathcal{E}$  é não-nula. Para garantir isto, é necessário assegurar que pelo menos dois estados de entrada no canal sejam não-adjacentes. A Definição 2.7 formaliza este conceito.

**Definição 2.7 (Adjacência de Estados Quânticos)** *Seja um canal quântico  $\mathcal{E}$  e dois estados quânticos  $\rho_i, \rho_j \in \mathcal{S}$ ,  $i \neq j$ , oriundos do alfabeto de entrada do canal. Diz-se que  $\rho_i$  e  $\rho_j$  são adjacentes (ou indistinguíveis) na saída de  $\mathcal{E}$  se os subespaços de Hilbert gerados pelos suportes de  $\rho_i$  e  $\rho_j$  são não-ortogonais. Em caso contrário, diz-se que  $\rho_i$  e  $\rho_j$  são ortogonais (ou distinguíveis) na saída do canal  $\mathcal{E}$  e denota-se por  $\rho_i \perp_{\mathcal{E}} \rho_j$ .*

A Figura 5 auxilia na compreensão do conceito apresentado na Definição 2.7. Sejam dois produtos tensoriais de estados da entrada  $\rho_i = \rho_{i,1} \otimes \dots \otimes \rho_{i,n}$  e  $\rho_j = \rho_{j,1} \otimes \dots \otimes \rho_{j,n}$ . Caso exista pelo menos um  $\rho_{i,k} \perp_{\mathcal{E}} \rho_{j,k}$ , então  $\rho_i \perp_{\mathcal{E}} \rho_j$ .

Figura 5: Dois estados quânticos  $\rho_i$  e  $\rho_j$  são distinguíveis na saída de um canal  $\mathcal{E}$  caso exista pelo menos um  $\rho_{i,k} \perp_{\mathcal{E}} \rho_{j,k}$ ,  $1 \leq k \leq n$ .

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

Fonte: Elaborada por Medeiros (MEDEIROS, 2008).

Levando a noção de adjacência em consideração, um canal quântico  $\mathcal{E}$  possui capacidade erro-zero positiva se, e somente se, o conjunto  $\mathcal{S}$  contém pelo menos dois estados não-adjacentes. Seja  $\mathcal{M}$  um POVM com  $m > \ell$  elementos tal que  $\sum_{j=1}^m M_j = \mathbb{1}$ . Consideram-se os subconjuntos

$$A_k = \{j \in \{1, \dots, m\}; \text{Tr}[\mathcal{E}(\rho_k)M_j] > 0\}; \quad k \in \{1, \dots, \ell\}. \quad (2.13)$$

O canal quântico  $\mathcal{E}$  possui capacidade erro-zero maior que zero se, e somente se, existe um conjunto  $\mathcal{S}$  e um POVM  $\mathcal{M}$  para os quais pelo menos um par  $(i, j) \in \{1, \dots, \ell\}^2$ ,  $i \neq j$ , se os subconjuntos  $A_i$  e  $A_j$  são disjuntos, i.e.,  $A_i \cap A_j = \emptyset$  (MEDEIROS et al., 2006b).

Na tentativa de alcançar a capacidade erro-zero dos canais quânticos, é necessário levar em consideração os esquemas de codificação-decodificação que maximizem a taxa de envio erro-zero. Levando isto em consideração, enuncia-se a seguinte definição.

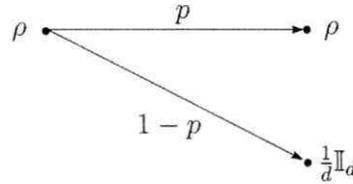
**Definição 2.8 (Par Ótimo  $(\mathcal{S}, \mathcal{M})$ )** *Um par  $(\mathcal{S}, \mathcal{M})$  é dito ser ótimo para um canal quântico  $\mathcal{E}$ , em que  $\mathcal{S} = \{\rho_i\}$  é um conjunto de estados e  $\mathcal{M} = \{M_j\}$  é um POVM, para os quais a capacidade erro-zero de  $\mathcal{E}$  é alcançada.*

A tese de Medeiros (MEDEIROS, 2008) discorre sobre a cardinalidade do ótimo  $\mathcal{S}$ , afirmando que este conjunto pode ser composto de, no máximo,  $d$  estados puros, em que  $d$  é

a dimensão do espaço de Hilbert de entrada (MEDEIROS; DE ASSIS, 2005a; MEDEIROS et al., 2006a). Além deste aspecto, o autor argumenta a respeito das medições, afirmando que as medições coletivas realizadas com o POVM  $\mathcal{M}$  de fato permitem que a capacidade erro-zero de um canal quântico seja atingida, o que nem sempre é válido para medições individuais.

**Exemplo 2.2 (Canal Quântico com Capacidade Erro-Zero Igual a Zero)** *Seja o canal quântico de despolarização em que um estado quântico de entrada  $\rho$  pode ser transmitido intacto com probabilidade  $p$  ou é trocado por um estado completamente misto com probabilidade  $1 - p$ , em que  $d$  é a dimensão do espaço de Hilbert  $\mathcal{H}$  e  $\mathbb{1}$  denota a matriz identidade de dimensão  $d$ . Esse canal é ilustrado na Figura 6.*

Figura 6: Canal quântico de despolarização.



Fonte: Elaborada por Medeiros (MEDEIROS, 2008).

A representação formal deste canal é feita como segue

$$\mathcal{E}(\rho) = p \cdot \rho + (1 - p) \frac{1}{d} \mathbb{1}_d, \quad (2.14)$$

em que  $0 < p < 1$ . Para verificar se este canal possui capacidade erro-zero positiva, basta verificar se dois estados quaisquer distintos são distinguíveis na saída do canal, isto é

$$\text{Tr}[\mathcal{E}(\rho_i)\mathcal{E}(\rho_j)] = \text{Tr} \left[ \left( p\rho_i + (1 - p) \frac{1}{d} \mathbb{1}_d \right) \left( p\rho_j + (1 - p) \frac{1}{d} \mathbb{1}_d \right) \right] \quad (2.15)$$

$$= \text{Tr} \left[ p^2 \text{Tr}[\rho_i \rho_j] + \frac{p(1 - p)}{d} \text{Tr}[\rho_i + \rho_j] + \frac{(1 - p)^2}{d} \right] \quad (2.16)$$

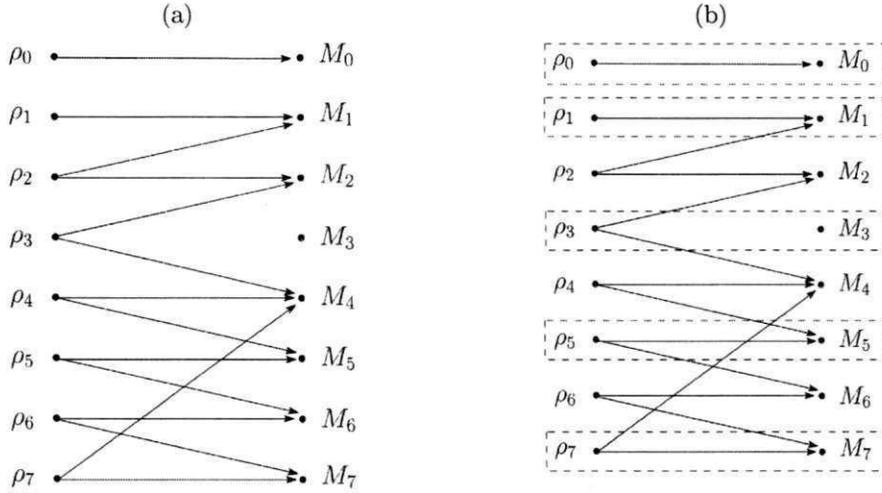
$$> 0, \quad (2.17)$$

uma vez que  $0 < p < 1$ . Assim, a capacidade erro-zero do canal de despolarização  $\mathcal{E}$  é igual a zero, i.e.,  $C^{(0)}(\mathcal{E}) = 0$ .

**Exemplo 2.3 (Canal Quântico com Capacidade Erro-Zero Positiva)** *Suponha um canal quântico  $\mathcal{E}$  em um espaço de Hilbert 8-dimensional. Considere um conjunto de mensagens clássicas  $\{0, 1, \dots, 7\}$  associado a um conjunto de entrada de estados quânticos puros  $\mathcal{S} = \{\rho_0 = |0\rangle\langle 0|, \rho_1 = |1\rangle\langle 1|, \dots, \rho_7 = |7\rangle\langle 7|\}$ , em que  $0 \mapsto \rho_0, 1 \mapsto \rho_1, \dots, 7 \mapsto \rho_7$ .*

Considere um conjunto POVM  $\mathcal{M}$  definido da seguinte forma  $\mathcal{M} = \{M_i = |i\rangle\langle i|\}_{i=0}^7$ . Note que  $\sum_{i=0}^7 M_i = \mathbb{1}$ . Suponha que este canal atua sobre a entrada da seguinte maneira, como ilustrado na Figura 7a.

Figura 7: Grafo representando as transições efetuadas pelo canal quântico  $\mathcal{E}$  sobre a entrada.



Fonte: Elaborado pela autora.

Este canal possui capacidade erro-zero positiva, pois é possível identificar um subconjunto de estados não-adjacentes na saída do canal. Este subconjunto é composto por  $\{\rho_0, \rho_1, \rho_3, \rho_5, \rho_7\}$  e é maximal. Levando isto em consideração, tem-se que

$$C^{(0)}(\mathcal{E}) \geq \frac{1}{1} \log_2 5 \tag{2.18}$$

$$\geq 2.321 \text{ bits por símbolo por uso do canal.} \tag{2.19}$$

É importante enfatizar que neste exemplo não é possível afirmar que a capacidade erro-zero do canal quântico  $\mathcal{E}$  é igual a 2.321 bits por símbolo por uso do canal, pois uma taxa maior pode ser alcançada em dois ou mais usos do canal.

### 2.2.1 Representação em Termos de Grafos

A capacidade clássica erro-zero de um canal quântico também permite uma interpretação em termos de Teoria dos Grafos (MEDEIROS, 2008). Dado um canal quântico, assim como no caso clássico, também é possível construir um grafo característico, cuja definição é apresentada a seguir.

**Definição 2.9 (Grafo Característico de um Canal Quântico)** *Seja  $\mathcal{E}$  um canal quântico cujo conjunto de estados de entrada é dado por  $\mathcal{S} = \{\rho_1, \rho_2, \dots, \rho_\ell\}$ . É possível construir um grafo característico para o canal  $\mathcal{E}$ , denotado por  $\mathcal{G}(\mathcal{E}) = \langle V, E \rangle$ , da seguinte forma:*

1.  $V = \{1, 2, \dots, \ell\}$  é o conjunto de vértices, em que cada vértice está associado a um estado de  $\mathcal{S}$ ;
2.  $E = \{(i, j) | \rho_i \perp_{\mathcal{E}} \rho_j; \rho_i, \rho_j \in \mathcal{S}; i \neq j\}$ .

*Esta noção de grafo característico também pode ser estendida para o  $n$ -produto  $\mathcal{G}^n(\mathcal{E})$ , em que  $V = V^n$  e  $E$  é composto pelos estados quânticos de dimensão  $n$  que são não-adjacentes em  $\mathcal{E}$ .*

A partir desta representação, é possível verificar que estados quânticos conectados por uma aresta no grafo  $\mathcal{G}(\mathcal{E})$  são mutuamente não-adjacentes na saída do canal quântico  $\mathcal{E}$ . Portanto, o número máximo de mensagens que podem ser transmitidas sem erro utilizando um código quântico  $(m, n)$  livre de erros com alfabeto de entrada  $\mathcal{S}$  é o número de clique de  $\mathcal{G}^n(\mathcal{E})$ , o qual é denotado por  $\omega(\mathcal{G}^n)$ . Desta maneira, é possível obter uma versão alternativa, porém equivalente, para a capacidade clássica erro-zero em canais quânticos em termos da Teoria dos Grafos.

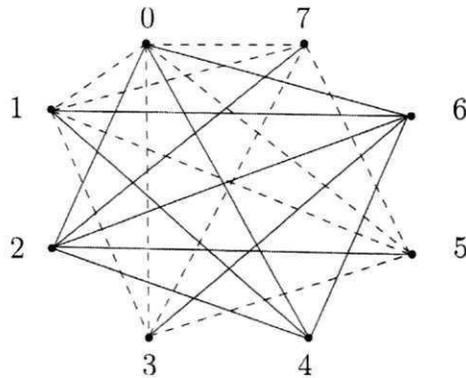
**Teorema 2.2 (Capacidade Quântica Erro-Zero em Termos de Grafos)** *A capacidade clássica erro-zero de um canal quântico  $\mathcal{E}$  é dada por*

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n(\mathcal{E})), \quad (2.20)$$

*em que o supremo é tomado sobre todos os conjuntos de entrada  $\mathcal{S}$  e sobre todos os comprimentos de código  $n$ .*

**Exemplo 2.4 (Capacidade Erro-Zero Obtida por Meio de um Grafo)** *Levando em consideração o canal  $\mathcal{E}$  apresentado no Exemplo 2.3 e ilustrado na Figura 7a, o grafo característico derivado deste canal encontra-se ilustrado na Figura 8. O número de clique para o grafo característico correspondente a um uso do canal é igual a 5, sendo obtido do clique que contém as arestas  $\{(0, 1), (1, 3), (3, 5), (5, 7), (7, 0)\}$ . O clique do grafo característico de  $\mathcal{E}$  encontra-se ilustrado na Figura 8 por meio das arestas pontilhadas.*

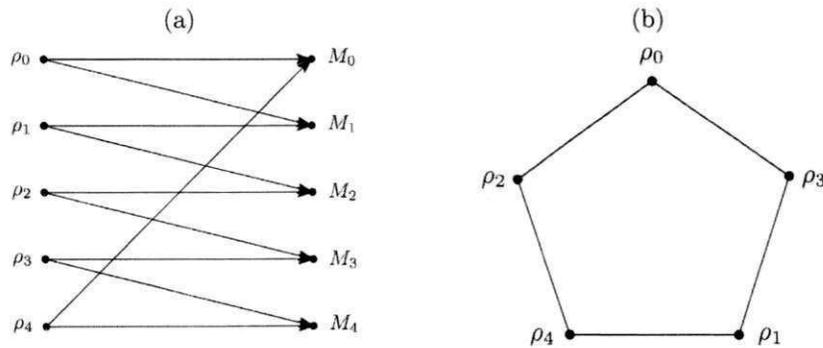
Figura 8: Grafo característico para o canal  $\mathcal{E}$  do Exemplo 2.3.



Fonte: Elaborado pela autora.

**Exemplo 2.5 (Versão Quântica do Problema do Pentágono)** O problema do pentágono, apresentado anteriormente para o caso clássico no Exemplo 2.1, foi adaptado por Medeiros (MEDEIROS, 2008) para o caso quântico. O alfabeto da fonte consiste no conjunto de estados quânticos  $\{\rho_0, \rho_1, \dots, \rho_4\}$  e a medição destes estados após a saída do canal quântico  $\mathcal{E}$  é feita com o POVM  $\{M_i\}_{i=0}^4$ , conforme ilustrado na Figura 9a. O grafo característico deste canal quântico, construído conforme descrito na Definição 2.9, encontra-se ilustrado na Figura 9b.

Figura 9: Canal quântico cuja obtenção da capacidade erro-zero é não-trivial.



Fonte: Elaborado pela autora.

Conforme os resultados obtidos por Medeiros (MEDEIROS, 2008), a capacidade erro-zero é alcançada com o uso de um código quântico ( $m = 5, n = 2$ ) livre de erros no qual os estados quânticos  $\{\rho_{00}, \rho_{12}, \rho_{24}, \rho_{31}, \rho_{43}\}$  podem ser utilizados, em que  $\rho_{ij} = \rho_i \otimes \rho_j$ . Assim, a capacidade erro-zero deste canal é igual a

$$C^{(0)}(\mathcal{E}) = \frac{1}{2} \log 5 \quad (2.21)$$

$$\approx 1.1609 \text{ bits por símbolo por uso do canal.} \quad (2.22)$$

## 2.2.2 Relação com a Capacidade Holevo-Schumacher-Westmoreland

Canais quânticos possuem um número diferente de capacidades, a depender fundamentalmente do tipo de informação a ser enviada (clássica ou quântica) e do protocolo de comunicações a ser utilizado (NIELSEN; CHUANG, 2010).

Considerando o envio de mensagens clássicas por canais quânticos, em que as mensagens são produtos tensoriais de estados quânticos, e as medições são realizadas de maneira coletiva ao longo de múltiplos usos do canal, a capacidade deste canal para transmitir informações com uma probabilidade de erro desprezível ao longo de muitas utilizações deste canal, denotada por  $C_{1,\infty}$ , é dada pelo *Teorema de Holevo-Schumacher-Westmoreland* (HSW) (HOLEVO, 1998; SCHUMACHER; WESTMORELAND, 1997). De acordo com o Teorema HSW, esta capacidade, também conhecida por *capacidade ordinária de um canal quântico*  $\mathcal{E}$ , é dada por

$$C_{1,\infty}(\mathcal{E}) \equiv \max_{p_i, \rho_i} \chi_{p_i, \rho_i}, \quad (2.23)$$

em que

$$\chi_{p_i, \rho_i} = S \left( \mathcal{E} \left( \sum_i p_i \rho_i \right) \right) - \sum_i p_i S(\mathcal{E}(\rho_i)), \quad (2.24)$$

em que  $S$  é a entropia de von Neumann; o máximo na Eq. (2.23) considera todas as distribuições de probabilidades  $p_i$  sobre a entrada  $\rho_i$  do canal  $\mathcal{E}$ ; e  $\chi_{p_i, \rho_i}$  denomina-se *quantidade de Holevo*.

Ao se comunicar por um canal quântico  $\mathcal{E}$  utilizando o protocolo sugerido pelo teorema HSW, porém com uma taxa menor que  $C_{1,\infty}(\mathcal{E})$ , é possível transmitir informações clássicas de maneira confiável pelo canal quântico com probabilidade de erro *assintoticamente* igual a zero. Porém, apesar do erro tender assintoticamente a zero, este ainda pode acontecer. Portanto, a capacidade  $C_{1,\infty}(\mathcal{E})$  não exclui a possibilidade de ocorrerem erros.

Para que haja a eliminação total de erros, é necessário utilizar um código livre de erros, o que leva à capacidade erro-zero de um canal quântico. Esta capacidade diferencia-se apenas da ordinária de um canal quântico por impor ausência de erros na decodificação.

Com isto, Medeiros (MEDEIROS, 2008) provou que a capacidade ordinária de um canal quântico é um limite superior para a capacidade erro-zero, ou seja

$$C^{(0)}(\mathcal{E}) \leq C_{1,\infty}(\mathcal{E}) \equiv \max_{\rho_i, \rho_i'} \chi_{\rho_i, \rho_i'}, \quad (2.25)$$

em que  $\mathcal{E}$  é um canal quântico. De acordo com o autor, este é um resultado intuitivo, pois ao se tolerar uma pequena quantidade de erros, tem-se um aumento na taxa de transmissão da informação.

### 2.2.3 Desenvolvimentos Recentes

Na seção anterior, foi abordado o trabalho desenvolvido na tese de Medeiros (MEDEIROS, 2008), o qual considera o envio de mensagens clássicas via canais quânticos com probabilidade de erro de decodificação igual a zero. Embora este trabalho tenha sido um ponto de partida para o desenvolvimento da Teoria da Informação Quântica Erro-Zero, outros desenvolvimentos posteriores ampliaram os conceitos e as possibilidades no envio de informação considerando a ausência de erros. O objetivo desta seção é mostrar alguns destes trabalhos e as contribuições para a referida área de pesquisa.

Um trabalho posterior do próprio Medeiros (MEDEIROS; DE ASSIS, 2005b) sugeriu o envio de informação quântica sem erros, resultando na *capacidade quântica erro-zero de canais quânticos ruidosos*, denotada por  $Q^{(0)}$ . Esta capacidade engloba todas as propriedades quânticas e não demanda que medições sejam realizadas ao final da transmissão com o intuito de encontrar uma mensagem clássica associada. A noção desta capacidade está associada principalmente aos códigos corretores de erros quânticos.

Ainda contemplando a busca de diferentes formulações para a capacidade de canais erro-zero, os trabalhos liderados por Winter (DUAN; SEVERINI; WINTER, 2011; CUBITT et al., 2009; CUBITT et al., 2010b) consideraram uma perspectiva diferente da tomada por Medeiros (MEDEIROS, 2008) para a construção de grafos. Ao invés de conectar os vértices que são distinguíveis na saída do canal, eles optaram por uma formulação em que as entradas que se confundem são conectadas, criando um *grafo de confusabilidade*<sup>1</sup>  $G$ . A partir desta definição, um código consiste no anti-clique deste grafo correspondente. O maior anti-clique, denominado *número de independência*, denotado por  $\alpha(G)$ , corresponde ao máximo número de mensagens que podem ser transmitidas pelo canal com probabilidade de erro igual a zero. Desta maneira, a capacidade erro-zero

<sup>1</sup> Confusabilidade: tradução livre do termo em inglês *confusability*.

de um canal clássico com grafo de confusabilidade  $G$  é dada por

$$C_0(G) = \lim_{n \rightarrow \infty} \log \alpha(G^n) = \sup_n \log \alpha(G^n) \quad (2.26)$$

Ao transpor este conceito para os canais quânticos, tem-se que um canal quântico  $\mathcal{E} : \mathcal{B}(\mathcal{H}_X) \rightarrow \mathcal{B}(\mathcal{H}_Y)$ , em que  $\mathcal{B}(\cdot)$  representa o espaço de operadores lineares de um espaço de Hilbert passado como parâmetro. Assim, o evento  $E_{x,y} : \mathcal{H}_X \rightarrow \mathcal{H}_Y$ , que corresponde a entrada de um estado quântico  $x \in \mathcal{X}$  e a saída de um estado quântico  $y \in \mathcal{Y}$  desse canal, pode ser dado por

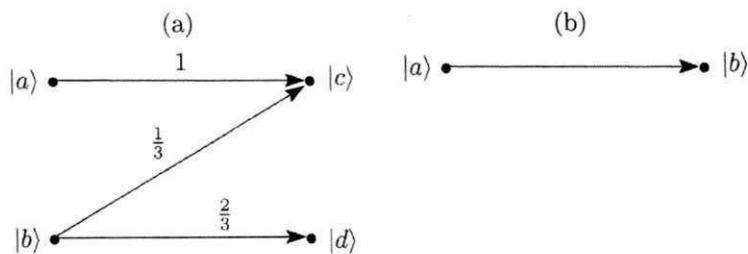
$$E_{x,y} = \sqrt{p(y|x)} |y\rangle \langle x|. \quad (2.27)$$

Assim, define-se um *grafo não-comutativo (de confusabilidade)* como sendo um subespaço

$$S = \text{span} \left\{ E_{x',y'}^\dagger \cdot E_{x,y} \neq 0; x, x' \in \mathcal{X}, y, y' \in \mathcal{Y} \right\}. \quad (2.28)$$

**Exemplo 2.6 (Grafo Não-Comutativo)** *Seja o canal quântico  $\mathcal{E}$  ilustrado na Figura 10. Tem-se como alfabeto de entrada os símbolos  $\mathcal{X} = \{a, b\}$  e como alfabeto de saída os símbolos  $\mathcal{Y} = \{c, d\}$ .*

Figura 10: Exemplo de grafo característico de um canal quântico e de grafo não-comutativo correspondente.



Fonte: Elaborado pela autora.

De acordo com a Eq. (2.27), tem-se os seguintes eventos:

$$E_{a,c} = 1 \cdot |c\rangle \langle a| = |c\rangle \langle a|, \quad (2.29)$$

$$E_{a,d} = 0 \cdot |d\rangle \langle a| = 0, \quad (2.30)$$

$$E_{b,c} = \sqrt{\frac{1}{3}} |c\rangle \langle b|, \quad (2.31)$$

$$E_{b,d} = \sqrt{\frac{2}{3}} |d\rangle \langle b|. \quad (2.32)$$

Vale salientar que tais eventos possuem uma correspondência direta com o canal quântico em questão. A partir de tais eventos é possível considerar o seguintes elementos que irão compor o grafo não-comutativo (vide Eq. (2.28))

$$E_{a,c}^\dagger \cdot E_{a,c} = |a\rangle \langle a|, \quad (2.33)$$

$$E_{a,c}^\dagger \cdot E_{b,c} = \sqrt{\frac{1}{3}} |a\rangle \langle b|, \quad (2.34)$$

$$E_{b,c}^\dagger \cdot E_{a,c} = \sqrt{\frac{1}{3}} |b\rangle \langle a|, \quad (2.35)$$

$$E_{b,c}^\dagger \cdot E_{b,c} = \frac{1}{3} |b\rangle \langle b|, \quad (2.36)$$

$$E_{b,d}^\dagger \cdot E_{b,d} = \frac{2}{3} |b\rangle \langle b|. \quad (2.37)$$

Assim,

$$S = \text{span} \left\{ E_{a,c}^\dagger \cdot E_{a,c}, E_{a,c}^\dagger \cdot E_{b,c}, E_{b,c}^\dagger \cdot E_{a,c}, E_{b,c}^\dagger \cdot E_{b,c}, E_{b,d}^\dagger \cdot E_{b,d} \right\}. \quad (2.38)$$

A partir deste conjunto  $S$  é possível denotar a capacidade erro-zero de um canal quântico. Esta capacidade é dada pela expressão a seguir, considerando o maior conjunto de estados ortogonais entre si denotado por  $\{|\phi_m\rangle : m = 1, \dots, N\}$

$$\forall m \neq m' : |\phi_m\rangle \langle \phi_{m'}| \in S^\perp, \quad (2.39)$$

em que  $S^\perp$  é um subespaço ortogonal ao subespaço  $S$  dado na Eq. (2.28). A expressão da Eq. (2.39) possui relação com a obtenção do número de independência do grafo correspondente. No Exemplo 2.6, em particular, tem-se que  $S^\perp = \emptyset$ . Isto implica que a capacidade quântica erro-zero do canal  $\mathcal{E}$  abordado neste exemplo é igual a zero.

Para todo grafo não-comutativo  $S \leq \mathcal{B}(\mathcal{H}_X)$  tem-se a seguinte relação

$$\alpha_q(S) \leq \alpha(S) \leq \tilde{\alpha}_V(S) \leq \tilde{\alpha}(S) \leq \hat{\alpha}(S) \quad (2.40)$$

em que cada um destes  $\alpha$ , denominados *números de independência*, possui uma relação com a capacidade erro-zero em canais quânticos, como sintetizado na Tabela 1. O detalhamento da obtenção destes números pode ser obtido nos trabalhos de Duan et al. (DUAN; SEVERINI; WINTER, 2011; DUAN; SEVERINI; WINTER, 2013).

Tabela 1: Sumário de outras definições de capacidade erro-zero para canais quânticos.

Capacidade	Expressão	Observações
<b>Capacidade Clássica Erro-Zero</b>	$C_0(S) = \lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha(S^{\otimes n})$	Abordada anteriormente na Eq. (2.26)
<b>Capacidade Quântica Erro-Zero</b>	$Q_0(S) = \lim_{n \rightarrow \infty} \frac{1}{n} \log \alpha_q(S^{\otimes n})$	$\alpha_q$ denota o número de independência quântico, cujo valor está relacionado à existência de uma dilatação de Stienespriing no canal.
<b>Capacidade Erro-Zero Assistida por Emarranhamento</b>	$C_{0E}(S) = \lim_{n \rightarrow \infty} \frac{1}{n} \log \tilde{\alpha}(S^{\otimes n})$	$\tilde{\alpha}$ denota o maior inteiro $N$ para o qual existem (i) espaços de Hilbert $\mathcal{H}_{X0}$ e $\mathcal{H}_{Y0}$ ; (ii) $\omega \in S(\mathcal{H}_{X0} \otimes \mathcal{H}_{Y0})$ ; (iii) um mapa $\mathcal{E}_m : \mathcal{B}(\mathcal{H}_{X0}) \rightarrow \mathcal{B}(\mathcal{H}_X)$ , tal que existem $N$ estados $\rho_m = (\mathcal{E} \circ \mathcal{E}_m \otimes \mathbb{1}_{Y0})\omega$ que são mutuamente adjacentes.
<b>Capacidade Erro-Zero Assistida por Emarranhamento Generalizado</b>	$\hat{C}_{0E}(S) = \lim_{n \rightarrow \infty} \frac{1}{n} \log \hat{\alpha}(S^{\otimes n})$	$\hat{\alpha}$ denota o número de independência assistido por emaranhamento generalizado o qual exige que $\mathcal{E}_m(\sigma) = \sum_j E_{jm} \sigma E_{jm}^\dagger$ e que $\sum_j E_{jm}^\dagger E_{jm} \in GL(\mathcal{H}_{X0})$ seja inversível.

O único número de independência que não se relaciona diretamente com uma capacidade erro-zero é  $\tilde{\alpha}_U(S)$ , por levar em conta restrições de unitariedade na sua definição. Os números  $\alpha_q(S)$ ,  $\alpha(S)$ ,  $\tilde{\alpha}(S)$  e  $\hat{\alpha}(S)$  são *computáveis*. Porém, encontrar uma expressão computável para a capacidade erro-zero associada pode não ser uma tarefa trivial.

Ao considerar esta dificuldade de computar a capacidade erro-zero de canais quânticos, Beigi e Shor (BEIGI; SHOR, 2008) e Beikidezfuli (BEIKIDEZFULI, 2009) confirmaram esta intratabilidade, ainda que para canais quânticos com QZEC positiva, mas estruturalmente simples. Tomando como ponto de partida que encontrar o clique de um grafo é um problema  $\mathcal{NP}$ -Completo, utilizando a Teoria da Informação Quântica, estes autores traduziram o problema para o domínio quântico, mostrando que este é  $\mathcal{QMA}$ -Completo. Graças a estrutura dos grafos característicos dos canais quânticos erro-zero, esta “tradução” de  $\mathcal{NP}$ -Completo para  $\mathcal{QMA}$ -Completo foi possível e outros problemas em que isto também é possível permanece ainda uma questão em aberto. Estes trabalhos não só ampliaram o conhecimento sobre as dificuldades de computar  $C^{(0)}$ , como também

as relações entre as classes de complexidade  $QMA$  e  $\mathcal{NP}$ .

O trabalho de Duan e Shi (DUAN; SHI, 2008) mostrou que a QZEC comporta-se drasticamente diferente da capacidade correspondente em canais clássicos. Mais precisamente, estes autores mostraram que no cenário de comunicações multi-usuário é possível transmitir informações clássicas perfeitamente em dois ou mais usos de um canal quântico ruidoso, embora não seja possível fazê-lo em apenas um uso. Este é um resultado alcançado graças às propriedades intrinsecamente quânticas, as quais não possuem correspondentes nos canais clássicos. Para possibilitar tal feito, os autores propuseram o uso de estados emaranhados, uma modificação em relação ao protocolo de comunicações proposto por Medeiros (MEDEIROS, 2008). Apesar disso, uma limitação deste canal é a necessidade de haver pelo menos dois emissores ou dois receptores e requerer que os emissores ou receptores realizem operações locais e comunicações clássicas apenas.

Se dois canais quânticos ruidosos não possuem determinada capacidade, mas quando combinados são capazes de tornar esta capacidade em não negativa, diz-se que há *superativação do canal* para esta capacidade. No caso de canais quânticos ruidosos, a superativação da capacidade erro-zero foi demonstrada ser possível assintoticamente (CUBITT; CHEN; HARROW, 2009; DUAN, 2009). Posteriormente, Chen et al. (CHEN et al., 2010) mostraram que esta superativação pode ir além, envolvendo não só  $C^{(0)}$ , como também  $Q^{(0)}$ . Estes autores provaram a existência de pares de canais que, individualmente, não podem comunicar nenhum tipo de informação com erro-zero, mesmo informação clássica. Porém, quando utilizados em conjunto, até mesmo um único uso da junção de canais é suficiente para transmitir com erro-zero todos os tipos de informação, quer seja clássica ou quântica. Este resultado, assim como o anterior, não possui correspondente em canais clássicos e, particularmente, foi considerado inesperado pelos autores, que o denominaram de “hiper-ultra superativação de canais quânticos”.

Um trabalho recente apresentado por Cubitt e Smith (CUBITT; SMITH, 2012) apresentou uma versão considerada “extrema” da superativação da capacidade erro-zero. Estes autores mostraram que existem canais  $\mathcal{E}_1$  e  $\mathcal{E}_2$  com capacidade erro-zero clássica igual a zero ( $C_0(\mathcal{E}_1) = C_0(\mathcal{E}_2) = 0$ ), mas que cuja combinação permite que a capacidade quântica de erro zero seja ativada, ou seja,  $Q^{(0)}(\mathcal{E}_1 \otimes \mathcal{E}_2) \geq 1$ . Este resultado implica numa superativação tanto da capacidade erro-zero clássica quanto da quântica, simultaneamente, em canais quânticos ruidosos.

O trabalho de Kohout et al. (BLUME-KOHOUT et al., 2010) consistiu na construção de um *framework* para lidar com a informação quântica na ausência de erros. Segundo os autores, a dinâmica do sistema afeta o tipo de informação que pode ser carregada ou armazenada (clássica, quântica, ou nenhum tipo de informação, por exemplo). Levando isto

em consideração, o objetivo deste *framework* é caracterizar um ferramental operacional capaz de descrever como preservar perfeitamente a informação apesar desta dinâmica do sistema. Com isso, abrange-se não somente os canais quânticos com capacidade erro-zero, como também os códigos quânticos corretores de erros, os subespaços e subsistemas livres de descoerência, e até mesmo outros tipos de métodos propostos pelos próprios autores, a exemplo dos códigos incondicionalmente preservados. Em suma, a principal contribuição destes autores é efetuar uma classificação exaustiva de maneiras em que a informação pode ser preservada.

A função  $\vartheta$  de Lovász (LOVÁSZ, 1979), cujo logaritmo define um limitante superior para a capacidade erro-zero de um canal clássico, também foi transposta para o domínio quântico (DUAN; SEVERINI; WINTER, 2011). Ao considerar qualquer grafo não-comutativo (vide Eq. (2.28))  $S \leq \mathcal{B}(\mathcal{H}_X)$ , i.e.,  $\mathbb{1} \in S$  e  $S = S^\dagger$ , tem-se a seguinte definição para esta função

$$\vartheta(S) = \max \{ \|\mathbb{1} + T\| : T \in S^\perp, \mathbb{1} + T \geq 0 \}, \quad (2.41)$$

em que a norma corresponde à norma do operador, e  $T$  é a matriz que possui zeros em todas as entradas  $T_{x,x'}$  quando  $(x, x')$  encontra-se no conjunto de arestas do grafo ou quando  $x = x'$ . O máximo valor da Eq. (2.41) iguala-se à expressão de  $\vartheta(G)$  para o caso clássico. Apesar desta similaridade, a quantidade de Lovász para o caso quântico possui algumas propriedades que a diferem desta mesma quantidade para o caso clássico.

Uma variante da capacidade erro-zero em canais quânticos foi proposta por Cubitt et al. (CUBITT et al., 2010a), a qual considera a existência de emaranhamento entre os participantes da comunicação. Como consequência, há um aumento da taxa em que informação clássica livre de erro pode ser enviada por tais canais quânticos. Embora nem todos os canais quânticos com capacidade erro-zero positiva forneçam as condições necessárias para a criação de tal tipo de emaranhamento, este é um exemplo de como as propriedades quânticas podem melhorar o desempenho de uma tarefa clássica. Alguns trabalhos recentes na literatura apresentaram resultados considerando esta variante, tais como obtenção de limitantes inferiores e superiores, verificação de melhorias em questões como codificação e aplicações em protocolos de teleportação (MANCINSKA; SCARPA; SEVERINI, 2013; BRIET et al., 2013).

Em termos de implementações práticas, um dos primeiros trabalhos a reportar a implementação física de um canal erro-zero foi proposto por Gyongyosi e Imre (GYONGYOSI; IMRE, 2012). Estes autores utilizaram-se de múltiplos canais ópticos, tais como fibra óptica, para o envio de informação. Cada um destes canais possui capacidade erro-zero nula, mas a junção deles habilita a superativação da capacidade erro-zero quântica, abordada

anteriormente. Este é um dos artifícios utilizados pelos autores para garantir uma boa taxa de envio de informação sem erros. A idéia é utilizar esta estratégia como parte da implementação de *repetidores quânticos*, dispositivos que compõem uma rede de dados quântica e cujo objetivo é a transmissão de estados quânticos emaranhados entre os diversos repetidores existentes na rede. Se tais repetidores vierem a ser construídos, haverá a possibilidade de efetuar comunicações quânticas sem erros em longa distância com um menor uso de recursos, pois etapas como a de purificação passam a ser desnecessárias.

## 2.3 Subespaços e Subsistemas Livres de Descoerência

Suponha um sistema quântico composto fechado formado pelo sistema de interesse, denotado por  $S$  e definido em um espaço de Hilbert  $\mathcal{H}$ , e pelo ambiente, denotado por  $E$ . Este sistema possui Hamiltoniano descrito por:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \quad (2.42)$$

em que  $\mathbb{1}$  denota o operador identidade,  $\mathbb{H}_S$  denota o operador puro para o sistema de interesse,  $\mathbb{H}_E$  denota o operador puro para o ambiente, e  $\mathbb{H}_{SE}$  denota o operador da interação entre sistema e ambiente (LIDAR; WHALEY, 2003).

Para a ausência total de erros, tem-se que o cenário ideal ocorre quando  $\mathbb{H}_{SE}$  é igual a zero, indicando que sistema e ambiente estão completamente desacoplados e evoluem independentemente e unitariamente de acordo com seus respectivos hamiltonianos  $\mathbb{H}_S$  e  $\mathbb{H}_E$ , respectivamente (LIDAR; WHALEY, 2003). Porém, em situações realísticas este cenário ideal não ocorre, uma vez que nenhum sistema pode ser completamente livre de erro. Então, após isolar o sistema tão bem quanto possível, deve-se adotar pelo menos uma das seguintes medidas: identificar e corrigir erros quando eles ocorrerem; evitar o erro quando possível; suprimir o ruído no sistema (BYRD; WU; LIDAR, 2004).

Se algumas simetrias existirem na interação entre sistema e ambiente, é possível encontrar um “lugar seguro” no espaço de Hilbert que não sofre os efeitos adversos da descoerência. Seja  $\{A_i(t)\}$  um conjunto de operadores na *representação da soma de operadores* (OSR – *Operator-Sum Representation*) representando a evolução do sistema. Diz-se que a matriz densidade  $\rho_S$  é *invariante* perante os operadores  $\{A_i(t)\}$  se  $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$ . A partir disto, é possível definir os *subespaços e subsistemas livres de descoerência* (DFS – *Decoherence-Free Subspaces and Subsystems*), cujos estados são invariantes apesar da existência de um acoplamento não trivial entre sistema e ambiente.

**Definição 2.10 (Subespaços Livres de Descoerência (BACON, 2001))** *Um subespaço  $\tilde{\mathcal{H}}$  de um espaço de Hilbert  $\mathcal{H}$  é dito ser livre de descoerência em relação ao acopla-*

mento entre sistema e ambiente se todo estado puro deste subespaço é invariante perante a correspondente OSR da evolução, para quaisquer condição inicial do ambiente

$$\sum_i A_i(t) |\tilde{k}\rangle \langle \tilde{k}| A_i^\dagger(t) = |\tilde{k}\rangle \langle \tilde{k}|, \forall |\tilde{k}\rangle \langle \tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \quad (2.43)$$

Seja o hamiltoniano da interação entre sistema e ambiente dado por  $H_{SE} = \sum_j S_j \otimes E_j$ , em que  $S_j$  e  $E_j$  são os operadores do sistema e ambiente, respectivamente. Considere-se que os operadores do ambiente  $E_j$  são linearmente independentes. As simetrias requeridas para a existência de um subespaço livre de descoerência são descritas no teorema a seguir (a prova deste teorema é apresentada em (LIDAR; WHALEY, 2003, Seção 5))

**Teorema 2.3 (Condições para os Subespaços Livres de Descoerência)** *Um subespaço  $\tilde{\mathcal{H}}$  é livre de descoerência se, e somente se, os operadores do sistema  $S_j$  atuam proporcionalmente à identidade neste subespaço, ou seja*

$$S_j |\tilde{k}\rangle = c_j |\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \quad (2.44)$$

A noção de um subespaço que permanece livre de descoerência durante a evolução de um sistema não é, entretanto, o método mais geral de prover codificação livre de descoerência em um sistema quântico (LIDAR; WHALEY, 2003). Knill et al. (KNILL; LAFLAMME; VIOLA, 2000) desenvolveram um método para codificação em subsistemas ao invés de subespaços, como será apresentado a seguir.

**Definição 2.11 (Subsistemas Livre de Descoerência)** *Seja um superoperador positivo que preserva o traço  $\mathcal{E} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$  em um espaço de Hilbert  $\mathcal{H}$ . Suponha  $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ . Diz-se que  $\mathcal{H}^B$  ( $\dim(\mathcal{H}^B) \geq 1$ ) é um subsistema livre de descoerência se, para  $\forall \sigma^A \in B(\mathcal{H}^A)$  e para  $\forall \sigma^B \in B(\mathcal{H}^B)$ , existe um  $\tau^A \in B(\mathcal{H}^A)$  tal que*

$$\mathcal{E}(\sigma^A \otimes \sigma^B) = \tau^A \otimes \sigma^B. \quad (2.45)$$

Em termos de traços parciais, esta definição é equivalente a

$$(\text{Tr}_A \circ \mathcal{E})(\sigma) = \text{Tr}_A(\sigma) \quad \forall \sigma = \sigma^A \otimes \sigma^B. \quad (2.46)$$

No caso particular em que  $\dim(\mathcal{H}^A) = 1$ , diz-se que  $\mathcal{H}^B$  é um subespaço livre de descoerência para  $\mathcal{E}$ .

É possível construir códigos a partir de estados de um DFS, os quais são denominados *códigos quânticos de prevenção de erros* (QEAC – *Quantum error-avoiding code*).

Neste tipo de código, a perturbação e a recuperação são triviais. Estes códigos podem ser contrastados com os *códigos quânticos corretores de erro* (QECC – *Quantum Error-Correcting Code*) em alguns aspectos. Enquanto os QECCs são projetados para corrigir erros após a sua ocorrência, QEACs não possuem habilidades para corrigir erros, uma vez que eles os previnem; QECCs utilizados em cenários práticos pertencem a classe dos códigos não-degenerados, enquanto os QEACs são códigos altamente degenerados; QEACs usualmente requerem um menor número de qubits físicos para representar um qubit lógico que os QECCs. Em particular, se a degenerescência de um QECC atinge o máximo, este se reduz a um QEAC, ilustrando uma circunstância em que um tipo de código torna-se equivalente ao outro (DUAN; GUO, 1999).

Embora o DFS seja uma maneira de prevenir erros, nem sempre é possível que as condições de simetria necessárias para a sua existência sejam satisfeitas. Zanardi e Rasetti (ZANARDI; RASETTI, 1997) afirmam que tais condições emergem apenas em cenários onde há *descoerência coletiva* que acontece quando vários qubits se acoplam identicamente ao ambiente, ao passo que sofrem defasamento e dissipação.

**Exemplo 2.7 (Canal Quântico de Defasamento Coletivo)** *Defasamento é um fenômeno no qual a fase relativa de um qubit é perdida. Canais quânticos com defasamento coletivo atuam da seguinte forma nos qubits de entrada*

$$|0\rangle \rightarrow |0\rangle, \quad (2.47)$$

$$|1\rangle \rightarrow e^{i\phi} |1\rangle, \quad (2.48)$$

em que  $\phi$  é o parâmetro de defasamento coletivo que varia com o tempo  $t$ . Um qubit lógico composto de dois qubits físicos com paridade antiparalela é imune ao defasamento coletivo, i.e.,

$$|0_L\rangle = |01\rangle, \quad (2.49)$$

$$|1_L\rangle = |10\rangle. \quad (2.50)$$

Um qubit pode, portanto, ser codificado como  $|\psi_L\rangle = \alpha |0_L\rangle + \beta |1_L\rangle$ . É interessante observar que  $|\psi_L\rangle$  não sofre os efeitos da descoerência neste canal

$$\mathcal{E}(|\psi_L\rangle) = \mathcal{E}(\alpha|0_L\rangle + \beta|1_L\rangle) \quad (2.51)$$

$$= \alpha e^{i\phi}|01\rangle + \beta e^{i\phi}|10\rangle \quad (2.52)$$

$$= e^{i\phi}(\alpha|01\rangle + \beta|10\rangle) \quad (2.53)$$

$$= e^{i\phi}|\psi_L\rangle \quad (2.54)$$

$$= |\psi_L\rangle, \quad (2.55)$$

pois o fator de fase global  $e^{i\phi}$  adquirido devido ao processo de defasamento não possui significância física (BENENTI; CASATI; STRINI, 2007). Isto significa que os estados  $|01\rangle$  e  $|10\rangle$  pertencem a  $\tilde{\mathcal{H}}$ , um subespaço livre de descoerência do espaço de Hilbert  $\mathcal{H}$  no canal quântico de defasamento coletivo.

Resultados práticos da literatura já consideram a identificação, implementação e utilização de DFS em Computação e Comunicações Quânticas (KWIAT et al., 2000; VIOLA et al., 2001; BEIGE et al., 2000; LIDAR; CHUANG; WHALEY, 1998; FENG, 2001; KIELPINSKI, 2001; ZHANG; ZHANG; WANG, 2006; IVANOV et al., 2010; MOHSENI et al., 2003; XUE; XIAO, 2006). Para as Comunicações Quânticas, em particular, há destaque dos DFS para a construção de repetidores quânticos pois, em teoria, estes dispositivos podem ser utilizados em comunicações para distribuição quântica de chaves, esquemas de teleportação quântica e também para redes de computadores quânticos (DORNER; KLEIN; JAKSCH, 2008). O trabalho de Xue (XUE, 2008) se destaca por já efetuar uma caracterização do uso de DFS em repetidores para comunicações quânticas de longa distância.

### 2.3.1 Método para Obtenção de Subespaços e Subsistemas Livres de Descoerência

Embora a utilização dos DFS seja vantajosa por preservar a fidelidade dos estados quânticos, uma das limitações na utilização destes subespaços e subsistemas está na dificuldade em identificá-los (BYRD; WU; LIDAR, 2004). Para minimizar os efeitos desta problemática, Choi e Kribs (CHOI; KRIBS, 2006) propuseram um método sistemático para a identificação de DFS quando o modelo de erros é conhecido. O objetivo desta seção é a caracterização deste método, que é essencialmente algébrico.

Seja  $\mathcal{E} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$  uma operação quântica. Denota-se  $\mathcal{E} \equiv \{E_a\}$  quando o modelo de erros para  $\mathcal{E}$  é conhecido. Os elementos de operação  $\{E_a\}$  determinam a atuação de  $\mathcal{E}$  por meio da OSR, i.e.,  $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ .

O comutador de ruído  $\mathcal{A}'$  para  $\mathcal{E}$  é o conjunto de todos os operadores em  $\mathcal{B}(\mathcal{H})$  que comutam com os operadores  $E_a$  e  $E_a^\dagger$ . No caso de canais unitais (que satisfazem a propriedade  $\mathcal{E}(\mathbb{1}) = \mathbb{1}$ ), tem-se que todo  $\sigma \in \mathcal{A}'$  satisfaz  $\mathcal{E}(\sigma) = \sigma$ . Como consequência,  $\mathcal{A}$  é uma  $\dagger$ -álgebra<sup>2</sup> gerada por  $E_a$ , a qual é denominada *álgebra de interação* associada a  $\mathcal{E}$ .

Porém, nem todos os canais são unitais e, em virtude disto, é necessário explorar um formalismo para o caso mais geral. Sabe-se que neste caso mais geral, os operadores  $\sigma \in \mathcal{A}'$  satisfazem  $\mathcal{E}(\sigma) = \sigma\mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$ . Dado um projetor  $P$  em  $\mathcal{B}(\mathcal{H})$ , o objetivo será a identificação de uma subálgebra  $P\mathcal{B}(\mathcal{H})P$  de  $\mathcal{B}(\mathcal{H})$  com álgebra  $\mathcal{B}(P\mathcal{H})$ . Para tanto, lança-se mão do seguinte teorema.

**Teorema 2.4 (Choi e Kribs (CHOI; KRIBS, 2006))** *Seja  $\mathcal{E} = \{E_a\}$  uma operação quântica em  $\mathcal{B}(\mathcal{H})$ . Suponha que  $P$  é uma projeção em  $\mathcal{H}$  que satisfaz*

$$\mathcal{E}(P) = P\mathcal{E}(P)P, \quad (2.56)$$

então  $E_a P = P E_a P, \forall a$ . Defina

$$\mathcal{A}'_P \equiv \{ \sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, P E_a P] = 0 = [\sigma, P E_a^\dagger P] \}, \quad (2.57)$$

e

$$\text{Fix}_P(\mathcal{E}) \equiv \{ \sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma, \quad (2.58)$$

$$\mathcal{E}(\sigma^\dagger\sigma) = \sigma^\dagger\mathcal{E}(P)\sigma, \mathcal{E}(\sigma, \sigma^\dagger) = \sigma\mathcal{E}(P)\sigma^\dagger \}. \quad (2.59)$$

Então  $\text{Fix}_P(\mathcal{E})$  é uma  $\dagger$ -álgebra dentro de  $\mathcal{B}(P\mathcal{H})$  a qual coincide com a álgebra  $\mathcal{A}'_P$ , isto é

$$\text{Fix}_P(\mathcal{E}) = \mathcal{A}'_P. \quad (2.60)$$

A prova deste teorema não será apresentada na íntegra, apenas alguns aspectos da mesma serão ressaltados. Se  $P$  satisfaz a Eq. (2.56), então

$$0 \leq P^\perp E_a P E_a^\dagger P^\perp \leq P^\perp \mathcal{E}(P) P^\perp = 0 \quad \forall a. \quad (2.61)$$

<sup>2</sup> O formalismo das  $\dagger$ -álgebras, também conhecida por álgebras- $C^*$ , foi desenvolvido para seu uso na Mecânica Quântica da Física de Observáveis. Uma  $\dagger$ -álgebra é uma álgebra- $*$  de Banach com uma condição adicional para a norma:  $\|A^* \cdot A\| = \|A^2\|$  para todo  $A \in \mathcal{U}$ , em que  $\mathcal{U}$  é uma álgebra de norma complexa. Um tutorial completo sobre as  $\dagger$ -álgebras pode ser encontrado na obra de Davidson (DAVIDSON, 1996).

Para quaisquer operadores  $A, B \in \mathcal{B}(\mathcal{H})$ ,  $A \leq B \Rightarrow \langle \psi | B - A | \psi \rangle \geq 0$ ,  $\forall |\psi\rangle \in \mathcal{H}$ . Assim,  $P^\perp E_a P = 0$  ou, equivalentemente,  $E_a P = P E_a P$ ,  $\forall a$ . Ao tomar um  $\sigma \in \mathcal{A}'_P$  então

$$\mathcal{E}(\sigma) = \sum_a E_a P \sigma P E_a^\dagger \quad (2.62)$$

$$= \sigma \sum_a E_a P E_a^\dagger = \sum_a E_a P E_a^\dagger \sigma \quad (2.63)$$

$$= \sigma \mathcal{E}(P) = \mathcal{E}(P) \sigma. \quad (2.64)$$

Os projetores  $P$  que satisfazem a Eq. (2.56) possuem algumas propriedades. Por exemplo, um canal quântico  $\mathcal{E} \equiv \{E_a\}$  atua em um estado quântico  $\sigma \in \mathcal{A}'_P$  projetando-o em um outro estado  $\sigma'$  no subespaço de  $P$ . Para comprovar esta afirmação, tem-se

$$\sigma' = \mathcal{E}(\sigma) \quad (2.65)$$

$$= \sigma \mathcal{E}(P) \quad (2.66)$$

$$= (P \sigma P) (P \mathcal{E}(P) P) \quad (2.67)$$

$$= P[\sigma P \mathcal{E}(P)] P \in \mathcal{B}(P\mathcal{H}). \quad (2.68)$$

Neste caso em particular, tem-se que  $\mathcal{E}(\sigma) = \sigma$  somente se  $\mathcal{E}(P) = 1$ .

O passo seguinte é explicitar como projetores com esta caracterização capturam o DFS de uma operação quântica  $\mathcal{E}$  (CHOI; KRIBS, 2006).

**Teorema 2.5 (Método para obtenção de DFS)** *Seja  $\mathcal{E}$  uma operação quântica em  $\mathcal{B}(\mathcal{H})$ . Seja  $P$  um projetor que satisfaz a Eq. (2.56) e seja  $P\mathcal{H} = \bigoplus_k (\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$  a decomposição de  $P\mathcal{H}$  induzida pela estrutura da  $\dagger$ -álgebra  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$ . Então, os subsistemas  $\mathcal{H}^{B_k}$ , com  $\dim(\mathcal{H}^{B_k}) > 1$ , são subsistemas livres de descoerência para  $\mathcal{E}$ .*

Pode-se afirmar então que a essência deste método consiste na determinação de todos os projetores  $P$  satisfazendo a Eq. (2.56). A partir disto, utiliza-se a estrutura de  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$  para determinar os estados pertencentes ao DFS.

Um aspecto que deve ser frisado é a *otimalidade* do método proposto, ou seja, este é capaz de obter todos os projetores que satisfazem a Eq. (2.56) (vide (CHOI; KRIBS, 2006, Teorema 3)). Apesar da caracterização consistente do método, os autores afirmam que ainda não há um procedimento computacional automatizado para a realização do mesmo.

**Exemplo 2.8 (Identificação de um DFS em um Canal Quântico)** *Suponha o canal  $\mathcal{E} \equiv \{E_0, E_1, E_2\}$  que atua em um estado de 2 qubits e cujos operadores de Kraus são dados por*

$$E_0 = \alpha(|00\rangle\langle 00| + |11\rangle\langle 11|) + |01\rangle\langle 01| + |10\rangle\langle 10| \quad (2.69)$$

$$E_1 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|) \quad (2.70)$$

$$E_2 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| - |01\rangle\langle 01| - |10\rangle\langle 10|) \quad (2.71)$$

em que  $q$  é um escalar,  $0 < q < 1$ ;  $\alpha = \sqrt{1-2q}$ ;  $\beta = \sqrt{q/2}$ . É possível perceber que  $\mathcal{E}(\mathbb{1}) = \sum_{a=0}^2 E_a E_a^\dagger \neq \mathbb{1}$  e que, portanto, este canal não é unital.

Neste modelo de canal, há apenas um qubit  $\rho$  tal que  $\mathcal{E}(\rho) = \rho$ . Porém, a invariância deste estado não é advinda da ação de  $\mathcal{E}$  em si, mas trata-se de um ponto fixo. Porém, há um outro DFS neste estado se for considerada a atuação do projetor  $P = |01\rangle\langle 01| + |10\rangle\langle 10|$ , i.e., todos os operadores suportados por  $P$  são invariantes perante  $\mathcal{E}$ . Isto significa que  $\mathcal{E}(\sigma') = \sigma'$  para todo  $\sigma' = P\sigma P$ .

Para exemplificar esta afirmação, seja o operador densidade do estado  $|\psi\rangle$  dado por

$$|\psi\rangle\langle\psi| = \frac{|01\rangle\langle 01| + |01\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 00|}{2} \quad (2.72)$$

A projeção deste estado com o projetor  $P$  resulta em

$$|\psi'\rangle\langle\psi'| = P|\psi\rangle\langle\psi|P \quad (2.73)$$

$$= (|01\rangle\langle 01| + |10\rangle\langle 10|) \left( \frac{|01\rangle\langle 01| + |01\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 00|}{2} \right) P \quad (2.74)$$

$$= \left( \frac{|01\rangle\langle 01| + |01\rangle\langle 00|}{2} \right) (|01\rangle\langle 01| + |10\rangle\langle 10|) \quad (2.75)$$

$$= \frac{|01\rangle\langle 01|}{2} \quad (2.76)$$

Note que  $|\psi'\rangle\langle\psi'|$  é invariante ao canal  $\mathcal{E}$ , apesar deste não pertencer inicialmente ao comutador de ruído  $\mathcal{A}'$  para  $\mathcal{E}$ :

$$\mathcal{E}(|\psi'\rangle\langle\psi'|) = \sum_{a=0}^2 E_a |\psi'\rangle\langle\psi'| E_a^\dagger \quad (2.77)$$

$$= \frac{|01\rangle\langle 01|}{2} + \beta \cdot \frac{|01\rangle\langle 01|}{2} - \beta \cdot \frac{|01\rangle\langle 01|}{2} \quad (2.78)$$

$$= \frac{|01\rangle\langle 01|}{2} \quad (2.79)$$

### 2.3.2 Relação com a Capacidade Erro-Zero de Canais Quânticos

O trabalho de Medeiros et al. (MEDEIROS et al., 2006b) explora a relação entre os DFS e a capacidade de erro-zero em canais quânticos. Esta relação é estabelecida a partir do método de obtenção de DFS em canais arbitrários proposto por Choi e Kribs (CHOI; KRIBS, 2006), detalhado na seção anterior. O objetivo desta seção é tornar clara esta relação.

Sabe-se que um canal quântico possui capacidade erro-zero se, e somente se, existirem pelo menos dois estados não-adjacentes dentre os estados quânticos de entrada. Considerando um par  $(\mathcal{S}, \mathcal{M})$  ótimo, conforme Definição 2.8, é possível derivar um par  $(\mathcal{S}', \mathcal{M}')$ , em que  $\mathcal{S}' \subset \mathcal{S}$ ,  $\mathcal{M}' = \{M_1, \dots, M_k, M_{k+1}\} \subset \mathcal{M}$ , e  $M_{k+1} = \mathbb{1} - \sum_{i=1}^k M_i$ . Os projetores  $M_i \in \mathcal{M}'$ , com  $1 \leq i \leq k$ , satisfazem

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i \quad (2.80)$$

e

$$M_i M_j = \delta_{ij} M_i M_j \quad (2.81)$$

em que  $\delta$  denota o delta de Kronecker. Ao escolher os projetores com estas restrições, nota-se que os elementos de  $\mathcal{S}'$  podem vir a definir um DFS, tal como estabelecido pelo método para obtenção de DFS explorado na Seção 2.3.1.

Como consequência, tem-se que o conjunto  $(\mathcal{S}', \mathcal{M}')$  é ótimo e que a capacidade erro-zero  $C^{(')}(\mathcal{E})$  definida para este conjunto pode ser maior que a capacidade erro-zero  $C^{(0)}(\mathcal{E})$  definida para  $(\mathcal{S}, \mathcal{P})$ , ou seja  $C^{(')}(\mathcal{E}) \geq C^{(0)}(\mathcal{E})$ . As provas destas consequências são adequadamente apresentadas no artigo original e fazem uso de Teoria dos Grafos e de propriedades de mapeamentos (MEDEIROS et al., 2006b).

Em suma, a conclusão dos autores a respeito da relação entre DFS e capacidade erro-zero é de que se um canal erro-zero possui um DFS, então a capacidade erro-zero deve ser calculada a partir deste DFS, utilizando para tal projetores que atendem a algumas propriedades.

## 2.4 Capacidade Quântica de Sigilo

A privacidade em sistemas quânticos foi inicialmente considerada por Schumacher e Westmoreland (SCHUMACHER; WESTMORELAND, 1998). Estes pesquisadores conceberam um modelo no qual dois participantes legítimos (Alice e Bob) desejam trocar mensagens clássicas por um canal quântico ruidoso. Um espião (Eva) possui acesso total ao ambiente no qual este canal quântico inserido, podendo capturar informações dos participantes

legítimos. Alice envia mensagens a partir de um conjunto de inteiros  $\mathcal{U} = \{1, 2, \dots, |\mathcal{U}|\}$  e as mapeia em um *ensemble* de estados quânticos  $\{\rho(u), p_u : u \in \mathcal{U}\}$ . Os estados no *ensemble* são produtos tensoriais de estados quânticos denominados *palavras-código quânticas*:

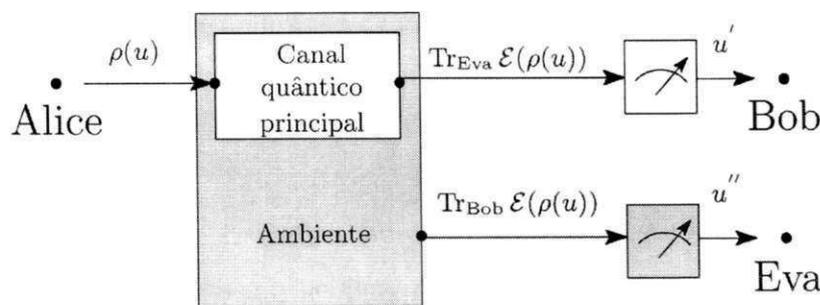
$$\rho(u) = \rho_1(u) \otimes \rho_2(u) \otimes \dots \otimes \rho_n(u) \quad u \in \mathcal{U}, \rho_i(u) \in \mathcal{H}, i = 1, 2, \dots, n. \quad (2.82)$$

O mapeamento descrito caracteriza um *código quântico de blocos* com comprimento de bloco igual a  $n$  e taxa igual a  $R = \frac{1}{n} \log |\mathcal{U}|$ . Um esquema de decodificação para um código quântico de blocos de comprimento  $n$  é uma função de decodificação que associa univocamente cada estado quântico saído do canal a um conjunto de inteiros, i.e.,  $g : \mathcal{H} \rightarrow \mathcal{U}, \hat{u} = g(\mathcal{E}(\rho(u))) \in \mathcal{U}$ . Um erro ocorre quando  $g(\mathcal{E}(\rho(u))) \neq u$ . A privacidade quântica entre Alice e Bob é limitada pela *informação coerente*<sup>3</sup> entre eles.

Ao considerar esta formulação, Cai et al. (CAI; WINTER; YEUNG, 2004) e Devetak (DEVETAK, 2005) observaram algumas similaridades com os canais *wiretap* clássicos propostos por Wyner (WYNER, 1975) e, a partir desta observação, propuseram uma versão quântica destes canais, apresentada na Definição 2.12 e ilustrada na Figura 11.

**Definição 2.12 (Canal Wiretap Quântico)** *Um canal wiretap quântico sem memória é descrito por um superoperador  $\mathcal{E}$  em um espaço de Hilbert complexo  $\mathcal{H} = \mathcal{H}_{Bob} \otimes \mathcal{H}_{Eva}$ . Quando Alice envia um estado quântico  $\rho \in \mathcal{H}^{\otimes n}$ , Bob recebe  $\rho_{Bob} = \text{Tr}_{Eva}[\mathcal{E}^{\otimes n}(\rho)]$  e Eva recebe  $\rho_{Eva} = \text{Tr}_{Bob}[\mathcal{E}^{\otimes n}(\rho)]$ , em que  $n$  é a dimensão do espaço de Hilbert da entrada.*

Figura 11: Idéia geral do canal de *wiretap* quântico.



Fonte: Elaborada pela autora.

Ao utilizar um canal *wiretap* quântico, pode-se ter segurança ao utilizar um tipo particular de código quântico de blocos, os chamados *códigos wiretap quânticos*. Dois

<sup>3</sup> A informação coerente é uma medida de informação da diferença entre a entropia de von Neumann de um sistema quântico de interesse e a troca de entropia deste sistema com o ambiente (SCHUMACHER; WESTMORELAND, 1998).

parâmetros adicionais são incorporados:  $\lambda$ , que representa um limitante superior para a probabilidade de erro; e  $\mu$ , que representa um limitante superior para o máximo de informação acessível ao adversário. Um código *wiretap* quântico é referido como uma 4-tupla  $(n, |\mathcal{U}|, \lambda, \mu)$ . A caracterização formal destes códigos é dada a seguir.

**Definição 2.13 (Código *Wiretap* Quântico de Blocos)** *Seja um código quântico de blocos de comprimento  $n$  e taxa  $R = \frac{1}{n} \log |\mathcal{U}|$  em que  $\mathcal{U} = \{1, 2, \dots, |\mathcal{U}|\}$  é um conjunto de mensagens clássicas. O conjunto de palavras-código rotuladas pelos índices das mensagens é dado como segue:*

$$\Omega(\mathcal{U}) = \{\rho(u) : u \in \mathcal{U}\}. \quad (2.83)$$

Assume-se que a função de decodificação é dada por um POVM  $\{\mathcal{D}_u : u \in \mathcal{U}\}$  em que  $\sum_u \mathcal{D}_u \leq \mathbb{1}$ .

Este código é dito ser um código *wiretap* quântico de blocos com parâmetros  $(n, |\mathcal{U}|, \lambda, \mu)$  (ou, simplesmente, código *wiretap* quântico) se as duas condições seguintes são satisfeitas:

$$P_e = 1 - \frac{1}{|\mathcal{U}|} \sum_{u \in \mathcal{U}} \text{Tr}_{Eva}[\mathcal{E}(\rho(u))\mathcal{D}_u] \leq \lambda, \quad (2.84)$$

e

$$\frac{1}{n} \left\{ S \left( \sum_{u \in \mathcal{U}} \text{Tr}_{Bob}[\mathcal{E}^{\otimes n}(\rho(u))] \right) - \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} S(\text{Tr}_{Bob}[\mathcal{E}^{\otimes n}(\rho(u))]) \right\} \leq \mu. \quad (2.85)$$

A taxa deste código é dada por  $R_n = \frac{1}{n} \log |\mathcal{U}|$ .

Na definição de um código *wiretap* quântico com parâmetros  $(n, |\mathcal{U}|, \lambda, \mu)$ , a Eq. (2.84) assegura uma probabilidade média de erros de decodificação por Bob menor que  $\lambda$ , e a Eq. (2.85) limita a informação acessível do espião, o qual não captura praticamente nenhuma informação da mensagem enviada por Alice (CAI; WINTER; YEUNG, 2004).

Por fim, a *capacidade de sigilo de um canal quântico* é definida como segue.

**Definição 2.14 (Capacidade Quântica de Sigilo)** *A capacidade quântica de sigilo de um canal quântico é o maior número real  $C_S$ , tal que para todos  $\epsilon, \lambda, \mu > 0$  e  $n$  suficientemente grande, existe um código *wiretap* quântico com parâmetros  $(n, |\mathcal{U}|, \lambda, \mu)$  tal que*

$$C_S < \frac{1}{n} \log |\mathcal{U}| + \epsilon \quad (2.86)$$

Apesar das definições anteriores assumirem mensagens uniformemente distribuídas, o teorema a seguir é um resultado mais geral para a capacidade quântica de sigilo (CAI; WINTER; YEUNG, 2004, Seção 5).

**Teorema 2.6 (Capacidade Quântica de Sigilo)** *Para um canal wiretap quântico  $\mathcal{E}$  caracterizado como na Definição 2.12, a capacidade quântica de sigilo satisfaz:*

$$C_S(\mathcal{E}) \geq \max_{\{P\}} [\chi^{Bob} - \chi^{Eve}] \quad (2.87)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre  $\mathcal{U}$ ; e  $\chi^{Bob}$  e  $\chi^{Eve}$  são quantidades de Holevo dadas como seguem:

$$\chi^{Bob} = S(\rho_{Bob}) - \sum_i p_i S(\rho_{Bob}(i)) \quad (2.88)$$

$$\chi^{Eve} = S(\rho_{Eve}) - \sum_i p_i S(\rho_{Eve}(i)) \quad (2.89)$$

em que  $\rho_{Bob}$  é o estado recebido por Bob resultante do traço parcial sobre o ambiente; e  $\rho_{Eve}$  é o estado final de Eva.

Na prova deste teorema, utiliza-se a técnica de *random coding proof* para assegurar que a informação capturada por Eva é desprezível, culminando em *segurança incondicional* quando a taxa de envio de informação pelo canal é limitada superiormente pela capacidade quântica de sigilo (CAI; WINTER; YEUNG, 2004). Esta capacidade é equivalente à definição de privacidade quântica estabelecida por Schumacher e Westmoreland (SCHUMACHER; WESTMORELAND, 1998).

A capacidade quântica de sigilo definida na Eq. (2.87) é o análogo quântico da capacidade clássica de sigilo proposta por Wyner (WYNER, 1975). É possível, inclusive, perceber algumas similaridades nas definições clássica e quântica desta capacidade: ambas limitam uma probabilidade de erros de decodificação e também a informação que está acessível ao espião. Apesar destas similaridades, o caso quântico utiliza suas próprias medidas de informação, a exemplo da entropia de von Neumann e da quantidade de Holevo. Uma característica particular da capacidade quântica de sigilo é que esta não possui uma caracterização de letra isolada, i.e., ela não é computável pois considera todos os possíveis estados de entrada bem como todas as distribuições de probabilidade sobre eles (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005).

Algumas propostas de códigos para canais *wiretap* quânticos podem ser encontradas na literatura. Hamada (HAMADA, 2008a; HAMADA, 2008b) propôs uma família

de códigos clássicos e quânticos para canais *wiretap*. No caso dos códigos quânticos, estes são baseados nos códigos quocientes e conjugados, que são equivalentes aos Códigos Calderbank-Shor-Steane (CSS) (NIELSEN; CHUANG, 2010, Seção 10.4.2). A complexidade de tempo da codificação e da decodificação da proposição de Hamada é de tempo polinomial em função do número de usos do canal.

Uma outra família de códigos voltados para canais *wiretap* quânticos foi proposta por Wilde e Guha (WILDE; GUHA, 2011). Esta construção se baseia no uso de códigos polares para canais *wiretap* degradados que atinjam a capacidade simétrica de sigilo para um canal *wiretap* quântico com espião clássico. Embora esta família de códigos possua tempo polinomial para codificação e decodificação, a elaboração de exemplos com tais códigos é fortemente dependente de simulações numéricas (DUTTON; GUHA; WILDE, 2012). Apesar disso, os autores argumentam a adequação destes códigos para canais quânticos de decaimento de amplitude, de defasamento, de apagamento e de clonagem (WILDE; GUHA, 2011; DUTTON; GUHA; WILDE, 2012).

## 2.5 Informação Acessível

No estudo da informação acessível no contexto da Teoria da Informação Quântica, toma-se como ponto de partida um sistema de comunicações como ilustrado na Figura 12. A fonte quântica efetua a codificação de mensagens clássicas em estados quânticos, como apresentado na Definição 2.15.

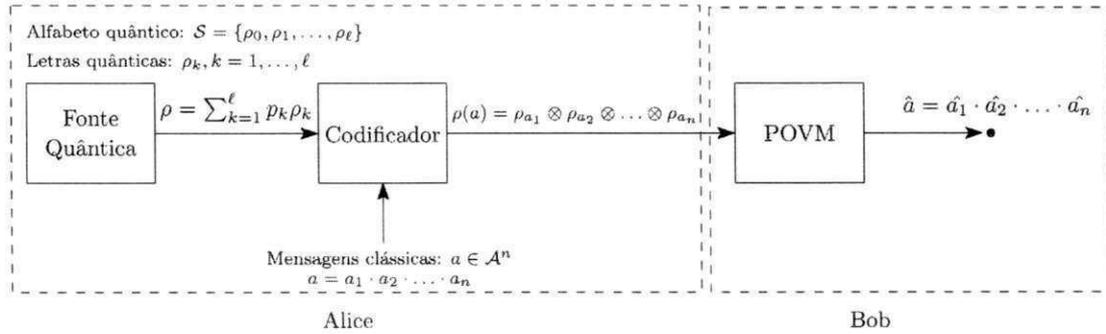
**Definição 2.15 (Fonte Quântica Sem Memória)** *Seja um conjunto de índices de mensagens clássicas dado por  $\mathcal{A} = \{0, 1, \dots, \ell\}$ . Uma fonte quântica sem memória é um dispositivo que prepara estados quânticos de acordo com um ensemble  $(\mathcal{S}, \mathbf{p})$ . O conjunto  $\mathcal{S} = \{\rho_0, \rho_1, \dots, \rho_\ell\}$ , denominado alfabeto da fonte, é composto de estados quânticos puros geralmente não-ortogonais, denominados letras quânticas. As letras quânticas estão em correspondência biunívoca com o conjunto de índices de mensagens clássicas. A distribuição de probabilidades  $\mathbf{p} = (p_0, p_1, \dots, p_\ell)$ ,  $\sum_{i=0}^{\ell} p_i = 1$ , descreve a probabilidade da fonte de emitir uma determinada letra quântica. Se há uma sequência  $a = a_1 \cdot a_2 \cdot \dots \cdot a_n \in \mathcal{A}^n$  de índices de mensagens clássicas, o estado quântico correspondente preparado pela fonte, denominado palavra quântica, é dado pelo produto tensorial das letras quânticas associadas a cada índice*

$$\rho(a) = \rho_{a_1} \otimes \rho_{a_2} \otimes \dots \otimes \rho_{a_n}. \quad (2.90)$$

Admite-se que a personagem Alice possui uma fonte quântica com a descrição dada e que prepara estados quânticos da forma  $\rho$ . Alice entrega tais estados preparados para o

personagem Bob, o qual pode utilizar um esquema de medições POVM (*Positive Operator-Valued Measurement*) com o intuito de identificar qual mensagem correspondente foi enviada por Alice. As saídas da medição são argumentos para a função de decodificação. O decodificador deve decidir qual mensagem clássica foi enviada por Alice.

Figura 12: Modelo de um sistema de comunicações quântico em que há apenas uma fonte e um receptor.



Fonte: Elaborado pela autora.

Levando a definição da fonte quântica em questão, a mesma pode ser vista por Bob como uma matriz densidade

$$\rho = \sum_{k=1}^{\ell} p_k \rho_k. \tag{2.91}$$

A partir do que foi apresentado, é possível definir o conceito de informação acessível de uma fonte quântica.

**Definição 2.16 (Informação Acessível)** *A informação acessível de uma fonte quântica  $F$  com ensemble  $(\mathcal{S}, \mathbf{p})$  cujos estados quânticos são emitidos de acordo com uma variável aleatória  $A$  e cujo resultado das respectivas medições está relacionado a uma variável aleatória  $B$  é o máximo da informação mútua entre estas variáveis aleatórias, isto é,*

$$I_{acc}(F) = \max_{\mathcal{M}} H(A : B), \tag{2.92}$$

em que o máximo é tomado sobre todos os esquemas de medição POVM  $\mathcal{M}$  possíveis (NIELSEN; CHUANG, 2010, Seção 12.1).

Se os estados de  $\mathcal{S}$  forem todos ortogonais entre si, a fonte pode ser considerada puramente clássica, pois os estados são completamente distinguíveis no receptor. Se os estados de  $\mathcal{S}$  são puros, porém não-ortogonais, então não há medição clássica capaz de

extrair a informação completa sobre o estado da fonte. Uma terceira situação considera que os estados da fonte são não-ortogonais, mas cujas matrizes de densidade comutam. Para esta última situação, a fonte é considerada de *broadcast*, ou seja, dados dois sistemas quânticos que não são cópias da fonte, o traço parcial de ambos os sistemas resulta no estado da fonte (BENNETT; SHOR, 1998).

A entropia de uma fonte quântica é dada pelo análogo quântico da entropia de Shannon, denominada *entropia de von Neumann*. A definição da entropia de tais fontes é apresentada na Definição 2.17.

**Definição 2.17 (Entropia de uma Fonte Quântica)** *Seja uma fonte quântica  $F$  tal como apresentada na Definição 2.15. Seja  $\rho = \sum_{k=0}^{\ell} p_k \rho_k$  uma média dos estados quânticos emitidos por esta fonte. A entropia de tal fonte quântica é dada por*

$$S(F) = -\text{Tr } \rho \log \rho, \quad (2.93)$$

em que  $S$  denota a entropia de von Neumann.

Na Teoria da Informação Quântica, nenhum método geral é conhecido para o cálculo da informação acessível de uma fonte quântica. Porém, alguns limitantes para tal medidas foram desenvolvidos, a exemplo do limitante de Holevo (NIELSEN; CHUANG, 2010, Cap. 12).

**Teorema 2.7 (Limitante de Holevo)** *Suponha que Alice possua uma fonte quântica  $F$  com ensemble  $(\mathcal{S}, \mathbf{p})$  e envie para Bob letras quânticas emitidas por esta fonte. Bob realiza medições nas letras quânticas recebidas com um POVM  $\{M_i\}_{i=0}^m$ , obtendo  $B$ . O limitante de Holevo enuncia que, para qualquer esquema de medições que Bob utilize, tem-se*

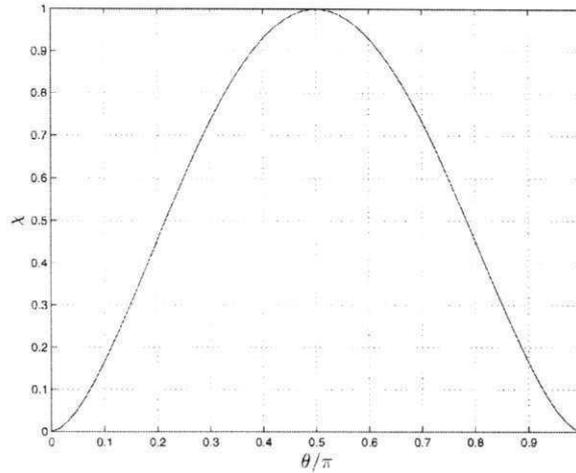
$$I_{\text{acc}}(F) \leq S(\rho) - \sum_{k=0}^{\ell} p_k S(\rho_k), \quad (2.94)$$

em que  $\rho$  é dado na Eq. (2.91).

O limitante de Holevo, frequentemente denotado por  $\chi$ , é um limitante superior para a informação acessível entre as variáveis  $A$  e  $B$  num cenário quântico. Levando em consideração a concavidade das entropias, tem-se que  $H(A : B) \leq \chi \leq H(A)$ .

**Exemplo 2.9 (Limitante de Holevo)** *Suponha que Alice possa enviar para Bob, de maneira equiprovável, dois estados quânticos  $\rho_0 = |0\rangle$  e  $\rho_1 = \cos \theta |0\rangle + \sin \theta |1\rangle$ , em que  $\theta$  é um parâmetro real. O limitante de Holevo em função do valor de  $\theta$  é mostrado na Figura 13, em que o máximo é atingido quando  $\theta = \pi/2$  e os estados  $\rho_0$  e  $\rho_1$  são ortogonais. Esta*

Figura 13: Valor da quantidade de Holevo para o exemplo em questão, exibido em função da relação  $\theta/\pi$  (NIELSEN; CHUANG, 2010, pp. 535).



Elaborada por Nielsen e Chuang (NIELSEN; CHUANG, 2010, pp. 535).

é a única situação em que Bob pode determinar exatamente qual estado foi preparado por Alice.

Levando em consideração que as letras quânticas não são estados necessariamente ortogonais entre si, em certos cenários não existe possibilidade de Bob recuperar completamente a informação enviada pela fonte quântica de Alice, independentemente do esquema de medições que venha a usar. Esta situação constitui um cenário contraintuitivo quando comparado ao caso clássico equivalente e encontra-se ilustrada no Exemplo 2.10.

**Exemplo 2.10 (Medições com Resultados Inconclusivos)** *Suponha que uma fonte quântica possa emitir dois estados  $|\psi_1\rangle = |0\rangle$  ou  $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$  de maneira equiprovável. Uma vez que  $\langle\psi_1|\psi_2\rangle \neq 0$ , não é possível determinar com total confiança qual estado foi emitido pela fonte. Porém, é possível realizar medições que conseguem distinguir tais estados em algumas ocasiões. Para tanto, faz-se uso de um POVM contendo três elementos:*

$$E_1 = \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle \langle 1|, \tag{2.95}$$

$$E_2 = \frac{\sqrt{2}}{1 + \sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \tag{2.96}$$

$$E_3 = 1 - E_1 - E_2. \tag{2.97}$$

Suponha que o estado  $|\psi_1\rangle$  tenha sido enviado. Ao realizar uma medição com o POVM  $\{E_1, E_2, E_3\}$ , a probabilidade de observar  $E_1$  é nula, pois  $\langle\psi_1|E_1|\psi_1\rangle = 0$ .

*Considerando apenas o resultado das medições, se este é  $E_1$ , é possível concluir que o estado enviado pela fonte foi  $|\psi_2\rangle$ . De maneira similar, se o resultado da medição é  $E_2$ , então é possível concluir que a fonte enviou  $|\psi_1\rangle$ . Algumas das vezes, porém,  $E_3$  irá ocorrer e, diante deste resultado, não será possível precisar qual estado foi enviado pela fonte. Isto significa que  $E_3$  gera uma medição inconclusiva. Apesar disso, dados os dois outros resultados de medição, a geração de conclusões sobre o estado originalmente enviado é feita sem erros.*

## Notas do Capítulo

Neste capítulo foi apresentada a fundamentação teórica necessária para dar suporte à compreensão dos conceitos desenvolvidos neste trabalho de tese, os quais serão apresentados nos capítulos posteriores. Esta fundamentação teórica compreendeu aspectos da Teoria da Informação, tais como a capacidade erro-zero de canais clássicos discretos e sem memória e a capacidade para envio de informação clássica sem erros por canais quânticos. Além disto, compreendeu também a teoria acerca dos subespaços e subsistemas livres de descoerência, bem como a apresentação de um método para obtenção dos mesmos. Por fim, também foram apresentados os conceitos ligados à informação acessível de fontes quânticas.

## Capítulo 3

# Capacidade Quântica de Sigilo Erro-Zero

A distribuição quântica de chaves é uma das técnicas mais consolidadas atualmente para a realização de comunicações seguras via canais quânticos (NIELSEN; CHUANG, 2010, pp. 586). Porém, embora tenham suas provas de segurança adequadamente estabelecidas (MAYERS, 2001), em cenários práticos muitos destes protocolos não se mostram adequados devido à existência de ruído no canal. Este ruído não apenas aumenta a taxa de erro no envio da mensagem, mas também pode dificultar a detecção de um espião num processo de controle de segurança (LIDAR; WHALEY, 2003).

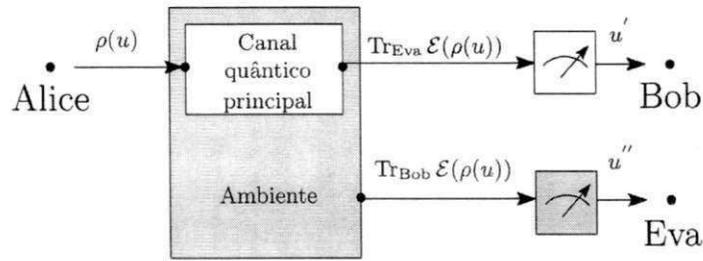
Levando em consideração esta dificuldade prática de realizar comunicações seguras em canais quânticos ruidosos, este capítulo apresenta algumas das contribuições desta tese, as quais consistem na caracterização das condições para a positividade da chamada *Capacidade Quântica de Sigilo Erro-Zero* (QZESC – *Quantum Zero-Error Secrecy Capacity*), a maior taxa que pode ser atingida em um canal ruidoso para que a comunicação ocorra de maneira segura e livre de erros de decodificação. Esta capacidade unifica conceitos da Teoria da Informação Quântica Erro-Zero, da capacidade de sigilo de canais quânticos e também dos subespaços e subsistemas livres de descoerência.

Para apresentar os resultados em questão, este capítulo está organizado como segue. O modelo de comunicações e a formalização dos conceitos e provas que caracterizam a QZESC encontram-se apresentados na Seção 3.1. A relação da QZESC com a Teoria dos Grafos é elucidada na Seção 3.2. Posteriormente, uma análise de segurança que esta abordagem de comunicações provê é apresentada na Seção 3.3. Exemplos detalhados e simulações realizadas são apresentadas na Seção 3.4. Por fim, a relação com outros trabalhos da literatura é apresentada na Seção 3.5.

### 3.1 Caracterização e Formalização

Considera-se o seguinte cenário. Dois participantes legítimos (Alice e Bob) desejam trocar mensagens clássicas entre si por um canal quântico  $\mathcal{E}$  de maneira sigilosa e livre de erros. Estas mensagens devem estar protegidas da ação de um espião (Eva), que possui acesso total ao ambiente. A caracterização deste cenário é ilustrada na Figura 14.

Figura 14: Cenário de comunicações considerado.



Fonte: Elaborada pela autora.

Este modelo de canal em que o espião possui acesso ao ambiente segue o formalismo de Cai et al. (CAI; WINTER; YEUNG, 2004) e de Devetak (DEVETAK, 2005) utilizado para caracterização dos canais *wiretap* quânticos, apresentados anteriormente na Seção 2.4. Embora em termos práticos considere-se principalmente a ação direta de um espião no canal principal e as implicações na comunicação e na aquisição não autorizada de informações (tais como nos protocolos quânticos de distribuição de chaves), o cenário considerado nesta proposição é passível de implementação e já é consolidado na literatura no estudo da privacidade quântica (SCHUMACHER; WESTMORELAND, 1998).

O canal  $\mathcal{E}$ , em particular, possui capacidade erro-zero positiva e os elementos  $\{E_a\}$ , tal que  $\mathcal{E} \equiv \{E_a\}$ , são conhecidos. A caracterização a seguir estabelece o tipo de canal quântico considerado.

**Caracterização 3.1 (Canal Quântico com Capacidade Erro-Zero Positiva)** *Seja  $\mathcal{E}$  um mapa quântico que preserva o traço representando um canal quântico ruidoso. O modelo de erros para  $\mathcal{E}$  é conhecido, sendo composto pelos elementos  $\{E_a\}$ , tal que  $\mathcal{E} \equiv \{E_a\}$ . Considera-se que  $\mathcal{E}$  possui uma capacidade erro-zero estritamente positiva,  $C^{(0)}(\mathcal{E}) > 0$ , alcançada por um par ótimo  $(\mathcal{S}, \mathcal{M})$ .*

Se houver um conjunto  $\mathcal{M}' = \{M_1, \dots, M_k\}$  de  $\mathcal{M}$  que satisfaça às condições das Eqs. (3.1) e (3.2), ou seja

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i, \quad (3.1)$$

$$M_i M_j = \delta_{i,j} M_i M_j, \quad (3.2)$$

para todo  $i, j \leq k$ , tem-se então um par  $(\mathcal{S}', \mathcal{M}')$  que também é ótimo, com  $\mathcal{S}' = \left\{ \rho_i = |s_i\rangle \langle s_i|_{i=1}^k, \rho_i \in M_i \mathcal{H} \text{ e } [\rho_i, M_i E_a M_i] = 0 = [\rho_i, M_i E_a^\dagger M_i] \right\}$ .

O par  $(\mathcal{S}', \mathcal{M}')$  foi obtido de acordo com o método descrito na Seção 2.3.1, definindo um subespaço livre de descoerência  $\tilde{\mathcal{H}}$ , que pode ser utilizado para codificar informações de maneira que estas estejam protegidas de um espião, como será provado nos seguintes lemas.

**Lema 3.1 (Par Ótimo  $(\mathcal{S}', \mathcal{M}')$  Define um QEAC)** *O par ótimo  $(\mathcal{S}', \mathcal{M}')$  é um código quântico de prevenção de erros (vide Seção 2.3).*

**Prova** *Para provar este lema é necessário mostrar que a partir do par  $(\mathcal{S}', \mathcal{M}')$  é possível caracterizar os elementos de um código deste tipo.*

Seja  $\mathcal{U} = \{u_1, \dots, u_k\}$  um conjunto de mensagens clássicas biunivocamente associadas a estados de  $\mathcal{S}'$ . Isto define um conjunto de palavras código  $\tilde{\mathcal{P}}(\mathcal{U}) = \{\tilde{\rho}(u_i) = \rho_i\} \equiv \mathcal{S}'$  de comprimento  $n$ . A decodificação é realizada por um conjunto de operadores positivos  $M_i \in \mathcal{M}'$ ,  $i \in 1, \dots, |\mathcal{U}|$ , com  $\sum_{i=1}^{|\mathcal{U}|} M_i \leq \mathbb{1}$ . Cada  $M_i$  é unicamente associado a uma mensagem  $u_i \in \mathcal{U}$ . Então, o par  $(\tilde{\mathcal{P}}(\mathcal{U}), \mathcal{M}')$ , que é equivalente a  $(\mathcal{S}', \mathcal{M}')$ , define um código quântico de prevenção de erros de comprimento  $n$  com taxa  $\frac{1}{n} \log |\mathcal{U}|$ .

Um código quântico de prevenção de erros só existe se houver um DFS no espaço de Hilbert definido para o canal  $\mathcal{E}$  considerado na Caracterização 3.1. Isto implica que o canal  $\mathcal{E}$  está sujeito à descoerência coletiva e é regido pelo hamiltoniano apresentado na Eq. (2.42). Vale salientar que, em virtude da descoerência coletiva, os estados que se encontram no DFS não sofrem a ação do componente  $\mathbb{H}_{SE}$  de interação entre sistema e ambiente do hamiltoniano.

Utilizando o código em questão, se Alice quer enviar uma mensagem  $u$  para Bob, ela irá codificá-la em  $\tilde{\rho}(u)$ . Ao enviar este estado pelo canal  $\mathcal{E}$ , o estado enviado irá interagir com o ambiente, que é assumido iniciar em um estado puro  $|0_E\rangle \langle 0_E|$ . Devido à existência de descoerência, Bob e Eva irão receber, respectivamente, os seguintes estados:

$$\rho_{\text{Bob}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Eva}} [\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|)], \quad (3.3)$$

$$\rho_{\text{Eva}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Bob}} [\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|)]. \quad (3.4)$$

Uma vez que Alice utilizou um QEAC, então a simetria dinâmica existente protegeu a informação da interação com o ambiente. Isto significa que a evolução conjunta entre sistema e ambiente aconteceu de maneira desacoplada. Assim, o estado  $\rho_{\text{Bob}}(\tilde{\rho}(u))$  é dado por:

$$\rho_{\text{Bob}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Eva}} [\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|)] \quad (3.5)$$

$$= \text{Tr}_{\text{Eva}} \left[ \sum_a E_a (\tilde{\rho}(u) \otimes |0_E\rangle \langle 0_E|) E_a^\dagger \right] \quad (3.6)$$

$$= \text{Tr}_{\text{Eva}} [\tilde{\rho}(u) \otimes \rho_E] \quad (3.7)$$

$$= \tilde{\rho}(u), \quad (3.8)$$

em que o resultado da Eq. (3.7) acontece devido à invariância de um estado do DFS perante os operadores OSR.

Levando em conta o hamiltoniano do sistema quântico dado na Eq. (2.42) e o fato do sistema de interesse e o ambiente não terem interagido, então é possível garantir que o ambiente sofreu apenas a ação de  $\mathbb{H}_E$ , o qual indica uma evolução unitária restrita ao ambiente. Isto significa que  $\rho_{\text{Eva}}(\tilde{\rho}(u)) = \rho_E$  na Eq. (3.4) é um *estado puro*.

Prosseguindo com o desenvolvimento, é possível enunciar e provar o lema a seguir.

**Lema 3.2 (Par Ótimo  $(\mathcal{S}', \mathcal{M}')$  Define Código Wiretap)** *O par  $(\mathcal{S}', \mathcal{M}')$  define um código wiretap com parâmetros  $(n, |\mathcal{U}|, 0, 0)$ .*

**Prova** *Na Definição 2.13, de um código wiretap quântico tal como proposto por Cai et al. (CAI; WINTER; YEUNG, 2004), considera-se que para haver sigilo duas condições precisam ser satisfeitas: (i) deve haver uma baixa probabilidade média de erro na decodificação; e (ii) a informação acessível ao espião deve ser arbitrariamente pequena. A prova deste lema consiste em mostrar que estes dois requisitos são satisfeitos.*

*Em relação ao primeiro requisito, uma vez que o par  $(\mathcal{S}', \mathcal{M}')$  é ótimo, então ele permite que o canal  $\mathcal{E}$  atinja  $C^{(0)}(\mathcal{E})$ , o que implica que a comunicação é realizada sem erros de decodificação se a comunicação ocorrer abaixo desta taxa, o que implica em  $\lambda = 0$ . Portanto, o primeiro requisito é satisfeito.*

*O segundo requisito consiste em analisar a informação média acessível por Eva, que é dada da seguinte forma:*

$$S \left( \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} \text{Tr}_{\text{Bob}} \mathcal{E}(\tilde{\rho}(u)) \right) - \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} S(\text{Tr}_{\text{Bob}} \mathcal{E}(\tilde{\rho}(u))) \leq \mu, \quad (3.9)$$

em que  $\mu$  é um número arbitrariamente pequeno. Para provar este requisito, ao invés de calcular a informação acessível média diretamente, será utilizado um limitante para esta medida, a quantidade de Holevo, cuja definição é apresentada a seguir:

$$\chi^{Eva} = S(\rho_{Eva}(\tilde{\rho}(u))) - \sum_u p_u S(\rho_{Eva,u}\tilde{\rho}(u)). \quad (3.10)$$

Em virtude da utilização de estados de um DFS para codificação, é possível afirmar que não houve interação entre sistema e ambiente. Nesse caso, a evolução do ambiente foi governada apenas pelo hamiltoniano  $\mathbb{H}_E$ , o que indica uma evolução unitária dentro do ambiente. Isto significa que o estado final do ambiente é puro. Portanto:

$$\chi^{Eva} = S(\rho_{Eva}(\tilde{\rho}(u))) - \sum_u p_u S(\rho_{Eva,u}\tilde{\rho}(u)) \quad (3.11)$$

$$= S(\rho_E) - \sum_u p_u S(\rho_{Eva,u}\tilde{\rho}(u)) \quad (3.12)$$

$$= 0 - \sum_u p_u S(\rho_{Eva,u}\tilde{\rho}(u)). \quad (3.13)$$

Sabe-se que  $\chi^{Eva} \geq 0$ ,  $S(\rho) \geq 0$  para qualquer  $\rho$ , e que  $p_u \geq 0$  para todo  $u$ . Então, para assegurar a positividade, este é o caso em que o termo remanescente é igual a zero, implicando em  $\chi^{Eva} = 0$ . Dado que a quantidade de Holevo é um limitante superior para a informação acessível, tem-se que a Eq. (3.9) é igual a zero. Isto conclui a prova.

A partir dos Lemas 3.1 e 3.2, é possível afirmar que ao codificar informações em um DFS identificado no espaço de Hilbert de um canal quântico  $\mathcal{E}$ , tem-se que esta comunicação é realizada com segurança incondicional (GUEDES; DE ASSIS, 2013b).

Embora um par ótimo  $(\mathcal{S}', \mathcal{M}')$  defina um código *wiretap* com parâmetros  $(n, |\mathcal{U}|, 0, 0)$ , nem sempre é possível extrair um par  $(\mathcal{S}', \mathcal{M}')$  de um par ótimo  $(\mathcal{S}, \mathcal{M})$ . De acordo com o Lema 3.1, tem-se que este par é equivalente a identificar um DFS  $\tilde{\mathcal{H}}$ . Porém, considerando cenários práticos, tem-se que pode existir um DFS nestas condições, ainda que com dimensão menor que a cardinalidade do conjunto de mensagens, isto é, com  $\dim(\tilde{\mathcal{H}}) < |\mathcal{U}|$ . Para estas situações, utiliza-se um código  $(n, \dim(\tilde{\mathcal{H}}), 0, 0)$  que permite a comunicação livre de erros e sem vazamento de informação, embora numa taxa menor que a do código obtido nas condições mencionadas anteriormente. Levando isto em conta e também os resultados dos dois lemas provados anteriormente, tem-se que é possível caracterizar um novo tipo de capacidade para canais quânticos, cuja definição é dada a seguir.

**Definição 3.1 (Capacidade Quântica de Sigilo Erro-Zero)** A capacidade quântica de sigilo erro-zero de um canal quântico  $\mathcal{E}$ , como apresentado na Caracterização 3.1, é o maior número real  $C_S^{(0)}(\mathcal{E})$  tal que, para todo  $\epsilon > 0$  e  $n$  suficientemente grande, existe um código wiretap  $(n, |\mathcal{U}|, 0, 0)$  que satisfaz

$$C_S^{(0)}(\mathcal{E}) \leq \frac{1}{n} \log |\mathcal{U}| + \epsilon. \quad (3.14)$$

Duas características particulares desta capacidade é que não há erros de decodificação nem vazamento de informação para o espião. Isto contrasta com a capacidade de sigilo dos canais quânticos, em que erros de decodificação entre os participantes legítimos diminuem no limite assintótico de muitos usos do canal.

O teorema a seguir visa quantificar a capacidade quântica de sigilo erro-zero.

**Teorema 3.1 (Capacidade Quântica de Sigilo Erro-Zero)** A capacidade quântica de sigilo erro-zero de um canal quântico  $\mathcal{E}$  como apresentado na Caracterização 3.1 é dada por

$$C_S^{(0)}(\mathcal{E}) \equiv \min \{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\}, \quad (3.15)$$

$$\equiv \min \left\{ \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n, \max_{\{P\}} \chi^{Bob} \right\}. \quad (3.16)$$

em que  $n$  é o comprimento do código; o máximo é tomado sobre todas as distribuições de probabilidade  $P$  sobre  $\mathcal{U}$ ; e  $\chi^{Bob}$  denota um limitante superior para a informação acessível de Bob, a qual possui expressão dada por

$$\chi^{Bob} = S \left( \sum_u p_u \rho_{Bob}(\tilde{\rho}(u)) \right) - \sum_u p_u S(\rho_{Bob}(\tilde{\rho}(u))), \quad (3.17)$$

em que  $p_u$  é a probabilidade a priori do símbolo  $u \in \mathcal{U}$ .

**Prova** Esta prova leva em consideração alguns fatos sobre as capacidades do canal quântico  $\mathcal{E}$ . Seja  $C_{1,\infty}(\mathcal{E})$  a capacidade clássica ordinária de  $\mathcal{E}$  como definida pelo teorema de Holevo-Shumacher-Westmoreland (HOLEVO, 1998; SCHUMACHER; WESTMORELAND, 1997). Seja  $C_S(\mathcal{E})$  a capacidade de sigilo de  $\mathcal{E}$  (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005). E, por fim, seja  $C^{(0)}(\mathcal{E})$  a capacidade erro-zero de  $\mathcal{E}$  (MEDEIROS, 2008). Tem-se que  $C_S(\mathcal{E}) \leq C_{1,\infty}(\mathcal{E})$ , como também  $C^{(0)}(\mathcal{E}) \leq C_{1,\infty}(\mathcal{E})$ .

Considerando  $|\mathcal{U}| = \dim(\tilde{\mathcal{H}})$ , um código com parâmetros  $(n, |\mathcal{U}|, 0, 0)$  é simultaneamente um código livre de erros e também um código wiretap. Por definição, sabe-se que

a capacidade erro-zero está relacionada ao maior número de mensagens que são distinguíveis na saída do canal. Como cada palavra do alfabeto foi associada a um estado de um DFS, de acordo com o Lema 3.1, então tem-se que:

$$C^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n \quad (3.18)$$

em que  $n$  é o comprimento do código.

No caso de ser wiretap, devido ao uso do DFS, tem-se que  $C_S(\mathcal{E}) = \chi^{Bob} - \chi^{Eva}$ . Como consequência do Lema 3.2, tem-se que

$$C_S^{(0)}(\mathcal{E}) \geq \max_{\{P\}} [\chi^{Bob} - \chi^{Eva}] \quad (3.19)$$

$$\geq \max_{\{P\}} [\chi^{Bob} - 0] \quad (3.20)$$

$$= \max_{\{P\}} \chi^{Bob}, \quad (3.21)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade  $P$  sobre  $\mathcal{U}$  na expressão da quantidade de Holevo de Bob dada na Eq. (3.17). A igualdade advém do teorema HSW.

Existem, porém, duas situações a considerar:

1. Existe um par ótimo  $(\mathcal{S}', \mathcal{M}')$  derivado de  $(\mathcal{S}, \mathcal{M})$  de acordo com as Eqs. (3.1) e (3.2), então  $|\mathcal{U}| = \dim(\tilde{\mathcal{H}})$  e  $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$ ;
2. Existe um DFS  $\tilde{\mathcal{H}}$  no canal, o qual não é obtido diretamente a partir do código livre de erros. Nesta situação,  $C_S(\mathcal{E}) < C^{(0)}(\mathcal{E})$ , ou seja, só há comunicação livre de erros e de vazamento se  $C_S^{(0)}(\mathcal{E}) = \min \{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\}$ .

Assim, a expressão final para a capacidade quântica de sigilo erro-zero pode ser apresentada em termos da relação entre a capacidade erro-zero e a capacidade de sigilo, isto é

$$C_S^{(0)}(\mathcal{E}) = \min \{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\} \quad (3.22)$$

em que  $C^{(0)}(\mathcal{E})$  e  $C_S(\mathcal{E})$  são as capacidades erro-zero e de sigilo do canal  $\mathcal{E}$ , respectivamente. Isto conclui a prova.

Nos casos em que, para um canal quântico  $\mathcal{E}$ ,  $C_S^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}})^n$ , tem-se que a capacidade quântica de sigilo erro-zero possui caracterização de letra isolada,

o que contrasta com a capacidade de sigilo ordinária que não a possui (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005). Além disso, de acordo com um resultado desenvolvido por Medeiros et al. (MEDEIROS et al., 2006a), a capacidade erro-zero pode ser alcançada se o conjunto de estados de entrada for composto apenas de estados puros. Isto também se mostra adequado com a definição feita neste trabalho em relação a  $S'$ , o que significa que existem casos em que a capacidade quântica de sigilo erro-zero também pode ser alcançada apenas com estados puros.

Em termos de segurança, os resultados apresentados nesta seção estão de acordo com o que foi estabelecido por Schumacher e Westmoreland (SCHUMACHER; WESTMORELAND, 1998), os quais afirmam que a habilidade de um canal quântico para enviar informação privada é pelo menos tão grande quanto a sua habilidade de enviar informação coerente. No caso em questão, como a informação enviada pode ser recuperada totalmente livre de erros, então a habilidade para enviar informação privada é maximizada.

Ao considerar a dificuldade em implementar canais quânticos totalmente livres de erro (LIDAR; WHALEY, 2003), a capacidade quântica de sigilo erro-zero permite que comunicações seguras e livres de erro sejam realizadas por canais quânticos ruidosos que atendam determinadas condições. Isto é interessante do ponto de vista prático, pois permite a utilização do esquema de comunicações proposto em canais já existentes, tais como os que possuem ruído coletivo (JAEGER; SERGIENKO, 2008; XIA et al., 2010; DORNER; KLEIN; JAKSCH, 2008) e os que possuem capacidade erro-zero positiva (GYONGYOSI; IMRE, 2012), incluindo também uma implementação de um canal quântico por Xue (XUE, 2008), o qual tem seu uso voltado para longas distâncias.

Embora a capacidade quântica de sigilo erro-zero tenha sido adequadamente definida, ela é nula para vários tipos de canais quânticos. Pode-se, inclusive, afirmar que esta emerge apenas quando o canal possui capacidade quântica erro-zero positiva e sofre os efeitos da descoerência coletiva, permitindo a existência de subespaços livres de descoerência. Apesar disso, a identificação de tal capacidade amplia os conhecimentos sobre as “habilidades” dos canais quânticos, permitindo um uso mais apropriado dos mesmos em determinadas situações.

## 3.2 Relação com a Teoria dos Grafos

Nesta seção será explicitada a relação entre a QZESC e a Teoria dos Grafos. Infelizmente, esta relação não é tão geral como para os canais quânticos erro-zero, conforme apresentado na Seção 2.2.1. Esta relação só é útil para descrever canais quânticos que atendem à primeira situação descrita na prova do Teorema 3.1.

Se existe um conjunto não-vazio  $\mathcal{M}'$  obtido a partir de  $\mathcal{M}$  de acordo com as Eqs. (3.1) e (3.2), então o par  $(\mathcal{S}', \mathcal{M}')$  caracteriza um DFS  $\tilde{\mathcal{H}}$  do espaço de Hilbert de entrada  $\mathcal{H}$ , de acordo com o método descrito por Choi e Kribs (CHOI; KRIBS, 2006) apresentado na Seção 2.3.1.

Levando em conta as considerações mencionadas, é possível construir um grafo característico para os canais quânticos com capacidade quântica de sigilo erro-zero positiva de maneira similar aos grafos característicos para canais quânticos com capacidade erro-zero, apresentados na Definição 2.9. A diferença reside no conjunto de vértices.

Seja  $\mathcal{E}$  um canal quântico com capacidade quântica de sigilo erro-zero positiva atendendo à primeira situação do Teorema 3.1. O grafo característico de  $\mathcal{E}$ , denotado por  $\tilde{\mathcal{G}}(\mathcal{E}) = \langle V, E \rangle$  é caracterizado como segue:

1. O conjunto de vértices  $V$  é composto pelos elementos em  $\tilde{\mathcal{H}}$ , os quais serão referenciados pelos índices das mensagens correspondentes, isto é,  $V = \{1, 2, \dots, \dim(\tilde{\mathcal{H}})\}$ ;
2. O conjunto de arestas  $E$  conecta dois vértices caso eles sejam não-adjacentes na saída do canal (ver adjacência entre estados quânticos na Definição 2.7).

O  $n$ -ésimo produto de  $\tilde{\mathcal{G}}(\mathcal{E})$ , denotado por  $\tilde{\mathcal{G}}^n(\mathcal{E})$ , possui  $V = V^n$  (produtos tensoriais de comprimento  $n$  de estados quânticos de  $\tilde{\mathcal{H}}$ ) e o conjunto de arestas  $E$  como sendo composto pelos estados quânticos  $n$ -dimensionais distinguíveis na saída de  $\mathcal{E}$ .

Levando em consideração o grafo em questão, uma vez que os elementos de um DFS  $\tilde{\mathcal{H}}$  são distinguíveis dois a dois na saída do canal, então o grafo resultante é um *grafo completo*. Assim, o maior número de mensagens que podem ser transmitidas sem erro pelo canal quântico  $\mathcal{E}$  é dado pelo número de clique de  $\tilde{\mathcal{G}}^n(\mathcal{E})$ .

Assim, a capacidade quântica de sigilo erro-zero para um canal quântico  $\mathcal{E}$  que atende à situação 1 do Teorema 3.1 é dada por:

$$C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \omega(\tilde{\mathcal{G}}^n(\mathcal{E})). \quad (3.23)$$

Dado um número inteiro e um grafo, encontrar um clique do tamanho do inteiro inicialmente fornecido é um problema  $\mathcal{NP}$ -Completo. Porém, algumas características do erro-zero e dos DFS podem ser levadas em consideração na determinação de  $C_S^{(0)}(\mathcal{E})$ , em particular. Uma vez que o grafo produzido a partir de  $\tilde{\mathcal{H}}$  é completo, tem-se que o número de clique de  $\tilde{\mathcal{G}}(\mathcal{E})$  é igual a  $\dim(\tilde{\mathcal{H}})$ , o que leva à expressão já conhecida dada na Eq. (3.18). Tal relação entre o número de clique e a cardinalidade do conjunto de arestas

no grafo correspondente não é observada em códigos livres de erro ordinários. Esta é uma particularidade devido ao uso dos DFS.

Quando um canal quântico  $\mathcal{E}$  satisfaz às condições para sua representação em termos de grafos, tem-se que sua QZESC possui *caracterização de letra isolada*, isto é, pode ser facilmente computada a partir da quantidade de elementos existentes no DFS  $\tilde{\mathcal{H}}$ . Com isto, tem-se um contraste significativo com as capacidades erro-zero e ordinária de um canal quântico, as quais não se sabe se são computáveis em tempo polinomial (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005; DUAN; SEVERINI; WINTER, 2013; HOLEVO, 1998; SCHUMACHER; WESTMORELAND, 1997)

### 3.3 Análise de Segurança

Para analisar a segurança deste esquema de comunicações proposto, inicialmente é necessário considerar que há três tipos de sigilo diferentes, com as seguintes caracterizações:

1. **Sigilo Forte (*Strong secrecy*)**. Requer que a informação total transferida para o espião tenda a zero no limite assintótico do número de comunicações;
2. **Sigilo Fraco (*Weak Secrecy*)**. Requer que a informação transferida por símbolo tenda a zero no limite assintótico do número de comunicações (SUBRAMANIAN et al., 2010).
3. **Sigilo Absoluto (*Perfect Secrecy*)**. Requer que a informação total transferida para o espião seja zero (SHANNON, 1949).

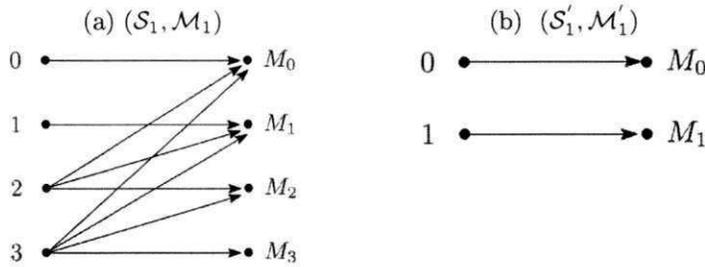
De acordo com o modelo proposto, quando Alice codifica uma mensagem utilizando o código  $(n, |\mathcal{U}|, 0, 0)$  e a envia para Bob, tem-se que o conjunto de estados utilizados pertence a um DFS e, em virtude disto, não interage com o ambiente. Como a espiã Eva tem acesso apenas ao ambiente, o estado deste permanece puro ao longo da interação, o que significa que a informação acessível de Eva é igual a zero, obtida via  $\chi^{\text{Eva}} = 0$  como mostrado na prova do Lema 3.2. Tem-se, portanto, que a incerteza de Eva sobre a mensagem transmitida é mantida, ainda que esta tenha observado por completo o estado do ambiente. Conclui-se, portanto, que o esquema de comunicações proposto possui sigilo absoluto.

### 3.4 Exemplos

Esta seção contempla alguns exemplos detalhados relacionados aos conceitos da QZESC.

**Exemplo 3.1 (QZESC Estritamente Positiva)** *Inicialmente, é assumido que um canal quântico  $\mathcal{E}_1$  possui capacidade erro-zero positiva alcançada pelo par ótimo  $(\mathcal{S}_1, \mathcal{M}_1)$ , como mostrado na Figura 15a. Ao seguir os procedimentos descritos na Seção 3.1, um par  $(\mathcal{S}'_1, \mathcal{M}'_1)$  pode ser derivado, como mostrado na Figura 15b.*

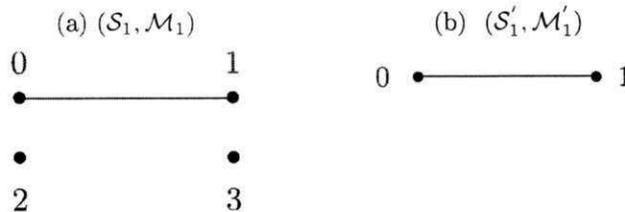
Figura 15: Representação das transições do canal  $\mathcal{E}_1$  para os estados de entrada dos pares ótimos  $(\mathcal{S}_1, \mathcal{M}_1)$  e  $(\mathcal{S}'_1, \mathcal{M}'_1)$ .



Fonte: Elaborada pela autora.

Os grafos característicos de  $(\mathcal{S}_1, \mathcal{M}_1)$  e  $(\mathcal{S}'_1, \mathcal{M}'_1)$  encontram-se ilustrados nas Figuras 16a e 16b, respectivamente.

Figura 16: Grafos característicos para  $(\mathcal{S}_1, \mathcal{M}_1)$  e  $(\mathcal{S}'_1, \mathcal{M}'_1)$ .



Fonte: Elaborada pela autora.

De acordo com os grafos característicos, o maior número de clique é 2, em ambos os casos obtidos pelos pares  $(0, 1)$ . Isto leva a uma capacidade quântica erro-zero igual a

$$C^{(0)}(\mathcal{E}_1) = \sup_{\tilde{\mathcal{H}}_1} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}}_1)^n \tag{3.24}$$

$$= \log 2 \tag{3.25}$$

$$= 1 \text{ bit por símbolo por uso do canal.} \tag{3.26}$$

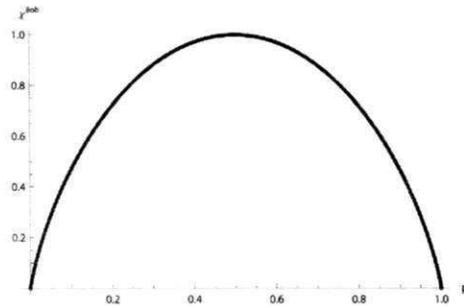
Vale salientar que os estados quânticos no DFS  $\tilde{\mathcal{H}}_1$  são aqueles definidos por  $\mathcal{S}'_1$ . Para obter a capacidade de sigilo do requerido canal, foi utilizado o software Mathematica<sup>®</sup> na tentativa de obter um valor máximo para  $\chi^{Bob}$  nas Eqs. (3.27)-(3.28).

$$C_S(\mathcal{E}_1) = \chi^{Bob} \tag{3.27}$$

$$= \max_{\{P\}} S(p_0 \cdot \rho_0 + p_1 \cdot \rho_1). \tag{3.28}$$

Para alcançar o objetivo considerado, foi realizada uma busca exaustiva entre 30000 pares de  $(p_0, p_1)$  levando em consideração a restrição  $p_0 + p_1 = 1$ . Como resultado, foi obtido o gráfico da Figura 17. Como pode ser visto, o valor máximo da quantidade de Holevo de Bob é igual a 1.

Figura 17: Resultados da simulação realizada na tentativa de maximizar o valor de  $\chi^{Bob}$  nas Eqs. (3.27)-(3.28) sobre os pares  $(p_0, p_1)$ .



Fonte: Elaborada pela autora.

Desta maneira, para o canal  $\mathcal{E}_1$ , tem-se que a capacidade quântica de sigilo erro-zero é dada por

$$C_S^{(0)}(\mathcal{E}_1) = \min \{C^{(0)}(\mathcal{E}_1), C_S(\mathcal{E}_1)\} \tag{3.29}$$

$$= \min \{1, 1\} \tag{3.30}$$

$$= 1 \text{ bit por símbolo por uso do canal.} \tag{3.31}$$

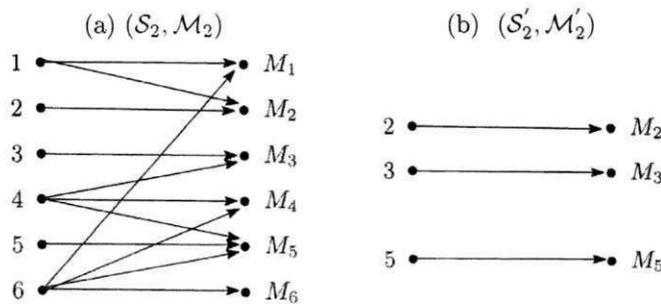
É possível concluir, por meio do primeiro exemplo, que existem canais quânticos  $\mathcal{E}$  cuja capacidade quântica de sigilo erro-zero é estritamente positiva, i.e. ,  $C_S^{(0)}(\mathcal{E}) > 0$ .

**Exemplo 3.2 (QZESC é Não-Trivial)** No segundo exemplo é considerado um canal quântico  $\mathcal{E}_2$  que possui capacidade erro-zero positiva alcançada pelo par ótimo  $(\mathcal{S}_2, \mathcal{M}_2)$  em que  $\mathcal{S}_2 = \{\rho_1, \dots, \rho_6\}$  e  $\mathcal{M}_2 = \{M_i = |\rho_i\rangle\langle\rho_i|\}_{i=1}^6$ . O modelo de erros para as entradas

do canal é ilustrado na Figura 18a. Uma vez que o interesse reside nas relações de adjacências, as probabilidades de transição foram omitidas.

A partir do par  $(\mathcal{S}_2, \mathcal{M}_2)$  e seguindo os procedimentos indicados na Seção 3.1, é possível derivar um par ótimo  $(\mathcal{S}'_2, \mathcal{M}'_2)$  em que  $\mathcal{S}'_2 = \{\rho_2, \rho_3, \rho_5\}$  e  $\mathcal{M}'_2 = \{M_2, M_3, M_5\}$ . A relação entre os estados de entrada de  $\mathcal{S}'_2$  e a saída do canal  $\mathcal{E}_2$  é ilustrada na Figura 18b.

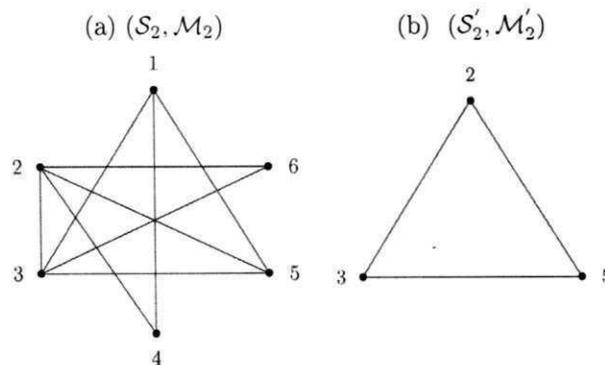
Figura 18: Representação das transições provocadas pelo canal  $\mathcal{E}_2$  sobre as entradas dos pares ótimos  $(\mathcal{S}_2, \mathcal{M}_2)$  e  $(\mathcal{S}'_2, \mathcal{M}'_2)$ .



Fonte: Elaborada pela autora.

Os grafos característicos de  $(\mathcal{S}_2, \mathcal{M}_2)$  e  $(\mathcal{S}'_2, \mathcal{M}'_2)$  encontram-se ilustrados nas Figuras 19a e 19b, respectivamente. O número de clique  $\omega(\tilde{\mathcal{G}}(\mathcal{E}_2))$  é igual a 3 e pode ser obtido a partir dos vértices  $(2, 3, 5)$ ,  $(1, 3, 5)$  ou também  $(2, 3, 6)$  considerando o grafo da Figura 19a. Por outro lado, o número de clique obtido a partir do grafo da Figura 19b é também igual a 3, mas pode ser obtido diretamente a partir dos vértices  $(2, 3, 5)$ .

Figura 19: Grafos característicos de  $(\mathcal{S}_2, \mathcal{M}_2)$  e  $(\mathcal{S}'_2, \mathcal{M}'_2)$ .



Fonte: Elaborada pela autora.

A capacidade quântica erro-zero de  $\mathcal{E}_2$  considerando o par  $(\mathcal{S}'_2, \mathcal{M}'_2)$  é igual a

$$C^{(0)}(\mathcal{E}_2) = \sup_{\tilde{\mathcal{H}}_2} \sup_n \frac{1}{n} \log \dim(\tilde{\mathcal{H}}_2)^n \quad (3.32)$$

$$= \log 3 \quad (3.33)$$

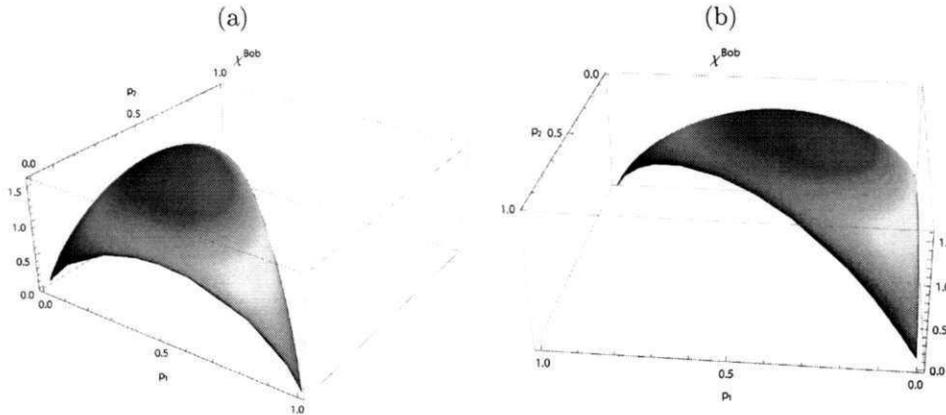
$$\approx 1,5849 \text{ bits por símbolo por uso do canal.} \quad (3.34)$$

Para obter  $C_S(\mathcal{E}_2)$ , ou seja, a quantidade de Holevo de Bob mostrada na Eq. (3.35), também foi utilizado o software Mathematica<sup>®</sup> na tentativa de maximizar o valor desta quantidade sobre as triplas  $(p_1, p_2, p_3)$  sob a restrição de que  $p_1 + p_2 + p_3 = 1$ .

$$C_S(\mathcal{E}_2) = \chi^{Bob} = \max_{\{P\}} S(p_1 \cdot \rho_2 + p_2 \cdot \rho_3 + p_3 \cdot \rho_5) \quad (3.35)$$

A busca exaustiva realizada considerou 20.000 triplas válidas de  $(p_1, p_2, p_3)$ . Os resultados obtidos estão apresentados na Figura 20, a qual mostra o gráfico obtido segundo duas perspectivas diferentes. De acordo com os resultados observados, o maior valor de  $\chi^{Bob}$  obtido foi 1,5849 bits por símbolo por uso do canal.

Figura 20: Duas diferentes perspectivas para o gráfico obtido da busca exaustiva sobre as triplas  $(p_1, p_2, p_3)$  na tentativa de maximizar a Eq. (3.35)



Fonte: Elaborada pela autora.

Desta maneira, tem-se que a capacidade quântica de sigilo erro-zero do canal  $\mathcal{E}_2$  é

$$C_S^{(0)}(\mathcal{E}_2) = \min \{C^{(0)}(\mathcal{E}_2), C_S(\mathcal{E}_2)\} \quad (3.36)$$

$$= \min \{1,5849, 1,5849\} \quad (3.37)$$

$$= 1,5849 \text{ bits por símbolo por uso do canal.} \quad (3.38)$$

Desta maneira, é possível concluir, por meio do segundo exemplo, que existem canais quânticos  $\mathcal{E}$  cuja capacidade quântica erro-zero é não-trivial, ou seja,  $C_S^{(0)}(\mathcal{E}) > 1$ . O canal quântico de decaimento coletivo de amplitude (BACON, 2001) possui capacidade QZESC igual à de  $\mathcal{E}_2$ , sendo, portanto, um exemplo prático da não-trivialidade desta capacidade.

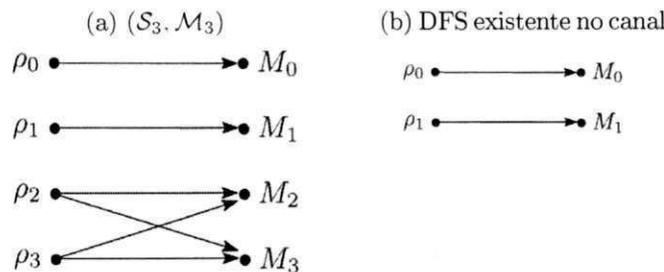
A igualdade verificada entre os resultados da capacidade erro-zero e da capacidade de sigilo do canal quântico  $\mathcal{E}_2$  neste exemplo é esperada. Isto acontece porque é possível derivar um par ótimo  $(\mathcal{S}'_2, \mathcal{M}'_2)$  a partir de  $(\mathcal{S}_2, \mathcal{M}_2)$ , ou seja, a obtenção da capacidade quântica de sigilo erro-zero do canal  $\mathcal{E}_2$  atende à primeira situação do Teorema 3.1.

**Exemplo 3.3 (Situação 2 do Teorema 3.1)** Nos exemplos mostrados anteriormente, tem-se que  $C^{(0)}(\mathcal{E}) = C_S(\mathcal{E})$ , ilustrando a primeira situação considerada na prova do Teorema 3.1. O terceiro exemplo considera a exemplificação da segunda situação descrita.

Tem-se um canal  $\mathcal{E}_3$  cujo modelo de erros é composto por quatro elementos:  $E_0 = |0\rangle\langle 0|$ ,  $E_1 = |1\rangle\langle 1|$ ,  $E_2 = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 2|$ , e  $E_3 = \frac{1}{2}|3\rangle\langle 3| + \frac{1}{2}|2\rangle\langle 3|$ , ou seja,  $\mathcal{E}_3 \equiv \{E_i\}_{i=0}^3$ . Tem-se que  $\mathcal{S}_3 = \{\rho_i = |i\rangle\langle i|, i = 0, \dots, 3\}$ . A atuação do canal  $\mathcal{E}$  sobre  $(\mathcal{S}_3, \mathcal{M}_3)$  é ilustrada na Figura 21a.

Ao considerar o canal  $\mathcal{E}_3$ , é possível constatar que sua capacidade quântica erro-zero é igual a  $C^{(0)}(\mathcal{E}_3) = \log 3$  bits por símbolo por uso do canal, considerando três mensagens clássicas associadas à entrada do canal da seguinte forma  $0 \mapsto \rho_0$ ,  $1 \mapsto \rho_1$ ,  $2 \mapsto \rho_2$  e  $2 \mapsto \rho_3$ . Porém, na tentativa de obter a capacidade quântica de sigilo de  $\mathcal{E}_3$  constata-se que não é possível obter um par  $(\mathcal{S}'_3, \mathcal{M}'_3)$  também ótimo, pois as transições que fazem com que  $\mathcal{E}_3(\rho_2) = \rho_3$  e  $\mathcal{E}_3(\rho_3) = \rho_2$  realizem uma interação com o ambiente. Tais transições culminam com o vazamento de informação para o ambiente, o que é indesejado neste cenário. Apesar disso, este canal possui um DFS com 2 estados, sendo eles  $\rho_0$  e  $\rho_1$  ilustrados na Figura 21b.

Figura 21: Representação da atuação do canal  $\mathcal{E}_3$  sob as entradas do par ótimo  $(\mathcal{S}_3, \mathcal{M}_3)$  e do DFS existente.



Fonte: Elaborada pela autora.

Desta maneira, a capacidade quântica de sigilo erro-zero de  $\mathcal{E}_3$  é igual a

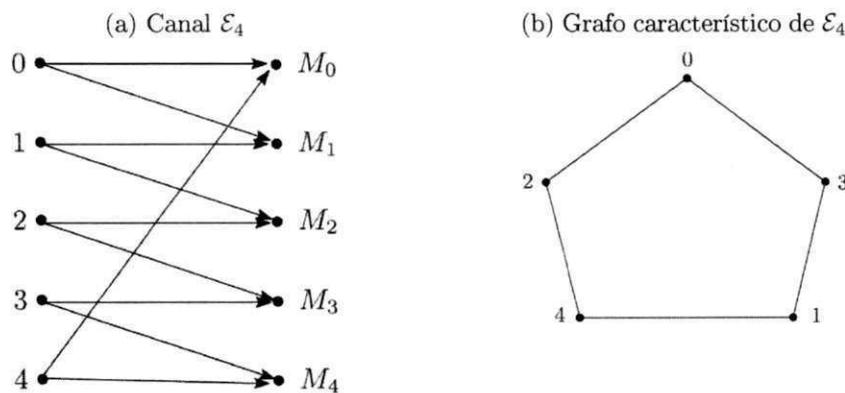
$$C_S^0(\mathcal{E}_3) = \min \{C^{(0)}(\mathcal{E}_3), C_S(\mathcal{E}_3)\} \tag{3.39}$$

$$= \min \{\log 3, \log 2\} \tag{3.40}$$

$$= 1 \text{ bit por símbolo por uso do canal.} \tag{3.41}$$

**Exemplo 3.4 (Canal Quântico com QZESC Igual a Zero)** Apesar dos exemplos anteriores mostrarem situações em que  $C_S^{(0)}(\mathcal{E}) \neq 0$ , nem sempre isso acontece. Para o canal quântico  $\mathcal{E}_4$  ilustrado na Figura 22a, cujo grafo característico é mostrado na Figura 22b, tem-se que  $C^{(0)}(\mathcal{E})$  é alcançada pelo par ótimo  $(\mathcal{S}_4, \mathcal{M}_4)$ , com  $\mathcal{S}_4 = \{ |00\rangle, |12\rangle, |24\rangle, |31\rangle, |43\rangle \}$  e  $\mathcal{M}_4 = \{M_{0,0}, M_{1,2}, M_{2,4}, M_{3,1}, M_{4,3}\}$ , em que  $\sum_{M \in \mathcal{M}_4} M \leq \mathbb{1}$ . Encontrar a capacidade erro-zero de  $\mathcal{E}_4$  considerando o canal clássico correspondente foi um problema proposto por Shannon (SHANNON, 1956) e resolvido 20 anos posteriormente por Lovász (LOVÁSZ, 1979). No caso da capacidade erro-zero quântica, a sua obtenção só é possível após dois ou mais usos do canal, conforme argumentado por Medeiros (MEDEIROS, 2008, pp. 70). A obtenção da capacidade erro-zero deste canal foi abordada anteriormente nos Exemplos 2.1 e 2.5.

Figura 22: Canal  $\mathcal{E}_4$  e seu respectivo grafo característico.



Fonte: Elaborada pela autora.

O canal  $\mathcal{E}_4$  em questão não é unital e não há  $M_i \in \mathcal{M}$  que satisfaça a condição  $\mathcal{E}(M_i) = M_i \mathcal{E} M_i$ . Desta maneira, não existe um DFS na estrutura interna do código livre de erros associado ao canal, fazendo com que quaisquer transições realizadas provoquem interações indesejadas com o ambiente, sendo passíveis de vazamento de informação. Portanto, tem-se que a capacidade quântica de sigilo erro-zero do canal  $\mathcal{E}_4$  é

$$C_S^{(0)} = \min \{C^{(0)}(\mathcal{E}), C_S(\mathcal{E})\} \quad (3.42)$$

$$= \min \left\{ \frac{1}{2} \log 5, 0 \right\} \quad (3.43)$$

$$= 0. \quad (3.44)$$

Este exemplo ilustra que embora alguns canais possuam uma capacidade quântica erro-zero positiva, não-trivial e obtida com dois ou mais usos do canal, a não existência de um DFS faz com que  $\mathcal{M}' = \emptyset$ , não sendo possível derivar um par  $(S', \mathcal{M}')$  para a transmissão de informação com ausência de erros de decodificação e em sigilo, ou seja, tem-se que  $C_S^{(0)}(\mathcal{E}_4) = 0$ .

### 3.5 Trabalhos Relacionados

Até a publicação dos primeiros trabalhos descrevendo os resultados apresentados na Seção 3.1 (GUEDES; DE ASSIS, 2012b; GUEDES; DE ASSIS, 2012c; GUEDES; DE ASSIS, 2012d; GUEDES; DE ASSIS, 2013b), muitos artigos na literatura que exploravam o uso de DFS em comunicações não consideravam a capacidade dos mesmos para enviar mensagens com segurança incondicional. Dentre os trabalhos investigados (QIN et al., 2009; BIN et al., 2009; DONG et al., 2010), foi possível perceber que estes consistiam de protocolos para comunicação quântica segura direta e para comunicação quântica segura determinística. Neles, havia redundância e checagem de espionagem, o que aumentava significativamente o número de troca de mensagens realmente necessárias para realizar a comunicação com segurança. Em função dos resultados obtidos, foi possível mostrar que todos estes protocolos poderiam ser simplificados, alcançando a segurança incondicional com um número significativamente menor de troca de mensagens, como mostrado detalhadamente em (GUEDES; DE ASSIS, 2012a).

Em relação aos canais *wiretap*, foram também encontradas poucas referências para a caracterização deste tipo de códigos, conforme apresentado anteriormente na Seção 2.4. O código proposto por Hamada (HAMADA, 2008a; HAMADA, 2008b) é baseado nos códigos Calderbank-Shor-Steane e, segundo o autor, são adequados para implementações práticas, por não demandarem o uso de emaranhamento. Porém, a taxa alcançada pelos mesmos encontra-se abaixo da capacidade de sigilo do canal quântico em uso. O trabalho de Wilde e Guha (WILDE; GUHA, 2011; DUTTON; GUHA; WILDE, 2012) também apresenta uma proposição de códigos *wiretap* quânticos baseados em códigos polares. Os próprios autores argumentam que o código apresentado pode estar restrito a certos tipos de canais quânticos. Em relação a proposição de códigos *wiretap* a partir de DFS e códigos

quânticos de prevenção de erros, tal como é mostrado nesta tese, não foram encontradas estratégias similares nas pesquisas realizadas na literatura.

Braunstein et al. (BRAUNSTEIN; KRIBS; PATRA, 2011) esclareceram a relação entre DFS e subespaços erro-zero, mostrando que o último é uma instância do primeiro. Além disto, também propuseram um método para busca de DFS contidos em subespaços erro-zero. Este método possui algumas similaridades com o método proposto por Medeiros et al. (MEDEIROS et al., 2006b). Neste trabalho, optou-se por utilizar este último por ser garantidamente ótimo e por prover uma abordagem mais intuitiva para encontrar um DFS dado um canal quântico com capacidade erro-zero positiva. Este é um componente central na contribuição apresentada neste capítulo. Vale salientar que o trabalho de Braunstein et al. (BRAUNSTEIN; KRIBS; PATRA, 2011) também apresenta outros resultados, tais como a obtenção de limites inferiores e superiores para a dimensão dos subespaços erro-zero em um canal quântico.

Partindo de grafos de confusabilidade de canais quânticos, o trabalho de Chiribella e Yang (CHIRIBELLA; YANG, 2013) considera a busca por componentes conectados com o intuito de identificar, dentre outros, subespaços livres de descoerência. O trabalho destes autores, porém, é voltado para canais quânticos covariantes e não há argumentação sobre a capacidade erro-zero destes canais nem sobre a relação dos grafos de confusabilidade analisados com os grafos de confusabilidade considerados por Duan et al. (DUAN; SEVERINI; WINTER, 2013).

Em termos de capacidade, Watanabe (WATANABE, 2012) caracteriza uma classe de *canais quânticos mais capazes que o ambiente*, nos quais as capacidades quânticas e de sigilo são iguais. Porém, este autor argumenta que as condições que fazem um canal ser desse tipo são, no geral, difíceis de verificar. O canal considerado na Caracterização 3.1 é mais capaz neste sentido, pois tal igualdade pode ser verificada em determinados cenários, como mostrado na prova do Teorema 3.1.

## Notas do Capítulo

Este capítulo contemplou a apresentação da *capacidade quântica de sigilo erro-zero*, segundo a qual, sob certas condições, é possível trocar mensagens por canais quânticos ruidosos e espionados sem que haja vazamento de informação nem erros de decodificação. Esta capacidade agrega conhecimentos oriundos da Teoria da Informação Erro-Zero, da capacidade de sigilo de canais quânticos e também dos subespaços e subsistemas livres de descoerência. Foi apresentada uma abordagem em termos de Teoria dos Grafos para esta capacidade e também uma análise de segurança, que permitiu concluir que as co-

municações ocorrem sob sigilo incondicional. Exemplos foram elaborados para ilustrar os conceitos apresentados e também foi mostrada a relação dos resultados apresentados com outros trabalhos da literatura.

## Capítulo 4

# Informação Acessível Erro-Zero de Fontes Quânticas

A fonte quântica é um componente essencial em sistemas de comunicação quânticos, pois corresponde ao conjunto de símbolos quânticos utilizados para codificar as mensagens clássicas. Neste processo de codificação, há um mapeamento biunívoco entre as mensagens e os estados, mas cada estado quântico está associado a uma probabilidade. Diferentemente das mensagens clássicas que são completamente distinguíveis entre si, os estados quânticos não necessariamente o são, fazendo com que a informação clássica codificada pela fonte possa não ser adequadamente recuperada após uma medição.

Considerando esta dificuldade inerente de recuperar informação oriunda de fontes quânticas, uma medida de informação denominada *informação acessível* foi proposta na literatura (NIELSEN; CHUANG, 2010, Seção 12.1). Esta medida estabelece qual a maior quantidade de informação clássica que pode ser recuperada após a codificação da mesma por uma fonte quântica. Todos os esquemas de medição possíveis são considerados na determinação desta medida, o que a torna de difícil obtenção. Para contornar esta dificuldade, ao invés de utilizar diretamente esta medida, alguns limitantes inferiores e superiores para a mesma são preferíveis (HOLEVO, 1973; CERF; ADAMI, 1996; WOOTTERS, 1993; JOZSA; ROBB; WOOTTERS, 1994; FUCHS, 1995).

Com o intuito de desconsiderar erros no processo de decodificação das mensagens enviadas por uma fonte quântica, este capítulo apresenta algumas das contribuições desta tese, as quais consistem na proposição e caracterização de uma medida de informação sobre fontes quânticas denominada *Informação Acessível Erro-Zero* (ZEAI – *Zero-Error Accessible Information*). Esta medida de informação representa a maior quantidade de bits por símbolo que podem ser recuperados de uma fonte quântica sem que hajam erros neste processo de decodificação. A informação acessível erro-zero de uma fonte quântica

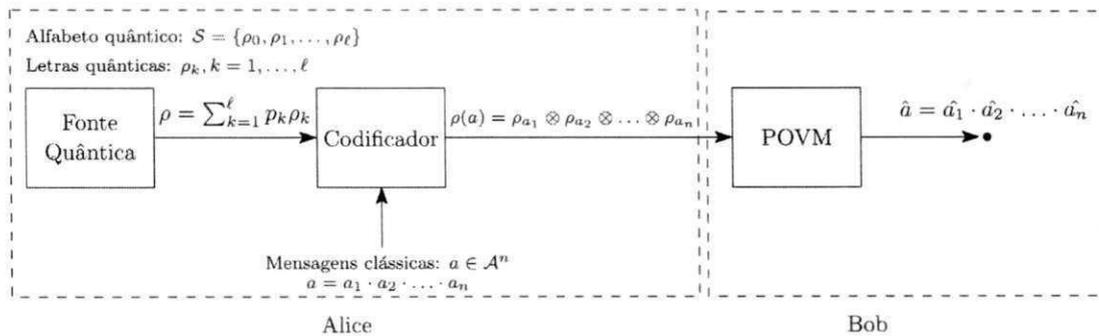
unifica conceitos das fontes quânticas, da informação acessível, da Teoria da Informação Erro-Zero Clássica e também da Teoria dos Grafos.

Para apresentar os resultados em questão, este capítulo está organizado como segue. A caracterização da fonte e da decodificação, bem como a formalização dos conceitos e provas que caracterizam a ZEAI são apresentados na Seção 4.1. A relação da ZEAI com a Teoria dos Grafos é elucidada na Seção 4.2. Posteriormente, exemplos detalhados são apresentadas na Seção 4.3. Por fim, a relação com outros trabalhos da literatura é apresentada na Seção 4.4.

### 4.1 Caracterização e Formalização

Seja um sistema de comunicações simplificado no qual há dois participantes, Alice e Bob. Alice possui uma fonte quântica sem memória, conforme apresentada na Definição 2.15, a qual emite palavras quânticas que serão medidas por Bob com o auxílio de um POVM. Este sistema de comunicações é ilustrado na Figura 23.

Figura 23: Modelo de um sistema de comunicações quântico em que há apenas uma fonte e um receptor.



Fonte: Elaborado pela autora.

No processo de identificação das mensagens recebidas por Bob, admite-se que *erros de decodificação não são tolerados*, ou seja, considera-se apenas o caso que, com 100% de certeza, Bob é capaz de identificar precisamente, por meio da medição realizada, qual mensagem foi enviado por Alice. A partir destas considerações é possível definir o conceito de *Informação Acessível Erro-Zero* (ZEAI – *Zero-Error Accessible Information*) de uma fonte quântica.

**Definição 4.1 (Informação Acessível Erro-Zero)** *Seja F uma fonte quântica sem memória e N(n) o número de palavras quânticas de comprimento n que podem ser envi-*

adas por  $F$  e recuperadas livres de erro por meio de medições POVM sobre letras individuais. A informação acessível erro-zero de  $F$  é definida por

$$I_{acc,ind}^{(0)}(F) \triangleq \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n). \quad (4.1)$$

O seguinte teorema visa apresentar a expressão numérica para a informação acessível erro-zero de uma fonte quântica.

**Teorema 4.1 (Expressão Numérica para a ZEAI)** *A informação acessível erro-zero de uma fonte quântica  $F$  é igual à capacidade erro-zero do seu canal clássico equivalente.*

**Prova** *A demonstração deste teorema considera que a emissão de palavras pela fonte quântica e a medição realizada sem erros de decodificação é equivalente à capacidade erro-zero de um canal clássico discreto e sem-memória.*

*É possível descrever o estado produzido pela fonte e a saída do POVM como um canal clássico discreto sem memória  $W : \mathcal{A} \rightarrow \mathcal{B}$  com a seguinte matriz estocástica*

$$W(a, b) \triangleq \Pr[B = b | A = a] = \text{Tr}(\rho_a M_b), (a, b) \in \mathcal{A} \times \mathcal{B}, \quad (4.2)$$

*em que  $\rho_a$  é a letra quântica emitida pela fonte;  $M_b$  é o elemento de operação do POVM utilizado para medição; e  $\mathcal{A}$  e  $\mathcal{B}$  são os alfabetos das variáveis aleatórias  $A$  e  $B$ . No caso da fonte emitir uma palavra quântica de comprimento  $n$ , tem-se*

$$W^n(a^n, b^n) = \prod_{i=1}^n W(a_i, b_i). \quad (4.3)$$

*Considerando esta interpretação, a maior quantidade de mensagens que podem ser enviados pelo canal  $W$  sem erros de decodificação é igual à sua capacidade erro-zero, ou seja,  $I_{acc}^{(0)}(F) = C_0(W) = \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n)$ . Conclui-se, então, a prova em questão.*

O Teorema 4.1 revela um aspecto interessante: embora a informação acessível erro-zero seja uma medida de informação sobre um dispositivo quântico, o cálculo da mesma considera a obtenção da capacidade erro-zero de um canal clássico. Este resultado é contra-intuitivo, especialmente considerando que não há nenhum tipo de imposição sobre as letras quânticas emitidas pela fonte nem sobre as probabilidades associadas à elas.

Embora não haja restrições sobre a ortogonalidade das letras quânticas emitidas pela fonte, há um caso especial que deve ser considerado. Se a fonte quântica é do tipo *puramente clássica*, tem-se que todas as letras quânticas emitidas pela mesma são

distinguíveis entre si, o que implica que a informação acessível erro-zero da mesma é, pelo menos, igual a  $\log |\mathcal{S}|$ , em que  $\mathcal{S}$  é o alfabeto da fonte quântica.

A informação acessível de uma fonte clássica é uma medida de informação considerada não-relevante devido ao fato de dois estados clássicos serem trivialmente distinguíveis. Porém, no cenário quântico isto não acontece devido à natureza mais complexa do tipo de informação. A informação acessível erro-zero de uma fonte quântica, por sua vez, é uma medida de informação que não possui contrapartida clássica e está intrinsecamente ligada à capacidade erro-zero de canais clássicos.

É importante enfatizar que a definição de informação acessível erro-zero de uma fonte quântica impõe uma restrição, que é a ausência de erros. Com isto, tem-se que as desigualdades  $I_{\text{acc}}^{(0)}(F) \leq I_{\text{acc}}(F) \leq \chi(F)$  para uma fonte quântica  $F$  podem ser verificadas.

## 4.2 Relação com a Teoria dos Grafos

A capacidade erro-zero de canais clássicos possui uma formulação em termos da Teoria dos Grafos, conforme abordado na Seção 2.2.1. O cálculo da informação acessível erro-zero de uma fonte quântica reduz-se ao problema de calcular a capacidade erro-zero de um canal clássico. Com isso, é importante investigar uma maneira natural de endereçar o problema do cálculo da informação acessível erro-zero de uma fonte por meio da utilização da Teoria dos Grafos. Para tanto, é necessário que alguns conceitos sejam estabelecidos.

**Definição 4.2 (Ortogonalidade de Letras Quânticas)** *Dadas duas letras quânticas  $\rho_i = |\psi_i\rangle\langle\psi_i|$  e  $\rho_j = |\psi_j\rangle\langle\psi_j|$  pertencentes ao alfabeto  $\mathcal{S}$  de uma fonte quântica, diz-se que  $\rho_i$  e  $\rho_j$  são ortogonais entre si, denotado por  $\rho_i \perp \rho_j$ , quando o produto interno  $\langle\psi_i|\psi_j\rangle$  é igual a zero.*

O conceito de ortogonalidade entre letras quânticas pode ser estendido para palavras quânticas. Duas palavras quânticas  $\rho^{(i)} = \rho_{i_1} \otimes \rho_{i_2} \otimes \dots \otimes \rho_{i_n}$  e  $\rho^{(j)} = \rho_{j_1} \otimes \rho_{j_2} \otimes \dots \otimes \rho_{j_n}$  são ditas serem ortogonais se existe pelo menos um índice  $k$ ,  $1 \leq k \leq n$ , tal que as letras quânticas  $\rho_{i_k}$  e  $\rho_{j_k}$  são ortogonais.

Com as noções de ortogonalidade entre letras e palavras quânticas definidas, é possível construir o grafo característico de uma fonte quântica.

**Definição 4.3 (Grafo Característico de uma Fonte Quântica)** *Seja  $F$  uma fonte quântica sem memória como apresentada na Definição 2.15. O grafo característico de  $F$  é dado por  $\mathcal{G}(F) = \langle V, E \rangle$ , em que os vértices e arestas são dados como segue:*

1. O conjunto de vértices  $V$  é dado pelas mensagens clássicas associadas às letras quânticas do alfabeto da fonte  $S$ ;
2. Existe uma aresta conectando os vértices  $(i, j)$  se as letras quânticas correspondentes  $\rho_i$  e  $\rho_j$ ,  $i \neq j$ , forem ortogonais entre si.

O grafo  $\mathcal{G}(F)$  pode ser generalizado para  $n$  usos da fonte, denotado por  $\mathcal{G}^n(F)$ , em que o conjunto de vértices é dado por  $V^n$  e o conjunto de arestas é dado pelos pares de palavras quânticas de comprimento  $n$  que são ortogonais.

É interessante notar que o grafo característico da fonte conecta letras ou palavras quânticas que podem ser distinguidas na saída da fonte com 100% de certeza, ou seja, com total ausência de erros de decodificação. Isto acontece porque a ortogonalidade é considerada na construção do grafo característico da fonte.

Dando prosseguimento, é possível definir a informação acessível erro-zero da fonte quântica em termos da Teoria dos Grafos, como mostrado no teorema a seguir.

**Teorema 4.2 (ZEAI em Termos da Teoria dos Grafos)** *Seja uma fonte quântica  $F$  com grafo característico  $\mathcal{G}(F)$  construído conforme especificado na Definição 4.3. A informação acessível erro-zero de  $F$  em termos da Teoria dos Grafos é dada por*

$$I_{\text{acc}}^{(0)}(F) = \sup_n \log \omega(\mathcal{G}^n(F)), \quad (4.4)$$

em que  $\omega(\cdot)$  denota o número do clique do grafo correspondente.

**Prova** Conforme provado no Teorema 4.1, há uma equivalência entre o cálculo da informação acessível erro-zero de uma fonte quântica  $F$  e a obtenção da capacidade erro-zero de um canal clássico discreto sem memória  $W$ . Considerando que há uma formulação em termos da Teoria dos Grafos para obtenção da capacidade erro-zero de  $W$ , conforme apresentado na Seção 2.1, para provar que esta formulação é aplicável no cálculo da informação acessível erro-zero de  $F$ , basta provar o isomorfismo do grafo característico de  $F$  com o grafo característico de  $W$ .

Se  $W$  é um canal clássico obtido conforme descrito na Eq. (4.2), o grafo característico de  $W$  contém como vértices os elementos do conjunto de índices das mensagens. Dois vértices estão conectados no grafo característico de  $W$  se eles são distinguíveis na saída deste canal.

Como há um mapeamento biunívoco entre os índices das mensagens e as letras quânticas do alfabeto da fonte quântica  $F$ , o isomorfismo entre os grafos característicos de  $W$  e  $F$  é verificado. Conclui-se então a prova em questão.

Ao reduzir o cálculo da informação acessível erro-zero ao problema de identificar o número de clique de um grafo, verifica-se que o cálculo da primeira é um problema  $\mathcal{NP}$ -Completo. A dificuldade de ordem exponencial em realizar este cálculo reside na dificuldade em identificar o melhor POVM para a medição erro-zero e também na determinação do comprimento  $n$  das palavras quânticas que maximizam a informação acessível erro-zero da fonte quântica.

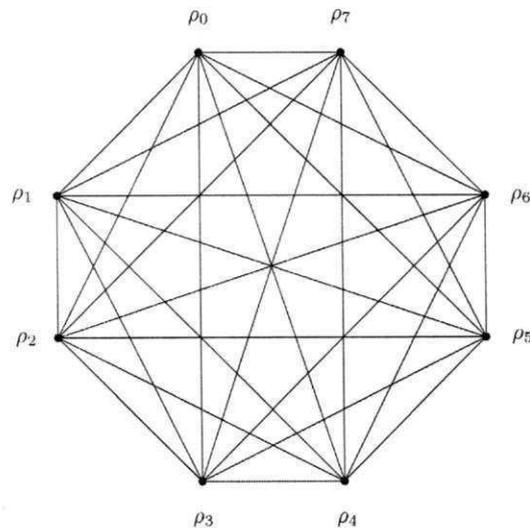
### 4.3 Exemplos

Esta seção apresenta a obtenção da informação acessível erro-zero de algumas fontes quânticas obedecendo aos procedimentos apresentados na Seção 4.1.

**Exemplo 4.1 (Fonte Quântica com ZEAI Igual a Zero)** *Seja uma fonte quântica  $F_1$  que emite dois estados  $\rho_1 = |0\rangle\langle 0|$  e  $\rho_2 = |+\rangle\langle +| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$  de maneira equiprovável. Associada à fonte  $F_1$  está, portanto, o ensemble  $\{\mathcal{S} = \{\rho_1, \rho_2\}, \mathbf{p} = \{p_1 = 0,5, p_2 = 0,5\}\}$ . É possível verificar que as letras quânticas  $\rho_1$  e  $\rho_2$  não são ortogonais entre si, conforme Definição 4.2, pois  $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$ . Logo, uma vez que não há ortogonalidade entre as letras quânticas em  $\mathcal{S}$ , tem-se que  $I_{acc}^{(0)}(F_1) = 0$ .*

**Exemplo 4.2 (ZEAI de uma Fonte Quântica Puramente Clássica)** *Seja uma fonte quântica  $F_2$  que emite mensagens clássicas associadas aos estados da base de um espaço de Hilbert 8-dimensional  $\{\rho_0 = |0\rangle\langle 0|, \rho_1 = |1\rangle\langle 1|, \dots, \rho_7 = |7\rangle\langle 7|\}$  de maneira equiprovável. O grafo característico de  $F_2$ , construído conforme os procedimentos descritos na Definição 4.3, encontra-se ilustrado na Figura 24.*

Figura 24: Grafo característicos da fonte quântica  $F_2$ .



Fonte: Elaborado pela autora.

Considerando que os estados emitidos pela fonte são puros e ortogonais entre si, tem-se que esta  $F_2$  é uma fonte quântica puramente clássica. Um esquema de medições individuais com o POVM  $\{M_{2,i} = |i\rangle\langle i|\}_{i=0}^7$  é capaz de distinguir perfeitamente os estados enviados. Assim, a informação acessível erro-zero de  $F_2$  é dada por

$$I_{\text{acc}}^{(0)}(F_2) = \sup_n \log \omega(\mathcal{G}^n(F)) \tag{4.5}$$

$$= \frac{1}{1} \log 8 \tag{4.6}$$

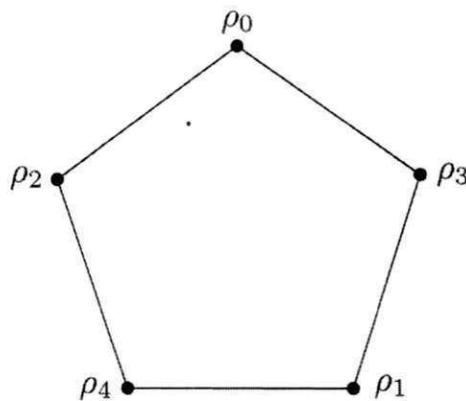
$$= 3 \text{ bits por símbolo.} \tag{4.7}$$

Neste exemplo é interessante notar que com  $n = 1$  já é possível alcançar a informação acessível erro-zero. Para valores de  $n$  maiores que 1, o valor desta medida de informação não se altera, uma vez que  $V^n = |\mathcal{S}|^n$ , o que implica em  $\frac{1}{n} \log |\mathcal{S}|^n = \log |\mathcal{S}|$ .

Vale salientar que a informação acessível erro-zero de  $F_2$  é maior que 1, ilustrando uma situação em que esta medida de informação é não-trivial.

**Exemplo 4.3 (ZEAI de uma Fonte Quântica Correspondente ao Pentágono)** Seja uma fonte quântica  $F_3$  que emite letras quânticas de um alfabeto  $\mathcal{S} = \{\rho_0, \rho_1, \dots, \rho_4\}$  as quais são compostas apenas de estados puros, mas não necessariamente ortogonais entre si. Estes estados são emitidos pela fonte de maneira equiprovável. O grafo característico de  $F_3$ , que mostra as relações de ortogonalidade entre as letras quânticas do alfabeto da fonte, encontra-se ilustrado na Figura 25.

Figura 25: Grafo característico da fonte quântica  $F_3$ .



Fonte: Elaborado pela autora.

É interessante notar que o grafo característico da Figura 25 é isomorfo ao grafo característico do problema do pentágono proposto por Shannon (SHANNON, 1956) e resolvido por Lovasz (LOVÁSZ, 1979), cuja adaptação para o caso quântico foi feita por

Medeiros (MEDEIROS, 2008). Este problema é apresentado anteriormente nos Exemplos 2.1 e 2.5. Graças ao isomorfismo existente, é possível utilizar os resultados obtidos por estes pesquisadores para obter a informação acessível erro-zero da fonte em questão.

No caso da fonte  $F_3$ , consideram-se palavras quânticas de comprimento  $n = 2$  e a utilização do POVM  $\mathcal{M} = \{M_{00}, M_{12}, M_{24}, M_{31}, M_{43}\}$ . Com isto, tem-se que a informação acessível erro-zero de  $F_3$  é igual à capacidade erro-zero do canal clássico do problema do pentágono, que é igual a

$$I_{acc}^{(0)}(F_3) = \frac{1}{2} \log 5 \quad (4.8)$$

$$\approx 1,1609 \text{ bits por símbolo.} \quad (4.9)$$

Este exemplo ilustra um caso em que medições sobre palavras quânticas ( $n > 1$ ) implicam em uma maior informação acessível erro-zero da fonte quântica do que medições sobre as letras quânticas ( $n = 1$ ). Além disso, ressalta outra situação em que a informação acessível erro-zero de uma fonte quântica é positiva e não-trivial ( $I_{acc}^{(0)}(F_3) > 1$ ).

## 4.4 Trabalhos Relacionados

Dadas as dificuldades práticas em calcular a informação acessível no cenário quântico, um dos trabalhos pioneiros na tentativa de estabelecer um limitante para esta medida foi desenvolvido por Holevo (HOLEVO, 1973). Este pesquisador definiu a chamada *quantidade de Holevo*, denotada por  $\chi$ , que estabelece um limite superior para a informação acessível. Cerf e Adami (CERF; ADAMI, 1996) apresentaram uma prova formal para a validade deste limitante e o estenderam para considerar medições sequenciais baseadas nas entropias quânticas mútua e condicional.

O primeiro limitante inferior para a informação acessível foi conjecturado por Wootters (WOOTTERS, 1993) e provado posteriormente por Jozsa et al. (JOZSA; ROBB; WOOTTERS, 1994). Outros limitantes baseados em medidas da Teoria da Informação e nas desigualdade de Jensen, Schwarz e em esquemas de purificação também foram propostos na literatura e podem ser encontrados na tese de Fuchs (FUCHS, 1995, Seção 3.5).

Além do estabelecimento de limitantes para a informação acessível, uma outra linha de pesquisa considera o desenvolvimento de métodos numéricos para encontrar o POVM que venha a ser utilizado no esquema de medição para alcançar a informação acessível. Nascimento e de Assis (NASCIMENTO; DE ASSIS, 2006a; NASCIMENTO; DE ASSIS, 2006b) desenvolveram um método para este fim baseado na utilização de algo-

ritmos genéticos. A ferramenta *open-source* SOMIM (*Search for Optimal Measurements by an Iterative Method*) também considera esta abordagem e faz uso de um método iterativo para encontrar o melhor POVM (REHACEK; ENGLERT; KASZLIKOWSKI, 2005; SUZUKI; ASSAD; ENGLERT, 2007; LEE et al., 2011).

Sasaki e outros (SASAKI et al., 1999) endereçam diretamente o problema de calcular a informação acessível de uma fonte quântica, porém restringindo-o para o caso de fontes quânticas reais e simétricas. Uma fonte quântica é dita ser *real* quando os coeficientes relacionados aos estados quânticos que emite possuem apenas componentes do conjunto dos números reais. A simetria é verificada quando os estados quânticos que possuem apenas componentes reais encontram-se igualmente espaçados em um plano  $x-z$  da esfera de Bloch. Para encontrar a informação acessível deste tipo de fonte quântica, os autores em questão desenvolveram um método baseado na Teoria dos Grupos para determinação do POVM ótimo para realização da medição. Este POVM possui apenas três elementos de medição e o método proposto é passível de implementação prática com tecnologia atualmente existente, conforme argumentam os autores. Porém, é importante enfatizar que embora trate da questão da informação acessível, os resultados obtidos por Sasaki et al. (SASAKI et al., 1999) restringem-se às fontes quânticas reais e simétricas.

As pesquisas realizadas na literatura até o momento da escrita deste trabalho de tese não identificaram trabalhos de outros autores que enderecem a obtenção da informação acessível de fontes quânticas em um cenário de completa ausência de erros. Apesar da importância de propor uma medida de informação sobre fontes quânticas que agrega o caráter erro-zero, é importante mencionar que há uma custo exponencial intrínseco no cálculo da mesma, que reside na dificuldade em determinar qual o melhor POVM para realização da medição. Esta dificuldade, entretanto, também é verificada no cálculo da informação acessível.

## Notas do Capítulo

Neste capítulo foi apresentada a *informação acessível erro-zero de fontes quânticas*, uma medida de informação que quantifica a maior quantidade de informações que podem ser extraídas sem erros de uma fonte quântica. O cálculo da informação acessível erro-zero de uma fonte quântica é redutível ao problema de calcular a capacidade erro-zero de um canal clássico equivalente. A informação acessível erro-zero agrega conhecimentos acerca das fontes quânticas, da informação acessível, da Teoria da Informação Erro-Zero Clássica e também da Teoria dos Grafos. Foi também apresentada uma abordagem em termos de Teoria dos Grafos para obtenção da informação acessível erro-zero de uma fonte quântica, a qual permitiu utilizar o clique do grafo característico da fonte quântica como uma forma

de obtenção desta medida de informação. Exemplos foram apresentados para ilustrar os conceitos apresentados e também foi mostrada a relação com os trabalhos existentes na literatura.

## Capítulo 5

### Considerações Finais

Este capítulo contempla a descrição das contribuições deste trabalho de tese, bem como sugestões para pesquisas que foram motivadas por problemas em aberto identificados no decorrer da pesquisa. As contribuições do trabalho e os artigos produzidos e publicados encontram-se apresentados na Seção 5.1. As sugestões de trabalho futuro encontram-se apresentadas na Seção 5.2.

#### 5.1 Contribuições

Como aspecto motivador para a realização deste trabalho de tese, foi identificado que ainda não há um conhecimento amplo das potencialidades, limitações e aplicações da Teoria da Informação Quântica Erro-Zero. Na tentativa de minimizar esta lacuna, duas linhas de investigação foram propostas para este trabalho.

A primeira delas possuiu como objetivo a investigação do uso de canais quânticos erro-zero para a transmissão de informação sigilosa. Para verificar esta possibilidade, foi utilizado o modelo dos canais *wiretap* (CAI; WINTER; YEUNG, 2004; DEVETAK, 2005) e o uso de subespaços e subsistemas livres de descoerência que residem na estrutura interna de alguns códigos livres de erro. Com isto, foi possível caracterizar uma abordagem que permite o envio de informação clássica por meio de tais canais quânticos com ausência de erros de decodificação e de vazamento de informação. Assim, houve a descoberta de uma nova capacidade de tais canais quânticos, a chamada *capacidade quântica de sigilo erro-zero*.

No Capítulo 3 foi feita a caracterização da QZESC, incluindo a sua definição formal, as provas necessárias e um teorema que a quantifica, o qual relaciona a capacidade erro-zero e a capacidade de sigilo do canal em questão. Exemplos foram construídos para ilustrarem a QZESC, incluindo não apenas situações em que esta é positiva, mas também

não-trivial. Além disso, foi efetuada a análise de segurança, que mostrou que o esquema adotado possui segurança incondicional, e também uma relação com os trabalhos existentes na literatura. Também foram identificados canais quânticos já existentes que podem vir a implementar tais resultados em um cenário prático.

A segunda linha de investigação possuiu como objetivo a proposição de uma medida de informação sobre fontes quânticas. Como resultado, foi proposta a *informação acessível erro-zero de fontes quânticas*, a qual especifica o máximo de informação que pode ser decodificada da saída da fonte quântica sem que hajam erros. Foi verificado que a obtenção desta medida é equivalente ao cálculo da capacidade erro-zero de um canal clássico, evidenciando uma relação não-trivial entre fontes quânticas e canais clássicos com capacidade erro-zero. Em virtude desta equivalência, foi possível determinar que, assim como para a informação acessível, calcular a informação acessível erro-zero de uma fonte quântica é um problema  $\mathcal{NP}$ -completo, cuja dificuldade reside na determinação do melhor POVM para realização das medições.

No Capítulo 4 foi feita a completa caracterização da ZEAI, incluindo a sua definição formal e um teorema que a quantifica, o qual relaciona tal medida de informação com a capacidade erro-zero de um canal clássico. Exemplos foram construídos para ilustrar a obtenção desta medida de informação, sua relação com a informação acessível e a quantidade de Holevo foi estabelecida e também as contribuições relacionadas na literatura foram identificadas.

A proposição da QZESC e da ZEAI resultante dos desdobramentos deste trabalho de tese endereçam o problema que motivou a realização deste trabalho. Estes dois novos conceitos mostram aplicações da Teoria da Informação Quântica Erro-Zero junto à outras áreas do conhecimento, propõem novas maneiras de enviar informação por canais quânticos com capacidade erro-zero, apresentam uma nova medida de informação sobre fontes quânticas que agrega o caráter erro-zero e desvendam relações não-triviais entre diversos conceitos, tais como, subespaços e subsistemas livres de descoerência e segurança incondicional, informação acessível erro-zero de fontes quânticas e a capacidade erro-zero de canais clássicos, dentre outras. Tais contribuições também estão alinhadas com o desafio de caráter teórico da Teoria da Informação, que diz respeito à determinação de limites para a classe de tarefas de processamento de informação que são possíveis considerando a utilização da Mecânica Quântica.

Tanto na proposição da QZESC quanto da ZEAI foi possível elaborar uma formulação em termos da Teoria dos Grafos. Esta formulação se deu por meio da proposição de grafos característicos para os canais quânticos, no caso da QZESC, e para as fontes quânticas, no caso da ZEAI. Tal formulação permitiu estabelecer meios de obter a QZESC

e a ZEAI por meio de problemas já conhecidos na Teoria dos Grafos, a exemplo do número de clique de um grafo. No caso da ZEAI, em particular, o isomorfismo entre o grafo característico da fonte e o grafo característico de um canal clássico equivalente permitiu o uso da redução polinomial de problemas, um artefato da Ciência da Computação, para determinação da complexidade do cálculo desta medida de informação. Além da possibilidade de reformulações dos problemas mencionados, o uso da Teoria dos Grafos ajudou a consolidar uma representação gráfica, a qual favorece uma melhor compreensão dos conceitos propostos.

Embora o trabalho de tese desenvolvido tenha uma natureza majoritariamente teórica, vale ressaltar que os conceitos propostos são passíveis de implementação com tecnologia atualmente existente. No caso da QZESC, em particular, como esta capacidade pode emergir em canais quânticos com ruído coletivo, as implementações de canais quânticos com este tipo de ruído se mostram adequadas (JAEGER; SERGIENKO, 2008; XIA et al., 2010; DORNER; KLEIN; JAKSCH, 2008). Além destas implementações, canais quânticos que possuem capacidade erro-zero positiva também podem ser viáveis, tal como a implementação sugerida por Gyongyosi e Imre (GYONGYOSI; IMRE, 2012). Dentre as implementações existentes, entretanto, a que pode ser de maior destaque na identificação da QZESC é a proposta por Xue (XUE, 2008), a qual possui descoerência coletiva e tem seu uso voltado para longas distâncias. No caso da ZEAI, por sua vez, esta medida de informação pode ser útil no processo de escolha de fontes quânticas, especialmente se um dos parâmetros considerados nesse processo de escolha for a possibilidade de recuperar sem erros as informações enviadas pela mesma.

### 5.1.1 Artigos Produzidos

Ao longo do desenvolvimento deste trabalho de tese, artigos científicos relacionados ao tema em questão foram desenvolvidos, alguns dos quais já publicados e outros ainda sob avaliação. A lista a seguir apresenta tais artigos, incluindo uma breve descrição do conteúdo e das contribuições de cada um.

1. **Utilização de Subespaços Livres de Descoerência em Comunicações Quânticas Incondicionalmente Seguras** (GUEDES; DE ASSIS, 2012d). Artigo completo publicado no XXX Simpósio Brasileiro de Telecomunicações, descreve como utilizar subespaços e subsistemas livres de descoerência em comunicações quânticas garantindo a segurança incondicional. Apresenta as primeiras provas formais de que tal tipo de comunicação é possível;
2. *On the Security of Decoherence-Free Subspaces and Subsystems for Clas-*

- sical Information Conveying through Quantum Channels* (GUEDES; DE ASSIS, 2013b). Artigo completo publicado no periódico *International Journal of Quantum Information* consolidando os resultados sobre a segurança dos subespaços e subsistemas livres de descoerência para envio de informação clássica por canais quânticos com segurança incondicional. Apresenta provas formais mais elaboradas, exemplos e sugestões de outros trabalhos na literatura de como consolidar este tipo de comunicação utilizando tecnologia atualmente existente;
3. ***Quantum Zero-Error Secrecy Capacity*** (GUEDES; DE ASSIS, 2012b). Artigo completo publicado no IV Workshop-Escola de Computação e Informação Quânticas, unifica conhecimentos dos canais quânticos erro-zero, dos subespaços livres de descoerência e da capacidade quântica de sigilo para estabelecer as condições nas quais a chamada capacidade quântica de sigilo erro-zero pode ser alcançada por alguns canais quânticos;
  4. ***Quantum Zero-Error Secrecy Capacity***. Artigo completo com 16 páginas submetido em 4 de Junho de 2013 aos editores do periódico *Quantum Information & Computation*, com primeira avaliação informada em 20 de Setembro de 2013. Consolida a capacidade quântica de sigilo erro-zero de canais quânticos em termos de notação, provas formais e exemplos. Apresenta referências na literatura acerca da implementação de canais quânticos, inclusive em longa distância, que podem ser utilizados para transmitir informação quântica com ausência de erros de decodificação e em sigilo absoluto;
  5. **Informação Acessível Erro-Zero de Fontes Quânticas** (GUEDES; DE ASSIS, 2013a). Artigo completo publicado no XXXI Simpósio Brasileiro de Telecomunicações. Este artigo apresenta os primeiros resultados sobre a informação acessível erro-zero de fontes quânticas considerando o caso de medições individuais.

Alguns resultados que possuem uma relação menos direta com o trabalho de tese também foram obtidos. Estes resultados encontram-se listados a seguir.

6. ***An Approach to Evaluate Quantum Authentication Protocols*** (GUEDES; DE ASSIS, 2011). Artigo completo publicado no X Congresso Brasileiro de Inteligência Computacional, apresenta uma abordagem para avaliar e comparar protocolos de autenticação quânticos considerando a complexidade comunicacional dos mesmos. Além de propor esta abordagem, o artigo contempla resultados da aplicação da mesma em 10 protocolos de autenticação quânticos (autenticação de identidade e de mensagem) existentes na literatura;

7. ***Enhancing Quantum Protocols with the Security of Decoherence-Free Subspaces and Subsystems*** (GUEDES; DE ASSIS, 2012a). Artigo completo publicado no IV Workshop-Escola de Computação e Informação Quânticas, contempla implicações dos resultados sobre a segurança incondicional dos subespaços e subsistemas livres de descoerência na simplificação de protocolos de comunicação quânticas que fazem uso de canais quânticos com descoerência coletiva;
8. ***Unconditional Security with Decoherence-Free Subspaces***. Artigo completo aceito pelo periódico *Brazilian Journal of Information Security and Cryptography*, com 10 páginas, em 30 de Novembro de 2013. Este artigo descreve detalhadamente melhorias em protocolos de comunicação quântica segura direta e em protocolos de comunicação quântica determinística segura a partir dos resultados obtidos sobre a segurança incondicional dos subespaços e subsistemas livres de descoerência. Apresenta a análise de 4 protocolos propostos na literatura para canais quânticos com rotação, defasamento e decaimento de amplitude coletivos. Em todos os protocolos analisados, foi possível realizar uma simplificação significativa nos procedimentos de codificação, decodificação e no número de mensagens trocadas entre os participantes legítimos;
9. ***Quantum Key Distribution over Collective Amplitude Damping Quantum Channels*** (GUEDES; DE ASSIS, 2013c). Artigo completo publicado na VIII *International Multi-Conference on Computing in the Global Information Technology*. Enquanto no modelo *wiretap* considerado na proposição da capacidade quântica de sigilo erro-zero é considerada a espionagem passiva, este trabalho considera o modelo de espião ativo capaz de realizar ataques do tipo “intercepta e reenvia” nos estados quânticos que trafegam em um canal utilizado por dois participantes legítimos. Com o intuito de permitir a realização de comunicação segura independentemente da ação deste espião, o artigo em questão apresenta um protocolo para distribuição quântica de chaves neste cenário, considerando que o canal quântico possui decaimento coletivo de amplitude. O protocolo proposto é fortemente baseado no BB84 (BENNETT; BRASSARD, 1984) e faz uso do subespaço livre de descoerência existente no canal quântico em questão e dos resultados obtidos sobre a segurança destes;
10. ***Simulating the Quantum Fourier Transform***. Artigo completo publicado no II *Workshop-Escola de Informática Teórica*. Trata do desenvolvimento de um simulador para a transformada quântica de Fourier e da análise estatística do desempenho desta ferramenta, a qual pode simular até 12 qubits. Além da simulação da transformada quântica de Fourier, esta ferramenta também implementa a transformada rápida de Fourier e gera gráficos em  $\text{\LaTeX}$  dos resultados obtidos.

Os artigos mencionados que foram publicados encontram-se no Apêndice C desta tese, na ordem em que foram apresentados.

## 5.2 Perspectivas para Pesquisa

Em virtude do desenvolvimento de novos conceitos e medidas de informação nesta tese, algumas ideias para pesquisa foram identificadas, bem como outros caminhos que não puderam ser completamente explorados. Uma lista de tais ideias com algumas referências na literatura para auxiliar a exploração das mesmas é apresentada. Embora não seja uma listagem exaustiva, as ideias apresentadas dão perspectivas para o desenvolvimento de novas pesquisas que venham a contribuir para a Teoria da Informação Quântica.

### 5.2.1 Utilização de Emaranhamento e Medidas Negativas na Teoria da Informação Quântica Erro-Zero

O trabalho seminal da Teoria da Informação Quântica Erro-Zero de Medeiros (MEDEIROS, 2008) considera apenas o envio de estados quânticos puros ou mistos por canais quânticos e a ausência de erros na decodificação destes estados. A possibilidade de criar emaranhamento entre duas partes distintas e trocar informações sem erros de decodificação foi explorada posteriormente em um trabalho de Cubitt et al. (CUBITT et al., 2010a), provendo uma extensão da Teoria da Informação Quântica Erro-Zero.

Como consequência do emaranhamento em canais quânticos com capacidade erro-zero, abre-se uma perspectiva para a proposição de medidas de informação negativas, conforme propostas inicialmente por Cerf e Adami (CERF; ADAMI, 1997). Tais medidas poderiam vir a quantificar, por exemplo, quantos estados de entrada de um canal quântico sem capacidade erro-zero não deveriam ser utilizados a fim de garantir a positividade da capacidade erro-zero no uso deste canal. Idéias similares podem ser consideradas no uso de fontes quânticas e na obtenção da informação acessível erro-zero das mesmas.

### 5.2.2 Superativação da Capacidade Quântica de Sigilo Erro-Zero

Vários avanços em relação à Teoria da Informação Quântica Erro-Zero consideraram a combinação de múltiplos canais quânticos que não possuíam capacidade erro-zero e, quando utilizados em conjunto, possuíam tal capacidade não-negativa, ilustrando a superativação da capacidade quântica erro-zero (DUAN; SHI, 2008; CUBITT; CHEN; HARROW, 2009; DUAN, 2009; CHEN et al., 2010; CUBITT; SMITH, 2012).

Dada a caracterização de uma nova capacidade de canais quânticos, a capacidade quântica de sigilo erro-zero, é possível identificar situações nas quais há superativação desta capacidade? A característica de descoerência coletiva assume um papel importante na combinação de canais quânticos distintos para alcançar esta capacidade? Responder a estas perguntas pode trazer à tona mais tipos de canais quânticos que podem ser utilizados para comunicações livres de erros de decodificação e em sigilo absoluto.

### 5.2.3 Subespaços e Subsistemas Livres de Descoerência e a Capacidade Quântica de Sigilo Erro-Zero

A definição da capacidade quântica de sigilo erro-zero considera a existência de subespaços e subsistemas livres de descoerência em canais quânticos com capacidade erro-zero para garantir a ausência de erros de decodificação e o sigilo absoluto.

As pesquisas de Shabani et al. (SHABANI; LIDAR, 2005; SHABANI, 2009) discorrem sobre a existência de condições “mais relaxadas” para a existência de subespaços e subsistemas livres de descoerência. Levando isto em consideração, como tais condições podem ser aproveitadas e implementadas em cenários práticos para garantir a positividade da capacidade quântica de sigilo erro-zero de determinados canais? Responder a esta pergunta pode vir a colaborar na identificação de uma maior gama de canais quânticos capazes de alcançar a positividade desta capacidade, com menor rigor em relação ao modelo de erros.

Simplesmente identificar condições menos restritivas para a existência de subespaços e subsistemas livres de descoerência tem uma importância significativa para a realização de comunicações quânticas em sigilo absoluto, visto os resultados sobre a segurança de tais subespaços e subsistemas identificadas no decorrer deste trabalho de tese (GUEDES; DE ASSIS, 2012d; GUEDES; DE ASSIS, 2013b).

### 5.2.4 Desenvolvimento de Métodos para Obtenção de POVMs

Como argumentado na Seção 4.2, o problema de determinar a informação acessível erro-zero de uma fonte quântica é equivalente ao de identificar o número de clique de um grafo, que é  $\mathcal{NP}$ -Completo. Em se tratando da informação acessível erro-zero, esta dificuldade encontra-se na identificação do POVM que maximize esta medida de informação, mesmo problema verificado para a informação acessível, medida de informação sobre fontes quânticas consolidada na literatura e apresentada nesta tese na Seção 2.5.

Alguns trabalhos de diferentes autores propuseram heurísticas para obtenção do melhor POVM, baseando-se em métodos iterativos (REHACEK; ENGLERT; KASZLI-

KOWSKI, 2005; SUZUKI; ASSAD; ENGLERT, 2007; LEE et al., 2011) ou no uso de algoritmos genéticos (NASCIMENTO; DE ASSIS, 2006a; NASCIMENTO; DE ASSIS, 2006b). Considerando a importância do POVM para a determinação da informação acessível e da informação acessível erro-zero, é desejável que mais métodos desta natureza sejam desenvolvidos. A proposição de novos métodos não colabora especificamente apenas para a obtenção de tais medidas de informação, mas pode ser útil também como meio de análise e comparação dos métodos de obtenção de POVMs já existentes.

## Referências Bibliográficas

ACM SIGACT. *Challenges for Theoretical Computer Science*. 2000. Workshop on Challenges for Theoretical Computer Science. Disponível em: <<http://www2.research.att.com/~dsj/nsflist.html>>. Acesso em: 20 de dezembro de 2013. Citado na página 27.

BACON, D. M. *Decoherence, Control, and Symmetry in Quantum Computers*. Tese (Doutorado) — University of California at Berkeley, 2001. Citado nas páginas 16, 49 e 79.

BEIGE, A. et al. Quantum computing using dissipation to remain in a decoherence-free subspace. *Phys. Rev. Lett.*, v. 85, p. 1762, 2000. Citado na página 52.

BEIGI, S.; SHOR, P. W. *On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels*. 2008. arxiv:quant-ph/0709.2090. Citado nas páginas 23 e 46.

BEIKIDEZFULI, S. A. *Quantum proof systems and entanglement theory*. Tese (Doutorado) — Massachusetts Institute of Technology, 2009. Citado na página 46.

BENENTI, G.; CASATI, G.; STRINI, G. *Principles of Quantum Computation and Information – Volume II: Basic Tools and Special Topics*. Cingapura: World Scientific, 2007. Citado na página 52.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. In: *IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, Índia: IEEE Computer Society, 1984. p. 175–179. Citado nas páginas 22, 98 e 127.

BENNETT, C. H.; SHOR, P. W. Quantum information theory. *IEEE Transactions on Information Theory*, v. 44, n. 6, p. 2724–2742, 1998. Citado nas páginas 29 e 62.

BIN, G. et al. Deterministic secure quantum communication over a collective-noise channel. *Science in China Series G: Physics, Mechanics and Astronomy*, v. 52, n. 12, p. 1913–1918, 2009. Citado na página 81.

BLUME-KOHOOUT, R. et al. *Information preserving structures: A general framework for quantum zero-error information*. 2010. arxiv:quant-ph/1006.1358v1. Citado na página 47.

BRAUNSTEIN, S. L.; KRIBS, D. W.; PATRA, M. K. Zero-error subspaces of quantum channels. In: *IEEE International Symposium on Information Theory*. São Petersburgo, Rússia: IEEE Press, 2011. p. 104–108. Citado na página 82.

BRIET, J. et al. *Zero-error source-channel coding with entanglement*. 2013. arxiv:quantum-ph/1308.4283. Citado na página 48.

BYRD, M. S.; WU, L.-A.; LIDAR, D. A. Overview of quantum error prevention and leakage elimination. *Journal of Modern Optics*, v. 51, n. 16-18, p. 2449–2460, 2004. Citado nas páginas 49 e 52.

CAI, N.; WINTER, A.; YEUNG, R. W. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, v. 40, p. 318–336, 2004. Citado nas páginas 24, 57, 58, 59, 66, 68, 70, 72, 74 e 94.

CERF, N. J.; ADAMI, C. *Accessible Information in Quantum Measurement*. 1996. arxiv:quantum-ph/9611032v1. Citado nas páginas 84 e 91.

CERF, N. J.; ADAMI, C. Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, v. 79, n. 26, p. 5194–5197, 1997. Citado na página 99.

CHEN, J. et al. Super-duper-activation of the zero-error quantum capacity. In: *IEEE International Symposium on Information Theory*. Texas, Estados Unidos: IEEE Press, 2010. p. 1–19. Citado nas páginas 23, 47 e 99.

CHIRIBELLA, G.; YANG, Y. Confusability graphs for symmetric sets of quantum states. In: *XXIX International Colloquium on Group-Theoretical Methods in Physics*. Tianjin, China: World Scientific, 2013. p. 251–256. Citado na página 82.

CHOI, M.-D.; KRIBS, D. W. A method to find quantum noiseless subsystems. *Phys. Rev. Lett.*, v. 96, p. 050501, 2006. Citado nas páginas 18, 52, 53, 54, 56 e 73.

COVER, T. M.; THOMAS, J. A. *Elements of Information Theory*. New Jersey, Estados Unidos: John Wiley & Sons, 2006. Citado nas páginas 29, 30, 121, 122 e 125.

CUBITT, T. S.; CHEN, J.; HARROW, A. W. *Super-Activation of Zero-Error Capacity of Noisy Quantum Channels*. 2009. arxiv:quant-ph/0906.2547. Citado nas páginas 23, 47 e 99.

CUBITT, T. S. et al. *Improving zero-error classical communication with entanglement*. 2009. arxiv:quant-ph/0911.5300. Citado na página 43.

CUBITT, T. S. et al. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.*, v. 104, p. 230503, 2010. Citado nas páginas 48 e 99.

CUBITT, T. S. et al. *Zero-error channel capacity and simulation assisted by non-local correlations*. 2010. arxiv:quant-ph/1003.3195. Citado na página 43.

CUBITT, T. S.; SMITH, G. An extreme form of superactivation for quantum zero-error capacities. *IEEE Transactions on Information Theory*, v. 58, n. 3, 2012. Citado nas páginas 23, 47 e 99.

- DAVIDSON, K. *C\*-algebras by example*. Rhode Island, Estados Unidos: Fields Institute Monographs, Amer. Math. Soc., 1996. Citado na página 53.
- DESURVIRE, E. *Classical and Quantum Information Theory*. Cambridge, Inglaterra: Cambridge University Press, 2009. Citado nas páginas 29, 121 e 122.
- DEUTSCH, D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London A*, v. 400, p. 97–117, 1985. Citado nas páginas 22 e 128.
- DEVETAK, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, v. 51, n. 1, p. 44–55, 2005. Citado nas páginas 24, 57, 59, 66, 70, 72, 74 e 94.
- DIRAC, P. *The principles of Quantum Mechanics*. 4th. ed. Oxford, Inglaterra: Oxford University Press, 1982. Citado nas páginas 28, 110, 111 e 120.
- DONG, H.-K. et al. A deterministic secure quantum communication protocol through a collective rotation noise channel. *Int. J. of Quantum Inf.*, v. 8, n. 8, p. 1389–1395, 2010. Citado na página 81.
- DORNER, U.; KLEIN, A.; JAKSCH, D. A quantum repeater based on decoherence free subspaces. *Quant. Inf. Comp.*, v. 8, p. 468, 2008. Citado nas páginas 26, 52, 72 e 96.
- DUAN, L.-M.; GUO, G.-C. Quantum error avoiding codes versus quantum error correcting codes. *Phys. Lett. A*, v. 255, p. 209–212, 1999. Citado na página 51.
- DUAN, R. *Super-Activation of Zero-Error Capacity of Noisy Quantum Channels*. 2009. arxiv:quant-ph/0906.2527v1. Citado nas páginas 23, 47 e 99.
- DUAN, R.; SEVERINI, S.; WINTER, A. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz  $\vartheta$  function. In: *IEEE International Symposium on Information Theory*. São Petersburgo, Rússia: IEEE Press, 2011. p. 64–68. Citado nas páginas 23, 43, 46 e 48.
- DUAN, R.; SEVERINI, S.; WINTER, A. Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovasz  $\vartheta$  function. *IEEE Transactions on Information Theory*, v. 59, n. 2, p. 1164–1174, 2013. Citado nas páginas 23, 46, 74 e 82.
- DUAN, R.; SHI, Y. Entanglement between two uses of a noisy multipartite quantum channel enables perfect transmission of classical information. *Phys. Rev. Lett.*, American Physical Society, v. 101, p. 020501, Jul 2008. Citado nas páginas 47 e 99.
- DUTTON, Z.; GUHA, S.; WILDE, M. M. Performance of polar codes for quantum and private classical communication. In: *50th Annual Allerton Conference on Communication, Control, and Computing 2012*. Illinois, Estados Unidos: IEEE Press, 2012. p. 1–8. Citado nas páginas 60 e 81.
- FENG, M. *Quantum computing and communication with decoherence-free atomic states*. 2001. arxiv:quant-ph/0111041v1. Citado na página 52.

FUCHS, C. A. *Distinguishability and Accessible Information in Quantum Theory*. Tese (Doutorado) — University of New Mexico, Estados Unidos, 1995. Citado nas páginas 25, 84 e 91.

GUEDES, E. B.; DE ASSIS, F. M. An approach to evaluate quantum authentication protocols. In: *Congresso Brasileiro de Inteligência Computacional*. Fortaleza, Ceará, Brasil: Sociedade Brasileira de Inteligência Computacional, 2011. p. 1–8. Citado na página 97.

GUEDES, E. B.; DE ASSIS, F. M. Enhancing quantum protocols with the security of decoherence-free subspaces and subsystems. In: *Workshop School of Quantum Computation and Information*. Fortaleza, Ceará, Brasil: WECIQ, 2012. p. 1–8. Citado nas páginas 26, 81 e 98.

GUEDES, E. B.; DE ASSIS, F. M. Quantum zero-error secrecy capacity. In: *Workshop School of Quantum Computation and Information*. Fortaleza, Ceará, Brasil: WECIQ, 2012. p. 1–8. Citado nas páginas 25, 81 e 97.

GUEDES, E. B.; DE ASSIS, F. M. *Unconditional Security with Decoherence-Free Subspaces*. 2012. 1-6 p. arxiv:quant-ph/1204.3000. Citado na página 81.

GUEDES, E. B.; DE ASSIS, F. M. *Utilização de Subespaços Livres de Descoerência em Comunicações Quânticas Incondicionalmente Seguras*. Brasília: Sociedade Brasileira de Telecomunicações, 2012. 1-5 p. Citado nas páginas 25, 81, 96 e 100.

GUEDES, E. B.; DE ASSIS, F. M. Informação acessível erro-zero de fontes quânticas. In: *XXXI Simpósio Brasileiro de Telecomunicações*. Fortaleza, Ceará, Brasil: Sociedade Brasileira de Telecomunicações, 2013. p. 1–5. Citado nas páginas 26 e 97.

GUEDES, E. B.; DE ASSIS, F. M. On the security of decoherence-free subspaces and subsystems for classical information conveying through quantum channels. *International Journal of Quantum Information*, v. 11, n. 2, p. (1350022–1)–(1350022–14), 2013. Citado nas páginas 25, 69, 81, 97 e 100.

GUEDES, E. B.; DE ASSIS, F. M. Quantum key distribution over collective amplitude damping quantum channels. In: *International Multi-Conference on Computing in the Global Information Technology*. Nice, França: IARIA, 2013. v. 8, p. 1–6. Citado na página 98.

GYONGYOSI, L.; IMRE, S. Long-distance quantum communications with superactivated gaussian optical quantum channels. *Optical Engineering*, v. 51, n. 1, 2012. Citado nas páginas 23, 26, 48, 72 e 96.

HAMADA, M. Algebraic and quantum theoretical approach to coding on wiretap channels. In: *International Symposium on Communications, Control and Signal Processing*. Malta: IEEE Press, 2008. p. 1–6. Citado nas páginas 59 e 81.

HAMADA, M. Constructive codes for classical and quantum wiretap channels. In: ROLAND E. CHEN. *Cryptography and Research Perspectives*. Nova York, Estados Unidos: Nova Science Publishers, 2008. p. 1–48. Citado nas páginas 59 e 81.

- HAYASHI, M. *Quantum Information – An introduction*. Tóquio, Japão: Springer, 2006. Citado na página 121.
- HOLEVO, A. S. Information theoretical aspects of quantum measurements. *Problems of Information Transmission*, v. 9, n. 2, p. 110–118, 1973. Citado nas páginas 25, 84 e 91.
- HOLEVO, A. S. *Probabilistic and Statistical Aspects of Quantum Theory*. North-Holland, Amsterdam: North-Holland Series in Statistics and Probability, 1982. Citado nas páginas 22 e 127.
- HOLEVO, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Info. Theory*, v. 4, n. 1, p. 269–273, 1998. Citado nas páginas 42, 70 e 74.
- IEEE. *Task Force on Quantum Computing*. 2012. Disponível em: <<http://web.cecs.pdx.edu/~whung/ETTC/>>. Acesso em: 20 de dezembro de 2013. Citado na página 27.
- IMRE, S.; BALAZS, F. *Quantum Computing and Communications - An Engineering Approach*. Chichester, Inglaterra: John Wiley & Sons, 2005. Citado na página 110.
- IVANOV, P. A. et al. Quantum gate in the decoherence-free subspace of trapped-ion qubits. *Europhysics Letters*, v. 92, n. 3, p. 30006, 2010. Citado na página 52.
- JAEGER, G.; SERGIENKO, A. Constructing four-photon states for quantum communication and information processing. *Int. J. Theor. Phys.*, v. 47, p. 2120, 2008. Citado nas páginas 26, 72 e 96.
- JOZSA, R.; ROBB, D.; WOOTTERS, W. K. Lower bound for accessible information in quantum mechanics. *Phys. Rev. A*, v. 49, p. 668–677, 1994. Citado nas páginas 84 e 91.
- KAYE, P.; LAFLAMME, R.; MOSCA, M. *An Introduction to Quantum Computing*. Oxford, Inglaterra: Oxford University, 2007. Citado nas páginas 29 e 110.
- KIELPINSKI, D. A decoherence-free quantum memory using trapped ions. *Science*, v. 291, p. 1013, 2001. Citado na página 52.
- KNILL, E.; LAFLAMME, R.; VIOLA, L. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, v. 84, p. 2525, 2000. Citado na página 50.
- KORNER, J.; ORLITSKY, A. Zero-error information theory. *IEEE Transactions on Information Theory*, v. 44, p. 2207–2229, 1998. Citado nas páginas 16, 30, 31 e 33.
- KWIAT, P. G. et al. Experimental verification of decoherence-free subspaces. *Science*, v. 290, p. 498–501, 2000. Citado na página 52.
- LEE, K. L. et al. *SOMIM : An open-source program code for the numerical Search for Optimal Measurements by an Iterative Method*. 2011. <http://www.quantumlah.org/publications/software/SOMIM/>. Citado nas páginas 25, 92 e 101.
- LIDAR, D. A.; CHUANG, I. L.; WHALEY, K. B. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, v. 81, p. 2594–2597, 1998. Citado na página 52.

- LIDAR, D. A.; WHALEY, K. B. *Decoherence-Free Subspaces and Subsystems*. 2003. arxiv: quantum-ph/0301032v1. Citado nas páginas 26, 49, 50, 65 e 72.
- LOVÁSZ, L. On the Shannon capacity of a graph. *IEEE Trans. Info. Theory*, Springer-Verlag, v. 25, n. 1, p. 1–7, 1979. Citado nas páginas 24, 34, 48, 80 e 90.
- MANCINSKA, L.; SCARPA, G.; SEVERINI, S. A generalization of Kochen-Specker sets relates quantum coloring to entanglement-assisted channel capacity. *IEEE Transactions on Information Theory*, v. 59, n. 6, p. 4025–4032, 2013. Citado na página 48.
- MAYERS, D. Unconditional security in quantum cryptography. *Journal of the ACM*, v. 48, n. 3, p. 351–406, 2001. Citado na página 65.
- MCMAHON, D. *Quantum Computing Explained*. 1. ed. Nova Jersey, Estados Unidos: John Wiley & Sons, 2008. Citado na página 110.
- MEDEIROS, R. et al. *Quantum states characterization for the zero-error capacity*. 2006. arxiv:quant-ph/0611042. Citado nas páginas 38 e 72.
- MEDEIROS, R. et al. Zero-error capacity of quantum channels and noiseless subsystems. In: *IEEE International Telecommunications Symposium*. Fortaleza, Ceará, Brasil: IEEE Press, 2006. p. 900–905. Citado nas páginas 25, 37, 56 e 82.
- MEDEIROS, R. A. C. *Zero-Error Capacity of Quantum Channels*. Tese (Doutorado) — Universidade Federal de Campina Grande – TELECOM Paris Tech, 2008. Citado nas páginas 16, 22, 23, 32, 34, 35, 36, 37, 38, 39, 41, 43, 47, 70, 80, 91, 99 e 128.
- MEDEIROS, R. A. C.; DE ASSIS, F. M. Capacidade erro-zero de canais quânticos e estados puros. In: *Simpósio Brasileiro de Telecomunicações*. Campinas, São Paulo: Sociedade Brasileira de Telecomunicações, 2005. p. 1–6. Citado na página 38.
- MEDEIROS, R. A. C.; DE ASSIS, F. M. Quantum zero-error capacity. *International Journal of Quantum Information*, v. 3, n. 1, p. 135–139, 2005. Citado na página 43.
- MERMIN, N. D. *Quantum Computer Science – An Introduction*. Cambridge, Inglaterra: Cambridge University Press, 2007. Citado na página 116.
- MOHSENI, M. et al. Experimental application of decoherence-free subspaces in an optical quantum-computing algorithm. *Phys. Rev. Lett.*, v. 91, p. 187903, 2003. Citado na página 52.
- NASCIMENTO, E. J.; DE ASSIS, F. M. A numerical solution for the accessible quantum information problem. In: *International Telecommunications Symposium*. Ceará, Brasil: IEEE Press, 2006. p. 495–500. Citado nas páginas 25, 91 e 101.
- NASCIMENTO, E. J.; DE ASSIS, F. M. Soluções numéricas para o cálculo da informação acessível. In: *Workshop-Escola de Computação e Informação Quânticas*. Porto Alegre, Brasil: WECIQ, 2006. p. 265–274. Citado nas páginas 25, 91 e 101.
- NIelsen, M. A. *Quantum Information Theory*. Tese (Doutorado) — University of New Mexico – Albuquerque, New Mexico, USA, 1998. Citado na página 22.

- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge, Inglaterra: Cambridge University Press, 2010. Citado nas páginas 11, 22, 25, 29, 42, 60, 61, 62, 63, 65, 84, 110, 120, 122, 127, 130 e 131.
- QIN, S. et al. Quantum secure direct communication over the collective amplitude damping channel. *Science in China Series G: Physics, Mechanics and Astronomy*, v. 52, n. 8, p. 1208–1212, 2009. Citado na página 81.
- REHACEK, J.; ENGLERT, B.-G.; KASZLIKOWSKI, D. Iterative procedure for computing accessible information in quantum communication. *Phys. Rev. A*, v. 71, p. 054303, 2005. Citado nas páginas 25, 92 e 101.
- SASAKI, M. et al. Accessible information and optimal strategies for real symmetrical quantum sources. *Phys. Rev. A*, v. 59, n. 5, p. 3325–3335, 1999. Citado nas páginas 25 e 92.
- SCHUMACHER, B.; WESTMORELAND, M. Quantum privacy and quantum coherence. *Phys. Rev. Lett.*, v. 80, n. 25, p. 5695–5697, 1998. Citado nas páginas 24, 56, 57, 59, 66 e 72.
- SCHUMACHER, B.; WESTMORELAND, M. D. Sending classical information via noisy quantum channels. *Phys. Rev. A*, v. 56, p. 131–138, 1997. Citado nas páginas 42, 70 e 74.
- SHABANI, A. *Open Quantum Systems and Error Correction*. Tese (Doutorado) — University of Southern California, Califórnia, Estados Unidos, 2009. Citado na página 100.
- SHABANI, A.; LIDAR, D. A. Theory of initialization-free decoherence-free subspaces and subsystems. *Phys. Rev. A*, v. 72, p. 042303, 2005. Citado na página 100.
- SHANNON, C. E. A mathematical theory of communication. *The Bell System Tech. Journal*, v. 27, p. 379–423, 623–656, 1948. Citado nas páginas 29, 121, 122 e 127.
- SHANNON, C. E. Communication theory of secrecy systems. *Bell System Technical Journal*, July, p. 623, 1949. Citado na página 74.
- SHANNON, C. E. The zero error capacity of a noisy channel. *IRE Transactions on Information Theory*, v. 2, n. 3, p. 8–19, 1956. Citado nas páginas 16, 22, 24, 30, 32, 33, 34, 80 e 90.
- SMITH, G. Quantum channel capacities. In: KOUNTOURIS, M. (Ed.). *IEEE Information Theory Workshop*. Cairo, Egito: IEEE, 2010. p. 1–5. Citado nas páginas 23 e 131.
- SUBRAMANIAN, A. et al. Strong and weak secrecy in wiretap channels. In: *International Symposium on Turbo Codes and Iterative Information Processing*. Brest, França: IEEE, 2010. p. 30–34. Citado na página 74.

- SUZUKI, J.; ASSAD, S. M.; ENGLERT, B.-G. *Accessible information about quantum states: An open optimization problem*. Boca Raton, Estados Unidos: Chapman & Hall, 2007. 309-348 p. In *Mathematics of Quantum Computation and Quantum Technology*. Citado nas páginas 25, 92 e 101.
- VIOLA, L. et al. Experimental realization of noiseless subsystems for quantum information processing. *Science*, v. 293, p. 2059–2063, 2001. Citado na página 52.
- WATANABE, S. Private and quantum capacities of more capable and less noisy quantum channels. *Phys. Rev. A*, v. 85, p. 012326, 2012. Citado na página 82.
- WILDE, M. M.; GUHA, S. *Polar codes for degradable quantum channels*. 2011. arxiv/quantum-ph:1109.5346. Citado nas páginas 60 e 81.
- WILLIAMS, C. P. *Explorations in Quantum Computing*. 2. ed. Califórnia, Estados Unidos: Springer, 2011. Citado nas páginas 23, 29 e 110.
- WOLF, S.; WULLSCHLEGER, J. Zero-error information and applications in cryptography. In: *IEEE Information Theory Workshop*. Texas, Estados Unidos: IEEE Press, 2004. p. 1–6. Citado na página 30.
- WOOTTERS, W. K. Two extremes of information in quantum mechanics. In: SOCIETY, I. C. (Ed.). *Workshop on Physics and Computation*. Califórnia, Estados Unidos: IEEE Computer Society, 1993. p. 181–183. Citado nas páginas 25, 84 e 91.
- WYNER, A. D. The wire-tap channel. *The Bell System Technical Journal*, October, p. 1355–1387, 1975. Citado nas páginas 57 e 59.
- XIA, Y. et al. Generation of four-photon polarization-entangled decoherence-free states within a network. *Appl. Phys. B*, v. 99, p. 651–656, 2010. Citado nas páginas 26, 72 e 96.
- XUE, P. Long-distance quantum communication in a decoherence-free subspace. *Phys. Lett. A*, v. 372, p. 6859–6866, 2008. Citado nas páginas 26, 52, 72 e 96.
- XUE, P.; XIAO, Y.-F. Universal quantum computation in decoherence-free subspace with neutral atoms. *Phys. Rev. Lett.*, v. 97, p. 140501, 2006. Citado na página 52.
- ZANARDI, P.; RASETTI, M. Noiseless quantum codes. *Phys. Rev. Lett.*, v. 79, p. 3306, 1997. Citado na página 51.
- ZHANG, X. D.; ZHANG, Q.; WANG, Z. D. Physical implementation of holonomic quantum computation in decoherence-free subspaces with trapped ions. *Phys. Rev. A*, v. 74, p. 034302, 2006. Citado na página 52.

## Apêndice A

# Noções Gerais da Mecânica Quântica

A *Mecânica Quântica* é parte componente da Teoria Quântica e visa dar suporte à uma descrição da natureza quando se leva em consideração a Física das partículas subatômicas, ou Física Quântica. Pode também ser compreendida como um arcabouço matemático para descrever sistemas quânticos isolados, cujo comportamento não pode ser capturado pela Física Clássica (WILLIAMS, 2011). Portanto, para definir algoritmos e construir dispositivos para a Computação Quântica é preciso respeitar os postulados da Mecânica Quântica. Tais postulados especificam como se dá a representação, processamento e medição da informação na Computação e Comunicações Quânticas.

Neste apêndice é apresentada uma síntese dos conceitos básicos da Mecânica Quântica. Tais conceitos encontram-se denotados com a notação de Dirac (DIRAC, 1982), uma forma concisa de representação dos conceitos da Mecânica Quântica, que acarreta em uma simplificação dos cálculos a serem realizados.

Este apêndice está organizado como segue: a Seção A.1 apresenta a noção de qubit, o elemento mais básico de informação em um sistema quântico; a Seção A.2 descreve como é a evolução de um sistema quântico, como os operadores responsáveis por esta tarefa são caracterizados; a Seção A.3 mostra como trazer as informações que estão em um sistema quântico para o nível clássico, por meio da medição projetiva. O formalismo dos operadores densidade, bastante útil para as Comunicações Quânticas, é apresentado na Seção A.4. Os postulados da Mecânica Quântica são enunciados utilizando a notação dos operadores densidade, na Seção A.5. Por fim, os conceitos sobre medição POVM são apresentados na Seção A.6.

Os conteúdos apresentados neste apêndice foram obtidos e organizados a partir de diversos trabalhos: Nielsen e Chuang (NIELSEN; CHUANG, 2010), Kaye et al. (KAYE; LAFLAMME; MOSCA, 2007), Williams (WILLIAMS, 2011), Imre e Balazs (IMRE; BALAZS, 2005) e McMahon (MCMAHON, 2008). Sugere-se que o leitor consulte as obras

mencionadas caso queira expandir os seus conhecimentos sobre os assuntos abordados ou caso queira ver exemplos ilustrativos destes conceitos.

## A.1 Representação da Informação

Nas Computações e Comunicações Clássicas, a unidade básica de informação é o bit (*binary digit*), que assume valor 0 ou 1 (falso ou verdadeiro, respectivamente). A representação de uma informação é feita por meio da sua codificação em uma seqüência finita de bits.

Nas Computações e Comunicações Quânticas, a unidade básica de representação da informação é um sistema quântico de dois estados: o *qubit* (*quantum bit*). Um qubit  $|\psi\rangle$  é representado por meio de um vetor bidimensional em um espaço de Hilbert complexo como mostrado na Definição A.1.

**Definição A.1 (Qubit)** *Um qubit  $|\psi\rangle$  é um vetor bidimensional em um espaço de Hilbert  $\mathcal{H}$  complexo com expressão geral dada por:*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (\text{A.1})$$

em que  $\alpha$  e  $\beta$  são números complexos ( $\alpha, \beta \in \mathbb{C}$ ) e que devem satisfazer à restrição de unitariedade

$$|\alpha|^2 + |\beta|^2 = 1. \quad (\text{A.2})$$

Nos casos em que os valores de  $\alpha$  e  $\beta$  na Eq. (A.1) são diferentes de zero simultaneamente ( $\alpha, \beta \neq 0$ ), diz-se que o qubit está em uma *superposição* destes estados. Quando um qubit está em superposição, não é possível afirmar se este qubit está em  $|0\rangle$  ou  $|1\rangle$  – estados da base computacional. Para os casos particulares em que  $|\alpha| = |\beta|$ , diz-se que o qubit está em uma *superposição igualmente distribuída* de estados.

De acordo com a notação de Dirac (DIRAC, 1982), os estados quânticos (qubits) são representados por *kets* ( $|\cdot\rangle$ ) ou por *bras* ( $\langle\cdot|$ ). Por exemplo, os kets  $|0\rangle$  e  $|1\rangle$ , estados da base computacional correspondentes aos bits 0 e 1, são representados da seguinte forma

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (\text{A.3})$$

e o estado geral de um qubit  $|\psi\rangle$  tem a seguinte notação

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (\text{A.4})$$

$$= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (\text{A.5})$$

$$= \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \quad (\text{A.6})$$

Diz-se que  $\alpha$  e  $\beta$  são as *amplitudes* associadas aos  $|0\rangle$  e  $|1\rangle$ , respectivamente.

O conjugado transposto de um ket  $|\psi\rangle$ , denomina-se *bra* e é denotado da seguinte forma,  $\langle\psi| = |\psi\rangle^\dagger$  em que  $\dagger$  denota duas operações: a operação de conjugado de números complexos e a transposição de uma matriz

$$\langle\psi| = |\psi\rangle^\dagger \quad (\text{A.7})$$

$$= (|\psi\rangle^*)^T \quad (\text{A.8})$$

$$= \begin{bmatrix} \alpha^* \\ \beta^* \end{bmatrix}^T \quad (\text{A.9})$$

$$= \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix}. \quad (\text{A.10})$$

Uma distinção importante em relação à Computação e a Comunicação Clássica é que enquanto um bit pode assumir apenas dois valores distintos, um qubit pode assumir infinitos estados, desde que a restrição de unitariedade, descrita na Eq. (A.1), seja respeitada. Isto significa que a unidade básica de informação quântica é ilimitada, enquanto que a unidade básica de informação clássica é limitada aos valores “verdadeiro” e “falso”.

### A.1.1 Produto Tensorial de Qubits

No caso da Computação e Comunicação Clássicas, um bit é capaz de representar dois valores e um conjunto de  $n$  bits, ou registrador de  $n$  bits, pode representar  $2^n$  valores diferentes, um por vez. Na Computação e Comunicação Quânticas, um registrador de  $n$  qubits também pode armazenar  $2^n$  valores, porém todos ao mesmo tempo, graças à superposição. Este conceito é apresentado na Definição A.2.

**Definição A.2 (Sistemas Multi-Qubit)** *A notação para representar registradores quânticos – denominados sistemas multi-qubit – faz uso do produto tensorial, denotado por  $\otimes$ . O produto tensorial de dois qubits  $|a\rangle$  e  $|b\rangle$ , denotado por  $|a\rangle \otimes |b\rangle = |ab\rangle = |a\rangle |b\rangle$ , é mostrado a seguir*

$$|a\rangle \otimes |b\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{bmatrix} \quad (\text{A.11})$$

$$= \begin{bmatrix} a_1 \cdot |b\rangle \\ a_2 \cdot |b\rangle \\ \dots \\ a_n \cdot |b\rangle \end{bmatrix}. \quad (\text{A.12})$$

Seja  $|\psi\rangle$  o estado de um sistema de 2-qubits. A representação do estado geral de  $|\psi\rangle$  é dada por:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \quad (\text{A.13})$$

$$= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \quad (\text{A.14})$$

$$= \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_2 \beta_2 |11\rangle \quad (\text{A.15})$$

$$= \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \quad (\text{A.16})$$

$$= \alpha'_0 |0\rangle + \alpha'_1 |1\rangle + \alpha'_2 |2\rangle + \alpha'_3 |3\rangle \quad (\text{A.17})$$

$$= \sum_{i=0}^{2^2-1} \alpha'_i |i\rangle. \quad (\text{A.18})$$

É interessante notar que, do passo ilustrado na Eq. (A.16) para o passo da Eq. (A.17), a notação binária foi substituída pela notação decimal – este é um recurso freqüentemente adotado para promover uma simplificação. O estado  $|\psi\rangle$  de dois qubits, contém os estados 0, 1, 2 e 3 ao mesmo tempo, cada um deles com sua amplitude  $\alpha'_i$  associada. Neste caso, se todos os  $\alpha'_i \neq 0$ , então o  $|\psi\rangle$  está em superposição. Caso esta mesma informação fosse ser representada em um Computador Clássico, seriam necessários quatro registradores, ao invés de um único como é feito na Computação Quântica.

De forma genérica, o estado geral de um sistema de  $n$ -qubits pode ser denotado como segue:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \quad (\text{A.19})$$

com  $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$  e a base computacional  $\{|0\rangle, |1\rangle, \dots, |2^n - 1\rangle\}$ .

## A.2 Processamento da Informação

O processamento da informação clássica é realizado por meio da aplicação de operações aos bits que armazenam a informação. Com a informação quântica, o processamento da informação também é realizado por meio de operadores, denotados tipicamente por letras maiúsculas do alfabeto. A formalização de tais operadores é dada na Definição A.3.

**Definição A.3 (Operador Quântico)** *Um sistema quântico isolado originalmente no estado  $|\psi_1\rangle$  evolui para o estado  $|\psi_2\rangle$  por meio da aplicação de um operador quântico  $U$*

$$|\psi_2\rangle = U |\psi_1\rangle. \quad (\text{A.20})$$

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

$$U \cdot U^\dagger = U^\dagger \cdot U = \mathbb{1}, \quad (\text{A.21})$$

em que  $^\dagger$  denota o conjugado transposto e  $\mathbb{1}$  denota a matriz identidade.

Por serem unitários, os operadores quânticos também são reversíveis. Para o estado  $|\psi_2\rangle$ , denotado na Eq. (A.20), existe um operador  $U^\dagger$ , inverso de  $U$ , tal que

$$U^\dagger |\psi_2\rangle = |\psi_1\rangle. \quad (\text{A.22})$$

Várias definições de operadores unitários são possíveis na Computação Quântica. Dentre estas definições, destacam-se as matrizes de Pauli:

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (\text{A.23})$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (\text{A.24})$$

O operador  $X$ , em particular, merece destaque, pois é o análogo quântico da porta *NOT* clássica. Se este operador for aplicado ao estado  $|0\rangle$ , por exemplo, resulta em  $X \cdot |0\rangle = |1\rangle$ . O operador  $X$  e as demais matrizes de Pauli são utilizados em diversos algoritmos da Computação e Comunicação Quânticas.

O operador de Hadamard, denotado por  $H$ , é considerado de grande importância na Computação e Comunicação Quânticas por ser capaz de produzir superposições igualmente distribuídas. A representação matricial deste operador é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (\text{A.25})$$

Se aplicado ao estado  $|1\rangle$ , este operador cria a superposição  $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$ . Os estados  $|-\rangle$  e  $|+\rangle$  (mostrado anteriormente na Eq. (??)) compõem a *base de Hadamard*.

### A.2.1 Produto Tensorial de Operadores

Para que os operadores quânticos possam ser aplicados em sistemas multi-qubit, é necessário que a atuação de operadores também seja estendida por meio do produto tensorial. O produto tensorial de operadores é mostrado na Definição A.4.

**Definição A.4 (Produto Tensorial de Operadores Quânticos)** *Sejam  $A$  e  $B$  dois operadores quânticos de dimensões  $m \times n$  e  $p \times q$ , respectivamente. O produto tensorial  $A \otimes B$  resulta em*

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}. \quad (\text{A.26})$$

O operador resultante,  $A \otimes B$ , possui dimensões  $n \cdot q \times m \cdot p$  e pode então ser aplicado a um produto tensorial de vetores de modo já conhecido. Quando deseja-se denotar o produto tensorial de um operador  $U$  com ele mesmo, abrevia-se a notação para  $U^{\otimes n}$ , em que  $n$  é o número de vezes que o produto tensorial é efetuado.

O operador de Hadamard, em particular, é bastante útil em diversos algoritmos da Computação e Comunicação Quânticas, pois ao criar uma superposição igualmente distribuída de estados, permite que qualquer operador seja aplicado a todos os estados da superposição de forma simultânea, graças ao *paralelismo quântico*. Este paralelismo não é realizado eficientemente pelos computadores clássicos que, para simular uma superposição igualmente distribuída de  $n$  qubits, necessitaria de  $2^n$  registradores clássicos nos quais a operação desejada deveria ser repetida em cada um deles de forma sequencial.

## A.2.2 Operadores de Projeção

Quando se efetua o produto externo de um vetor por ele mesmo define-se um tipo especial de operador denominado *operador de projeção*. Os operadores de projeção quando aplicados a um vetor de um espaço vetorial, projetam este vetor em um subespaço vetorial do espaço original. O subespaço vetorial em questão é definido pelos autovalores do vetor que definiu o operador de projeção.

Uma propriedade importante sobre operadores é a *relação de completude*. A relação de completude estabelece que o somatório de todos os projetores obtidos a partir de vetores de uma base de um espaço vetorial é igual à matriz identidade.

## A.3 Medição da Informação

Um sistema quântico isolado possui sua evolução descrita por transformações unitárias. Mas, para acessar o estado de um sistema quântico é necessário realizar uma tarefa denominada *medição*. A medição é uma “interface” entre os níveis quântico e clássico, caracterizando-se como um meio de extrair informações úteis de qubits após determinado processamento.

No caso clássico, a extração de informação do estado de bits é conceitualmente simples e, portanto, não costuma ser considerada como uma parte do processo de computação. Porém, no caso quântico, a medição é uma tarefa não-trivial, pois afeta o sistema quântico isolado, provocando um *colapso* (redução) no espaço de estados deste sistema após a medição. Em virtude disto, a medição é a única operação irreversível em sistemas quânticos – uma vez que um qubit é medido, não há meios de fazê-lo voltar ao estado anterior à medição (MERMIN, 2007).

A medição a ser apresentada nesta seção é a *medição projetiva*, definida como segue.

**Definição A.5 (Medição Projetiva)** *Seja o conjunto de projetores  $\{M_m\}$  que atuam sobre o espaço de estados de um sistema quântico ou, equivalentemente, o conjunto de todos os projetores geradores pelos vetores uma base. O índice  $m$  refere-se aos possíveis resultados da medição. Se o estado de um sistema quântico for  $|\psi\rangle$ , imediatamente antes da medição, então a probabilidade  $p(m)$  do valor  $m$  ocorrer como resultado da aplicação dos operadores de medição é dada por:*

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle, \quad (\text{A.27})$$

e o estado  $|\psi'\rangle$  do sistema após a medição será

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \quad (\text{A.28})$$

## A.4 Operador Densidade

Os chamados *estados puros* são representados por vetores unitários da base de um espaço de Hilbert. Este tipo de sistema sugere o mínimo de ignorância, pois não há nada mais a determinar senão o estado em si. Porém, existem situações em que esse formalismo não se aplica. Em particular:

1. Um sistema encontra-se em um dos estados puros  $|\psi_1\rangle, |\psi_2\rangle, \dots$  com probabilidades  $p_1, p_2, \dots$ ;
2. Um sistema (denominado  $A$ ) é parte de um sistema maior  $AB$ .

Para tais situações, o formalismo matemático dos *operadores de densidade* é adequado.

**Definição A.6 (Operador Densidade)** *Suponha que um sistema quântico está em um dos  $|\psi_i\rangle$  estados com probabilidade  $p_i$ , em que  $i$  é um índice, ou seja, encontra-se em um agrupamento de estados puros  $\{|\psi_i\rangle, p_i\}$ . O operador densidade que descreve este sistema é definido como*

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|. \quad (\text{A.29})$$

Também chamado de *matriz de densidade* do sistema, o operador de densidade é caracterizado por meio do seguinte teorema.

**Teorema A.1 (Operador Densidade)** *Um operador  $\rho$  é um operador densidade associado a um agrupamento  $\{|\psi_i\rangle, p_i\}$  se, e somente se, satisfaz duas condições:*

1. **Condição do traço.**  $\rho$  possui traço igual a 1;<sup>1</sup>
2. **Condição de positividade.**  $\rho$  é um operador positivo.<sup>2</sup>

<sup>1</sup> O traço de uma matriz é igual a soma dos elementos de sua diagonal principal.

<sup>2</sup> Operador positivo é aquele que, para todo  $|v\rangle \in \mathcal{H}$  (espaço de Hilbert), então  $\langle v|\rho|v\rangle \geq 0$ .

Um sistema quântico que encontra-se em um único estado  $|\psi\rangle$  conhecido é dito ser *puro* e, na linguagem dos operadores densidade, é denotado por  $\rho = |\psi\rangle\langle\psi|$ . Quando isto não acontece, diz-se que  $\rho$  é um estado *misto* (do inglês, *mixed*), ou ainda, uma mistura de estados puros no agrupamento  $\rho$ .

Para ilustrar o conceito de estados mistos, suponha um sistema quântico que encontra-se no estado  $\rho_j$  com probabilidade  $p_j$ . Este estado pode ser denotado por  $\sum_j p_j \rho_j$ , conforme a notação apresentada anteriormente. A partir da Equação (A.29), foi visto que  $\rho_j = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ , em que os  $|\psi_i\rangle$ ,  $i = 1, 2, \dots$ , são estados puros. O estado  $\rho$ , que é dito estar em uma mistura de estados  $\rho_j$  com probabilidade  $p_j$ , é, então, denotado por:

$$\rho = \sum_j p_j \rho_j \quad (\text{A.30})$$

Esta notação é freqüentemente utilizada para determinados problemas, em particular, àqueles ligados aos canais quânticos ruidosos, em que o efeito introduz uma ignorância em relação ao conhecimento do estado quântico.

## A.5 Postulados da Mecânica Quântica

Comumente os postulados da Mecânica Quântica são denotados por meio de vetores de estados, como foi apresentado nas seções anteriores. Porém, também é possível enunciarlos utilizando a notação dos operadores densidade, os quais, em algumas situações, são mais convenientes e acarretam em uma simplificação dos cálculos a serem realizados. A seguir, os quatro postulados da Mecânica Quântica são enunciados por meio desta notação.

**Postulado A.1 (Espaço de Estados de um Sistema Quântico Isolado)** *A um sistema físico isolado está associado um vetor complexo com produto interno (i.e., um espaço de Hilbert) conhecido como espaço de estados do sistema. Este sistema é completamente descrito por um operador densidade, que é um operador positivo  $\rho$  com traço igual a um, atuando sobre o espaço de estados do sistema. Se o sistema quântico está no estado  $\rho_i$  com probabilidade  $p_i$ , então o operador densidade deste sistema é  $\sum_i p_i \rho_i$ .*

A evolução de um sistema quântico fechado é descrito por um operador unitário  $U$ . Se o sistema está inicialmente no estado  $|\psi_i\rangle$  com probabilidade  $p_i$ , depois da atuação de  $U$  estará no estado  $U|\psi_i\rangle$  com probabilidade  $p_i$ . Assim, a evolução segundo o operador densidade é descrita como segue

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger. \quad (\text{A.31})$$

**Postulado A.2 (Evolução de Sistemas Quânticos Isolados)** *A evolução de um sistema quântico isolado é descrito por uma transformação unitária. Isto é, o estado do sistema  $\rho$  no tempo  $t_1$  está associado ao estado  $\rho'$  no tempo  $t_2$  por meio de um operador unitário  $U$  que depende apenas de  $t_1$  e  $t_2$*

$$\rho' = U\rho U^\dagger. \quad (\text{A.32})$$

Medições também são facilmente descritas na linguagem dos operadores densidade. Suponha que a medição é descrita por um conjunto de operadores  $M_m$ . Se o estado inicial era  $|\psi_i\rangle$ , a probabilidade de obter  $m$  após a medição é dada por

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = \text{tr}(M_m^\dagger M_m | \psi_i \rangle \langle \psi_i |). \quad (\text{A.33})$$

De acordo com a Lei das probabilidade total, a probabilidade de obter  $m$  é

$$p(m) = \text{tr}(M_m^\dagger M_m \rho). \quad (\text{A.34})$$

Se o estado antes da medição era  $|\psi_i\rangle$  e uma medição retornou  $m$ , o estado que o sistema assume é dado por

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}}. \quad (\text{A.35})$$

O operador de densidade correspondente é, portanto

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (\text{A.36})$$

**Postulado A.3 (Medição de Sistemas Quânticos)** *Medições projetivas são descritas por uma coleção de operadores de medição  $\{M_m\}$ . Estes operadores atuam no espaço de estados do sistema que está sendo medido. O índice  $m$  refere-se à saída que pode ocorrer na medição. Se o estado do sistema é  $\rho$  antes da medição, a probabilidade de obter  $m$  será*

$$p(m) = \text{tr}(M_m^\dagger M_m \rho), \quad (\text{A.37})$$

e o sistema assumirá o estado

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}. \quad (\text{A.38})$$

Os operadores de medição satisfazem a equação de completude  $\sum_m M_m^\dagger M_m = \mathbb{1}$ .

**Postulado A.4 (Sistemas Quânticos Compostos)** *O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos que o compõem. Se os sistemas são numerados de 1 a  $n$ , e o sistema  $i$  é preparado no estado  $\rho_i$ , então o estado composto será  $\rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$ .*

## A.6 Medição POVM

O terceiro postulado da Mecânica Quântica lida com dois elementos. O primeiro deles é a regra de descrição da estatística da medição, isto é, as probabilidades associadas aos diferentes resultados da medição. O segundo elemento contempla a descrição do estado do sistema após a medição.

Em algumas aplicações, o estado do sistema após a medição não é de tanto interesse, apenas as probabilidades dos resultados possíveis têm maior foco. Nestes casos, o *formalismo POVM* (do inglês, *Positive Operator-Valued Measurement*) é o ferramental teórico mais adequado para análise das medições, ao invés das medições projetivas apresentadas na Seção A.3.

Suponha que uma medição projetiva seja descrita por operadores de medição  $\{M_m\}$  que irão atuar sobre o estado de um sistema  $|\psi\rangle$ . A probabilidade de obter um certo  $m$  ao efetuar a medição é dada por  $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ . Considerando a seguinte definição

$$E_m = M_m^\dagger M_m, \quad (\text{A.39})$$

então a partir do Postulado 3 e de conceitos da Álgebra Linear, é possível verificar que  $E_m$  é um operador positivo, que  $\sum_m E_m = \mathbb{1}$  e que  $p(m) = \langle\psi|E_m|\psi\rangle$ . O conjunto de operadores  $\{E_m\}$  é suficiente para determinar as probabilidades dos diferentes resultados da medição. O operador  $E_m$  é conhecido como *elemento POVM* e o conjunto  $\{E_m\}$  é conhecido como um *POVM* (NIELSEN; CHUANG, 2010, Seção 2.2.6).

## Notas do Apêndice

Neste apêndice foi apresentada uma visão geral dos conceitos da Mecânica Quântica. Inicialmente apresentou-se a noção de qubit, evolução de sistemas quânticos e medição projetiva utilizando a notação de Dirac (DIRAC, 1982), consagrada por simplificar os cálculos a serem realizados. Posteriormente, foram apresentados os operadores densidade e os Postulados da Mecânica Quântica foram enunciados de acordo com este formalismo. Por fim, um outro tipo de medição, denominada Medição *POVM* foi caracterizada.

## Apêndice B

# Noções Gerais da Teoria da Informação

As tarefas de armazenar, transmitir e processar dados constituem uma necessidade crucial para toda a humanidade. Em meados do século *XX*, dada a importância e a necessidade prática de realizar tais tarefas, é que foi proposta a *Teoria da Informação* (COVER; THOMAS, 2006).

Teoria da Informação é um ramo da Matemática Aplicada, da Engenharia Elétrica e da Ciência da Computação. Ela lida com os problemas relacionados à codificação, transmissão e recuperação da informação. As três principais aplicações desta teoria consistem na transmissão de dados por meio de códigos que habilitam a *correção de erros* (acurácia na transmissão), *compressão* (transmissão e armazenamento concisos), e *cifragem* de dados (sigilo e segurança nas transmissões) (DESURVIRE, 2009).

Shannon lançou as bases da Teoria da Informação com a publicação do artigo “*A Mathematical Theory of Communications*” (SHANNON, 1948). Neste trabalho, além de definir precisamente o que é informação e como fazer sua medida, demonstrou a existência de códigos que permitem a comunicação livre de erros, desde que a taxa de transmissão de informação fique abaixo de um parâmetro escalar denominado capacidade do canal.

Recentemente, os conceitos da Teoria da Informação foram atualizados para considerar o paradigma quântico da informação. Diversos desenvolvimentos neste sentido foram realizados e algumas questões ainda permanecem em aberto (HAYASHI, 2006).

Neste apêndice são apresentados alguns conceitos elementares da Teoria da Informação Clássica e Quântica. Em relação à Teoria da Informação Clássica, abordada na Seção B.1, são apresentadas algumas medidas de informação baseadas na entropia de Shannon e é feita a caracterização da capacidade ordinária de canais clássicos. No tocante à Teoria da Informação Quântica, abordada na Seção B.2, são apresentadas algumas medidas de informação quânticas baseadas na entropia de von Neumann e também uma visão geral da caracterização de canais quânticos.

Para os leitores que quiserem aprofundar seus conhecimentos na Teoria da Informação, a obra de Cover e Thomas (COVER; THOMAS, 2006) é recomendada para o cenário clássico, e as obras de Nielsen e Chuang (NIELSEN; CHUANG, 2010, Capítulo 12) e de Desurvire (DESURVIRE, 2009, Capítulo 21) para o cenário quântico. Estas referências também devem ser consultadas pelo leitor caso queira examinar exemplos dos conceitos apresentados.

## B.1 Teoria da Informação Clássica

Como mencionado anteriormente, a Teoria da Informação Clássica teve origem com o trabalho de Shannon (SHANNON, 1948), o qual tinha como principal problema resolver questões práticas ligadas a transmissão de informação via canais ruidosos.

Os resultados mais fundamentais desta teoria são o Teorema para codificação de fonte, o qual estabelece que, na média, o número de bits para representar o resultado de um certo evento é dado pela *entropia*; e o Teorema da codificação para canais ruidosos, que estabelece que a comunicação confiável é possível, ainda que o canal seja ruidoso, desde que a taxa da comunicação fique abaixo de um certo limiar, a chamada capacidade do canal. A capacidade do canal pode ser aproximada em cenários práticos pela utilização de esquemas de codificação e decodificação eficientes (COVER; THOMAS, 2006).

O objetivo geral desta seção é apresentar uma visão geral sobre os conceitos elementares da Teoria da Informação Clássica.

### B.1.1 Medidas de Informação

A Teoria da Informação é baseada na Teoria da Probabilidade e na Estatística. A medida de informação considerada mais importante é a entropia, a informação contida em uma variável aleatória. Há também a informação mútua, que quantifica o que há em comum entre duas variáveis aleatórias. Estas medidas de informação, juntamente com outras enunciadas na literatura, são de extrema importância na criação de códigos para comunicação, na compressão da informação e também no envio de informação sigilosa.

O objetivo desta seção é conceituar algumas destas medidas, bem como algumas regras e desigualdades relacionadas à elas. Para exemplos relativos aos conceitos apresentados, é recomendada a consulta da obra de Cover e Thomas (COVER; THOMAS, 2006, Cap. II).

### B.1.1.1 Entropia, Entropia Conjunta e Entropia Condicional

**Definição B.1 (Entropia de Shannon)** A entropia de Shannon, ou simplesmente entropia, denotada por  $H$ , é uma medida de incerteza de uma variável aleatória. Seja  $X$  uma variável aleatória discreta com alfabeto  $\mathcal{X}$  e função de massa de probabilidade dada por  $p(x) = \Pr[X = x]$ ,  $x \in \mathcal{X}$ . A entropia de  $X$ , denotada por  $H(X)$ , é definida da seguinte forma:

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log p(x) \quad (\text{B.1})$$

Considera-se que o logaritmo é tomado na base 2 e que a entropia é expressa em termos de bits por símbolo. Por convenção, considera-se que  $0 \log 0 = 0$ . É interessante observar que a entropia não possui relação com os valores que a variável assume, apenas depende das probabilidades associadas a estes. Além disso, a entropia é uma medida positiva, ou seja,  $H(X) \geq 0$ .

É possível ampliar a definição de entropia fazendo com que esta compreenda um par de variáveis aleatórias. Tal extensão é denominada *entropia conjunta*.

**Definição B.2 (Entropia Conjunta)** Sejam duas variáveis aleatórias  $X$  e  $Y$  com distribuição conjunta  $p(x, y)$ . A entropia conjunta destas variáveis aleatórias, denotada por  $H(X, Y)$ , é dada por:

$$H(X, Y) = - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y) \quad (\text{B.2})$$

Também define-se a *entropia condicional* como o valor esperado em  $X$  das entropias das distribuições condicionais  $p(y|X = x)$  como segue.

**Definição B.3 (Entropia Condicional)** Sejam duas variáveis aleatórias  $X$  e  $Y$ . A entropia de  $Y$  condicionada à  $X$  é dada por:

$$H(Y|X) = \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) \quad (\text{B.3})$$

$$= - \sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|X = x) \log p(y|X = x) \quad (\text{B.4})$$

$$= - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(y|X = x) \quad (\text{B.5})$$

em que  $p(x, y)$  é a distribuição de probabilidade conjunta das variáveis aleatórias  $X$  e  $Y$ .

Das Eqs. (B.1), (B.2) e (B.5), tem-se que:

$$H(X, Y) = H(X) + H(Y|X) \quad (\text{B.6})$$

### B.1.1.2 Entropia Relativa e Informação Mútua

A *entropia relativa* é uma medida de distância entre duas distribuições, uma maneira de mensurar a ineficiência de se assumir a distribuição  $q$  quando a real distribuição utilizada é  $p$ . Também conhecida como distância de Kullback-Leibler, a entropia relativa é dada conforme a Definição B.4.

**Definição B.4 (Entropia Relativa)** *Sejam duas funções de massa de probabilidade  $p(x)$  e  $q(x)$ . A entropia relativa entes estas duas funções é dada por:*

$$D(p||q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)}. \quad (\text{B.7})$$

Nesta definição considera-se que  $0 \log 0 = 0$ ,  $0 \log \frac{0}{q} = 0$  e que  $p \log \frac{p}{0} = \infty$ .

De acordo com a definição de entropia relativa apresentada, se existe algum  $x \in \mathcal{X}$  tal que  $p(x) > 0$  e  $q(x) = 0$ , então  $D(p||q) = \infty$ . A entropia relativa é sempre não-negativa e é igual a zero quando  $p = q$ .

Uma outra medida é a *informação mútua*, que denota o quanto de informação que uma variável aleatória contém a respeito de outra variável. Ela pode ser compreendida como uma redução da incerteza de  $X$  devido ao conhecimento de  $Y$ .

**Definição B.5 (Informação Mútua)** *Sejam duas variáveis aleatórias  $X$  e  $Y$ . A informação mútua entre estas variáveis, denotada por  $I(X; Y)$ , é dada por:*

$$I(X; Y) = H(X) - H(X|Y) \quad (\text{B.8})$$

$$= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x) \cdot p(y)}. \quad (\text{B.9})$$

A informação mútua é uma medida simétrica, ou seja:

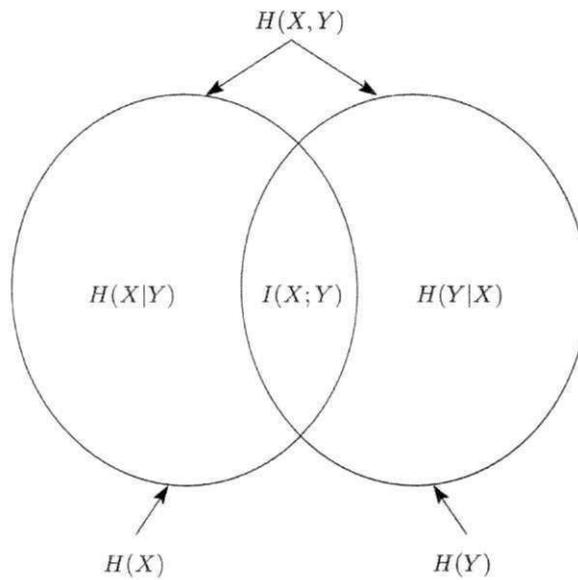
$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y; X) \quad (\text{B.10})$$

Das Equações (B.6) e (B.10), tem-se que a informação mútua entre duas variáveis aleatórias pode ser obtida da seguinte forma:

$$I(X; Y) = H(X) + H(Y) - H(X, Y) \tag{B.11}$$

A relação entre as medidas de entropia e a informação mútua é mostrada na Figura 26.

Figura 26: Relações entre entropia e informação mútua.

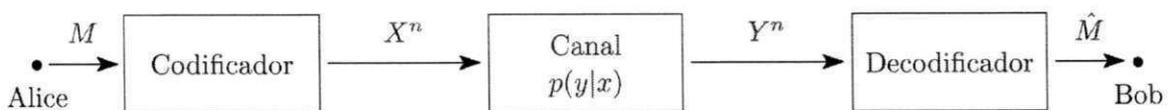


Fonte: Elaborada por Cover e Thomas (COVER; THOMAS, 2006).

### B.1.2 Capacidade Ordinária de Canais Clássicos

No estudo da Teoria da Informação, toma-se como ponto de partida um modelo de um sistema de comunicações digitais ponto-a-ponto, como ilustrado na Figura 27. Neste modelo, um emissor (Alice) deseja enviar uma mensagem  $M$  para um receptor (Bob).

Figura 27: Modelo simplificado de um sistema de comunicações digitais ponto-a-ponto.



Fonte: Elaborada por Cover e Thomas (COVER; THOMAS, 2006).

Neste modelo, o primeiro passo a ser realizado é a codificação, na qual os símbolos da mensagem  $M$  são mapeados para símbolos do canal, resultando em uma *palavra-código*

que é enviada pelo canal. O canal pode ser qualquer meio físico, a exemplo de uma linha telefônica, o ar, a Internet, um disco rígido, etc.

Os dados que trafegam pelo canal estão sujeitos a distorções, ruído e interferências. Em virtude disto, diz-se que a saída do canal é um mapeamento aleatório cuja distribuição de probabilidade depende da seqüência de entrada. Com a seqüência de saída do canal, tenta-se recuperar a mensagem  $M$ , por meio de uma decodificação. Se Bob e Alice concordam sobre o que foi enviado, então diz-se que a comunicação foi bem-sucedida.

O canal é matematicamente representado por uma tripla  $(\mathcal{X}, P_{Y^N|X^N}, \mathcal{Y})$ , em que  $\mathcal{X}$  é o alfabeto de entrada do canal,  $\mathcal{Y}$  é o alfabeto de saída e  $P_{Y^N|X^N}$  é a matriz de probabilidades de transições do canal a cada  $N$  usos. O valor  $P_{Y^N|X^N}(y^N, x^N)$  indica a probabilidade de obter a saída  $y^N$  quando a entrada do canal é um certo  $x^N$ .

Um tipo de canal amplamente abordado é o denominado *canal discreto sem memória* (DMC – *Discrete Memoryless Channel*). Neste tipo de canal, as probabilidades das transições do canal podem ser fatoradas da seguinte maneira:

$$P_{Y^N|X^N}(y^N|x^N) = \prod_{i=1}^N P_{Y_i|X_i}(y_i|x_i). \quad (\text{B.12})$$

Para fins de simplificação, a tripla que representa este tipo de canal é denotada por  $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ .

Um *código*  $(m, n)$  para um canal DMC  $W$  com tripla  $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$  consiste de um conjunto de mensagens  $M = \{1, \dots, m\}$ , um codificador  $f: M \rightarrow \mathcal{X}^n$  e um decodificador  $g: \mathcal{Y}^n \rightarrow \hat{M}$ . A *taxa*  $R$  deste código é definida como sendo a razão entre o logaritmo do número de mensagens possíveis e o número de palavras-código existentes:

$$R = \frac{1}{n} \log m. \quad (\text{B.13})$$

Como mencionado anteriormente, o canal pode introduzir erros, fazendo com que a mensagem recebida seja diferente da original. A *probabilidade média de erro de decodificação* é definida tal como segue:

$$P_e^n = \frac{1}{m} \sum_{i \in M} \Pr \{g(Y^N) \neq i | X^N = f(i)\}. \quad (\text{B.14})$$

Esta probabilidade considera a ocorrência de erros quando todas as mensagens em  $M$  são equiprováveis. Levando estes conceitos em consideração, é possível definir quando uma taxa é alcançável.

**Definição B.6 (Taxa Alcançável)** Diz-se que uma taxa  $R$  é alcançável por um DMC  $W$  com tripla  $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$  se existe uma seqüência  $(\lceil 2^{nR_n} \rceil, n)$  de códigos tais que, para todo  $\epsilon > 0$ :

$$\liminf_{n \rightarrow \infty} R_n > R - \epsilon, \quad (\text{B.15})$$

$$\lim_{n \rightarrow \infty} P_e^n < \epsilon. \quad (\text{B.16})$$

Considerando todas as taxas alcançáveis, Shannon (SHANNON, 1948) caracterizou a capacidade ordinária de um canal clássico, definida como segue.

**Definição B.7 (Capacidade Ordinária de um Canal Clássico)** O valor supremo de todas as taxas alcançáveis por um DMC  $W$  com tripla  $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$  é denominado capacidade ordinária de um canal clássico, denotado pela letra  $C$  e dado como segue:

$$C(W) = \sup \{R : R \text{ é alcançável}\}. \quad (\text{B.17})$$

Shannon (SHANNON, 1948) mostrou que a capacidade ordinária de um canal  $W$  é igual ao máximo da informação mútua  $I(X; Y)$  entre a entrada e a saída do canal, em que esta maximização é tomada sobre todas as distribuições possíveis da entrada, isto é:

$$C(W) = \max_{p(x)} \{I(X; Y)\}, \quad (\text{B.18})$$

em que  $I$  denota a informação mútua entre a saída  $Y$  e a entrada  $X$  entre todas as distribuições da entrada  $p(x)$  possíveis.

## B.2 Teoria da Informação Quântica

A *Teoria da Informação Quântica* pode ser definida como o estudo dos limites máximos possíveis para o processamento da informação, considerando que esta última encontra-se representada de acordo com as leis da Mecânica Quântica (NIELSEN; CHUANG, 2010, Capítulo 12).

O desenvolvimento desta área teve início durante os anos 1960 e 1970, nos quais diversos pesquisadores e engenheiros se questionavam quais tarefas seriam possíveis de serem realizadas ao usar estados quânticos como recursos intermediários (HOLEVO, 1982). Alguns anos mais tarde, com a proposição de protocolos para distribuição quântica de chaves (BENNETT; BRASSARD, 1984) e a concepção de um computador quântico (DEUTSCH,

1985), foi possível vislumbrar e impulsionar a realização de determinadas tarefas consideradas impraticáveis na Teoria da Informação Clássica.

Nas seções a seguir serão apresentados alguns conceitos elementares relacionados a Teoria da Informação Quântica.

### B.2.1 Entropia de von Neumann

Para a Teoria da Informação Clássica, o conceito de *entropia de Shannon*, apresentado na Definição B.1, é de extrema importância, pois quantifica a incerteza sobre uma variável aleatória antes de se descobrir qual o valor de sua realização.

Na Teoria da Informação Quântica, o conceito análogo é o de *entropia de von Neumann*, a qual mensura a incerteza sobre o estado de um determinado sistema físico. Enquanto a entropia de Shannon utiliza distribuições de probabilidade para medir a incerteza sobre uma variável aleatória, a entropia de von Neumann baseia-se nos operadores densidade para descrever a incerteza sobre estados quânticos. A definição formal desta medida de incerteza é dada a seguir.

**Definição B.8 (Entropia de von Neumann)** *A entropia de von Neumann de um estado quântico  $\rho$  é definida como:*

$$S(\rho) = -\text{tr}[\rho \log \rho], \quad (\text{B.19})$$

em que o logaritmo é tomado na base 2 e define-se  $0 \log 0 = 0$ . O logaritmo do operador densidade é calculado a partir da decomposição espectral  $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$  do operador densidade, em que  $\log \rho = \sum_i \log \lambda_i |\psi_i\rangle \langle \psi_i|$ .

Considerando que  $\lambda_i$  são autovalores de  $\rho$  e que  $\{|\psi_i\rangle\}$  formam uma conjunto ortogonal, a entropia de von Neumann também pode ser denotada como:

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i \quad (\text{B.20})$$

A entropia de von Neumann tem algumas propriedades que devem ser destacadas (MEDEIROS, 2008):

1. É uma medida não-negativa. O valor  $S(\rho)$  é igual a zero se, e somente se,  $\rho$  é um estado puro;

2. Em um espaço de Hilbert de dimensão  $d$ , o valor máximo da entropia de von Neumann é  $\log d$ . O estado para o qual  $S(\rho) = \log d$  é  $\rho = \mathbb{I}_d/d$ , o qual corresponde a um estado completamente despolarizado;
3. Assumindo que um sistema composto  $AB$  encontra-se em um estado puro, então  $S(A) = S(B)$ ;
4. Suponha que  $p_i$  são probabilidades e  $\rho_i$  possuem suporte em subespaços ortogonais. Então:

$$S\left(\sum_i p_i \rho_i\right) = H(p) + \sum_i p_i S(\rho_i) \quad (\text{B.21})$$

O conceito de entropia de von Neumann também é aplicável em sistemas conjuntos, quando há condicionamento e também para informação mútua.

**Definição B.9 (Entropia Conjunta de von Neumann)** *A entropia conjunta de von Neumann  $S(A, B)$  para o sistema composto  $AB$  é definida como sendo:*

$$S(A, B) = -\text{Tr}[\rho_{AB} \log \rho_{AB}], \quad (\text{B.22})$$

em que  $\rho_{AB}$  é o operador densidade do sistema  $AB$ .

**Definição B.10 (Entropia Condicional de von Neumann)** *A entropia condicional de von Neumann é definida como:*

$$S(A|B) = S(A, B) - S(B) \quad (\text{B.23})$$

em que  $AB$  é um sistema quântico composto.

**Definição B.11 (Informação Mútua de von Neumann)** *Sejam  $A$  e  $B$  dois sistemas quânticos. A informação mútua de von Neumann para estes dois sistemas é dada por*

$$S(A : B) = S(A) + S(B) - S(A, B) \quad (\text{B.24})$$

$$= S(A) - S(A|B) = S(B) - S(B|A). \quad (\text{B.25})$$

É interessante notar que as definições de entropia conjunta, condicional e informação mútua de von Neumann são uma contrapartida quântica para as medidas de informação relacionadas na Teoria da Informação Clássica.

## B.2.2 Caracterização de Canais Quânticos

A evolução de um sistema quântico fechado  $\rho$  é completamente descrita pela atuação de operadores unitários. Se o sistema permanece fechado, é sempre possível que este retorne ao seu estado inicial. Suponha que o sistema quântico interaja, de alguma maneira, com um sistema físico aberto, chamado de *ambiente*. Adicionalmente, suponha que após esta interação inicial, o sistema volte a ser fechado novamente. Neste cenário, o estado do sistema após a interação é denotado por  $\mathcal{E}(\rho)$ . Porém, diferentemente dos sistemas quânticos fechados, não é sempre o caso que  $\mathcal{E}(\rho)$  pode ser relacionado ao estado inicial  $\rho$  por meio de operações unitárias.

O formalismo adequado para descrever estes cenários é o de *operações quânticas*. Este formalismo é uma ferramenta geral para descrever a evolução de sistemas quânticos sob variadas circunstâncias, a exemplo de mudanças estocásticas nos estados quânticos (NIELSEN; CHUANG, 2010).

Uma operação quântica pode ser vista como um mapa  $\mathcal{E}$  que atua no estado inicial da seguinte forma:

$$\rho' = \mathcal{E}(\rho) \quad (\text{B.26})$$

Dois exemplos de operações quânticas são as operações unitárias e a medição, abordadas conforme o formalismo de operadores de densidade na Seção A.5. Uma operação quântica captura a mudança dinâmica de estado que ocorre como resultado de um processo físico –  $\rho$  é o estado inicial antes do processo,  $\mathcal{E}(\rho)$  é o estado final após a ocorrência do processo, possivelmente sujeito a um fator de normalização (NIELSEN; CHUANG, 2010).

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

1. O valor  $\text{Tr}[\mathcal{E}(\rho)]$  representa a probabilidade que o processo representado por  $\mathcal{E}$  ocorra, considerando  $\rho$  como o estado inicial. Tem-se que  $0 \leq \text{Tr}[\mathcal{E}(\rho)] \leq 1$  para qualquer estado inicial  $\rho$ ;
2. O mapa  $\mathcal{E}$  é convexo-linear no conjunto de operadores de densidade, isto é, para as probabilidades  $\{p_i\}$ :

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i). \quad (\text{B.27})$$

3. O mapa  $\mathcal{E}$  é completamente positivo. Isto significa que se  $\mathcal{E}$  mapeia operadores densidade de  $\mathcal{H}_1$  para operadores densidade de  $\mathcal{H}_2$ , então  $\mathcal{E}(A)$  deve ser positivo

para qualquer operador positivo  $A$ . Mais ainda, se for introduzido um sistema extra  $R$  de dimensão arbitrária, tem-se que  $(\mathbb{1} \otimes \mathcal{E})(A)$  é positivo para qualquer operador positivo  $A$  do sistema combinado  $R\mathcal{H}_1$ , em que  $\mathbb{1}$  denota o mapa identidade no sistema  $R$ .

Em decorrência dos axiomas apresentados, o teorema a seguir pode ser enunciado. Uma prova detalhada do mesmo pode ser encontrada na obra de Nielsen e Chuang (NIELSEN; CHUANG, 2010, pp. 368)

**Teorema B.1 (Mapeamento Quântico)** *O mapa  $\mathcal{E}$  satisfaz os axiomas 1, 2 e 3 se, e somente se:*

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \quad (\text{B.28})$$

para um conjunto de operadores  $\{E_i\}$  que mapeiam o espaço de Hilbert de entrada  $\mathcal{H}_1$  no espaço de Hilbert de saída  $\mathcal{H}_2$ , e  $\sum_i E_i^\dagger E_i \leq \mathbb{I}$ .

A Equação B.28 é conhecida como representação da soma de operadores (OSR – *Operator-Sum Representation*) do canal quântico  $\mathcal{E}$ . Operadores em  $\{E_i\}$  são conhecidos por *elementos de operação* ou por *operadores de Kraus*.

Uma notação alternativa considera que o ambiente inicia em um estado puro  $|0\rangle_E$  e que o estado inicial do sistema é  $\rho_A$ . Nesta notação,  $U$  é uma operação unitária de  $AE$  em  $BE$ , em que  $B$  denota o espaço de saída do sistema inicialmente fechado. A evolução do sistema é descrita como sendo  $\mathcal{E}(\rho_A) = \text{Tr}_E[U \rho_A \times |0\rangle\langle 0|_E U^\dagger]$  (SMITH, 2010).

Independentemente da formalização utilizada, o tipo de mapa apresentado é denominado mapa completamente positivo de preservação do traço ou *canal quântico*.

Um canal quântico pode ser utilizado de diversas maneiras: para transmitir informação clássica; informação clássica, mas de maneira privada; ou informação quântica. Ele pode ser usado sozinho, com emaranhamento compartilhado, ou juntamente a outros canais, clássicos ou quânticos. Para cada uma destas configurações, existe uma capacidade que quantifica o potencial do canal para comunicação. O artigo de Smith (SMITH, 2010) contempla a caracterização de algumas destas capacidades e os recentes desenvolvimentos em relação a este tema.

## Notas do Apêndice

Neste apêndice foi apresentada uma breve fundamentação teórica nos conceitos da Teoria da Informação. Inicialmente, considerando o cenário clássico, algumas medidas

de informação foram apresentadas, bem como a caracterização da capacidade ordinária de canais clássicos. Em relação aos conceitos da Teoria da Informação Quântica, foram apresentadas algumas medidas de informação quânticas baseadas na entropia de von Neumann. Além destas medidas, também foi apresentado o formalismo necessário para a caracterização de canais quânticos.

## Apêndice C

### Artigos Publicados

# Utilização de Subespaços Livres de Descoerência em Comunicações Quânticas Incondicionalmente Seguras

Elloá B. Guedes e Francisco M. de Assis

**Resumo**—Neste trabalho será mostrado como subespaços livres de descoerência em canais quânticos com descoerência coletiva podem ser usados para transmitir informação clássica com sigilo absoluto. Além disso, também será mostrado que, se determinadas condições de simetrias forem garantidas, então a taxa máxima em que estas comunicações sigilosas acontecem iguala-se à capacidade ordinária do canal quântico para o envio de mensagens clássicas. Estes resultados caracterizam uma nova técnica para enviar mensagens clássicas via canais quânticos com segurança incondicional.

**Palavras-Chave**—Subespaços Livres de Descoerência; Capacidade de Sigilo; Segurança Incondicional.

**Abstract**—We show how to use decoherence-free subspaces over collective-noise quantum channels to convey classical information in perfect secrecy. We also show that if some symmetry conditions are guaranteed, the maximum rate on which such secret communications take place is equal to the ordinary capacity of a quantum channel to convey classical information. These results characterize a new technique to convey classical messages via quantum channels with unconditional security.

**Keywords**—Decoherence-Free Subspaces; Secrecy Capacity; Unconditional Security.

## 1. INTRODUÇÃO

A interação de um sistema quântico com o ambiente no qual ele está inserido e a subsequente *descoerência* em função deste acoplamento é uma das principais causas de erros nestes sistemas. Em função da natureza frágil dos estados quânticos, a descoerência é considerada um dos maiores obstáculos para a transmissão de informação coerente [1].

Considerando um contexto criptográfico, a ocorrência de descoerência também causa o vazamento da informação para o ambiente. Se um espião passa a ter acesso ao estado do ambiente, pode vir a adquirir informações sobre uma dada mensagem secreta, por exemplo, o que é altamente indesejado neste cenário. Então, combater a descoerência é uma maneira de colaborar para o envio de informação secreta.

Em sistemas quânticos perfeitamente isolados, não há interação com o ambiente externo e, portanto, a descoerência não ocorre. Porém, construir sistemas desta natureza é uma tarefa altamente complexa e distante dos dias atuais [2]. Uma alternativa que resta é lidar com a descoerência e tentar prover meios de minimizá-la ou evitá-la. Neste sentido, diversas técnicas já vêm sendo propostas, a citar: códigos corretores

de erros quânticos (QECC – *Quantum error-correcting codes*), desacoplamento dinâmico, subespaços livres de descoerência (DFS – *Decoherence-free subspaces*), dentre outros [3].

Em se tratando dos DFS, em particular, utilizam-se simetrias existentes nos operadores de erro para encontrar estados quânticos que são imunes aos efeitos da descoerência. Com isto, uma consequência que se tem é a preservação da coerência. Muitos trabalhos já exploram os DFS neste sentido [4]–[6], inclusive até com implementações experimentais [7]–[10].

Enquanto os trabalhos existentes na literatura focam na preservação da coerência, há um grande potencial no uso de DFS para Comunicações Quânticas. O presente trabalho se propõe a explorar esta perspectiva, tomando como objetivo verificar a adequação dos DFS para troca de mensagens com segurança incondicional.

Como resultado, foi verificado que é possível trocar mensagens clássicas via canais quânticos com segurança incondicional, desde que (i) o canal em uso possua algumas simetrias que possibilitem a existência de DFS; e que (ii) um espião da comunicação tenha acesso *apenas* ao ambiente. Foi possível constatar que a capacidade de enviar sigilo torna-se igual a capacidade de enviar informação clássica ordinária nesse cenário, ou seja, tem-se o caso particular em que a taxa de sigilo é maximal.

Uma das vantagens da estratégia proposta é a possibilidade de facilitar a construção de dispositivos para troca segura de mensagens quânticas. Ao invés de demandar um avanço tecnológico que combata completamente a descoerência, esta estratégia permite que dispositivos sejam construídos sem um total isolamento entre sistema de interesse e ambiente, mas ainda assim sendo capazes de prover comunicação com sigilo absoluto. Isto é bastante factível, especialmente já considerando resultados existentes sobre a utilização de DFS em comunicações [11]–[13], inclusive de longa distância [14].

Para apresentar os resultados mencionados, o presente artigo está organizado como segue. Os conceitos de DFS serão apresentados na Seção II. Após isto, a caracterização e os resultados da aplicação do mesmo em comunicações quânticas incondicionalmente seguras serão apresentados na Seção III. Um exemplo detalhado ilustrando um canal quântico com descoerência coletiva será apresentado na Seção IV. Por fim, as considerações finais serão apresentadas na Seção V.

## II. SUBESPAÇOS LIVRES DE DESCOERÊNCIA

A *descoerência* emerge como resultado de um acoplamento inevitável entre um sistema quântico e o ambiente no qual

ele está inserido. Em função deste acoplamento indesejado, o sistema pode, por exemplo, começar a perder energia para o ambiente, decaindo para um estado de baixa energia e tendo sua fase relativa apagada, o que culmina com a perda da informação [15].

Seja um sistema quântico fechado composto pelo sistema de interesse  $S$  definido sob um espaço de Hilbert  $\mathcal{H}$  e pelo ambiente  $E$ . O hamiltoniano que descreve este sistema é definido como segue:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \quad (1)$$

em que  $\mathbb{1}$  é o operador identidade; e  $\mathbb{H}_S$ ,  $\mathbb{H}_E$  e  $\mathbb{H}_{SE}$  denotam os hamiltonianos do sistema, ambiente e interação sistema-ambiente, respectivamente.

Para prevenir erros, seria ideal fazer  $\mathbb{H}_{SE}$  igual a zero, indicando que sistema e ambiente estão desacoplados e evoluem independentemente e unitariamente de acordo com seus respectivos hamiltonianos  $\mathbb{H}_S$  e  $\mathbb{H}_E$  [2]. Porém, em cenários práticos, tal situação ideal não é possível visto que nenhum sistema é totalmente imune a erros. Então, após isolar o sistema de interesse da melhor maneira possível, deve-se buscar meios realísticos para identificação e correção de erros quando eles ocorrerem, para prevenção de erros quando possível, ou para supressão de erros no sistema [3].

Se algumas simetrias existem na interação entre sistema e ambiente, é possível encontrar "locais seguros" no espaço de Hilbert que não experienciam a descoerência. Seja  $\{A_i(t)\}$  um conjunto de operadores segundo a *representação operator-sum* (OSR), correspondendo à evolução do sistema. Diz-se que a matriz densidade  $\rho_S$  é *invariante* perante os operadores  $\{A_i(t)\}$  se  $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$ . Levando isto em consideração, agora é possível definir os DFS, cujos estados são invariantes apesar de existir um acoplamento não-trivial entre sistema e ambiente:

**Definição 1.** (*Subespaço Livre de Descoerência* [16]) *Um subespaço  $\tilde{\mathcal{H}}$  de um espaço de Hilbert  $\mathcal{H}$  é chamado livre de descoerência com respeito ao acoplamento entre sistema e ambiente se cada estado puro<sup>1</sup> deste subespaço é invariante perante a evolução OSR para quaisquer condição inicial possível do ambiente:*

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \quad (2)$$

Sistemas quânticos definidos sobre DFS são totalmente desacoplados do ambiente e, por esta razão, completamente imunes aos efeitos da descoerência. Códigos quânticos construídos a partir de estados de um DFS são classificados como *códigos quânticos de prevenção de erros* (QEAC – *Quantum Error-Avoiding Codes*), nos quais as tarefas de perturbação e recuperação são triviais [17].

O próximo passo na caracterização dos DFS é especificar as condições onde eles ocorrem. Seja o hamiltoniano da interação entre sistema e ambiente dado por:  $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$ , em que  $\mathbf{S}_j$  e  $\mathbf{E}_j$  são os operadores do sistema e ambiente, respectivamente. Considera-se que os operadores  $\mathbf{E}_j$  são linearmente

independentes. As simetrias requeridas para a existência de um DFS são apresentadas no teorema a seguir. Para uma prova detalhada ou diferentes formulações, ver [2, Sec. 5].

**Teorema 1.** (*Condições para DFS* [18]) *Um subespaço  $\tilde{\mathcal{H}}$  é um DFS se, e somente se, os operadores do sistema  $\mathbf{S}_j$  atuam proporcionalmente à identidade neste subespaço:*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \quad (3)$$

Na prática, identificar uma simetria útil e tirar proveito dela pode ser difícil, pois deve-se: (i) identificar a simetria; e (ii) encontrar os estados imunes à interação. Para facilitar esta tarefa, um método proposto por Choi e Kribs [19] visa encontrar os estados pertencentes a um DFS dado o modelo de erros que atua sobre o sistema quântico de interesse.

Em se tratando dos DFS como QEACs, eles podem ser contrastados com os QECCs em alguns aspectos. Enquanto os QECCs são projetados para corrigir erros apenas após a sua ocorrência, QEACs não possuem habilidades de corrigir erros, uma vez que eles atuam prevenindo-os; QECCs em cenários práticos pertencem à classe dos códigos não-degenerados, ao passo que os QEACs são altamente degenerados; QEACs possuem distância infinita, enquanto os QECCs não-degenerados possuem distância finita; QEACs costumam demandar menos qubits físicos para representar um qubit lógico que os QECCs. Em particular, se a degenerescência atinge o máximo, um QECC se reduz a um QEAC, o que ilustra uma circunstância em que um tipo de código torna-se equivalente ao outro [17].

A ausência de descoerência nos DFS tem se mostrado de grande utilidade em implementações de memórias e algoritmos quânticos. Outras aplicações dos DFS incluem codificação em pontos quânticos, dissipação coletiva, redução de ruído, dentre outras [2], [3].

### III. DFS EM COMUNICAÇÕES QUÂNTICAS INCONDICIONALMENTE SEGURAS

A partir de agora serão consideradas as aplicações do DFS em Comunicações Quânticas. Para tanto, será considerado o uso de *canais quânticos com ruído coletivo*, i.e., um modelo de canais quânticos no qual diversos qubits se acoplam identicamente ao mesmo ambiente, ao passo que sofrem defasamento e dissipação [20]. O foco a ser considerado nesta análise, em particular, será nos aspectos da troca de mensagens seguras.

Para caracterizar a troca segura de mensagens, é necessário caracterizar o modelo de comunicações e a estratégia utilizada pelo espião. Neste trabalho será utilizado um modelo análogo ao proposto Wyner [21], no qual os participantes legítimos (Alice e Bob) utilizam um canal, denominado *canal principal*, e o espião (Eva) utiliza um canal *wiretap*, uma versão degradada do canal principal. A depender do código utilizado pelos participantes legítimos, pode haver sigilo absoluto. Para tanto, a taxa do código utilizado por Alice e Bob deve ficar abaixo da chamada *capacidade de sigilo clássica*, dada por

$$C_S = \max_{\{P\}} \{I(A; B) - I(A; E)\}, \quad (4)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre o símbolos de entrada;  $I$  denota a

<sup>1</sup>Um estado puro é um vetor unitário no espaço de Hilbert  $\mathcal{H}$ .

informação mútua; e,  $A$ ,  $B$  e  $E$  são variáveis aleatórias, representando a entrada do canal principal provida por Alice, a saída do canal principal recebida por Bob, e a saída do canal *wiretap* recebida por Eva, respectivamente.

Mais especificamente, o modelo a ser utilizado neste trabalho consiste na versão quântica do modelo proposto por Wyner [21], adaptada por Cai et al. [22] e por Devetak [23]. Neste modelo, Alice e Bob utilizam um sistema quântico, chamado de *canal quântico principal*, para trocar mensagens, enquanto a espiã Eva tem acesso total ao ambiente no qual este sistema quântico está inserido, conforme ilustrado Figura 1. Há sigilo sempre que a taxa do código quântico utilizado estiver abaixo da *capacidade quântica de sigilo*, denotada por

$$C_S \geq \max_{\{P\}} \{\chi^{\text{Bob}} - \chi^{\text{Eva}}\} \quad (5)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade sobre a entrada, e  $\chi^{\text{Bob}}$  e  $\chi^{\text{Eva}}$  representam as quantidades de Holevo de Bob e Eva, respectivamente.

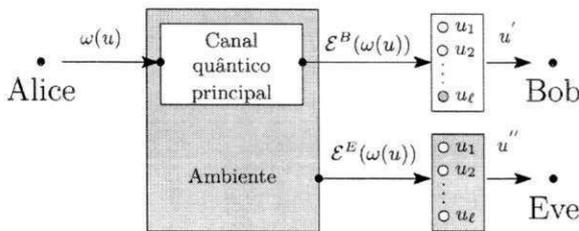


Fig. 1. Idéia geral do canal *wiretap* quântico.

Uma particularidade a ser considerada neste trabalho diz respeito à existência de um DFS no canal quântico principal utilizado por Alice e Bob, cujos estados serão empregados na codificação da mensagem secreta. A formalização do canal em questão é dada a seguir.

**Definição 2.** (*Canal Wiretap Quântico com Ruído Coletivo*) Um canal wiretap quântico com superoperador  $\mathcal{E}$  em um espaço de Hilbert complexo  $\mathcal{H}$  é um canal wiretap quântico como definido por [22, Sec. 3, Def. 1], mas com a particularidade dos operadores de erro  $\{A_i\}$  respeitarem às condições do Teorema 1, dando origem a um DFS  $\tilde{\mathcal{H}} \subset \mathcal{H}$ .

Embora o canal já esteja caracterizado, é necessário definir um código para Alice e Bob se comunicarem. Este código será um QEAC definido sobre  $\tilde{\mathcal{H}}$ , cuja formalização se dá como segue.

**Definição 3.** Seja  $\tilde{\mathcal{H}}$  um DFS gerado pelo conjunto de autovetores  $\{\tilde{k}\}$ , i.e.,  $\tilde{\mathcal{H}} = \text{Span}[\{\tilde{k}\}]$ . Um conjunto de palavras código de comprimento  $n$  para um conjunto de mensagens clássicas  $\mathcal{U}$  é um conjunto de estados de entrada rotulados por mensagens em  $\mathcal{U}$ ,  $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$ , e um processo de decodificação trivial composto por operadores positivos  $\tilde{D}_u$ ,  $u \in \mathcal{U}$  com  $\sum_{u \in \mathcal{U}} \tilde{D}_u \leq \mathbb{1}$ . O par  $(\tilde{K}(\mathcal{U}), \{\tilde{D}_u : u \in \mathcal{U}\})$  é chamado um QEAC de comprimento  $n$  para o conjunto de mensagens  $\mathcal{U}$ . A taxa deste código é igual a  $R = \frac{1}{n} \log |\mathcal{U}|$ .

Usando o código definido, se Alice quer enviar uma mensagem  $u$ , ela irá codificá-la utilizando o QEAC definido sobre  $\tilde{\mathcal{H}}$ , obtendo  $\tilde{k}(u)$ . Quando ela envia o estado  $\tilde{k}(u)$  pelo canal, este irá interagir com o ambiente, que é assumido iniciar no estado  $|0_E\rangle\langle 0_E|$ . Bob então recebe  $\rho_{\text{Bob}}(\tilde{k}(u))$  e Eva recebe  $\rho_{\text{Eva}}(\tilde{k}(u))$ , os quais serão dados por:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_E \left[ \mathcal{E}^{\otimes n}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|) \right], \quad (6)$$

$$\rho_{\text{Eva}}(\tilde{k}(u)) = \text{Tr}_B \left[ \mathcal{E}^{\otimes n}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|) \right]. \quad (7)$$

Uma vez que Alice utilizou um QEAC como na Definição 3, então a simetria dinâmica existente protegeu a informação da interação com o ambiente. Isto significa que a evolução conjunta entre sistema e ambiente aconteceu de maneira desacoplada. Assim, o estado  $\rho_{\text{Bob}}(\tilde{k}(u))$  é dado por:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_E \left[ \mathcal{E}^{\otimes n}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|) \right] \quad (8)$$

$$= \text{Tr}_E \left[ \sum_i A_i \left( \tilde{k}(u) \otimes |0_E\rangle\langle 0_E| \right) A_i^\dagger \right] \quad (9)$$

$$= \text{Tr}_E \left[ \tilde{k}(u) \otimes \rho_E \right] \quad (10)$$

$$= \tilde{k}(u), \quad (11)$$

em que (10) acontece devido à invariância de um estado do DFS perante os operadores OSR. Levando em conta o hamiltoniano do sistema quântico dado em (1) e o fato do sistema de interesse e o ambiente não terem interagido, então é possível garantir que o ambiente sofreu apenas a ação de  $\mathbb{H}_E$ , o qual indica uma evolução unitária restrita ao ambiente. Isto significa que  $\rho_{\text{Eva}}(\tilde{k}(u)) = \rho_E$  em (7) é um estado puro.

Para mostrar que a informação enviada pelo canal, utilizando o código apresentado, é protegida de Eva, o seguinte lema é apresentado.

**Lema 1.** Um QEAC como na Definição 3 sobre um canal wiretap com ruído coletivo como na Definição 2 é um código para wiretap quântico com parâmetros  $(n, |\mathcal{U}|, \lambda, \mu)$  sobre este mesmo canal.

**Demonstração.** Um código para *wiretap* quântico é definido por Cai et al. [22, Sec. 3]. De acordo com estes autores, para que haja sigilo duas condições precisam ser satisfeitas: (i) deve haver uma baixa probabilidade média de erro na decodificação e (ii) a informação acessível média do espião deve ser arbitrariamente pequena.<sup>2</sup> A prova de que o QEAC é equivalente a um código *wiretap* quântico é feita de maneira direta, mostrando pontualmente como cada um destes requisitos são satisfeitos.

Primeiro a probabilidade média de erro na decodificação será analisada. Uma vez que  $\tilde{k}(u)$  pertence a  $\tilde{\mathcal{H}}$ , então é possível garantir que não houve interação com o ambiente. Então,  $\rho_{\text{Bob}} = \tilde{k}(u)$ , como mostrado em (8)-(10). Por consequência, tem-se que o processo de decodificação é trivial e que a mensagem enviada por Alice pode ser perfeitamente recuperada por Bob, visto que há um operador  $\tilde{D}_u$  para cada

<sup>2</sup>A formulação matemática de tais requisitos é apresentada em (9) e (10) no trabalho de Cai et al. [22].

$u \in \mathcal{U}$ . É possível constatar, portanto, que a probabilidade de erro média na decodificação é desprezível.

O segundo passo consiste em analisar a informação média acessível por Eva, que é dada da seguinte forma, em que  $S$  é a entropia de von Neumann:

$$S\left(\sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} \text{Tr}_B \mathcal{E}^{\otimes n}(\tilde{k}(u))\right) - \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} S\left(\text{Tr}_B \mathcal{E}^{\otimes n}(\tilde{k}(u))\right) \leq \mu \quad (12)$$

em que  $\mu$  é um número arbitrariamente pequeno. Para provar este requisito, ao invés de calcular a informação acessível média diretamente, será utilizado um limitante para esta medida, denominado *quantidade de Holevo*, cuja definição é apresentada a seguir:

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_k p_k S(\rho_{\text{Eve},k} \tilde{k}(u)) \quad (13)$$

Em virtude da utilização de estados de um DFS para codificação, é possível afirmar que não houve interação entre sistema e ambiente. Nesse caso, a evolução do ambiente foi governada apenas pelo hamiltoniano  $\mathbb{H}_E$ , o que indica uma evolução unitária dentro do ambiente. Isto significa que o estado final do ambiente é puro. Portanto:

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_k p_k S(\rho_{\text{Eve},k} \tilde{k}(u)) \quad (14)$$

$$= S(\rho_E) - \sum_k p_k S(\rho_{\text{Eve},k} \tilde{k}(u)) \quad (15)$$

$$= 0 - \sum_k p_k S(\rho_{\text{Eve},k} \tilde{k}(u)). \quad (16)$$

Sabe-se que  $\chi^{\text{Eve}} \geq 0$ ,  $S(\rho) \geq 0$  para qualquer  $\rho$ , e que  $p_k \geq 0$ . Então, para assegurar a positividade, este é o caso em que o termo remanescente é igual a zero, implicando em  $\chi^{\text{Eve}} = 0$ . Dado que a quantidade de Holevo é um limitante superior para a informação acessível, tem-se que (12) é igual a zero. Isto conclui a prova.  $\square$

Outra medida de informação que enfatiza a ausência de interação entre sistema e ambiente é a *troca de entropia*, a qual é determinada inteiramente pelo estado inicial do sistema de interesse e pela dinâmica do canal [24]. Neste caso, esta medida é igual a  $S_e = S(\rho_{\text{Eve}}(\tilde{k}(u))) = S(\rho_E) = 0$  porque  $\rho_E$  é um estado puro. É possível concluir, então, que sistema e ambiente estão completamente desacoplados.

Para finalizar a caracterização do uso de QEACs em comunicações incondicionalmente seguras, o último passo consiste em caracterizar a capacidade de sigilo no canal.

**Teorema 2.** *A capacidade de sigilo de um canal wiretap quântico com ruído coletivo  $\mathcal{E}$ , caracterizado como na Definição 2, satisfaz:*

$$C_{S,DFS}(\mathcal{E}) = \max_{\{P\}} [\chi^{\text{Bob}}], \quad (17)$$

em que o máximo é tomado sobre todas as distribuições de probabilidade  $P$  sobre  $\mathcal{U}$ ; e  $\chi^{\text{Bob}}$  é a quantidade de Holevo de Bob.

*Demonstração.* A capacidade de sigilo de um canal quântico arbitrário é dada por (5). Como visto no Lema 1, tem-se que  $\chi^{\text{Eva}} = 0$ . Este resultado é substituído na referida equação. A igualdade é advinda do Teorema de Holevo-Schumacher-Westmoreland [25], [26].  $\square$

Assim, pode-se concluir que é possível realizar comunicações quânticas seguras por meio de canais wiretap quânticos com ruído coletivo quando os operadores de erro satisfazem alguns critérios de simetria. O critério de segurança incondicional é satisfeito, uma vez que  $\chi^{\text{Eve}} = 0$ , significando que nenhuma informação foi capturada por Eva e que, portanto, a comunicação foi realizada em *sigilo absoluto*.

A expressão resultante da capacidade de sigilo para os DFS possui relação com os resultados apresentados por Schumacher e Westmoreland [24]. Estes autores mostram que a habilidade de um canal quântico de enviar informação privada pode ser feita tão grande quanto a habilidade de enviar informação coerente. Uma vez que a informação codificada em um DFS não perde coerência, então a sua probabilidade de enviar informação privada é máxima.

#### IV. EXEMPLO – DEFASAMENTO COLETIVO

Para ilustrar os conceitos e resultados apresentados neste artigo, será apresentado um exemplo detalhado de como enviar informações clássicas através de um canal quântico com defasamento coletivo  $\mathcal{E}$ . Neste canal, os qubits se acoplam ao ambiente de maneira simétrica ao passo que sofrem um processo de defasamento, definido por

$$|0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow e^{i\phi} |1\rangle. \quad (18)$$

Alice quer enviar mensagens clássicas para Bob por meio deste canal. Porém, Eva o espiona, com acesso total ao ambiente. Se ocorre descoerência, então Eva captura informação sobre a mensagem secreta trocada entre eles.

Para minimizar os efeitos da descoerência, Alice e Bob podem tirar vantagem de uma simetria existente no canal. Se eles codificarem as mensagens utilizando estados imunes à descoerência, Eva não é capaz de descobrir nada a respeito da mensagem trocada. Para tirarem proveito desta simetria, Alice e Bob utilizarão o seguinte esquema de codificação:

$$|0_L\rangle = |01\rangle, \quad |1_L\rangle = |10\rangle. \quad (19)$$

Um qubit pode, portanto, ser codificado como  $|\psi_L\rangle = \alpha |0_L\rangle + \beta |1_L\rangle$ . É interessante comprovar que  $|\psi_L\rangle$  não sofre os efeitos da descoerência

$$\mathcal{E}(|\psi_L\rangle) = \mathcal{E}(\alpha |0_L\rangle + \beta |1_L\rangle) \quad (20)$$

$$= \alpha e^{i\phi} |01\rangle + \beta e^{i\phi} |10\rangle \quad (21)$$

$$= e^{i\phi} (\alpha |01\rangle + \beta |10\rangle) \quad (22)$$

$$= e^{i\phi} |\psi_L\rangle \quad (23)$$

$$= |\psi_L\rangle. \quad (24)$$

Este resultado é alcançado pois o fator de fase global  $e^{i\phi}$ , adquirido durante o defasamento, não possui significância física. Isto significa que ambos os estados  $|01\rangle$  e  $|10\rangle$  estão

em  $\tilde{\mathcal{H}}$ , um DFS do espaço de Hilbert  $\mathcal{H}$  no canal quântico com defasamento coletivo.

Supondo, neste exemplo, que as mensagens enviadas por Alice sejam binárias, então  $\mathcal{U} = \{0, 1\}$ , e a codificação se dará da seguinte forma:  $\tilde{k}(0) = |01\rangle$  and  $\tilde{k}(1) = |10\rangle$ . Logo,  $\tilde{K}(\mathcal{U}) = \{|01\rangle, |10\rangle\}$ . Assume-se que os bits 0 e 1 são equiprováveis. Assim, Alice escolhe uma mensagem  $u$ , a codifica como  $\tilde{k}(u)$  e a envia pelo canal.

Uma vez que Alice usou estados do DFS para codificar as mensagens destinadas a Bob, o sistema e o ambiente não interagiram. De acordo com o Lema 1, tem-se que Eva não capturou informação alguma, visto que  $\chi^{\text{Eva}} = 0$ .

Levando em consideração o estado recebido por Bob,  $\rho_{\text{Bob}}(\tilde{k}(u)) = \tilde{k}(u)$ , tem-se que a decodificação é trivial e usa os seguintes POVM:  $\tilde{D}_0 = |01\rangle\langle 01|$  e  $\tilde{D}_1 = |10\rangle\langle 10|$ .

A quantidade de informação acessível a Bob é limitada pela quantidade de Holevo, dada da seguinte forma:

$$\begin{aligned} \chi^{\text{Bob}} &= S\left(\rho_{\text{Bob}}(\tilde{k}(u))\right) - \sum_{u \in \{0,1\}} p_u S(\rho_{\text{Bob},u}) \quad (25) \\ &= S\left(\frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|\right) - \frac{1}{2} \cdot 0 - \frac{1}{2} \cdot 0 \quad (26) \\ &= 1. \quad (27) \end{aligned}$$

Utilizando este resultado em (17), é possível concluir que a taxa de sigilo para este cenário é igual a  $C_{S,DFS}(\mathcal{E}) = 1$  bit por símbolo por uso do canal. Este exemplo ilustra o envio de informação sigilosa codificada em um DFS via um canal quântico ruidoso com taxa de sigilo positiva utilizando um esquema simples de codificação-decodificação.

## V. CONSIDERAÇÕES FINAIS

A partir da análise realizada, é possível concluir que existem certas simetrias nos operadores de erro de um canal quântico que podem ser exploradas para enviar informação clássica com segurança incondicional via canais quânticos. Para tanto, é necessário que (i) estes canais sejam caracterizados como na Definição 2; (ii) o espião tenha acesso apenas ao ambiente; e (iii) a codificação entre as partes legítimas seja feita segundo a Definição 3. Com isto, a informação é codificada em um DFS, o que pode ser visto, conforme Lema 1, como uma instância de um código *wiretap* quântico com a particularidade de que nenhuma informação é capturada pelo adversário.

A capacidade de sigilo de tais canais, mostrada em (17), é igual a capacidade clássica de um canal quântico [25], [26]. Este é um caso particular em que a habilidade de um canal quântico para enviar informação secreta pode ser tão grande quanto a capacidade de enviar informação clássica ordinária.

Apesar das vantagens, os resultados apresentados nesse trabalho não podem ser generalizados para todos os canais quânticos devido ao fato de nem todos eles satisfizerem às condições de um DFS. Zanardi e Rasetti [20] afirmam que as condições para um DFS são satisfeitas apenas em cenários onde há descoerência coletiva. Apesar disso, enquanto processos de codificação propostos para *wiretap* favorecem a generalidade, eles não capturam as características particulares e conseqüências que foram observadas neste trabalho para um tipo específico de canal.

## AGRADECIMENTOS

Os autores agradecem o auxílio financeiro do CNPq e as sugestões dadas por Gilson O. Santos.

## REFERÊNCIAS

- [1] M. Schlosshauer, *Decoherence and the Quantum-to-Classical Transition*, Springer, Ed. Springer, 2007.
- [2] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arxiv: quantum-ph/0301032v1, 2003.
- [3] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449-2460, 2004.
- [4] G. Bin, P. ShiXin, S. Biao, and Z. Kun, "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913-1918, 2009.
- [5] Q. SuJuan, W. QiaoYan, M. LuoMing, and Z. FuChen, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208-1212, 2009.
- [6] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389-1395, 2010.
- [7] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science*, vol. 293, pp. 2059-2063, 2001.
- [8] A. Beige, D. Braun, B. Tregenna, and P. Knight, "Quantum computing using dissipation to remain in a decoherence-free subspace," *Phys. Rev. Lett.*, vol. 85, p. 1762, 2000.
- [9] D. Kielpinski, "A decoherence-free quantum memory using trapped ions," *Science*, vol. 291, p. 1013, 2001.
- [10] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, "Experimental verification of decoherence-free subspaces," *Science*, vol. 290, pp. 498-501, 2000.
- [11] U. Dörner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.
- [12] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.
- [13] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651-656, 2010.
- [14] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859-6866, 2008.
- [15] A. S. Barzegar, "Open quantum systems and error correction," Ph.D. dissertation, University of Southern California, 2009.
- [16] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.
- [17] L.-M. Duan and G.-C. Guo, "Quantum error avoiding codes versus quantum error correcting codes," *Phys. Lett. A*, vol. 255, pp. 209-212, 1999.
- [18] A. Shabani and D. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.
- [19] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.
- [20] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, p. 3306, 1997.
- [21] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 1, pp. 1355-1387, 1975.
- [22] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318-336, 2004.
- [23] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44-55, 2005.
- [24] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence," *Phys. Rev. Lett.*, vol. 80, no. 25, pp. 5695-5697, 1998.
- [25] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131-138, 1997.
- [26] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269-273, 1998.

## ON THE SECURITY OF DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS FOR CLASSICAL INFORMATION CONVEYING THROUGH QUANTUM CHANNELS

ELLOÁ B. GUEDES\* and FRANCISCO M. DE ASSIS†

*IQuanta — Institute for Studies in Quantum Computation and Information,  
Federal University of Campina Grande,  
Av. Aprígio Veloso, 882–58429-140  
Campina Grande, Paraíba, Brazil*

\*elloaguedes@gmail.com

†fmarassis@gmail.com

Received 26 November 2012

Revised 20 April 2013

Accepted 21 April 2013

Published 22 May 2013

Decoherence is one of the main obstacles in quantum information processing. In cryptographic scenarios, in particular, decoherence is not only responsible for the loss of the quantum properties but also for information leakage out to a wiretapper. Given that decoherence must be fought in real-world quantum communication systems, we present a scheme, using decoherence-free subspaces and subsystems, to perform secure classical communications through noisy quantum channels. Using quantum information and wiretap theories, we establish a proof of unconditional security of our scheme. We illustrate our proposal with a non-trivial example and discuss some of its impacts on already existing quantum secure message exchange protocols. Furthermore, we present some up-to-date technologies that can be used for practical implementation of the scheme proposed.

*Keywords:* Decoherence-free subspaces and subsystems; unconditional security; quantum communication.

### 1. Introduction

The principles of quantum mechanics provide novel ways for quantum information transmission and processing, such as quantum computation and quantum communication. Regarding quantum communication, in particular, some intrinsic properties of quantum mechanics enable features that do not have counterpart in classical communication, such as: (i) a qubit has not a definite value until the moment after it is read; (ii) every measurement in a qubit may disturb it; (iii) arbitrary states of qubits cannot be copied; (iv) qubits can be entangled; among others. Thanks to these quantum mechanics principles, in certain scenarios unconditional security can be achieved in quantum information conveying through quantum channels.

In practical quantum communications scenarios, it is important to consider that no system is noiseless. The noise can increase not only the error rate of the sending message, but also the difficulty of finding a wiretapper in a process of security check. For this reason, some good methods have been proposed such as quantum error-correcting codes, dynamical decoupling, decoherence-free subspaces and subsystems (DFS), and so on.<sup>1</sup>

Regarding DFS, in particular, if the error operators that affect the qubits have some symmetries, then the qubits will suffer from the same noise in the quantum channel and that will compensate the resulting effects, keeping the invariability of these states, what means that no decoherence takes place in such subspaces and subsystems.<sup>2</sup>

Taking advantage of such characteristics, we present a scheme to convey classical messages through quantum channels which have DFS in such a way that no information leaks out to a wiretapper. It implies that unconditional security is achieved in such communication despite the existing decoherence. We show how this result impacts in the simplification of some quantum secure direct and deterministic secure quantum communication protocols existing in the literature. Furthermore, we discuss how such scheme can be implemented using current technology.

To present such results, our paper is organized as follows. The DFS are presented in Sec. 2 which also includes an example and a method to find such subspaces and subsystems given the error model. To support the formal proofs of security, some background concepts on quantum privacy and on quantum wiretap channels are introduced in Sec. 3. Our main results about the security of DFS are presented in Sec. 4. Lastly, final remarks are presented in Sec. 5.

*Notations and Conventions* — Here we introduce some notation and conventions that will be used throughout the paper. Logarithms are taken on base 2. Let  $\mathcal{B}(\mathcal{H})$  denote the set of operators in a  $d$ -dimensional Hilbert space  $\mathcal{H}$ . The quantum information theory measure  $S$  denotes the von Neumann entropy;  $\chi$  denotes the Holevo quantity; and  $\mathbb{1}$  denotes the identity matrix. The partial trace over a quantum state is denoted by  $\text{Tr}$ . Moreover, we use the Dirac notation to denote quantum states and operations.

## 2. Decoherence-Free Subspaces and Subsystems

Due to decoherence, a quantum system may begin to lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information it carries may be lost.<sup>3</sup> In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed by the *system of interest*  $S$  defined on a Hilbert space  $\mathcal{H}$  and by the *environment*  $E$ . The Hamiltonian that describes this system is defined as follows:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \quad (1)$$

where  $\mathbb{1}$  is the identity operator; and  $\mathbb{H}_S$ ,  $\mathbb{H}_E$  and  $\mathbb{H}_{SE}$  denote the Hamiltonians of system, environment and system–environment interaction, respectively.

In order to prevent errors, it would be ideal that  $\mathbb{H}_{SE}$  were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians  $\mathbb{H}_S$  and  $\mathbb{H}_E$ .<sup>2</sup> However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system.<sup>1</sup>

If some symmetries exist in the interaction between the system and the environment, it is possible to find a “quiet corner” in the system Hilbert space not experiencing decoherence. Let  $\{E_i(t)\}$  be a set of operators in the operator-sum representation (OSR) corresponding to the evolution of the system. We say that a system density matrix  $\rho_S$  is *invariant* under the OSR operators  $\{E_i(t)\}$  if  $\sum_i E_i(t)\rho_S E_i^\dagger(t) = \rho_S$ . We are now able to define the decoherence-free subspaces whose states are invariant despite a non-trivial coupling between the system and the environment.

**Definition 1 (Decoherence-Free Subspace — Ref. 2).** A subspace  $\tilde{\mathcal{H}}$  of a Hilbert space  $\mathcal{H}$  is called decoherence-free with respect to a system–environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:

$$\sum_i E_i(t)|\tilde{k}\rangle\langle\tilde{k}|E_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \quad (2)$$

Let the Hamiltonian of the system–environment interaction be  $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$ , where  $\mathbf{S}_j$  and  $\mathbf{E}_j$  are the system and environment operators, respectively. We consider that the environment operators  $\mathbf{E}_j$  are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations see Ref. 2 — Sec. 5.

**Theorem 1 (Decoherence-Free Subspace Conditions — Ref. 2).** A subspace  $\tilde{\mathcal{H}}$  is decoherence-free iff the system operators  $\mathbf{S}_j$  act proportional to the identity on the subspace:

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \quad (3)$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system.<sup>2</sup> Knill *et al.* discovered a method for decoherence-free encoding into subsystems instead of into subspaces which is presented below.<sup>4</sup>

**Definition 2 (Decoherence-Free Subsystem — Ref. 4).** Consider a decomposition of the whole Hilbert space  $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ , where  $\dim(\mathcal{H}) =$

$\dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$ . A subspace  $\mathcal{H}^B$  of the full Hilbert space is a *decoherence-free subsystem* if, for a quantum channel  $\mathcal{E}$ ,

$$\forall \rho^A, \forall \rho^B, \exists \tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B, \quad (4)$$

where  $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$ , and  $\rho^B \in \mathcal{B}(\mathcal{H}^B)$ .

In fact,  $\mathcal{H}^B$  is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when  $\dim(\mathcal{H}^A) = 1$ ,  $\mathcal{H}^B$  is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit  $\alpha|0\rangle + \beta|1\rangle$  into  $\alpha|01\rangle + \beta|10\rangle$ . In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose, now that the information is encoded only into the first qubit of the two qubits available, i.e.  $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$ . Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem*.

### 2.1. Example — decoherence-free subspaces and subsystems

The *collective rotation quantum channel* acts on the input as follows:

$$|0\rangle \mapsto \cos \theta |0\rangle + \sin \theta |1\rangle, \quad (5)$$

$$|1\rangle \mapsto -\sin \theta |0\rangle + \cos \theta |1\rangle, \quad (6)$$

where  $\theta$  is the collective rotation parameter which fluctuates over time  $t$ . Two states that are immune to the decoherence caused by this quantum noisy channel are the following Bell states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (7)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (8)$$

Despite being entangled, these states are distinguishable and can be properly obtained at the channel's end using Bell measurements.

If one encodes a generic quantum state  $|\psi\rangle = a|0\rangle + b|1\rangle$  using the mentioned Bell states as logic qubits, i.e.  $|\psi_L\rangle = a|\beta_{00}\rangle + b|\beta_{11}\rangle$ , we have that the resulting encoded state is protected from decoherence since the logic states are immune to the decoherence caused by the collective rotation quantum channel  $\mathcal{E}$  as follows

$$\begin{aligned} \mathcal{E}(|\beta_{00}\rangle) &= \frac{1}{\sqrt{2}} [(\cos \theta |0\rangle + \sin \theta |1\rangle) \otimes (\cos \theta |0\rangle + \sin \theta |1\rangle) \\ &\quad + (-\sin \theta |0\rangle + \cos \theta |1\rangle) \otimes (-\sin \theta |0\rangle + \cos \theta |1\rangle)] \quad (9) \\ &= |\beta_{00}\rangle, \quad (10) \end{aligned}$$

and

$$\begin{aligned} \mathcal{E}(|\beta_{11}\rangle) &= \frac{1}{\sqrt{2}} [(\cos\theta|0\rangle + \sin\theta|1\rangle) \otimes (-\sin\theta|0\rangle + \cos\theta|1\rangle) \\ &\quad + (-\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)] \end{aligned} \quad (11)$$

$$= |\beta_{11}\rangle. \quad (12)$$

Besides the collective rotation quantum channel, the collective amplitude damping and the collective dephasing quantum channels are also examples of noisy quantum channels that have subspaces and subsystems that are immune to the existing decoherence.

## 2.2. A method for obtaining decoherence-free subspaces and subsystems

In practice, identifying a useful symmetry and taking advantage of it can be very difficult.<sup>1</sup> To overcome such problem, Choi and Kribs proposed a systematic method to identify DFS when the model of errors is known.<sup>5</sup>

Let  $\mathcal{E} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$  be a quantum operation. We shall write  $\mathcal{E} \equiv \{E_a\}$  when the error model for  $\mathcal{E}$  is known. The operation elements  $\{E_a\}$  determine  $\mathcal{E}$  through the familiar OSR, i.e.  $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ .

The *noise commutant*  $\mathcal{A}'$  for  $\mathcal{E}$  is the set of all operators in  $\mathcal{B}(\mathcal{H})$  that commute with the operators  $E_a$  and  $E_a^\dagger$ , i.e. every  $B \in \mathcal{B}(\mathcal{H})$  such that  $[B, E_a] = [B, E_a^\dagger] = 0$ . In the unital case ( $\mathcal{E}(\mathbb{1}) = \mathbb{1}$ ), in particular, every  $\sigma \in \mathcal{A}'$  satisfies  $\mathcal{E}(\sigma) = \sigma$ . As a consequence,  $\mathcal{A}'$  is a  $C^*$ -algebra<sup>a</sup> generated by  $E_a$ , which is called *interaction algebra* associated with  $\mathcal{E}$ .

However, not all channels are unital and, because of that, it is necessary to propose a more general approach. In these more general cases, all that can be said for operators  $\sigma \in \mathcal{A}'$  is that they satisfy  $\mathcal{E}(\sigma) = \sigma \mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$ . Given a projection  $P$  in  $\mathcal{B}(\mathcal{H})$ , the goal will be the identification of a subalgebra  $P\mathcal{B}(\mathcal{H})P$  with the algebra  $\mathcal{B}(P\mathcal{H})$ . It is important because such subalgebra enables the obtention of DFS for arbitrary quantum operations. Such objective is achieved by the following theorem.

**Theorem 2 (Due to Ref. 5).** *Let  $\mathcal{E} = \{E_a\}$  be a quantum operation on  $\mathcal{B}(\mathcal{H})$ . Suppose  $P$  is a projection on  $\mathcal{H}$  such that*

$$\mathcal{E}(P) = P\mathcal{E}(P)P. \quad (13)$$

*Then  $E_a P = P E_a P, \forall a$ . Define*

$$\mathcal{A}'_P \equiv \{\sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, P E_a P] = 0 = [\sigma, P E_a^\dagger P]\}, \quad (14)$$

*and*

<sup>a</sup>The formalism of  $C^*$ -algebras (pronounced ‘‘C-star’’) was developed for its use in quantum mechanics to model algebras of physical observables. A  $C^*$ -algebra is a Banach  $*$ -algebra with the additional norm condition  $\|A^* \cdot A\| = \|A\|^2$  for all  $A \in \mathcal{U}$ , where  $\mathcal{U}$  is a complex normed algebra. A complete tutorial on  $C^*$ -algebras can be found in Ref. 6.

$$\text{Fix}_P(\mathcal{E}) \equiv \{\sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma, \quad (15)$$

$$\mathcal{E}(\sigma^\dagger\sigma) = \sigma^\dagger\mathcal{E}(P)\sigma, \mathcal{E}(\sigma\sigma^\dagger) = \sigma\mathcal{E}(P)\sigma^\dagger\}. \quad (16)$$

Then  $\text{Fix}_P(\mathcal{E})$  is a  $C^*$ -algebra inside  $\mathcal{B}(P\mathcal{H})$  that coincides with the algebra  $\mathcal{A}'_P$ ; that is,  $\text{Fix}_P(\mathcal{E}) = \mathcal{A}'_P$ .

Projectors  $P$  satisfying (13) have some properties. For instance, a quantum channel  $\mathcal{E} \equiv \{E_a\}$  acts in a quantum state  $\sigma \in \mathcal{A}'_P$  projecting it into another state  $\sigma'$  in the subspace  $P\mathcal{H}$ . To show this, we have

$$\sigma' = \mathcal{E}(\sigma) \quad (17)$$

$$\stackrel{(i)}{=} \sigma\mathcal{E}(P) \quad (18)$$

$$\stackrel{(ii)}{=} (P\sigma P)(P\mathcal{E}(P)P) \quad (19)$$

$$\stackrel{(iii)}{=} P[\sigma P\mathcal{E}(P)]P \in \mathcal{B}(P\mathcal{H}), \quad (20)$$

where (i) is due to Eq. (15); (ii) is due to Eq. (13) and to the definition of the projector; and (iii) is due to the structure of the algebras  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$ .

In this particular case, we have  $\mathcal{E}(\sigma) = \sigma$  only if  $\mathcal{E}(P) = \mathbb{1}$ . The next step is to show how projectors with such characterization identify the DFS in a quantum operation  $\mathcal{E}$ .

**Theorem 3 (Due to Ref. 5).** *Let  $\mathcal{E}$  be a quantum operation on  $\mathcal{B}(\mathcal{H})$ . Let  $P$  be a projection on  $\mathcal{H}$  that satisfies (13) and let  $P\mathcal{H} = \bigoplus_k (\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$  be the decomposition of  $P\mathcal{H}$  induced by the  $C^*$ -algebra structure of  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$ . Then the subsystems  $\mathcal{H}^{B_k}$ , with  $\dim(\mathcal{H}^{B_k}) > 1$ , are each decoherence-free subsystems for  $\mathcal{E}$ .*

It is possible to say, thus, that the essence of this method consists in the determination of all projectors  $P$  satisfying Eq. (13). From this, the structure of  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$  can be used to determine the states belonging to the DFS. An important remark about this method is its *optimality*, i.e. it is able to obtain *all* projectors satisfying Eq. (13) (vide Ref. 5 — Theorem 3). So far, however, there is no computational procedure already implemented to automatize the execution of this method.

### 2.3. Example — obtaining decoherence-free subspaces and subsystems

To exemplify the method of Choi and Kribs,<sup>5</sup> let  $\mathcal{E}$  be a quantum channel with OSR given by  $\mathcal{E} \equiv \{E_0, E_1, E_2\}$  where

$$E_0 = \alpha(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|), \quad (21)$$

$$E_1 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|), \quad (22)$$

$$E_2 = \beta(|00\rangle\langle 00| + |11\rangle\langle 11| - |01\rangle\langle 01| - |10\rangle\langle 10|), \quad (23)$$

where  $\alpha = \sqrt{1-2q}$ ;  $\beta = \sqrt{q/2}$ , for  $q$  being an scalar,  $0 < q < 1$ . It is possible to see that  $\mathcal{E}(\mathbb{1}) = \sum_{a=0}^2 E_a E_a^\dagger \neq \mathbb{1}$  which implies that the channel  $\mathcal{E}$  is not unital.

In this channel,  $\mathcal{E}$  there is only one qubit  $\rho$  such that  $\mathcal{E}(\rho) = \rho$ . However, such invariance does not come from a DFS, it is a fixed point in the map of  $\mathcal{E}$ .<sup>7</sup> If the action of the projector  $P = |01\rangle\langle 01| + |10\rangle\langle 10|$  is considered then all operators which have support in  $P$  are invariant for  $\mathcal{E}$ , characterizing a DFS. It means that  $\mathcal{E}(\sigma') = \sigma'$  for all  $\sigma' = P\sigma P$ .

To illustrate the action of  $P$  in the characterization of a DFS, let the density operator  $|\psi\rangle\langle\psi|$  be given by

$$|\psi\rangle\langle\psi| = \frac{|01\rangle\langle 01| + |01\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 00|}{2}. \quad (24)$$

Projecting  $|\psi\rangle\langle\psi|$  in the subspace  $P\mathcal{H}$  results in

$$|\psi'\rangle\langle\psi'| = P|\psi\rangle\langle\psi|P \quad (25)$$

$$= \frac{|01\rangle\langle 01|}{2}. \quad (26)$$

Notice that despite  $\mathcal{E}(|\psi\rangle\langle\psi|) \neq |\psi\rangle\langle\psi|$ ,  $|\psi'\rangle\langle\psi'|$  is invariant under the action of the channel  $\mathcal{E}$

$$\mathcal{E}(|\psi'\rangle\langle\psi'|) = \sum_{a=0}^2 E_a |\psi'\rangle\langle\psi'| E_a^\dagger \quad (27)$$

$$= \frac{|01\rangle\langle 01|}{2} + \beta \cdot \frac{|01\rangle\langle 01|}{2} - \beta \cdot \frac{|01\rangle\langle 01|}{2} \quad (28)$$

$$= \frac{|01\rangle\langle 01|}{2}. \quad (29)$$

So, with the aid of the projector  $P$ , it was possible to find a DFS in the channel  $\mathcal{E}$ , enabling communication through it without the undesired effects of the existing decoherence.

### 3. Quantum Privacy and Quantum Wiretap Channels

The privacy in quantum systems was considered by Schumacher and Westmoreland.<sup>8</sup> They conceived a model in which two legitimate parties (Alice and Bob) want to exchange classical messages through a noisy quantum channel. A wiretapper (Eve) has total access to the environment from which she can gather information from the legitimate parties. Alice sends messages which we may take to be the integers selected from a set  $\mathcal{U} = \{1, \dots, |\mathcal{U}|\}$  and maps them into an ensemble  $\{p_u, \rho(u) : u \in \mathcal{U}\}$ . The states in the ensemble are product states referred as *quantum codewords*:

$$\rho(u) = \rho_1(u) \otimes \rho_2(u) \otimes \dots \otimes \rho_n(u), \quad u \in \mathcal{U}, \quad \rho_i(u) \in \mathcal{H}, i = 1, \dots, n. \quad (30)$$

The overall mapping just described is called *quantum block code* of blocklength  $n$  of rate  $R = \frac{1}{n} \log |\mathcal{U}|$ . A decoding scheme for a quantum block code of length  $n$  is a decoding function that univocally associates each *output word*  $\sigma = \mathcal{E}(\rho(u))$  with integers to  $\hat{u} = g(\sigma) \in \mathcal{U}$ . An error occurs if  $g(\mathcal{E}(\rho(u))) \neq u$ . The *quantum privacy* between Alice and Bob is bounded by the coherent information between them.

By taking this formulation in consideration, Cai *et al.* and Devetak could see some similarities with an already existing theory of classical wiretap channels proposed by Wyner.<sup>9-11</sup> Taking this into account, they defined a *secrecy capacity* of *quantum wiretap channels*. Such channels are characterized below.

**Definition 3 (Quantum Wiretap Channels — Refs. 9 and 10).** A memoryless quantum wiretap channel is described by a superoperator  $\mathcal{E}$  in a complex Hilbert space  $\mathcal{H} = \mathcal{H}_{\text{Bob}} \otimes \mathcal{H}_{\text{Eve}}$ . When Alice sends a quantum state  $\rho \in \mathcal{H}^{\otimes n}$ , Bob receives  $\rho_{\text{Bob}} = \text{Tr}_{\text{Eve}}[\mathcal{E}^{\otimes n}(\rho)]$  and Eve receives  $\rho_{\text{Eve}} = \text{Tr}_{\text{Bob}}[\mathcal{E}^{\otimes n}(\rho)]$  where  $n$  is the dimension of the input Hilbert space.

Using a quantum wiretap channel, the security is achieved when a special tailored quantum block code, called *quantum wiretap code*, is used. Two additional parameters are introduced:  $\lambda$  that represents an upper bound to the acceptable error probability and  $\mu$  that represents an upper bound to the maximum accessible information to the adversary. We will refer to a quantum wiretap code by the Four-tuple  $(n, |\mathcal{U}|, \lambda, \mu)$ . The formal characterization of such codes is given as follows.

**Definition 4 (Quantum Wiretap Block Code — Ref. 9).** Consider a quantum block code of block length  $n$  and rate  $R = \frac{1}{n} \log |\mathcal{U}|$  where  $\mathcal{U} = \{1, 2, \dots, |\mathcal{U}|\}$  is a set of classical messages. We denote the set of codewords labeled by the message indices as follows:

$$\Omega(\mathcal{U}) = \{\rho(u) : u \in \mathcal{U}\}. \quad (31)$$

Assume that the decoding function is defined by a POVM  $\{\mathcal{D}_u : u \in \mathcal{U}\}$  where  $\sum_u \mathcal{D}_u \leq \mathbb{1}$ .

Such quantum block code is said to be a quantum wiretap block code with parameters  $(n, |\mathcal{U}|, \lambda, \mu)$  (quantum wiretap code, for short) if the following two conditions are satisfied

$$P_e = 1 - \frac{1}{|\mathcal{U}|} \sum_{u \in \mathcal{U}} \text{Tr}_{\text{Eve}}[\mathcal{E}(\rho(u))\mathcal{D}_u] \leq \lambda, \quad (32)$$

and

$$\frac{1}{n} \left\{ S \left( \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} \text{Tr}_{\text{Bob}}[\mathcal{E}^{\otimes n}(\rho(u))] \right) - \sum_{u \in \mathcal{U}} \frac{1}{|\mathcal{U}|} S(\text{Tr}_{\text{Bob}}[\mathcal{E}^{\otimes n}(\rho(u))]) \right\} < \mu. \quad (33)$$

In the definition of a quantum wiretap code with parameters  $(n, |\mathcal{U}|, \lambda, \mu)$ , Eq. (32) guarantees that the average decoding error probability for Bob is on average smaller

than  $\lambda$ , and Eq. (33) bounds the average accessible information in such a way that the wiretapper can obtain (almost) nothing about the message sent by Alice.<sup>9</sup>

Lastly, the *quantum secrecy capacity* is defined as:

**Definition 5 (Quantum Secrecy Capacity — Refs. 9 and 10).** The secrecy capacity of a quantum channel is the maximum real number  $C_S$  such that for all  $\epsilon, \lambda, \mu \geq 0$  and sufficiently large  $n$  there exists a quantum wiretap code  $(n, |\mathcal{U}|, \lambda, \mu)$  with:

$$C_S < \frac{1}{n} \log |\mathcal{U}| + \epsilon. \quad (34)$$

Despite the previous characterizations assume messages uniformly distributed, the following theorem about the secrecy capacity is a more general result.

**Theorem 4 (Due to Ref. 9 — Sec. 5).** For a quantum wiretap channel  $\mathcal{E}$  as formalized in Definition 3, the quantum secrecy capacity satisfies:

$$C_S(\mathcal{E}) \geq \max_{\{P\}} [\chi^{\text{Bob}} - \chi^{\text{Eve}}], \quad (35)$$

where the maximum is taken over all probability distributions over  $\mathcal{U}$ ; and  $\chi^{\text{Bob}}$  and  $\chi^{\text{Eve}}$  are the Holevo quantities given as follows:

$$\chi^{\text{Bob}} = S(\rho_{\text{Bob}}) - \sum_i p_i S(\rho_{\text{Bob}}(i)), \quad (36)$$

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}) - \sum_i p_i S(\rho_{\text{Eve}}(i)), \quad (37)$$

where  $\rho_{\text{Bob}}$ , the state resulting of the partial trace over the environment, is the state received by Bob; and  $\rho_{\text{Eve}}$  is the final state of Eve.

The quantum secrecy capacity can be understood as the capacity of a quantum channel to convey classical information in perfect secrecy. It is equivalent to the definition given by Schumacher and Westmoreland.<sup>8</sup>

The quantum secrecy capacity defined in Eq. (35) is the quantum analogous of the classical secrecy capacity proposed by Wyner.<sup>11</sup> It is possible to see some similarities between the definitions of quantum and classical secrecy capacities: both bound a decoding error probability and also the amount of information that should be accessible by the wiretapper. However, the quantum case use its own information measures, like the von Neumann entropy and the Holevo quantity. A particular characteristic of the quantum secrecy capacity is that it does not have a single-letter characterization, i.e. it is not computable since it considers all the input states and also all probability distributions over them.<sup>9,10</sup>

#### 4. Security of Decoherence-Free Subspaces and Subsystems

We will now examine the use of DFS in secure quantum communications. To do so, we consider the case that Alice wants to convey secret classical messages through a

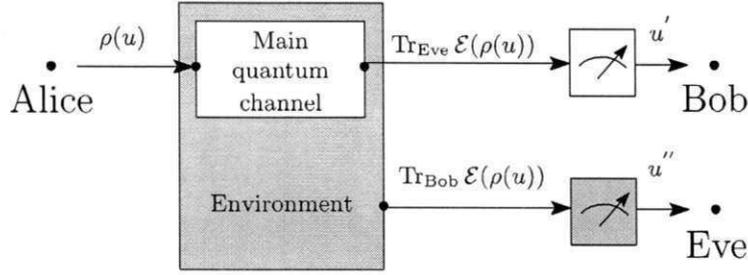


Fig. 1. General idea of the model of communications considered.

quantum channel to Bob. These messages must be protected from a wiretapper Eve that has full access to the environment. This model is shown in Fig. 1.

The channel between Alice and Bob has a DFS and it is presented below.

**Remark 1 (Quantum Wiretap Channel with a DFS).** Let  $\mathcal{E}$  be a quantum wiretap channel as presented in Definition 3. We impose that the input Hilbert space of this channel  $\mathcal{H}$  has a DFS  $\tilde{\mathcal{H}}$ .

Using the DFS existing in this channel it is possible to convey classical messages with unconditional security as will be shown. When Alice wants to send a message to Bob, now she will send a state belonging to the DFS, i.e. she will encode the message into a quantum error-avoiding code (QEAC). The formalism of QEACs is presented in Definition 6.

**Definition 6 (Quantum Error-Avoiding Code — Ref. 12).** Let  $\tilde{\mathcal{H}}$  be a DFS spanned by a set of eigenvectors  $\{|\tilde{\rho}\rangle\}$ , i.e.  $\tilde{\mathcal{H}} = \text{Span}\{|\tilde{\rho}\rangle\}$ . A set of codewords of length  $n$  ( $n = \dim(\tilde{\mathcal{H}})$ ) for a set  $\mathcal{U}$  of classical messages is a set of input states labeled by messages in  $\mathcal{U}$ ,  $\tilde{P}(\mathcal{U}) = \{\tilde{\rho}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$ , and a trivial decoding measurement composed of a set of positive operators  $\tilde{D}_u$ ,  $u \in \mathcal{U}$  with  $\sum_{u \in \mathcal{U}} \tilde{D}_u \leq \mathbb{1}$ . The pair  $(\tilde{P}(\mathcal{U}), \{\tilde{D}_u : u \in \mathcal{U}\})$  is called a QEAC of length  $n$  for the set  $\mathcal{U}$ . The rate of this code is  $\frac{1}{n} \log |\mathcal{U}|$ .

So, using a QEAC  $(\tilde{P}(\mathcal{U}), \{\tilde{D}_u : u \in \mathcal{U}\})$ , when Alice sends the message  $u \in \mathcal{U}$  encoded in the state  $\tilde{\rho}(u)$  through the communication channel, this state interacts with the environment which is assumed to start in a pure state  $(|0_E\rangle)$ .<sup>b</sup> Bob then receives  $\rho_{\text{Bob}}(\tilde{\rho}(u))$  and Eve receives  $\rho_{\text{Eve}}(\tilde{\rho}(u))$ , which are given by:

$$\rho_{\text{Bob}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Eve}}[\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle\langle 0_E|)], \quad (38)$$

$$\rho_{\text{Eve}}(\tilde{\rho}(u)) = \text{Tr}_{\text{Bob}}[\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle\langle 0_E|)]. \quad (39)$$

Since Alice used a QEAC, then the existing dynamical symmetry protected the quantum information from the interaction with the environment. It means that the joint evolution of the system and the environment occurred in a decoupled way.

<sup>b</sup>This is a clear assumption since we can always imagine that a “local” environment in a mixed state is just part of a larger system in a pure entangled state.<sup>8</sup>

Hence, the state  $\rho_{\text{Bob}}(\tilde{\rho}(u))$  is given by:

$$\rho_{\text{Bob}}(\tilde{\rho}(u)) = \text{Tr}_E[\mathcal{E}(\tilde{\rho}(u) \otimes |0_E\rangle\langle 0_E|)] \quad (40)$$

$$= \text{Tr}_{E^c} \left[ \sum_a E_a(\tilde{\rho}(u) \otimes |0_E\rangle\langle 0_E|) E_a^\dagger \right] \quad (41)$$

$$= \text{Tr}_{E^c}[\tilde{\rho}(u) \otimes \rho_E] \quad (42)$$

$$= \tilde{\rho}(u), \quad (43)$$

where Eq. (42) is due to the invariance of a state of the DFS under the OSR operators. We will now show how such QEAC protects the information conveyed through the channel from a wiretapper.

**Lemma 1.** *A QEAC is a quantum wiretap code with parameters  $(n, |\mathcal{U}|, \lambda = 0, \mu = 0)$ .*

**Proof.** The proof is straightforward. We have to prove that the QEAC satisfies the criteria of Eqs. (32) and (33).

Let us first analyze the average decoding error probability. Since  $\tilde{\rho}(u)$  is in  $\tilde{\mathcal{H}}$ , it did not interact with the environment. So,  $\rho_{\text{Bob}} = \tilde{\rho}(u)$  as shown in Eqs. (40)–(43). It turns out that the decoding is trivial and that the message sent by Alice can be perfectly recovered since there is a decoding measurement  $\tilde{D}_u$  for every  $u \in \mathcal{U}$ . We can see, thus, that there is a negligible average decoding error probability for Bob, what implies  $\lambda = 0$ , and the first criterion is satisfied.

Then we proceed to analyze Eq. (33). Recall that it is the average accessible information by Eve which is bounded by the Holevo quantity, defined in Eq. (37). We will try obtain the Holevo quantity first.

Despite the state of the environment  $\rho_E$  (vide Eq. (42)) is not known, the fact that Alice and Bob used states from a DFS guaranteed that the interaction Hamiltonian  $\mathbb{H}_{SE}$  did not govern the joint evolution of system and environment. Instead of that, each system evolved completely unitary under its own Hamiltonian, i.e. the environment suffered only the action of  $\mathbb{H}_E$ . It implies that the environment ended in a pure state. Using this result to calculate the Holevo quantity, we have:

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{\rho}(u))) - \sum_{u \in \mathcal{U}} p_u S(\rho_{\text{Eve},u} \tilde{\rho}(u)), \quad (44)$$

$$= S(\rho_E) - \sum_{u \in \mathcal{U}} p_u S(\rho_{\text{Eve},u} \tilde{\rho}(u)), \quad (45)$$

$$= 0 - \sum_{u \in \mathcal{U}} p_u S(\rho_{\text{Eve},u} \tilde{\rho}(u)). \quad (46)$$

It is well known that the Holevo quantity  $\chi^{\text{Eve}} \geq 0$ . Since  $S(\rho) \geq 0$  for any  $\rho$ , and that the probabilities  $p_u \geq 0$  for any  $u$ , then it is the case that the remaining term is zero. Thus,  $\chi^{\text{Eve}} = 0$ . Since the Holevo quantity is an upper bound of the accessible

information then Eq. (33) is also equal to zero, what leads to  $\mu = 0$ . This concludes the proof.  $\square$

We can now characterize the secrecy capacity of quantum wiretap channels with DFS.

**Theorem 5.** *The secrecy capacity of a quantum channel  $\mathcal{E}$  as described in Remark 1 is*

$$C_S(\mathcal{E}) = \max_{\{P\}}[\chi^{\text{Bob}}], \quad (47)$$

where the maximum is taken over all probability distributions  $P$  over  $\mathcal{U}$ ; and  $\chi^{\text{Bob}}$  is the Holevo quantity given in Eq. (36).

**Proof.** Let a QEAC  $(\tilde{P}(\mathcal{U}), \{\tilde{D}_u : u \in \mathcal{U}\})$  be used over the channel  $\mathcal{E}$ . As proved in Lemma 1, it was shown that  $\chi^{\text{Eve}} = 0$ . Firstly, this fact is substituted in Eq. (35). The equality is due to the Holevo–Schumacher–Westmoreland theorem (vide Refs. 13 and 14).  $\square$

We can therefore conclude that it is possible to perform unconditionally secure quantum communications through wiretapped collective noise quantum channels. The unconditional security criterion is satisfied since  $\chi^{\text{Eve}} = 0$ , meaning that no information was gathered by Eve and that the communication was carried out in perfect secrecy.

#### 4.1. Example

The phenomenon of energy dissipation when conveying a quantum state is modeled by the *collective amplitude damping quantum channel*. This channel has the following OSR

$$\mathcal{E}(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger, \quad (48)$$

where the operation elements  $E_0$  and  $E_1$  are as follows

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \quad (49)$$

where  $\gamma$  is the damping rate which can be thought of as the probability of losing a photon. The input Hilbert space  $\mathcal{H}$  of this quantum channel has three DFS of different dimensions

$$\tilde{\mathcal{H}}_1 = \{|1\rangle\}, \quad (50)$$

$$\tilde{\mathcal{H}}_2 = \left\{ |00\rangle, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}, \quad (51)$$

$$\tilde{\mathcal{H}}_3 = \left\{ \frac{1}{\sqrt{6}}(-2|001\rangle + |010\rangle + |100\rangle), \frac{1}{\sqrt{2}}(|011\rangle - |101\rangle), |000\rangle \right\}. \quad (52)$$

Let us consider the DFS of dimension 3. Let the three quantum states of this DFS be  $\tilde{\rho}_1, \tilde{\rho}_2$  and  $\tilde{\rho}_3$ , respectively. Alice and Bob can build the following QEAC to communicate in perfect secrecy. Let the alphabet  $\mathcal{U}$  be  $\mathcal{U} = \{1, 2, 3\}$  and let the encoding be as follows  $\tilde{P}(\mathcal{U}) = \{1 \mapsto \tilde{\rho}_1, 2 \mapsto \tilde{\rho}_2, 3 \mapsto \tilde{\rho}_3\}$ . The decoding is composed by the following POVM:  $\tilde{D}_i = |\tilde{\rho}_i\rangle\langle\tilde{\rho}_i|$ ,  $1 \leq i \leq 3$ . Let also  $\tilde{D}_{\text{error}}$  be given by  $\tilde{D}_{\text{error}} = \mathbb{1} - \sum_{i=1}^3 \tilde{D}_i$ .

Using the QEAC defined, Alice and Bob can communicate in a rate up to  $\log_2 3 \approx 1.585$  bits per symbol per channel using over a noisy quantum channel subject to collective amplitude damping with unconditional security. It is important to emphasize that they do not need additional resources as entanglement, private classical channels, secret keys nor previous secret communication. Since the rate achieved by the QEAC is higher than 1, it also shows that the scheme proposed is non-trivial.

## 5. Final Remarks

In this paper, we proposed a scheme to perform unconditionally secure communication over noisy quantum channels using their decoherence-free subspaces or subsystems, when possible. The security of this proposal was established by using quantum information and wiretap theories.

In practice, given the error model of the channel, one can identify its potential to use the proposed scheme by verifying the existence of a DFS using the method proposed by Choi and Kribs<sup>5</sup> showed in Sec. 2.2. If such DFS exists, then a QEAC must be build and used as described in Sec. 4.

By applying such results in the simplification of some existing quantum protocols for secure communications,<sup>15–17</sup> the proposed scheme decreased not only the number of communications to perform the secure message exchange, but also the efforts on eavesdropping checking and on the complexity of the encoding–decoding process. A complete description of such results can be obtained in Ref. 18.

Regarding its feasibility for practical implementation, some developments already reported in the literature show implementations of quantum channels that have DFS.<sup>19–21</sup> The work of Xue, in particular, must be emphasized because it already considers the use of DFS in long-distance communication.<sup>22</sup> All the mentioned quantum channels are suitable for the scheme proposed. Even when the conditions for the existence of DFS are not completely satisfied, our scheme can be adapted by following the procedures shown in Ref. 3.

The advantage of the proposed scheme is that no additional resources are required as entanglement, private classical channels, secret keys nor previous secret communication. However, it relies on the existence of a DFS. The quantum channels with collective decoherence, in particular, favors its use.

In future works, we aim at investigating more general conditions to perform unconditionally secure communications over noisy quantum channels.

## Acknowledgments

We acknowledge the financial support rendered by the Brazilian funding agencies CAPES and CNPQ and also by the project QUANTA/RENASIC/FINEP.

## References

1. M. S. Byrd *et al.*, *J. Modern Optics* **51** (2004) 2449.
2. D. A. Lidar and K. B. Whaley, Decoherence-free subspaces and subsystems, arXiv:quant-ph/0301032v1.
3. A. Shabani and D. A. Lidar, *Phys. Rev. A* **72** (2005) 042303.
4. E. Knill *et al.*, *Phys. Rev. Lett.* **84** (2000) 2525.
5. M.-D. Choi and D. W. Kribs, *Phys. Rev. Lett.* **96** (2006) 050501.
6. K. Davidson, *C\*-Algebras by Example* (Amer. Math. Soc., Providence, RI, 1996).
7. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
8. B. Schumacher and M. Westmoreland, *Phys. Rev. Lett.* **80** (1998) 5695.
9. N. Cai *et al.*, *Problems Inform. Transmission* **40** (2004) 318.
10. I. Devetak, *IEEE Trans.* **51** (2005) 44.
11. A. D. Wyner, *The Bell Syst. Tech. J.* **10** (1975) 1355.
12. L.-M. Duan and G.-C. Guo, *Phys. Lett. A* **255** (1999) 209.
13. B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56** (1997) 131.
14. A. S. Holevo, *IEEE Trans. Info. Theor.* **4** (1998) 269.
15. G. Bin *et al.*, *Sci. China Ser. G: Phys. Mech. Astron.* **52** (2009) 1913.
16. S. Qin *et al.*, *Sci. China Ser. G: Phys. Mech. Astron.* **52** (2009) 1208.
17. H.-K. Dong *et al.*, *Int. J. Quantum Inform* **8** (2010) 1389.
18. E. B. Guedes and F. M. de Assis, Enhancing quantum protocols with the security of decoherence-free subspaces and subsystems, in *Proc. 4th Workshop-School in Quantum Computation and Information* (2012).
19. U. Dorner *et al.*, *Quantum Info. Comput.* **8** (2008) 468.
20. G. Jaeger and A. Sergienko, *Int. J. Theor. Phys.* **47** (2008) 2120.
21. Y. Xia *et al.*, *Appl. Phys. B* **99** (2010) 651.
22. P. Xue, *Phys. Lett. A* **372** (2008) 6859.

# Quantum Zero-Error Secrecy Capacity

Elloá B. Guedes and Francisco M. de Assis

**Abstract**—Aiming at transmitting secret classical messages through noisy quantum channels, the present work proposes quantum codes in which no decoding errors occur nor information leakage out to a wiretapper. These codes are based on error-free codes and on decoherence-free subspaces and subsystems. A consequence of such proposition is the rise of the *quantum zero-error secrecy capacity* (ZESC), the maximum rate in which information can be transmitted through a noisy quantum channel using such codes with unconditional security. We also propose a graph-theoretic approach to obtain ZESC, and show that, in certain situations, this capacity is single-letter characterized.

**Index Terms**—Decoherence-Free Subspaces and Subsystems; Quantum Secrecy Capacity; Quantum Zero-Error Capacity.

## I. INTRODUCTION

QUANTUM *information theory* deals with problems related to information treatment and transmission through quantum channels. Its research areas include the study of quantum error-correction codes, quantum entanglement, and quantum channel capacity [1]. The *capacity* is defined as the transmission rate optimized over all possible quantum codes such that decoding errors vanish in the limit of asymptotically many uses of the channel.

In the case of noisy channels, the interaction with the environment and the subsequent *decoherence* is a source of errors and information leakage out to a wiretapper. Then, the *secrecy capacity* of a noisy quantum channel is the transmission rate optimized over all possible *wiretap codes* such that decoding errors between legitimate parts and information leakage to a wiretapper vanish in the limit of asymptotically many uses of the channel [2] [3].

For overcoming decoherence, some good methods have been proposed such as quantum error-correcting codes, dynamical decoupling, decoherence-free subspaces and subsystems (DFS), and so on [4]. Regarding DFS, in particular, if the error operators that affect the qubits have some symmetries, then the qubits will suffer from the same noise in the quantum channel and that will compensate the resulting effects, keeping the invariability of these states, what means that no decoherence takes place in such subspaces and subsystems [5].

Taking advantage of DFS to prevent information leakage out, Guedes and de Assis [6], [7] showed that quantum codes built with states from a DFS are instances of wiretap codes with the particularity that no information is gathered

by the wiretapper. They also showed that the rate of these codes can reach the maximum rate of the channel to send ordinary classical information, i.e., the Holevo-Schumacher-Westmoreland (HSW) capacity [8], [9].

Medeiros et al. [10] proposed a method to find DFS in error-free quantum codes, based on a technique for obtaining DFS created by Choi and Kribs [11]. Based on such ideas, the present paper characterizes a strategy to obtain (when possible) wiretap codes from error-free quantum codes, with the particularity that no decoding errors occur nor information leakage. It results in a new concept: the *quantum zero-error secrecy capacity* (ZESC), defined as the maximum rate that information can be conveyed through a noisy quantum channel using such codes and with unconditional security.

We show a graph-theoretic approach to ZESC, taking advantage of a similar procedure to the quantum zero-error capacity [12]. We also show that ZESC, in certain situations, has a single-letter characterization. It contrasts with the secrecy capacity of quantum channels which, so far, has been considered as not having a computable version [2].

The rest of this paper is structured as follows. Section II introduces the concepts regarding decoherence-free subspaces and subsystems as well as a method for obtaining them; Section III recalls the results of Guedes and de Assis [6], [7] on the use of DFS to build wiretap codes; Section IV introduces the theory of quantum zero-error capacity, including its graph theoretical approach, and the relation between error-free codes and DFS. Our main results are presented in Section V in which ZESC is formalized, its relation with Graph Theory is established, and detailed examples are presented. Relations of such propositions with already existing works in the literature are discussed in Section VI. Lastly, final remarks are presented in Section VII.

### A. Notation and Conventions

Here we introduce some notation and conventions that will be used throughout the paper. Logarithms are taken on base 2. Let  $\mathcal{B}(\mathcal{H})$  denote the set of operators in a  $d$ -dimensional Hilbert space  $\mathcal{H}$ . The quantum information theory measure  $S$  denotes the von Neumann entropy; and  $\chi$  denotes the Holevo quantity.  $\text{Tr}$  denotes the partial trace over a quantum state. Moreover, we use the Dirac notation to denote quantum states and operations.

## II. DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

Due to decoherence, a quantum system may begin to lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information

Elloá B. Guedes and Francisco M. de Assis. IQunta – Institute for Studies in Quantum Computation and Information, Federal University of Campina Grande, Av. Aprígio Veloso, 882 – 58429-140, Campina Grande – Paraíba – Brazil. E-mails: {elloaguedes,fmarassis}@gmail.com. This work was supported by the Brazilian funding agencies CAPES and CNPq.

it carries may be lost [13]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed by the *system of interest*  $S$  defined on a Hilbert space  $\mathcal{H}$  and by the *environment*  $E$ . The Hamiltonian that describes this system is defined as follows

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE} \quad (1)$$

where  $\mathbb{1}$  is the identity operator; and  $\mathbb{H}_S$ ,  $\mathbb{H}_E$  and  $\mathbb{H}_{SE}$  denote the Hamiltonians of system, environment and system-environment interaction, respectively.

In order to prevent errors, it would be ideal that  $\mathbb{H}_{SE}$  were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians  $\mathbb{H}_S$  and  $\mathbb{H}_E$  [5]. However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system [4].

If some symmetries exist in the interaction between the system and the environment, it is possible to find a “quiet corner” in the system Hilbert space not experiencing decoherence. Let  $\{A_i(t)\}$  be a set of operators in the *operator-sum representation* (OSR) corresponding to the evolution of the system. We say that a system density matrix  $\rho_S$  is *invariant* under the OSR operators  $\{A_i(t)\}$  if  $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$ . We are now able to define the decoherence-free subspaces whose states are invariant despite a non-trivial coupling between the system and the environment.

**Definition 1.** A subspace  $\tilde{\mathcal{H}}$  of a Hilbert space  $\mathcal{H}$  is called *decoherence-free* with respect to a system-environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0) \quad (2)$$

Let the Hamiltonian of the system-environment interaction be  $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$ , where  $\mathbf{S}_j$  and  $\mathbf{E}_j$  are the system and environment operators, respectively. We consider that the environment operators  $\mathbf{E}_j$  are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations see [5, Sec. 5].

**Theorem 1.** (Decoherence-Free Subspace Conditions) A subspace  $\tilde{\mathcal{H}}$  is decoherence-free iff the system operators  $\mathbf{S}_j$  act proportional to the identity on the subspace:

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}} \quad (3)$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system [5]. Knill et al. [14] discovered a method for decoherence-free encoding into subsystems instead of into subspaces which is presented below.

**Definition 2.** (Decoherence-Free Subsystem) Consider a decomposition of the whole Hilbert space  $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ , where  $\dim(\mathcal{H}) = \dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$ . A subspace  $\mathcal{H}^B$  of the full Hilbert space is a decoherence-free subsystem if

$$\forall \rho^A, \forall \rho^B, \exists \tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B \quad (4)$$

where  $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$ , and  $\rho^B \in \mathcal{B}(\mathcal{H}^B)$ .

In fact,  $B$  is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when  $\dim(\mathcal{H}^A) = 1$ ,  $B$  is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit  $\alpha|0\rangle + \beta|1\rangle$  into  $\alpha|01\rangle + \beta|10\rangle$ . In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose now that the information is encoded only into the first qubit of the two qubits available, i.e.,  $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$ . Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem* [15].

#### A. A Method for Obtaining DFS

In practice, identifying a useful symmetry and taking advantage of it can be very difficult [4]. To overcome such problem, Choi and Kribs [11] proposed a systematic method to identify DFS when the model of errors is known.

Let  $\mathcal{E} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$  be a quantum operation. We shall write  $\mathcal{E} \equiv \{E_a\}$  when the error model for  $\mathcal{E}$  is known. The operation elements  $\{E_a\}$  determine  $\mathcal{E}$  through the familiar OSR, i.e.,  $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ .

The *noise commutant*  $\mathcal{A}'$  for  $\mathcal{E}$  is the set of all operators in  $\mathcal{B}(\mathcal{H})$  that commute with the operators  $E_a$  and  $E_a^\dagger$ . In the unital case ( $\mathcal{E}(\mathbb{1}) = \mathbb{1}$ ), every  $\sigma \in \mathcal{A}'$  satisfies  $\mathcal{E}(\sigma) = \sigma$ . As a consequence,  $\mathcal{A}'$  is a  $\dagger$ -algebra generated by  $E_a$ , which is called *interaction algebra* associated with  $\mathcal{E}$ .

However, not all channels are unital and, because of that, it is necessary to propose a more general approach. In these more general cases, all that can be said for operators  $\sigma \in \mathcal{A}'$  is that they satisfy  $\mathcal{E}(\sigma) = \sigma \mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$ . Given a projection  $P$  in  $\mathcal{B}(\mathcal{H})$ , the goal will be the identification of a subalgebra  $P\mathcal{B}(\mathcal{H})P$  with the algebra  $\mathcal{B}(P\mathcal{H})$ .

**Theorem 2.** (Choi and Kribs [11]) Let  $\mathcal{E} = \{E_a\}$  be a quantum operation on  $\mathcal{B}(\mathcal{H})$ . Suppose  $P$  is a projection on  $\mathcal{H}$  such that

$$\mathcal{E}(P) = P\mathcal{E}(P)P \quad (5)$$

Then  $E_a P = P E_a P, \forall a$ . Define

$$\mathcal{A}'_P \equiv \{\sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, P E_a P] = 0 = [\sigma, P E_a^\dagger P]\} \quad (6)$$

and

$$\begin{aligned} \text{Fix}_P(\mathcal{E}) &\equiv \{\sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma \mathcal{E}(P) = \mathcal{E}(P)\sigma, \\ &\mathcal{E}(\sigma^\dagger \sigma) = \sigma^\dagger \mathcal{E}(P)\sigma, \mathcal{E}(\sigma, \sigma^\dagger) = \sigma \mathcal{E}(P)\sigma^\dagger\} \quad (7) \end{aligned}$$

Then  $\text{Fix}_P(\mathcal{E})$  is a  $\dagger$ -algebra inside  $\mathcal{B}(P\mathcal{H})$  that coincides with the algebra  $\mathcal{A}'_P$ ; that is

$$\text{Fix}_P(\mathcal{E}) = \mathcal{A}'_P \quad (9)$$

Projectors  $P$  satisfying (5) have some properties. For instance, a quantum channel  $\mathcal{E} \equiv \{E_a\}$  acts in a quantum state  $\sigma \in \mathcal{A}'_P$  projecting it into another state  $\sigma'$  in the subspace  $P$ . To show this, we have

$$\sigma' = \mathcal{E}(\sigma) \quad (10)$$

$$= \sigma \mathcal{E}(P) \quad (11)$$

$$= (P\sigma P)(P\mathcal{E}(P)P) \quad (12)$$

$$= P[\sigma P\mathcal{E}(P)]P \in \mathcal{B}(P\mathcal{H}) \quad (13)$$

In this particular case, we have  $\mathcal{E}(\sigma) = \sigma$  only if  $\mathcal{E}(P) = \mathbb{1}$ .

The next step is to show how projectors with such characterization identify the DFS in a quantum operation  $\mathcal{E}$ .

**Theorem 3.** (Choi and Kribs [11]) Let  $\mathcal{E}$  be a quantum operation on  $\mathcal{B}(\mathcal{H})$ . Let  $P$  be a projection on  $\mathcal{H}$  that satisfies (5) and let  $P\mathcal{H} = \oplus_k (\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$  be the decomposition of  $P\mathcal{H}$  induced by the  $\dagger$ -algebra structure of  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$ . Then the subsystems  $\mathcal{H}^{B_k}$ , with  $\dim(\mathcal{H}^{B_k}) > 1$ , are each decoherence-free subsystems for  $\mathcal{E}$ .

It is possible to say, thus, that the essence of this method consists in the determination of all projectors  $P$  satisfying (5). From this, the structure of  $\mathcal{A}'_P = \text{Fix}_P(\mathcal{E})$  can be used to determine the states belonging to the DFS.

An important remark about this method is its *optimality*, i.e., it is able to obtain all projectors satisfying (5) (vide [11, Theorem 3]). So far, however, there is no computational procedure already implemented to automatize the execution of this method.

### III. SECRECY CAPACITY AND DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

In a recent work, Guedes and de Assis [6], [7] investigated the impacts of the use of DFS in Quantum Communications. They considered the case that a sender (Alice) wants to convey secret classical messages through a quantum channel to a legitimate receiver (Bob). These messages must be protected from a wiretapper (Eve) that has full access to the environment.

To exchange the messages without being deceived by Eve, Alice and Bob use a *quantum error-avoiding code* (QEAC)

build from the states of a DFS according to the following definition.

**Definition 3.** Let  $\tilde{\mathcal{H}}$  be a DFS spanned by a set of eigenvectors  $\{|\tilde{k}\rangle\}$ , i.e.,  $\tilde{\mathcal{H}} = \text{Span}\{|\tilde{k}\rangle\}$ . A set of codewords of length  $n$  ( $n = \dim(\tilde{\mathcal{H}})$ ) for a set  $\mathcal{U}$  of classical messages is a set of input states labeled by messages in  $\mathcal{U}$ ,  $\tilde{K}(\mathcal{U}) = \{|\tilde{k}(u)\rangle : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$ , and a decoding measurement composed of a set of positive operators  $\tilde{\mathcal{D}}_u, u \in \mathcal{U}$  with  $\sum_{u \in \mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbb{1}$ . The pair  $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$  is called a QEAC of length  $n$  for the set  $\mathcal{U}$  of messages. The rate of this code is  $\frac{1}{n} \log |\mathcal{U}|$ .

Using the code defined, if Alice wants to send a classical message  $u$  through the quantum channel  $\mathcal{E}$ , now she encodes it according to the QEAC defined over  $\tilde{\mathcal{H}}$ , obtaining  $|\tilde{k}(u)\rangle$ . When she sends it through the communication channel, the message interacts with the environment (which is assumed to start in a pure state  $|0_E\rangle$ ). This scenario is depicted in Figure 1. Bob then receives  $\rho_{\text{Bob}}(|\tilde{k}(u)\rangle)$  and Eve receives  $\rho_{\text{Eve}}(|\tilde{k}(u)\rangle)$ , which are given by:

$$\rho_{\text{Bob}}(|\tilde{k}(u)\rangle) = \text{Tr}_E [\mathcal{E}(|\tilde{k}(u)\rangle \otimes |0_E\rangle \langle 0_E|)] \quad (14)$$

$$\rho_{\text{Eve}}(|\tilde{k}(u)\rangle) = \text{Tr}_B [\mathcal{E}(|\tilde{k}(u)\rangle \otimes |0_E\rangle \langle 0_E|)] \quad (15)$$

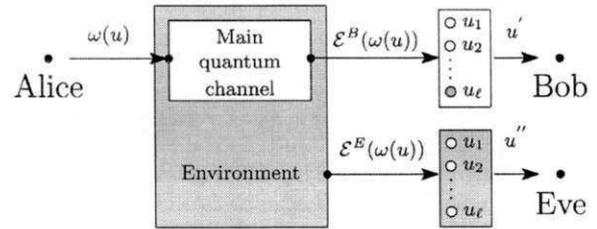


Fig. 1: General idea of the scenario described.

Since Alice used a QEAC, then the existing dynamical symmetry protected the quantum information from the interaction with the environment. It means that the joint evolution of the system and the environment occurred in a decoupled way. Hence, the state  $\rho_{\text{Bob}}(|\tilde{k}(u)\rangle)$  is given by:

$$\rho_{\text{Bob}}(|\tilde{k}(u)\rangle) = \text{Tr}_E [\mathcal{E}(|\tilde{k}(u)\rangle \otimes |0_E\rangle \langle 0_E|)] \quad (16)$$

$$= \text{Tr}_E \left[ \sum_i A_i (|\tilde{k}(u)\rangle \otimes |0_E\rangle \langle 0_E|) A_i^\dagger \right] \quad (17)$$

$$= \text{Tr}_E [|\tilde{k}(u)\rangle \otimes \rho_E] \quad (18)$$

$$= |\tilde{k}(u)\rangle \quad (19)$$

where (18) is due to the invariance of a state of the DFS under the OSR operators. The information accessible by Bob is upper bounded by the Holevo quantity which is given by

$$\chi^{\text{Bob}} = S \left( \sum_u p_u \rho_{\text{Bob}}(\tilde{k}(u)) \right) - \sum_u p_u S \left( \rho_{\text{Bob}}(\tilde{k}(u)) \right) \quad (20)$$

where  $p_u$  is the a priori distribution of the symbols in  $\mathcal{U}$ . Eve, in turn, will try to build a POVM based on the typicality of the sequences she gathers, following a strategy presented in [2, Sec. 4].

Using the theory of quantum wiretap channels [2], [3], Guedes and de Assis [6] showed that the information leaked out to the wiretapper is zero and that the secrecy capacity of such scenario is equal to the HSW capacity as showed in the theorem below.

**Theorem 4.** (Guedes and de Assis [6]) *The secrecy capacity of a quantum channel  $\mathcal{E}$  which has a DFS  $\tilde{\mathcal{H}}$  is*

$$C_{S,DFS}(\mathcal{E}) = \max_{\{P\}} [\chi^{\text{Bob}}] \quad (21)$$

where the maximum is taken over all probability distributions  $P$  over  $\mathcal{U}$ ; and  $\chi^{\text{Bob}}$  is the Holevo quantity given in (20).

This implies that the secrecy capacity when a QEAC is used can reach the maximum rate of classical information transmission through the channel.

#### IV. ZERO-ERROR CAPACITY OF QUANTUM CHANNELS

The *zero-error capacity* of a discrete classical channel was first defined by Shannon [16] as the least upper bound of rates for which one transmits information with zero probability of error. Its quantum analogous, the *quantum zero-error capacity* (QZEC) generalizes this concept to include quantum channels, in a scenario where classical information is conveyed [12].

Given a quantum channel, we ask for the maximum amount of classical information that can be transmitted through it with a zero probability of error. Before defining such quantity, it is necessary to define a *quantum error-free block code* that gives a general idea of the communication protocol employed.

**Definition 4.** ( $(K_n, n)$  error-free quantum block code [17]) *A  $(K_n, n)$  quantum error-free block code for a quantum channel  $\mathcal{E}$  is composed of:*

- 1) *A set of classical messages  $\{1, \dots, K_n\}$ ;*
- 2) *An encoding function:  $X^n : \{1, \dots, K_n\} \rightarrow \mathcal{S}^{\otimes n}$  that associates a product state to each classical message;*
- 3) *A decoding function  $g : \{1, \dots, m\} \rightarrow \{1, \dots, K_n\}$  which deterministically assigns a guess to each possible measurement output  $y \in \{1, \dots, m\}$  performed by a POVM  $\mathcal{M} = \{M_m\}$ . The decoding function has the following property*

$$\Pr[g(Y = y) \neq i | X^n(i)] = 0, \forall i \in \{1, \dots, K_n\} \quad (22)$$

The rate of this code is  $R_n = \frac{1}{n} \log K_n$  bits per channel use.

Thus, we can now define the QZEC:

**Definition 5.** (Quantum zero-error capacity [17]) *Let  $\mathcal{E}(\cdot)$  be*

*a positive, linear, trace-preserving quantum map representing a noisy channel. The quantum zero-error capacity of  $\mathcal{E}(\cdot)$ , denoted by  $C^{(0)}(\mathcal{E})$ , is the least upper bound of achievable rates with probability of error equal to zero, that is*

$$C^{(0)}(\mathcal{E}) = \sup_S \sup_n \frac{1}{n} \log K_n \quad (23)$$

where  $K_n$  stands for the maximum number of classical messages that the system can transmit without error, when a  $(K_n, n)$  error-free quantum block with input alphabet  $\mathcal{S}$  is used.

However, we are interested in a quantum channel where  $\mathcal{E}$  has a non-vanishing zero-error capacity. To guarantee this, it is necessary that the set  $\mathcal{S}$  contains at least two *non-adjacent states*, denoted by  $\rho_i \perp_{\mathcal{E}} \rho_j$ , where  $\rho_i, \rho_j \in \mathcal{S}$ . By non-adjacent states we mean states that are distinguishable at the channel's end, i.e., the Hilbert subspaces spanned by the supports of  $\rho_i$  and  $\rho_j$  are orthogonal.

In the attempt to reach the zero-error capacity, it is necessary to take into account error-free quantum codes that maximize the rate of transmission. It leads to the following definition.

**Definition 6.** (Optimum  $(\mathcal{S}, \mathcal{M})$  for  $\mathcal{E}$  [17]) *The optimum  $(\mathcal{S}, \mathcal{M})$  for a quantum channel  $\mathcal{E}$  is composed of a set  $\mathcal{S} = \{\rho_i\}$  and a POVM  $\mathcal{M} = \{M_m\}$  for which the zero-error capacity is reached.*

#### A. Graph-Theoretic Approach

The zero-error capacity allows an interpretation in terms of Graph Theory [17]. Given a quantum channel  $\mathcal{E}$  and a set of input states  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$ , it is possible to construct a characteristic graph  $\mathcal{G} = \langle V, E \rangle$  as follows:

- $V = \{1, \dots, \ell\}$  is the vertex set containing the index set of  $\mathcal{S}$ ;
- $E = \{(i, j) | \rho_i \perp_{\mathcal{E}} \rho_j, \rho_i, \rho_j \in \mathcal{S}, i \neq j\}$

This notion of characteristic graph can also be extended to the  $n$ -product  $\mathcal{G}^n$ , where  $V = V^n$  and  $E$  is composed of pairs of such indexes whose corresponding sequences are non-adjacent in  $\mathcal{E}$ .

From this interpretation, it is easy to see that quantum states corresponding to vertices in any complete subgraph of  $\mathcal{G}$  are mutually non-adjacent. Therefore, the maximum number of messages that can be transmitted without error with a  $(K_n, n)$  error-free quantum code with input alphabet  $\mathcal{S}$  is the clique number of  $\mathcal{G}^n$ , which is denoted by  $\omega(\mathcal{G}^n)$ . This way, we get an alternative and equivalent definition of the QZEC in terms of Graph Theory.

**Definition 7.** (QZEC in terms of Graph Theory) *The zero-error capacity of a quantum channel  $\mathcal{E}$  is given by*

$$C^{(0)}(\mathcal{E}) = \sup_S \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n) \quad (24)$$

where the supremum is taken over all subsets  $\mathcal{S}$  of input states, and  $\omega(\mathcal{G}^n)$  is the clique number of the  $n$ -product of the characteristic graph  $\mathcal{G}$  associated with  $\mathcal{S}$ .

### B. Relation with Decoherence-Free Subspaces and Subsystems

Medeiros et al. [10] investigated the relation between the QZEC and DFS. Let a pair  $(\mathcal{S}, \mathcal{M})$  be optimum in the sense of Definition 6. Let  $\{M_1, \dots, M_k\}$  be a subset of  $\mathcal{M}$  where each  $M_i$  satisfies

$$\mathcal{E}(M_i) = M_i \mathcal{E}(M_i) M_i \quad (25)$$

$$M_i M_j = \delta_{i,j} M_i M_j \quad (26)$$

for all  $i, j \leq k$ .

Select one state  $\rho_i = |s_i\rangle\langle s_i|$  from each subspace  $P_i \mathcal{H}$  satisfying  $[p_i, P_i E_a P_i] = 0$  and  $[p_i, P_i E_a^\dagger P_i] = 0$ . We can construct a pair  $(\mathcal{S}', \mathcal{M}')$  where  $\mathcal{S}' = \{\rho_i\}$ , and a POVM  $\mathcal{M}' = \{M_1, \dots, M_k, M_{k+1}\}$ ,  $M_{k+1} = \mathbb{1} - \sum_{i=1}^k M_i$  where  $M_1, \dots, M_k$  satisfies Eqs. (25) and (26). We have, then, the following theorem due to [10].

**Theorem 5.** *Let the pair  $(\mathcal{S}, \mathcal{M})$  be optimum in the sense of Definition 6. Then the pair  $(\mathcal{S}', \mathcal{M}')$  is also optimum.*

The results follows from Shannon's concept of adjacency-reducing mapping [16]. In the quantum-zero error scenario, this means a mapping of quantum states into letters  $\rho_i \mapsto \beta(\rho_i)$ , with the property that if  $\rho_i$  and  $\rho_j$  are not adjacent in the quantum channel then  $\beta(\rho_i)$  and  $\beta(\rho_j)$  are not adjacent. If all input states in the optimum  $\mathcal{S}$  can be mapped by an adjacency-reducing map into a subset of letters no two of which are adjacent, then the zero-error capacity of the channel is equal to the logarithm of the number of letters in this subset [10].

Let  $\mathcal{G}_{(\cdot)}$  be the characteristic graph for  $(\mathcal{S}', \mathcal{M}')$  then

$$C^{(\cdot)}(\mathcal{E}) = \sup_n \frac{1}{n} \log \omega(\mathcal{G}_{(\cdot)}^n) \quad (27)$$

Using results from adjacency-reducing map [16], the authors showed that  $C^{(\cdot)}(\mathcal{E}) \geq C^{(0)}(\mathcal{E})$ .

In summary, the authors show that if the optimum  $\mathcal{S}$  contains DFS, then the QZEC is readily calculated by finding projectors fulfilling some properties. So, it is reasonable to believe in a close connection between these subsystems and any scheme allowing information transmission with error probability equal to zero [10].

## V. QUANTUM ZERO-ERROR SECRECY CAPACITY

We consider the same scenario described in Section III in which Alice wants to send a secret classical message to Bob through a noisy channel wiretapped by Eve who has full access to the environment. This channel, in particular, has its zero-error capacity a greater than zero.

**Definition 8.** *Let  $\mathcal{E}$  be a trace-preserving quantum map representing a noisy channel. The error-model for  $\mathcal{E}$  is known and can be represented by the operation elements  $\{E_a\}$ , i.e.,  $\mathcal{E} \equiv \{E_a\}$ . We impose that  $\mathcal{E}$  has a strictly positive zero-error capacity,  $C^{(0)}(\mathcal{E}) > 0$ , reached by a optimum pair  $(\mathcal{S}, \mathcal{M})$ .*

Let's suppose that a subset  $\mathcal{M}' = \{M_1, \dots, M_k\}$  of  $\mathcal{M}$  satisfies the conditions of Eqs. (25) and (26) giving rise to a pair  $(\mathcal{S}', \mathcal{M}')$  which is also optimum, with  $\mathcal{S}' = \{\rho_i = |s_i\rangle\langle s_i|\}_{i=1}^k$ , where each  $\rho_i$  belongs to the subspace  $M_i \mathcal{H}$  satisfying  $[\rho_i, M_i E_a M_i] = 0$  and  $[\rho_i, M_i E_a^\dagger M_i] = 0$ .

The optimum pair  $(\mathcal{S}', \mathcal{M}')$  was obtained according to the procedures described in Section IV-B. Due to that, it defines a decoherence-free subsystem that can be used to encode information that is free from a wiretapper, as it is going to be proved by the following lemmas.

**Lemma 1.** *The pair  $(\mathcal{S}', \mathcal{M}')$  is a quantum-error avoiding code (vide Definition 3).*

*Proof:* To prove this lemma we must show that it is possible to characterize the elements of a QEAC from the pair  $(\mathcal{S}', \mathcal{M}')$ .

Let  $\mathcal{U} = \{u_1, \dots, u_k\}$  be a set of classical messages, each uniquely associated to a state of  $\mathcal{S}'$ . It defines a set of codewords  $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u_i) = \rho_i\} \equiv \mathcal{S}'$  of length  $n$  ( $n = \dim(\mathcal{H})$ ). The decoding measurement is composed of a set of positive operators  $M_i \in \mathcal{M}'$ ,  $i \in 1, \dots, |\mathcal{U}|$ , with  $\sum_{i=1}^k M_i \leq \mathbb{1}$ . Each  $M_i$  is uniquely associated with a message  $u_i \in \mathcal{U}$ . So, the pair  $(\tilde{K}(\mathcal{U}), \mathcal{M}')$  is a QEAC of length  $n$  with rate  $\frac{1}{n} \log |\mathcal{U}|$ . ■

**Lemma 2.** *The optimum pair  $(\mathcal{S}', \mathcal{M}')$  is a wiretap code<sup>1</sup> with parameters  $(n, |\mathcal{U}|, 0, 0)$*

*Proof:* In the previous lemma, it was proved that  $(\mathcal{S}', \mathcal{M}')$  is a QEAC. Guedes and de Assis [6, Lemma 1] established a proof that every QEAC is a wiretap code with parameters  $(n, |\mathcal{U}|, \lambda, \mu)$ . The parameters  $n$  and  $|\mathcal{U}|$  come from the proof of Lemma 1. We must recall that the parameter  $\lambda$  regards the average decoding error probability and that  $\mu$  is the average accessible information by the wiretapper. In this particular case, we must prove that  $\lambda = 0$  and  $\mu = 0$ .

Since the pair  $(\mathcal{S}', \mathcal{M}')$  is optimum, then it allows the channel  $\mathcal{E}$  to reach  $C^{(0)}$ , so the communication can be carried out without decoding errors, what implies  $\lambda = 0$ .

Then we proceed to analyze the second criterion. Recall from (18) that the final state of Eve is given by  $\rho_E$  which is not known. Since Alice and Bob used states from a DFS, it is possible to guarantee that the interaction Hamiltonian  $\mathbb{H}_{SE}$  from (1) did not govern the joint evolution of system and environment. Instead of that, each system evolved completely unitary under its own Hamiltonian, i.e., the environment suffered only the action of  $\mathbb{H}_E$ . It implies that the environment ended in a pure state. Taking this fact into account, we can obtain the Holevo quantity of Eve which is an upper bound to her accessible information

<sup>1</sup>The formal definition of a wiretap code and its requirements can be found in [2, Sec. 3, Eqs. (9) and (10)].

$$\chi^{\text{Eve}} = S(\rho_{\text{Eve}}(\tilde{k}(u))) - \sum_u p_u S(\rho_{\text{Eve},u}(\tilde{k}(u))) \quad (28)$$

$$= S(\rho_E) - \sum_u p_u S(\rho_{\text{Eve},u}(\tilde{k}(u))) \quad (29)$$

$$= 0 - \sum_u p_u S(\rho_{\text{Eve},k}(\tilde{k}(u))) \quad (30)$$

It is well known that the Holevo quantity  $\chi^{\text{Eve}} \geq 0$ . Since  $S(\rho) \geq 0$  for any  $\rho$ , and that the probabilities  $p_u \geq 0$  for any  $u$ , then it is the case that the remaining term is zero. Thus,  $\chi^{\text{Eve}} = 0$ . Since the Holevo quantity is an upper bound for the accessible information, then it is also equal to zero, what implies  $\mu = 0$ . This concludes the proof. ■

Although an optimum pair  $(S', \mathcal{M}')$  defines a wiretap code with parameters  $(n, |\mathcal{U}|, 0, 0)$ , it is not always the case that is possible to extract a pair  $(S', \mathcal{M}')$  from an optimum pair  $(S, \mathcal{M})$ . According to Lemma 1, we have that finding this pair is equivalent to identify a DFS  $\tilde{\mathcal{H}}$ . However, considering practical scenarios, a DFS may exist although with a smaller dimension than the one considered by the error-free code, i.e.,  $\dim(\tilde{\mathcal{H}}) < n$ . This consideration leads to the definition of a wiretap code  $(\dim(\tilde{\mathcal{H}}), |\mathcal{U}|, 0, 0)$  which still allows the communication between the parties without decoding errors and information leakage. Taking into account these considerations and also the two lemmas previously proved, it is possible to characterize a new capacity of quantum channels which definition is given as follows.

**Definition 9.** (*Quantum Zero-Error Secrecy Capacity*) The quantum zero-error secrecy capacity of a quantum channel  $\mathcal{E}$ , as given in Definition 8, is the maximum real number  $C_S^{(0)}$  such that for all  $\epsilon > 0$  and for sufficiently large  $n$  there exists a wiretap code  $(n, |\mathcal{U}|, 0, 0)$  such that

$$C_S^{(0)} \leq \frac{1}{n} \log |\mathcal{U}| + \epsilon \quad (31)$$

Two interesting features of the ZESC is that there are no decoding errors, and the information leakage out to a wiretapper is zero. It is in contrast with the regular secrecy capacity of quantum channels in which the decoding errors between legitimate parts and information leakage to a wiretapper vanish in the limit of asymptotically many uses of the channel.

The following theorem aims at quantifying ZESC.

**Theorem 6.** The zero-error secrecy capacity of a quantum channel  $\mathcal{E}$  as in Definition 8 is

$$C_S^{(0)} \equiv \min \left\{ C^{(0)}(\mathcal{E}), C_S(\mathcal{E}) \right\} \quad (32)$$

$$\equiv \min \left\{ \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log |\dim \tilde{\mathcal{H}}|^n, \max_{\{P\}} \chi^{\text{Bob}} \right\} \quad (33)$$

where  $n$  is the code length; the maximum is taken over all probability distributions  $P$  over  $\mathcal{U}$ ; and  $\chi^{\text{Bob}}$  denotes the Holevo quantity of Bob as given in (20).

*Proof:* This proof takes into account some facts about quantum capacities of the channel  $\mathcal{E}$ . Let  $C(\mathcal{E})$  denote the ordinary classical capacity of  $\mathcal{E}$  defined by the HSW theorem [8], [9];  $C_S(\mathcal{E})$  be the secrecy capacity of  $\mathcal{E}$  [2], [3]; and  $C^{(0)}$  be the zero-error capacity of  $\mathcal{E}$  [12]. We have that  $C_S(\mathcal{E}) \leq C(\mathcal{E})$  as well as  $C^{(0)}(\mathcal{E}) \leq C(\mathcal{E})$ .

Considering  $n = \dim(\tilde{\mathcal{H}})$ , a code with parameters  $(n, |\mathcal{U}|, 0, 0)$  is simultaneously error-free and also wiretap. By definition, it is known that the zero-error capacity is related to the maximum quantity of messages that are distinguishable at the channel's end. Since every word of the alphabet  $\mathcal{U}$  was associated to a state of a DFS, according to Lemma 1, we have that

$$C^{(0)}(\mathcal{E}) = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log |\dim \tilde{\mathcal{H}}|^n \quad (34)$$

where  $n$  is the code length.

Regarding the wiretap part, we have that  $C_S(\mathcal{E}) = \chi^{\text{Bob}} - \chi^{\text{Eva}}$ . As a consequence of Lemma 2 we have

$$C_S^{(0)}(\mathcal{E}) \geq \max_{\{P\}} [\chi^{\text{Bob}} - \chi^{\text{Eva}}] \quad (35)$$

$$\geq \max_{\{P\}} [\chi^{\text{Bob}} - 0] \quad (36)$$

$$= \max_{\{P\}} \chi^{\text{Bob}} \quad (37)$$

where the maximum is taken over all probability distributions  $P$  over  $\mathcal{U}$  in Bob's Holevo quantity. The equality comes from the HSW theorem.

There are, however, two situations to consider:

- 1) There is an optimum pair  $(S', \mathcal{M}')$  derived from  $(S, \mathcal{M})$  according to Eqs. (25) and (26). Thus,  $n = |S'|$  and  $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$ ;
- 2) There is a DFS  $\tilde{\mathcal{H}}$  in the channel which is not directly obtained from the error-free code. In this situation,  $C_S(\mathcal{E}) < C^{(0)}(\mathcal{E})$ , i.e., there is error and leakage free communication only if  $C_S^{(0)}(\mathcal{E}) = \min \{C^{(0)}, C_S(\mathcal{E})\}$ .

This way, the final expression for the quantum zero-error secrecy capacity of a quantum channel  $\mathcal{E}$  can be written by means of its zero-error and secrecy capacities, i.e.

$$C_S^{(0)}(\mathcal{E}) = \min \left\{ C^{(0)}(\mathcal{E}), C_S(\mathcal{E}) \right\} \quad (38)$$

where  $C^{(0)}(\mathcal{E})$  and  $C_S(\mathcal{E})$  are the zero-error and secrecy capacities, respectively. It concludes the proof. ■

When  $C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log |\dim \tilde{\mathcal{H}}|^n$ , the QZESC has single-letter characterization what is in sharp contrast with the ordinary quantum secrecy capacity which has not [2], [3]. Besides, according to a result provided by Medeiros et al. [18], the zero-error capacity can be reached when pure states are used in the input. It is also true for the definition made in this work regarding  $S'$ , what implies that the QZESC can also be reached using pure states in certain situations.

Regarding the security, the results shown in this section are in accordance with Schumacher and Westmoreland [19].

According to them, the ability of a quantum channel to send private information is at least as great as its ability to send coherent information. In our case, since the information sent can be retrieved completely free of errors, then the ability to send private information is maximized.

#### A. Relation with Graph Theory

Let  $\tilde{\mathcal{H}}$  be a DFS existing in the channel  $\mathcal{E}$  obtained as described in the previous section. The graph  $\mathcal{G}_{(\cdot)}$  =  $\langle V, E \rangle$  for  $\mathcal{E}$  is characterized as follows:

- The set of vertices  $V$  is composed by the elements in  $\tilde{\mathcal{H}}$  which will be referred by their corresponding index, i.e.,  $V = \{1, 2, \dots, k\}$ ;
- The set of edges  $E$  connects two vertices if they are distinguishable at the channel's end. Since the elements of a DFS characterize an error-free code, the states in  $\tilde{\mathcal{H}}$  taken pairwise are distinguishable (from the proof of the Theorem 6). This way, the resulting graph is *complete*.

The  $n$ -product of  $\mathcal{G}_{(\cdot)}$ , denoted by  $\mathcal{G}_{(\cdot)}^n$ , has  $V = V^n$  and the set of edges  $E$  is composed of pairs of such indexes whose corresponding sequences are non-adjacent in  $\mathcal{E}$ . The maximum number of messages that can be transmitted without error with  $\mathcal{G}_{(\cdot)}^n$  is the clique number of  $\mathcal{G}^n$ , which is denoted by  $\omega(\mathcal{G}^n)$

$$C_S^{(0)} = \sup_{\tilde{\mathcal{H}}} \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n) \quad (39)$$

Given an integer and a graph, finding a clique of the size of the given integer is a  $\mathcal{NP}$ -Complete problem. However, some characteristics of the zero-error and of the DFS can be taken into account in the determination of  $C_S^{(0)}$ . Since the graphs produced from  $\tilde{\mathcal{H}}$  are complete, the clique number of  $\mathcal{G}_{(\cdot)}^n$  turns out to be equal to  $|\dim(\tilde{\mathcal{H}})|^n$ . Such relation between the clique number and the cardinality of the vertices set in the corresponding graph is not observed in ordinary error-free codes. This is a particularity due to the use of DFS.

#### B. Examples

This section presents some detailed examples regarding the concepts of the ZESC. Initially let's suppose that a quantum channel  $\mathcal{E}_1$  has the positive zero-error capacity achieved by an optimum pair  $(\mathcal{S}_1, \mathcal{M}_1)$  as shown in Figure 2a. By following the procedures described in Section IV-B, a pair  $(\mathcal{S}'_1, \mathcal{M}'_1)$  can be derived which is shown in Figure 2b.

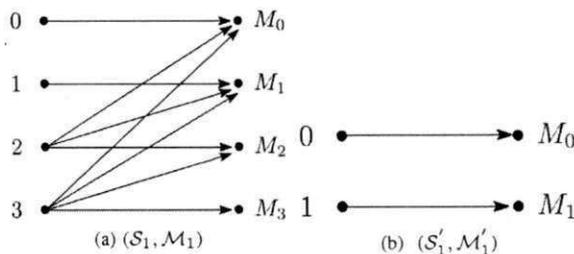


Fig. 2: Representation of the channel  $\mathcal{E}_1$  transitions to the input states of the optimum pairs  $(\mathcal{S}_1, \mathcal{M}_1)$  and  $(\mathcal{S}'_1, \mathcal{M}'_1)$ .

The characteristic graphs of  $(\mathcal{S}_1, \mathcal{M}_1)$  and  $(\mathcal{S}'_1, \mathcal{M}'_1)$  are illustrated in Figures 3a and 3b, respectively.

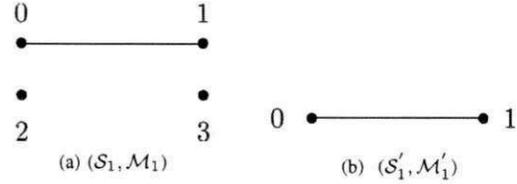


Fig. 3: Characteristic graphs for  $(\mathcal{S}_1, \mathcal{M}_1)$  and  $(\mathcal{S}'_1, \mathcal{M}'_1)$ .

According to these characteristic graphs, the maximum clique number is 2, in both cases obtained by the pairs (0, 1). It leads to a zero-error secrecy capacity equal to (for  $n = 1$  because the states are pure):

$$C_S^{(0)}(\mathcal{E}_1) = \sup_{\mathcal{S}'} \sup_n \frac{1}{n} \log |\mathcal{S}'_1|^n \quad (40)$$

$$= \frac{1}{1} \log 2 \quad (41)$$

$$= 1 \text{ bits per channel use.} \quad (42)$$

To verify this result according to the expression of secrecy capacity, we used Mathematica<sup>®</sup> in the attempt to obtain the maximum of  $\chi^{\text{Bob}}$  in Eqs. (43)-(44).

$$C_S^{(0)}(\mathcal{E}_1) = \chi^{\text{Bob}} \quad (43)$$

$$= \max_{\{P\}} S(p_0 \cdot \rho_0 + p_1 \cdot \rho_1) \quad (44)$$

We simulated 30000 pairs of  $(p_0, p_1)$  taking into account the restriction that  $p_0 + p_1 = 1$ . As a result, we obtained the graphic of Figure 4. As it can be seen, the maximum value of Bob's Holevo quantity is also equal to 1. It means that for the channel  $\mathcal{E}_1$ , we have that  $C_S^{(0)}(\mathcal{E}_1) = 1$  bit per channel use.

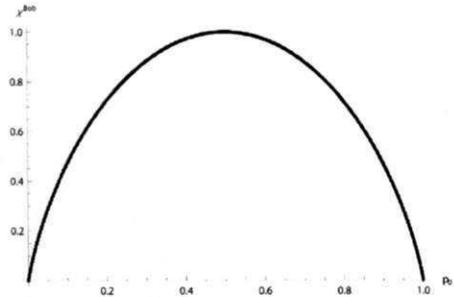


Fig. 4: Simulation performed in the attempt to maximize the value of  $\chi^{\text{Bob}}$  in Eqs. (43)-(44) over the pairs  $(p_0, p_1)$ .

In this second example, let's suppose that a quantum channel  $\mathcal{E}_2$  has positive zero-error capacity achieved by an optimum pair  $(\mathcal{S}_2, \mathcal{M}_2)$  where  $\mathcal{S}_2 = \{\rho_1, \dots, \rho_6\}$  and  $\mathcal{M}_2 = \{M_i = |\rho_i\rangle\langle\rho_i|\}_{i=1}^6$ . The model of errors of the channel for the input set is illustrated in Figure 5a. Since we are interested in adjacency relations, we omitted the transition probabilities.

From the pair  $(\mathcal{S}_2, \mathcal{M}_2)$  by following the procedures described in Section IV-B, it is possible to derive an optimum pair  $(\mathcal{S}'_2, \mathcal{M}'_2)$  where  $\mathcal{S}'_2 = \{\rho_2, \rho_3, \rho_5\}$  and  $\mathcal{M}'_2 = \{M_2, M_3, M_5\}$ . The relation between the input states in  $\mathcal{S}'_2$  and the output at the channel  $\mathcal{E}_2$  is illustrated in Figure 5b.

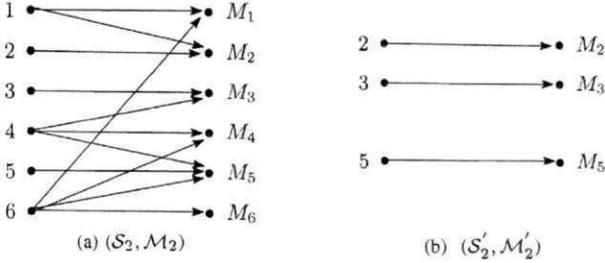


Fig. 5: Representation of the channel  $\mathcal{E}_2$  transitions to the input states of the optimum pairs  $(\mathcal{S}_2, \mathcal{M}_2)$  and  $(\mathcal{S}'_2, \mathcal{M}'_2)$ .

The characteristic graphs of  $(\mathcal{S}_2, \mathcal{M}_2)$  and  $(\mathcal{S}'_2, \mathcal{M}'_2)$  are illustrated in Figures 6a and 6b, respectively. Notice that the clique number  $\omega(\mathcal{G})$  of  $(\mathcal{S}_2, \mathcal{M}_2)$  is equal to 3 and can be obtained through the vertices  $(2, 3, 5)$ ,  $(1, 3, 5)$ , or also  $(2, 3, 6)$ . In other hand, the clique number of  $\omega(\mathcal{G}_{(\cdot)})$  of  $(\mathcal{S}'_2, \mathcal{M}'_2)$  is also equal to 3, but can be easily obtained from the vertices  $(2, 3, 5)$ .

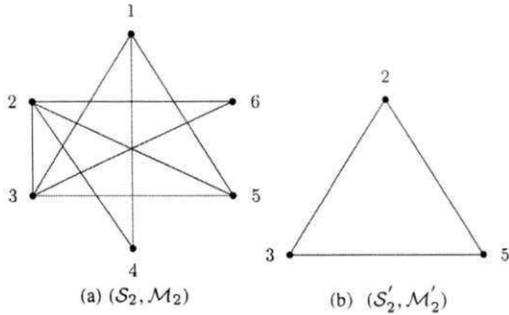


Fig. 6: Characteristic graphs for  $(\mathcal{S}_2, \mathcal{M}_2)$  and  $(\mathcal{S}'_2, \mathcal{M}'_2)$ .

Regarding the zero-error secrecy capacity of the optimum pair  $(\mathcal{S}'_2, \mathcal{M}'_2)$  for  $n = 1$ , according to (32), it is equal to

$$C_{\mathcal{S}'_2}^{(0)}(\mathcal{E}_2) = \sup_{\mathcal{S}'_2} \sup_n \frac{1}{n} \log |\mathcal{S}'_2|^n \quad (45)$$

$$= \frac{1}{1} \log 3 \quad (46)$$

$$\approx 1.58496 \text{ bits per channel use} \quad (47)$$

To show the equivalence between this expression of ZESC in terms of graphs and the secrecy capacity form, we set up a simulation to obtain the Holevo quantity of Bob. In this particular example, we know that the states  $\rho_2$ ,  $\rho_3$ , and  $\rho_5$  are pure, what will leave us with the following expression to the Holevo quantity of Bob.

$$\chi^{\text{Bob}} = \max_{\{P\}} S(p_1 \cdot \rho_2 + p_2 \cdot \rho_3 + p_3 \cdot \rho_5) \quad (48)$$

since  $S(\rho_2) = S(\rho_3) = S(\rho_5) = 0$  because they are pure states. The constrain that  $p_1 + p_2 + p_3 = 1$  must also be taken into account. A simulation was carried out using Mathematica<sup>®</sup> trying to maximize the value of (48) among 20,000 valid triples of  $(p_1, p_2, p_3)$ . The results obtained are plotted in the graphic of Figure 7 in which two different perspectives are shown. According to the results observed, the highest value of  $\chi^{\text{Bob}}$  obtained was 1.58491 bits per channel use, what can be considered a coincidence with the theoretical results using the graph-theoretical approach shown in (47).

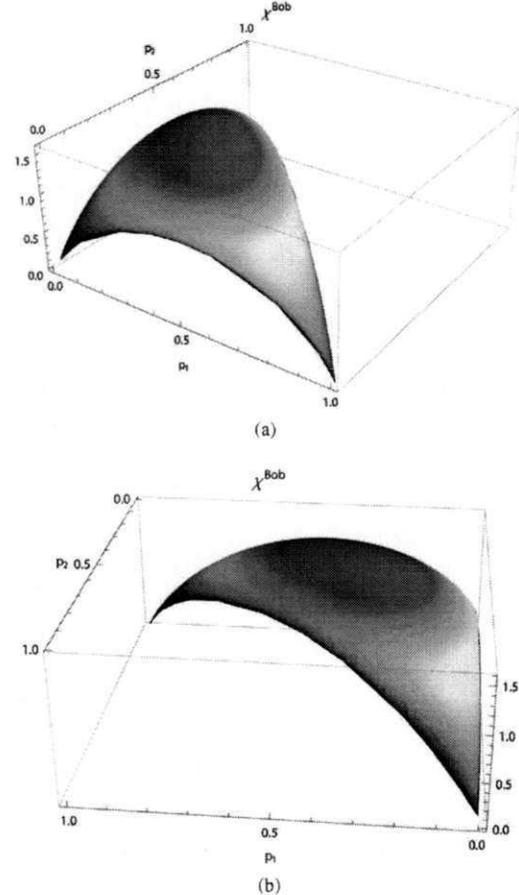


Fig. 7: Two different perspectives from the graphic obtained from the simulation of triples  $(p_1, p_2, p_3)$  in the attempt maximize (48)

A third-example is simple yet non-trivial. In this case, we have  $\mathcal{S}_3 = \{\rho_i = |i\rangle\langle i|, i = 0, \dots, 3\}$ . The model of errors is known, composed by the four following operator elements:  $E_0 = |0\rangle\langle 0|$ ,  $E_1 = |1\rangle\langle 1|$ ,  $E_2 = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 2|$ , and  $E_3 = \frac{1}{2}|3\rangle\langle 3| + \frac{1}{2}|2\rangle\langle 3|$ . The channel  $\mathcal{E}_3 \equiv \{E_i\}_{i=0}^3$  is illustrated in Figure 8a.

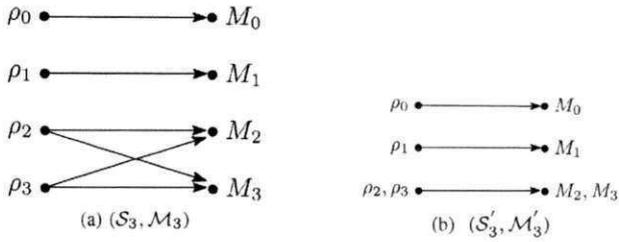


Fig. 8: Representation of the channel  $\mathcal{E}_3$  transitions to the input states of the optimum pairs  $(\mathcal{S}_3, \mathcal{M}_3)$  and  $(\mathcal{S}'_3, \mathcal{M}'_3)$ .

When considering this channel, one might think that there are only 2 states belonging to a DFS ( $\rho_0$  and  $\rho_1$ ). However, this is not the case. One might apply the procedures presented in Section IV-B and find out three projectors  $P_0 = |0\rangle\langle 0|$ ,  $P_1 = |1\rangle\langle 1|$ , and  $P_{2,3} = |2\rangle\langle 2| + |3\rangle\langle 3|$  satisfying (25) and (26) in such a way that the subsystems  $P_0\mathcal{H}$ ,  $P_1\mathcal{H}$  and  $P_{2,3}\mathcal{H}$  are a DFS. The channel resulting is illustrated in Figure 8b.

The characteristics graphs related to  $(\mathcal{S}_3, \mathcal{M}_3)$  and to  $(\mathcal{S}'_3, \mathcal{M}'_3)$  are illustrated in Figure 9. It is possible to see that the zero-error secrecy capacity of  $(\mathcal{S}'_3, \mathcal{M}'_3)$  is equal to the zero-error capacity  $(\mathcal{S}_3, \mathcal{M}_3)$  which is, for  $n = 1$ , equal to  $C_S^{(0)}(\mathcal{E}_3) = \log 3$  bits per symbol per channel use.

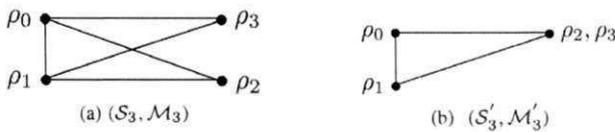


Fig. 9: Characteristic graphs for  $(\mathcal{S}_3, \mathcal{M}_3)$  and  $(\mathcal{S}'_3, \mathcal{M}'_3)$ .

Despite the previous examples in which ZESC is  $C_S^{(0)}(\mathcal{E}) = C_S(\mathcal{E}) = C^{(0)}(\mathcal{E})$ , there are other situations to consider. The graph in Figure 10a shows a channel  $\mathcal{E}_4$  which characteristic graph is shown in Figure 10b. The ZESC of this channel is  $C_S^{(0)}(\mathcal{E}_4) = \min\{C^{(0)}(\mathcal{E}_4), C_S(\mathcal{E}_4)\} = \{\frac{1}{2} \log 5, \frac{1}{3} \log 2\} = 1$  bit per symbol per channel use.

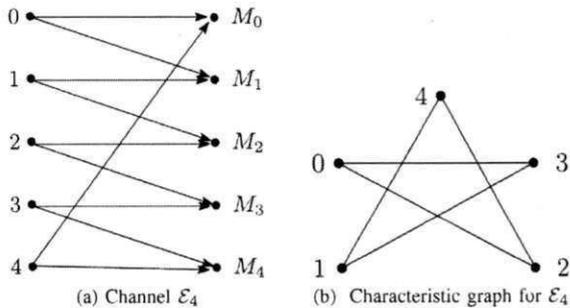


Fig. 10: Non-trivial example of ZESC.

## VI. RELATED WORK

Until the work of Guedes and de Assis [6], [7], many works exploring the use of DFS in communications did not consider

its ability to send messages with unconditional security. All of the works investigated [20]–[22] consist of protocols for quantum secure direct communication and deterministic secure quantum communications where redundancy and eavesdropping check are performed, increasing significantly the number of messages exchanges essentially necessary to carry out the communication with security.

So far, very few contributions to the characterization of wiretap codes have been found in the literature. The code proposed by Hamada [23], [24] is based on the Calderbank-Shor-Steane codes that are suitable for practical implementation, since they do not demand the use of entanglement. However, the rate achieved by such codes is below the secrecy capacity of the quantum channel in use. The work of Wilde and Guha [25] also presents a proposition of quantum wiretap codes, based on polar codes. Despite that, as argued by the own authors, the code proposed may be restricted to some types of quantum channels. Regarding the proposition of wiretap codes from DFS and error-free quantum codes as proposed by our work, no similar strategy was found in the literature.

Braunstein et al. [26] show the relation between DFS and zero-error subspaces, showing that the former is an instance of the latter. Besides that clarifying this relation, they also propose a method for searching DFS within zero-error subspaces. This method seems to have some similarities with the one proposed by Medeiros et al. [10]. We opted to use the latter method because it is guaranteed optimum and also because provides a more intuitive approach to find DFS given a quantum error-free code. It is a key component in the characterization of the codes proposed by us.

Regarding the capacity, Watanabe [27] characterizes a class of *more capable quantum channels* in which the private and quantum capacities are equal. However, he argues that the conditions such that a certain channel belongs to this class are hard to verify in general. The channel considered in our work is more capable in this sense since such equality can be verified, as shown in Section V.

## VII. FINAL REMARKS

In this paper, we presented the *quantum zero-error secrecy capacity*, the maximum rate in which one can send information through a wiretapped quantum channel without decoding error not information leakage out to the wiretapper. This capacity can be achieved with decoherence-free subspaces and subsystems that may rely in the inner structure of some error-free quantum codes.

The use of the codes defined in this paper provides unconditional security in the classical information conveying through quantum channels with an additional advantage that are no decoding errors. It is possible since the wiretapper has access only to the environment to which no accessible information about the secret message is leaked out. The maximum rate in which information can be conveyed can reach the HSW capacity of the quantum channel. A formulation in terms of

graphs appropriated from the zero-error quantum codes was also presented.

To illustrate the concepts regarding ZESC, detailed examples were shown in Section V-B. In all examples it was shown how to obtain a QEAC from an error-free quantum code, and latter how to determine the ZESC for such case. In some cases, simulations were necessary to determine the Holevo quantity.

This paper contributes in the understanding of the relation between noise and decoherence in quantum channels and their impacts in information leakage out to an wiretapper. In first instance, secrecy was reached by avoiding decoherence with the use of DFS in the work of Guedes and de Assis [6], [7]. However, with the recent results of Braunstein et al. [26] pointing out that DFS are instances of zero-error subspaces, fight decoherence also implied also in fight decoding errors. Thus, this work unifies both ideas creating secure codes based on DFS and on error-free quantum codes. This contributes to the characterization of an unconditional secure way to exchange messages without the use of classical channels nor private keys neither previous communications.

Due to the technical difficulties to build completely closed quantum system [4], the results shown here can be applied to build devices that perform unconditional secure message exchange even in the presence of noise and decoherence. It is very promising in practical applications especially considering already existing results regarding the use of DFS in communications [28]–[30], particularly in long-distance [31]. The same is true for the zero-error scenario in practical applications using optical quantum channels as reported recently by Gyongyosi and Imre [32].

In future work, we suggest the investigation of more general conditions to the existence of perfect secrecy in quantum systems.

#### REFERENCES

- [1] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Trans. Info. Theory*, vol. 44, no. 6, pp. 2724–2755, 1998.
- [2] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318–336, 2004.
- [3] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Th.*, vol. 51, no. 1, pp. 44–55, 2005.
- [4] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449–2460, 2004.
- [5] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arXiv:quant-ph/0301032v1, pp. 83–120, 2003.
- [6] E. B. Guedes and F. M. de Assis, "Unconditional security with decoherence-free subspaces," arXiv:quant-ph/1204.3000, pp. 1–6, 2012.
- [7] —, "Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras," in *XXX Simpósio Brasileiro de Telecomunicações – SBRT'12*, 2012.
- [8] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269–273, 1998.
- [9] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.
- [10] R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis, "Zero-error capacity of quantum channels and noiseless subsystems," in *IEEE International Telecommunications Symposium*, 2006, pp. 900–905.
- [11] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.
- [12] R. A. C. Medeiros and F. M. de Assis, "Quantum zero-error capacity," *International Journal of Quantum Information*, vol. 3, no. 1, pp. 135–139, 2005.
- [13] A. Shabani and D. A. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.
- [14] E. Knill, R. Laflamme, and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, p. 2525, 2000.
- [15] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.
- [16] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.
- [17] R. A. C. Medeiros, "Zero-error capacity of quantum channels," Ph.D. dissertation, Universidade Federal de Campina Grande – TELECOM Paris Tech, 2008.
- [18] R. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis, "Quantum states characterization for the zero-error capacity," arxiv:quant-ph/0611042, 2006.
- [19] B. Schumacher and M. Westmoreland, "Quantum privacy and quantum coherence," *Physical Review Letters*, vol. 80, no. 25, pp. 5695–5697, 1998.
- [20] G. Bin, P. ShiXin, S. Biao, and Z. Kun, "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913–1918, 2009.
- [21] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208–1212, 2009.
- [22] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389–1395, 2010.
- [23] M. Hamada, "Algebraic and quantum theoretical approach to coding on wiretap channels," in *ISCCP*, 2008.
- [24] —, "Constructive codes for classical and quantum wiretap channels," In *Cryptography and Research Perspectives*, Nova Science Publishers Inc., 2008, chapter 1, pgs. 1–48.
- [25] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," arxiv/quantum-ph:1109.5346, 2011.
- [26] S. L. Braunstein, D. W. Kribs, and M. K. Patra, "Zero-error subspaces of quantum channels," in *IEEE International Symposium on Information Theory*, 2011, pp. 104–108.
- [27] S. Watanabe, "Private and quantum capacities of more capable and less noisy quantum channels," *Phys. Rev. A*, vol. 85, p. 012326, 2012.
- [28] U. Dorner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.
- [29] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.
- [30] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651–656, 2010.
- [31] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859–6866, 2008.
- [32] L. Gyongyosi and S. Imre, "Long-distance quantum communications with superactivated gaussian optical quantum channels," *Optical Engineering*, vol. 51, no. 1, 2012.

# Informação Acessível Erro-Zero de Fontes Quânticas

Elloá B. Guedes e Francisco M. de Assis

**Resumo**— Neste artigo é apresentado um conceito denominado *informação acessível erro-zero de uma fonte quântica* o qual mede a quantidade de informação compartilhada por duas partes, uma que possui uma fonte quântica e outra que possui um esquema de medição dos estados desta fonte, com a restrição de que não deve haver erros de decodificação. Nenhum método geral é conhecido para o cálculo da informação acessível em um cenário quântico geral e, em virtude disto, o limitante superior de Holevo é utilizado. Porém, no cenário erro-zero descrito, é possível obter uma fórmula fechada para tal medida, a qual coincide com a capacidade erro-zero clássica de um canal discreto e sem memória equivalente. Os resultados propostos ampliam o entendimento da Teoria da Informação Quântica Erro-Zero e de suas particularidades.

**Palavras-Chave**— Teoria da Informação Quântica Erro-Zero; Informação Acessível; Fontes Quânticas; Limitante de Holevo.

**Abstract**— We introduce a new concept called *zero-error accessible information of a quantum source* which measures the amount of information shared by two parties, one which has a quantum source, and the other which uses a measurement scheme to decode the quantum states received, upon the restriction that no decoding errors must occur. No general method to obtain the accessible information in a general quantum scenario is known and due to that the Holevo upper bound is widely used. However, in the zero-error scenario described, it is possible to determine a closed formula for such measure which coincides with the classical zero-error capacity of an equivalent discrete memoryless channel. The results described increase the understanding of Quantum Zero-Error Information Theory and its particularities.

**Keywords**— Quantum Zero-Error Information Theory; Accessible Information; Quantum Source; Holevo Bound.

## I. INTRODUÇÃO

A Teoria da Informação Quântica é um novo paradigma para o processamento e transmissão da informação por considerar as Leis da Física Quântica. Em consequência, a informação não encontra-se representada apenas sob a forma de bits, mas também de *qubits* (abreviação de *quantum bits*). Algumas características como *superposição*, *emaranhamento*, *não-clonagem* de estados arbitrários, dentre outras, são inerentes à este paradigma [1].

Uma maneira natural de explorar novos conceitos da Teoria da Informação Quântica é por meio da analogia com os conceitos clássicos equivalentes. A partir desta estratégia é que foi proposta a Teoria da Informação Erro-Zero Quântica, a qual trata do envio de informação clássica por canais quânticos sem erros de decodificação [2]. Esta teoria foi inspirada na Teoria

da Informação Erro-Zero Clássica, proposta por Shannon, que considera comunicações clássicas sem erros de decodificação, ainda que o canal seja ruidoso [3].

Ao considerar comunicações livres de erro, mesmo no cenário clássico, novos conceitos e interpretações foram formulados, tais como a capacidade erro-zero de um canal e o estabelecimento de uma relação com a Teoria dos Grafos [3], [4]. No cenário quântico, a proposição de tal teoria também teve impactos de mesma natureza, a exemplo da definição da capacidade quântica erro-zero clássica, da capacidade quântica erro-zero quântica, de uma relação análoga ao caso clássico em termos de Teoria dos Grafos, a identificação de outras capacidades e outros avanços, como a identificação de uma relação entre a capacidade erro-zero e a capacidade de sigilo de um canal quântico [2], [5]–[7].

Visando a continuação da expansão do corpo de conhecimento sobre a Teoria da Informação Quântica Erro-Zero, este artigo apresenta a definição de *Informação Acessível Erro-Zero de uma Fonte Quântica*, a qual não possui contrapartida clássica e está intrinsecamente ligada à capacidade erro-zero de canais clássicos. Enquanto a informação acessível no cenário clássico não é considerada uma medida não relevante, visto que dois estados clássicos são trivialmente distinguíveis, no cenário quântico isto não acontece devido à natureza mais complexa do tipo de informação. No cenário erro-zero quântico, em particular, ao invés obter uma aproximação da informação acessível por um limitante superior, a quantidade de Holevo, será mostrado como obter tal valor diretamente.

Para apresentar os resultados propostos, este artigo está organizado como segue. Os conceitos de informação acessível para os casos clássico e quântico serão apresentados na Seção II. Uma breve fundamentação teórica sobre a Teoria da Informação Clássica Erro-Zero será apresentada na Seção III. A definição da Informação Acessível Erro-Zero de uma Fonte Quântica será caracterizada na Seção IV. Por fim, as considerações finais e sugestões de trabalhos futuros serão apresentados na Seção V.

**Notação e Convenções:** – A notação de Dirac será utilizada para denotar estados quânticos e operações sobre eles [8]. O símbolo  $\mathbb{1}$  denota a *matriz identidade*. Os logaritmos são tomados na base 2.

## II. INFORMAÇÃO ACESSÍVEL CLÁSSICA E QUÂNTICA

Esta seção tem como objetivo a caracterização da informação acessível de fontes nos cenários clássico e quântico. A caracterização da parte clássica, em particular, é baseada na obra de Cover e Thomas [9].

Elloá B. Guedes, e Francisco M. de Assis, Instituto de Estudos em Computação e Informação Quânticas (IQuanta), Universidade Federal de Campina Grande, Av. Aprígio Veloso, 882 – Campina Grande-PB – Brazil, E-mails: {elloaguedes, fmarassis}@gmail.com. Os autores agradecem ao CNPQ, a CAPES e ao projeto QUANTA/RENASIS/FINEP.

### A. Cenário Clássico

No estudo da Teoria da Informação Clássica, toma-se como ponto de partida um modelo de um sistema de comunicações digitais ponto-a-ponto, como ilustrado na Figura 1. Neste modelo, há uma fonte transmissora e um receptor.

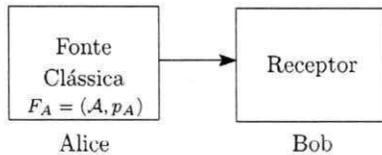


Fig. 1. Modelo simplificado de um sistema de comunicações clássico em que há apenas uma fonte e um receptor.

A *fonte*, em particular, pode ser classificada como sendo de dois tipos:

- 1) **Análogica.** Este tipo de fonte gera mensagens em forma de onda, a exemplo de um sinal de voz;
- 2) **Discreta.** Este tipo de mensagens gera símbolos de um conjunto discreto e finito, a exemplo dos bits gerados por um computador digital.

Considerando o uso de fontes discretas, uma definição formal para as mesmas é apresentada a seguir.

**Definição 1 (Fonte Clássica Discreta):** Uma fonte clássica discreta  $F_A$  é dada por um par  $F_A = (A, p_A)$  em que  $A$  é um alfabeto discreto e finito e  $p_A$  é a probabilidade de  $F_A$  gerar uma certa mensagem  $a_i$ , em que  $\sum_{i=1}^{|A|} p_A(a_i) = 1$ .

Uma medida que pode ser obtida sobre a fonte é a sua entropia, calculada de acordo com a entropia de Shannon, definida como segue.

**Definição 2 (Entropia de uma Fonte Clássica Discreta):** A entropia de uma fonte clássica  $F_A = (A, p_A)$  é dada por

$$H(F_A) = - \sum_{i=1}^{|A|} p_A(a_i) \log(p_A(a_i)), \quad (1)$$

em que  $H$  denota a entropia de Shannon. Esta medida revela o grau de incerteza sobre os símbolos gerados pela fonte.

Suponha que a fonte transmissora e o receptor realizem o seguinte “jogo”: a entidade Alice possui uma fonte clássica discreta  $A$ , a qual emite  $n$  símbolos para a entidade Bob, cujo objetivo é medir corretamente o máximo de símbolos enviados pela fonte  $A$ , ou seja, descobrir  $H(A)$ . Uma boa medida da Teoria da Informação para este fim é a *informação mútua*,  $H(A : B)$ , supondo  $B$  os resultados da medição obtidos por Bob. A partir da definição de informação mútua, define-se o conceito de *informação acessível de uma fonte clássica discreta*, conforme formalizado a seguir.

**Definição 3 (Informação Acessível de uma Fonte Clássica Discreta):** Sejam duas variáveis aleatórias  $A$  e  $B$ . A informação acessível entre estas duas variáveis, denotada por  $I_{acc}$  é dada por

$$I_{acc} = \max H(A : B), \quad (2)$$

em que  $H(A : B)$  denota a informação mútua entre as duas variáveis aleatórias em questão; e o máximo é tomado sobre todos os esquemas de medição possíveis.

Graças à desigualdade no processamento de dados, sabe-se que Bob pode inferir  $A$  a partir de  $B$  se, e somente se,  $H(A : B) = H(A)$  mas, em geral,  $H(A : B) \leq H(A)$ . Pode-se afirmar, portanto, que a proximidade entre  $H(A : B)$  e  $H(A)$  é uma medida quantitativa sobre a capacidade de Bob em determinar  $A$ .

No caso clássico, a informação acessível entre duas variáveis aleatórias não é objeto de tantas pesquisas, pois, em princípio, é sempre possível distinguir dois símbolos clássicos quaisquer, o que faz com que  $I_{acc} = H(A : B) = H(A)$ . No caso quântico, porém, como será mostrado a seguir, isto não acontece, fato que motiva a realização de estudos e pesquisas em relação a esta medida.

### B. Cenário Quântico

No estudo da informação acessível no contexto da Teoria da Informação Quântica, toma-se como ponto de partida o sistema de comunicações como ilustrado na Figura 2. A fonte quântica efetua a codificação de mensagens clássicas em estados quânticos, como apresentado na Definição 4.

**Definição 4 (Fonte Quântica):** Seja um conjunto de índices de mensagens clássicas dado por  $\{1, \dots, \ell\}$ . Uma fonte quântica é um ensemble de estados quânticos  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$  mapeados univocamente com o conjunto de índices de mensagens clássicas. A cada um destes estados quânticos está associada uma probabilidade  $p_i$ ,  $i = 1, \dots, \ell$ , tal que  $\sum_{i=1}^{\ell} p_i = 1$ .

Inicialmente, tem-se um conjunto  $\{1, \dots, \ell\}$  de mensagem clássicas e uma fonte quântica que mapeia tais mensagens em um conjunto  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$ . O receptor Bob realiza uma medição POVM (Positive Operator-Valued Measurement) no estado recebido. As saídas da medição são argumentos para a função de decodificação. O decodificador deve decidir qual mensagem clássica foi enviada por Alice.

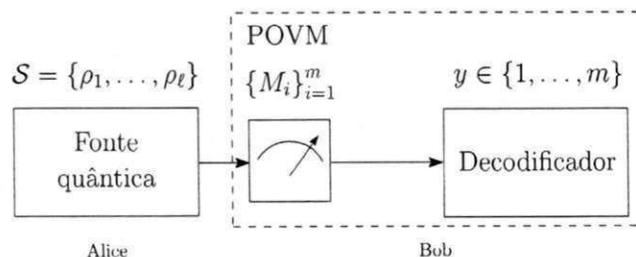


Fig. 2. Modelo simplificado de um sistema de comunicações quântico em que há apenas uma fonte e um receptor.

Levando a caracterização da fonte quântica em consideração, a mesma é um *ensemble* de estados puros ou mistos, dados por  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$  com probabilidades  $p_1, \dots, p_\ell$ . Assim como uma fonte clássica ao emitir uma seqüência de  $n$  bits pode transmitir  $2^n$  mensagens diferentes, uma fonte quântica ao enviar  $n$  qubits pode transmitir um estado quântico em um espaço de Hilbert de dimensão até  $2^n$  [10].

Se os estados de  $S$  forem todos ortogonais entre si, a fonte pode ser considerada *puramente clássica*, pois os estados são completamente distinguíveis no receptor. Se os estados de  $S$  são puros, porém não-ortogonais, então não há medição clássica capaz de extrair a informação completa sobre o estado da fonte. Uma terceira situação considera que os estados da fonte são não-ortogonais, mas cujas matrizes de densidade comutam. Para esta última situação, a fonte é considerada de *broadcast*, ou seja, dados dois sistemas quânticos que não são cópias da fonte, o traço parcial de ambos os sistemas resulta no estado da fonte [11].

A entropia de uma fonte quântica é dada pelo análogo quântico da entropia de Shannon, denominada *entropia de von Neumann*. A definição da entropia de tais fontes é apresentada na Definição 5.

**Definição 5 (Entropia de uma Fonte Quântica):** *Seja uma fonte quântica  $F$  tal como apresentada na Definição 4. Seja  $\rho = \sum_{i=1}^{\ell} p_i \rho_i$  uma média dos estados quânticos emitidos por esta fonte. A entropia de tal fonte quântica é dada por*

$$S(F) = -\text{Tr } \rho \log \rho, \quad (3)$$

em que  $S$  denota a entropia de von Neumann.

Na Teoria da Informação Quântica, nenhum método geral é conhecido para o cálculo da informação acessível de uma fonte quântica. Porém, alguns limitantes para tal medidas foram desenvolvidos, a exemplo do limitante de Holevo [10, Cap. 12].

**Teorema 1 (Limitante de Holevo):** *Suponha que Alice prepare um estado quântico  $\rho_A$ , com  $A = \{\rho_0, \dots, \rho_n\}$  e probabilidades  $p_0, \dots, p_n$ , e o envie para Bob, que realiza medições com um POVM  $\{M_i\}_{i=0}^m$  no estado recebido, obtendo  $B$ . O limitante de Holevo enuncia que, para qualquer esquema de medições que Bob utilize, tem-se*

$$H(A : B) \leq S(\rho) - \sum_{a \in A} p_a S(\rho_a), \quad (4)$$

em que  $\rho = \sum_{a \in A} p_a \rho_a$ .

O limitante de Holevo, frequentemente denotado por  $\chi$ , é um limitante superior para a informação acessível entre as variáveis  $A$  e  $B$  num cenário quântico. Levando em consideração a convicividade das entropias, tem-se que  $H(A : B) \leq \chi \leq H(A)$ . De acordo com tais condições, não existe possibilidade de Bob recuperar completamente a informação enviada por Alice, independente do esquema de medições que venha a usar. Esta situação constitui um cenário contraintuitivo quando comparado ao caso clássico equivalente.

Para exemplificar tal cenário, suponha que Alice possa enviar para Bob, de maneira equiprovável, dois estados quânticos  $\rho_0 = |0\rangle$  e  $\rho_1 = \cos \theta |0\rangle + \sin \theta |1\rangle$ , em que  $\theta$  é um parâmetro real. O limitante de Holevo em função do valor de  $\theta$  é mostrado na Figura 3, em que o máximo é atingido quando  $\theta = \pi/2$  e os estados  $\rho_0$  e  $\rho_1$  são ortogonais. Esta é a única situação em que Bob pode determinar exatamente qual estado foi preparado por Alice.

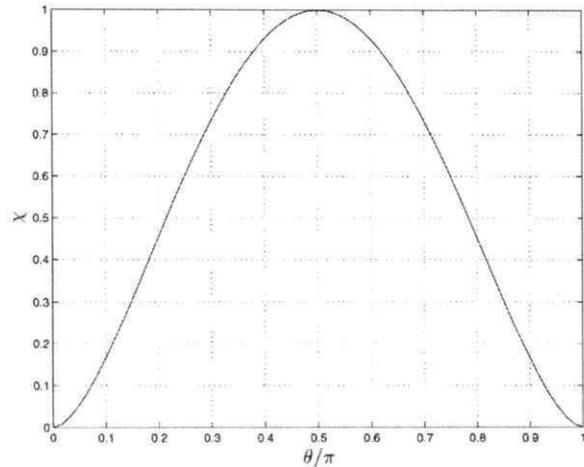


Fig. 3. Valor da quantidade de Holevo para o exemplo em questão, exibido em função da relação  $\theta/\pi$  [10, pp. 569].

### III. TEORIA DA INFORMAÇÃO ERRO-ZERO

A *capacidade erro-zero* de um canal clássico discreto e sem-memória (DSM)  $W$  foi definida por Shannon como a maior das taxas segundo a qual é possível transmitir informação com probabilidade nula de ocorrência de erros [3]. Para tanto, deve-se utilizar um código  $(M, n)$  livre de erros, cuja definição é dada a seguir.

**Definição 6 (Código  $(M, n)$  Livre de Erros):** *Um código  $(M, n)$  livre de erros para um DSM  $W : \mathcal{A} \rightarrow \mathcal{B}$  é composto dos seguintes elementos:*

- 1) Um conjunto de índices  $\{1, 2, \dots, M\}$ , em que cada índice está associado a uma mensagem clássica;
- 2) Uma função de codificação  $f_n : \{1, \dots, M\} \rightarrow \mathcal{A}^n$ , gerando palavras-código  $\mathbf{a}^1 = f_n(1), \dots, \mathbf{a}^M = f_n(M)$ ;
- 3) Uma função de decodificação  $g^n : \mathcal{B}^n \rightarrow \{1, \dots, M\}$  que associa deterministicamente um palpite para cada palavra recebida, com a seguinte propriedade

$$\Pr[g_n(\mathcal{B}^n) \neq i | \mathbf{A} = f_n(i)] = 0, \forall i \in \{1, \dots, M\}. \quad (5)$$

- 4) A taxa deste código é igual a  $R = \frac{1}{n} \log M$  bits por símbolo por uso do canal.

Na Definição 6, a Eq. (5) impõe a restrição de que erros de decodificação não são tolerados.

**Definição 7 (Capacidade Clássica Erro-Zero):** *Seja  $N(n)$  a cardinalidade máxima de um conjunto de vetores ortogonais entre os vetores de  $W^n(\cdot | \mathbf{a}^n)$ . A capacidade erro-zero clássica do canal DSM  $W$  é dada por*

$$C_0 = \limsup_{n \rightarrow \infty} \frac{1}{n} \log N(n). \quad (6)$$

#### A. Relação com a Teoria dos Grafos

A capacidade clássica erro-zero permite uma interpretação em termos da Teoria dos Grafos [3]. Dado um canal DSM  $W$  e

um conjunto de índices de mensagens  $\{1, \dots, M\}$ , é possível construir um grafo característico  $\mathcal{G} = \langle V, E \rangle$  como segue:

- $V = \{1, \dots, M\}$  é o conjunto de vértices contendo os índices do conjunto de mensagens clássicas;
- $E = \{(i, j) | f_n(i) \perp_W f_n(j), i \neq j\}$ , em que  $\perp_W$  denota dois vetores ortogonais na saída do canal  $W$ .

Esta noção de grafo característico também pode ser estendida para o  $n$ -produto de  $\mathcal{G}^n$ , em que  $V = V^n$  e  $E$  é composto pelos pares cujos índices correspondentes na sequência são não-adjacentes em  $W$ .

**Definição 8 (Capacidade Erro-Zero em Termos de Grafos):** A capacidade erro-zero de um canal DSM  $W$  é dada por

$$C_0(W) = \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n), \quad (7)$$

em que  $\omega(\mathcal{G}^n)$  é o número de clique do  $n$ -produto do grafo característico  $\mathcal{G}$ .

Para ilustrar a capacidade erro-zero, suponha um canal clássico  $W_1$  tal como ilustrado na Figura 4a. O grafo característico deste canal é mostrado na Figura 4b. Embora possa-se *a priori* cogitar que a capacidade erro-zero deste canal é 1 bit por símbolo por uso do canal, este é um caso não-trivial em que esta capacidade só é atingida após 2 ou mais usos do canal, sendo igual a  $C_0(W_1) = \frac{1}{2} \log 5$  bits por símbolo por uso do canal por meio do código  $\{00, 12, 24, 31, 43\}$ . O cálculo da capacidade erro-zero do canal em questão foi um problema proposto por Shannon [3] e resolvido mais de 20 anos depois por Lovász [12].

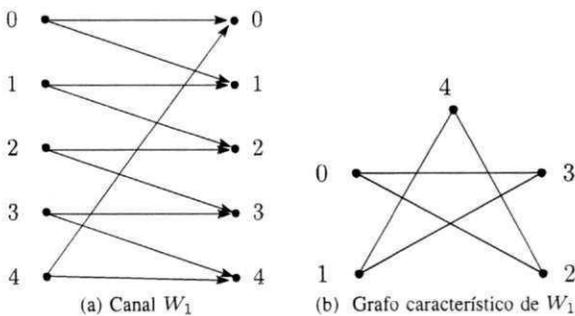


Fig. 4. Exemplo de positividade e não-trivialidade de capacidade erro-zero do canal DSM  $W_1$ .

#### IV. INFORMAÇÃO ACESSÍVEL ERRO-ZERO DE UMA FONTE QUÂNTICA

Seja uma fonte quântica discreta e sem-memória produzindo uma sequência i.i.d. de *letras quânticas* obtidas a partir de um conjunto  $\mathcal{S} = \{|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_\ell\rangle\}$  com probabilidades  $p_0, p_1, \dots, p_\ell$  associadas a um conjunto de índices de mensagens clássicas  $\{0, 1, \dots, \ell\}$ . O conjunto  $\mathcal{S}$  é o *alfabeto* da fonte quântica e, para fins de conveniência, será adotada a notação  $\rho_i = |\psi_i\rangle\langle\psi_i|$  em favor de  $|\psi_i\rangle$ . As letras de  $\mathcal{S}$  são estados puros, mas não necessariamente ortogonais entre si. À fonte quântica em questão está associada a seguinte matriz densidade

$$\rho = \sum_{i=0}^{\ell} p_i \rho_i. \quad (8)$$

Assume-se que *Alice* possui uma fonte quântica com a descrição dada. Ela envia diretamente os símbolos produzidos pela fonte para *Bob*, o qual utiliza *medições de letra isolada* via um POVM  $\mathcal{M} = \{M_i\}_{i=0}^m$  com o intuito de identificar qual mensagem correspondente foi enviada por *Alice*.

No processo de identificação das mensagens recebidas por *Bob*, admite-se que *erros de decodificação não são tolerados*, ou seja, considera-se apenas o caso que, com 100% de certeza, *Bob* é capaz de identificar precisamente, por meio da medição realizada, qual estado foi enviado por *Alice*. A partir destas considerações é possível definir o conceito de *Informação Acessível Erro-Zero (IAEZ)* de uma fonte quântica.

**Definição 9 (Informação Acessível Erro-Zero de uma Fonte Quântica):** Seja  $A$  uma variável aleatória discreta correspondendo ao índice de uma mensagem associado a uma letra quântica enviada por uma fonte quântica discreta e sem memória. Seja  $B$ , por sua vez, uma variável aleatória discreta correspondendo ao resultado da medição da letra quântica enviada pela fonte por meio da utilização de uma medição de letra isolada com um POVM  $\mathcal{M}$ . A informação acessível erro-zero da fonte quântica em questão, denotada por  $I_{acc}^{(0)}$ , corresponde ao maior número de mensagens enviadas pela fonte tais que  $H(A|B) = 0$ .

**Teorema 2 (Expressão Numérica para a IAEZ):** Seja  $N(n)$  o número de letras quânticas de comprimento  $n$  que podem ser enviados por uma fonte quântica discreta e sem memória e recuperados livres de erro por um POVM via medições de letra isolada. A informação acessível erro-zero de uma fonte quântica discreta e sem-memória é dada por

$$I_{acc}^{(0)} \triangleq \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n). \quad (9)$$

**Demonstração:** A demonstração deste teorema utiliza como estratégia a equivalência entre a emissão de uma letra pela fonte e a sua respectiva medição de letra isolada com um canal clássico discreto e sem-memória.

Levando em consideração o tipo de medição adotada, é possível descrever o estado produzido pela fonte e a saída do POVM como um canal clássico discreto sem memória  $W: A \rightarrow B$  com a seguinte matriz estocástica

$$W(a, b) \triangleq \Pr[B = b | A = a] = \text{Tr}(\rho_a M_b), \quad (a, b) \in \mathcal{A} \times \mathcal{B}, \quad (10)$$

em que  $\rho_a$  é a letra quântica emitida pela fonte;  $M_b$  é o elemento de operação do POVM utilizado para medição; e  $\mathcal{A}$  e  $\mathcal{B}$  são os alfabetos das variáveis aleatórias  $A$  e  $B$ . No caso da fonte emitir  $k$  letras quânticas, tem-se

$$W^k(a^k, b^k) = \prod_{i=1}^k W(a_i, b_i). \quad (11)$$

Considerando esta interpretação, a maior quantidade de símbolos que podem ser enviados pelo canal  $W$  sem erros de decodificação é igual à sua capacidade erro-zero, ou seja,  $I_{acc}^{(0)} = C_0(W) = \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n)$ . Conclui-se, então, a prova em questão. ■

A Definição 9 e o Teorema 2 revelam um aspecto interessante a respeito das fontes quânticas. Se medições de letra isolada forem adotadas, a IAEZ das fontes quânticas reduz-se ao caso de calcular a capacidade erro-zero de um canal clássico, isto é, os aspectos quânticos de obter tal medida de informação não emergem neste cenário em particular. Vale salientar ainda que não há a qualquer imposição sobre a ortogonalidade das letras quânticas emitidas pela fonte, o que poderia forçá-la, por exemplo, a equivaler a uma fonte clássica.

É importante enfatizar que a definição de informação acessível erro-zero de uma fonte quântica impõe uma restrição, que é a ausência de erros. Com isto, tem-se que as desigualdades  $I_{acc}^{(0)} \leq I_{acc} \leq \chi$  podem ser verificadas.

Para ilustrar os conceitos apresentados nesta seção, um exemplo detalhado será apresentado a seguir, no qual a IAEZ de uma fonte quântica será obtida e comparada com a quantidade de Holevo.

A. Exemplo

Suponha que Alice possui uma fonte quântica discreta e sem-memória cujo conjunto de mensagens clássicas  $\{0, 1, 2, 3\}$  é mapeado univocamente para o conjunto de letras quânticas  $\mathcal{S} = \{\rho_0, \rho_1, \rho_2, \rho_3\}$ , em que  $\rho_0 = |0\rangle\langle 0|$ ,  $\rho_1 = |1\rangle\langle 1|$ ,  $\rho_2 = |+\rangle\langle +|$  e  $\rho_3 = |-\rangle\langle -|$  com  $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$  e  $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ . Tais letras são emitidas pela fonte de maneira equiprovável, ou seja,  $p_i = \frac{1}{4}$ ,  $i = 0, \dots, 3$ . É interessante notar que os estados emitidos pela fonte são puros, embora não necessariamente ortogonais entre si. Por exemplo, embora  $\langle 0|1\rangle = 0$ , tem-se que  $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$ . Para efetuar as medições de letra isolada, Bob utiliza o POVM  $\mathcal{M} = \{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$ .

Levando em consideração a fonte quântica e o POVM utilizado para medição, como consequência do Teorema 2, é possível construir um canal clássico  $W_2$  como mostrado na Figura 5a. A partir desta representação é possível obter o grafo característico deste canal, o qual encontra-se ilustrado na Figura 5b.

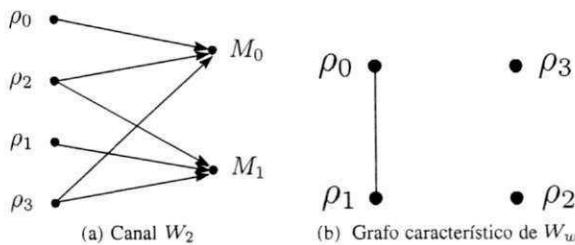


Fig. 5. Exemplo de canal clássico  $W_2$  construído a partir de uma fonte quântica conforme Teorema 2.

A partir do grafo característico de  $W_2$  é possível constatar que o número de clique do mesmo é igual a 2, ou seja, tem-se  $C_0(W_2) = \log 2 = 1$  bit por símbolo por uso do canal. Em virtude do Teorema 2, tem-se que a informação acessível erro-zero desta fonte quântica é igual a  $I_{acc}^{(0)} = 1$  bit por símbolo. A partir do exemplo em questão, embora a fonte quântica não seja redutível a uma fonte clássica, é possível que 1 bit por símbolo seja obtido a partir desta fonte por uma medição de letra isolada e livre de erros.

Utilizando os dados do conjunto  $\mathcal{S}$ , tem-se que a quantidade de Holevo para esta situação é igual a  $\chi = 1$ . Nota-se que, como previsto,  $\chi \geq I_{acc}^{(0)}$ .

V. CONSIDERAÇÕES FINAIS

Neste artigo foi apresentado o conceito de informação acessível erro-zero de uma fonte quântica, definido como sendo o maior conjunto de mensagens que podem ser emitidas por esta fonte e recuperadas por medições de letra isolada e sem erros de decodificação. Foi visto que esta medida de informação pode ser compreendida como a capacidade erro-zero de um canal clássico elaborado a partir de uma interpretação do cenário proposto.

A informação acessível de uma fonte clássica é trivialmente obtida. Para as fontes quânticas com estados não-ortogonais, não há uma forma direta de obtenção da informação acessível e, portanto, utiliza-se o limitante de Holevo. Em relação à informação acessível erro-zero de uma fonte quântica, por sua vez, existe uma fórmula conhecida para a sua obtenção. Embora a fonte seja verdadeiramente quântica, esta fórmula envolve a representação de um canal clássico, revelando uma característica peculiar e não-trivial do cenário erro-zero das comunicações quânticas.

Em trabalhos futuros almeja-se explorar esta medida das fontes quânticas, porém considerando o uso de medições coletivas e também pares ótimos de letras quânticas e POVMs para o cenário erro-zero, tal como proposto por Medeiros e outros [13].

REFERÊNCIAS

- [1] S. Inre and F. Balazs, *Quantum Computing and Communications - An Engineering Approach*. John Wiley & Sons, 2005.
- [2] R. A. C. Medeiros, "Zero-error capacity of quantum channels." Ph.D. dissertation, Universidade Federal de Campina Grande - TELECOM Paris Tech, 2008.
- [3] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8-19, 1956.
- [4] J. Korner and A. Orlitsky, "Zero-error information theory," *IEEE Transactions on Information Theory*, vol. 44, pp. 2207-2229, 1998.
- [5] R. A. C. Medeiros and F. M. de Assis, "Quantum zero-error capacity," *International Journal of Quantum Information*, vol. 3, no. 1, pp. 135-139, 2005.
- [6] R. Duan, S. Severini, and A. Winter, "Zero-error communication via quantum channels, non-commutative graphs and a quantum lovasz  $\vartheta$  function," 2011, in *IEEE International Symposium on Information Theory*. Disponível em arxiv:quant-ph/1002.2514.
- [7] E. B. Guedes and F. M. de Assis, "Quantum zero-error secrecy capacity," in *Workshop School of Quantum Computation and Information*, 2012, pp. 1-8.
- [8] P. Dirac, *The principles of Quantum Mechanics*, 4th ed. Oxford University Press, 1982.
- [9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2006.
- [10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Bookman, 2010.
- [11] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, 1998.
- [12] L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Info. Theory*, vol. 25, no. 1, pp. 1-7, 1979.
- [13] R. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis, "Zero-error capacity of quantum channels and noiseless subsystems," in *IEEE International Telecommunications Symposium*, 2006, pp. 900-905.

# AN APPROACH TO EVALUATE QUANTUM AUTHENTICATION PROTOCOLS

Elloá B. Guedes, Francisco M. de Assis

IQuanta – Institute for Studies in Quantum Computation and Quantum Information  
Federal University of Campina Grande  
Rua Aprígio Veloso, 882 – Campina Grande – Paraíba – Brazil  
{elloaguedes, fmarassis}@gmail.com

**Resumo** – Protocolos quânticos de autenticação possuem um papel importante em esquemas de Criptografia Quântica, pois visam assegurar a origem de certa informação ou a identidade de uma das partes da comunicação. Embora muitos protocolos com este propósito tenham sido propostos, não se conhecem métodos sistemáticos capazes de permitir comparações entre eles nem tampouco determinar quais os recursos demandados por um protocolo em particular. Na tentativa de minimizar esta limitação, este artigo apresenta uma abordagem baseada na Complexidade Comunicacional Quântica que possibilita avaliar protocolos quânticos de autenticação a partir do número de informações trocadas entre as partes – uma característica comum a todos os protocolos desta natureza. A abordagem proposta pode ser aplicada na Criptografia Quântica com o intuito de auxiliar a escolha e a classificação dos protocolos mais adequados para um determinado cenário, considerando os recursos disponíveis. Além disso, este artigo apresenta resultados sobre a aplicação da metodologia proposta em alguns protocolos quânticos de autenticação, ampliando os conhecimentos sobre a literatura existente.

**Palavras-chave** – Complexidade Comunicacional Quântica, Protocolos Quânticos de Autenticação, Computação e Informação Quânticas.

**Abstract** – Quantum authentication protocols play a major role in Quantum Cryptography schemes because they ensure the origin of data or the identity of a party in the communication. In face of different definitions for such protocols, no systematic procedures to allow comparisons between them nor to define the resources required were defined in the literature. In the attempt to overcome this limitation, this paper presents an approach based on Quantum Communication Complexity that enables the evaluation of quantum authentication protocols regarding the information exchanged between the parties – a characteristic present in every protocol. This approach can be applied in practical scenarios of Quantum Cryptography helping one to rank and choose the best protocol based on the communication resources available. Furthermore, this paper presents the results of the application of such approach in some quantum authentication protocols, increasing the knowledge about the existing literature.

**Keywords** – Quantum Communication Complexity, Quantum Authentication Protocols, Quantum Computation and Information.

## 1 INTRODUCTION

Quantum Cryptography comprehends both Quantum Mechanics and Information Theory. As the classical Cryptography, its objectives goes beyond confidentiality and include methods to provide data integrity, non repudiation and authentication [1]. In particular, *authentication* concerns the procedures to verify the origin of some data or to verify the identity of a party in the communication. For this reason, authentication is subdivided in *data origin authentication* and in *entity authentication*.

In the Quantum Cryptographic domain, authentication is performed by *quantum authentication protocols* which are *distributed algorithms* based on the intrinsic properties of Quantum Mechanics. Quantum authentication protocols differ from the classical ones in at least three aspects: they are not based in some computational difficulty; they don't allow information copy; and, they may allow eavesdropping detection [2]. In association with quantum key distribution protocols, they play an important role in providing trusty quantum communication in the presence of eavesdroppers.

Given the importance of authentication in quantum communication, several protocols for quantum authentication have been proposed in the literature [2–11]. They use different procedures and resources of the Quantum Mechanics to perform the authentication, such as: Einstein-Podolsky-Rosen (EPR) pairs (i.e., a maximally bipartite entangled state), superposition, catalysis, unitary operations, among others.

Considering that quantum states are very delicate [12], a crucial concern in the adoption of a certain quantum authentication protocol is the number of communications performed. A protocol that minimizes such number but that still ensures secure authentication can be considered well suited to practical scenarios of Quantum Cryptography. However, little is known about the existing protocols in this perspective and this lack of knowledge can unfavor comparisons and wise choices of quantum authentication protocols.

Taking into account these concerns, in this paper we propose an approach of evaluation and classification of quantum authentication protocols based on the determination of their *Quantum Communication Complexity* – a measurement of the amount of

communications carried out between the parties in order to accomplish some distributed task [13]. As far as we know, no similar approaches to analyze quantum authentication protocols were found in the literature.

The main result of our proposition is that it turns out to be possible the determination of the resources required by a certain protocol and the realization of systematic comparisons between different quantum authentication protocols. It is important in practical scenarios of Quantum Cryptography because authentication protocols can be ranked and chosen according to the communication resources available.

Furthermore, this paper presents the application of our proposed methodology in ten quantum authentication protocols. This illustrates how the approach can be applied and brings new results about the characteristics and advantages of quantum authentication protocols existing in the literature.

The rest of the paper is organized as follows. Section 2 introduces the basics concepts of the Quantum Communication Complexity. Section 3 presents the formalism and concepts regarding quantum authentication protocols. Section 4 introduces the approach proposed and Section 5 shows the results of our analysis in some existing quantum authentication protocols. Lastly, Section 6 draws the conclusions and suggestions for future work.

## 2 QUANTUM COMMUNICATION COMPLEXITY

With the advents of telegraph and telephone in the mid-twentieth century, there was an urge to perform the tasks of store, transmit and process data. Motivated by these practical problems, the *Information Theory* was proposed [14]. Shannon laid its foundations with an article entitled “*A Mathematical Theory of Communications*” [15] where he defined precisely what is information and how to measure it, and also demonstrated the existence of codes to error-free communication when the channel capacity is respected.

It is important to emphasize that the necessity to communicate arises when two or more parties need to collaborate jointly to accomplish a task that none of them can perform alone. In Information Theory, the objective is to study *how* this communication must be performed – which codes to use, how to deal with noisy channels, and so on. Another perspective that can be taken into account when a communication needs to be carried out is *what* needs to be communicated. This is the object of study of Communication Complexity [16, 17].

With the consideration of quantum information exchange mainly in theoretical but also in emergent practical scenarios, Yao [18] was a pioneer in considering the concerns of Communication Complexity in this domain. It was needed to understand the implications of a communication that makes use of Quantum Mechanics resources with the purpose to answer a central question: “Are there any advantages in the quantum communication model when compared to the classical existing ones?”

In the study of Quantum Communication Complexity it is considered that two *parties*, say Alice and Bob, are interested in evaluate a certain  $f(x, y)$ , where  $x$  is known only by Alice and  $y$  is known only by Bob. Alice and Bob must exchange information through a supposed error-free quantum *channel* according to some *protocol* which can be understood as a distributed algorithm. The main interest in this scenario is the *amount of communication* necessary to the parties accomplish their task.

According to the resources of Quantum Mechanics available to Alice and Bob, there are three variants of the Quantum Communication Complexity model that can be considered:

1. **Yao’s model** [18, 19]. This model considers a *quantum channel* which will enable exchanges of qubits between Alice and Bob. Each party of the communication interacts with the channel via unitary operations, depositing qubits that can be accessed by the other part also via unitary operations with the channel. When Alice and Bob determine precisely the value of  $f(x, y)$  the protocol ends and the number of communications is considered. In this variant, the Quantum Communication Complexity of a function  $f$  is denoted by  $Q(f)$ ;
2. **Cleve and Buhrman’s model** [20]. This model considers the existence of *prior entanglement* between the parties and allows the exchange of information via a classical channel. In this variant, the number of entangled pairs is not considered, just the number of classical bits exchanged. In this variant, the quantum communication complexity of a function  $f$  is denoted by  $C^*(f)$ . It is important to emphasize that this model is well suited to analyze protocols where superdense coding and teleportation are used;
3. **Hybrid Model**. This variant combines the characteristics of the previous two: there are *entangled pairs* available to the parties of the communication, a *quantum channel*, and also a *classical channel*. In the determination of the Quantum Communication Complexity the entangled pairs used are not considered, just the further information exchanged. In this variant, the Quantum Communication Complexity of a function  $f$  is denoted by  $Q^*(f)$ .

In all the three variants considered, we assume that the parties must determine precisely the value of  $f(x, y)$ , i.e., the function  $f$  must be evaluated with probability of error equal to zero. A more detailed description of these models and alternative definitions that enables a limited error can be found in the surveys of Wolf [13] and Brassard [21].

The theory of Quantum Communication Complexity has still open questions that need to be enlighten, such as about the existence or not of an exponential gap between Classical and Quantum Communication Complexity for all functions. Despite this, applications of Quantum Communication Complexity are growing every day. Results on quantum formula [18], finite automata size [22], data structures [23], and on security of quantum key distribution [24] have already been developed.

The most interesting aspect of Quantum Communication Complexity is that the advantage provided by Quantum Mechanics has been established rigorously. This is in sharp contrast with the field of Quantum Computing, in which it is merely believed that Quantum Mechanics allows for an exponential speedup in some computational tasks [21].

### 3 QUANTUM AUTHENTICATION PROTOCOLS

Authentication is a well-studied area of classical cryptography. It is concerned with assuring that a communication is authentic. In the case of a single message, the function of the authentication is to assure the recipient that the message is from the party that it claims to be from. In the case of an ongoing interaction, two aspects are involved: first, at an initial time, the objective is to assure that the two parties are authentic, that is, that each is the party that it claims to be; after that it must be assured that the connection is not interfered in such a way that an eavesdropper can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception [25].

Aiming to provide these two functions, authentication must be achieved in two branches:

1. **Data Origin Authentication.** Enables the recipient to verify that the message has not been tampered *en route* and that it originates from the expected sender;
2. **Identity Authentication.** Enables the recipient to verify that a sender is who his claims to be. If some security conditions are guaranteed, it also enables the recipient to ensure that no one else is impersonating the true sender.

To illustrate how authentication works consider a simple symmetric key model of authentication consisted of a sender (Alice), a receiver (Bob), and an eavesdropper (Eve) as illustrated in the Figure 1. The objective in this model is to enable Bob to authenticate a message sent by Alice. To do so, in a previous moment Alice and Bob securely share a key  $k$  that will be used to authentication.

Alice encrypts the original message  $m$  with the key  $k$  using an algorithm  $E$ , producing  $m_c = E(m, k)$  (Step 1). Alice sends  $m_c$  to Bob through an insecure channel which is being eavesdropped by Eve (Step 2). It is assumed that Eve can observe all the information transmitted from the sender to the receiver and also that, in general, she knows even the original message, but not the key used to encrypt it.

There are two kinds of possible attacks by the opponent: the *impersonation attack* in which Eve sends a message in the hope that it will be accepted by the receiver Bob as a valid one; and the *substitution attack* in which he opponent observes a transmitted message and then replaces it with another message.

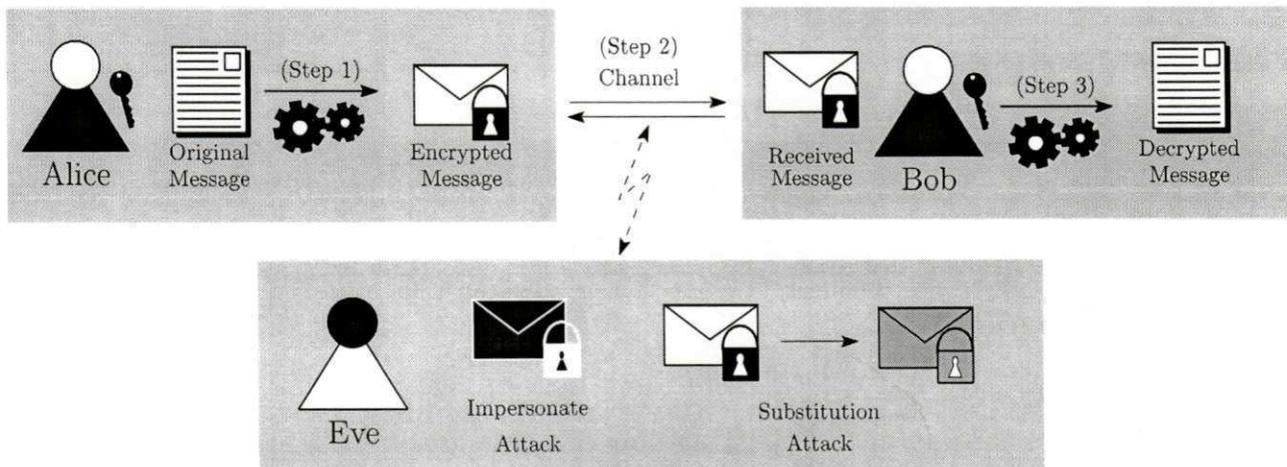


Figura 1: Symmetric Key Model of Authentication.

Upon receiving a message, Bob will use his key  $k$  and a decryption algorithm  $D$  to try recover the original message, i.e., he will perform  $D(m_c, k)$  (Step 3). If no tampering occurred, Bob will obtain a pair  $\langle m, 1 \rangle$  where  $m$  is the original message sent by Alice and 1 indicates that the authentication was successful. Otherwise, Bob must discard and ask Alice to send again [1, 26].

In the quantum setting, despite the same objective, quantum authentication workings is performed slightly differently from its classical counterpart. It happens because the information considered is *physical* and, for that reason, behaves according to the laws of Quantum Mechanics. Due to this, the *quantum authentication protocols* must obey such physical laws which define how to represent and exchange information.

To send a message  $m$  to Bob according to a quantum authentication protocol, Alice encodes  $m$  with a certain code before sending it. However, if the same code is always used, Eve can simply create errors that the code cannot detect, damaging the communication between the legitimate parties. Because of that Alice and Bob must use one of a family of codes which detect different kinds of errors. The key  $k$  now tells them which code to use. Since Eve doesn't know  $k$ , she doesn't know which errors

the code detects, and no matter what she tries to do, she has a good chance of getting caught. Besides, Alice and Bob must also encrypt the quantum state in order to avoid possibly undetectable changes in the quantum state performed by Eve [3].

In comparison with the classical protocols, the quantum ones differ in several potentially useful ways. The primary contrast between them regards how information is represented and exchanged – while the classical protocols are restricted to bits, in the quantum scenario the parties can use qubits, entangled particles and even bits. Another difference regards the action of the eavesdropper. In the classical scenario, Eve would break into the classical storage area and copy Bob's key without leave any evidence. After that, she would use it to communicate with Alice who might not realize anything wrong for quite a while. However, in the quantum scenario it is improbable to occur. The no-cloning theorem not only makes undetected theft of key more difficult, but also protects a stolen key from dissemination [10]. Furthermore, in the quantum domain, authentication implies encryption which is not always true in the classical scenario [3].

Quantum authentication plays a major role in Quantum Cryptography because they precede the execution of the so called quantum key distribution (QKD) protocols. Such protocols provide the conditions to the parties produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages [27]. Since QKD protocols require previous authentication and considering the recent successful results about their implementation over long distances [28], there was a motivation for the presentation of a formal definition [3] and for the proposition of quantum authentication protocols in the literature [2, 4–11].

## 4 THE PROPOSED APPROACH

As stated in the Section 3, the purpose of the interaction of the two parties in a quantum authentication protocol is to enable the verifier Bob to evaluate  $D(m_c, k) = \langle m, \text{valid} \rangle$ , where  $m$  is the original message sent by Alice. Introducing some formalism, a quantum authentication protocol can be represent as a function  $f_A : M \times K \rightarrow \{0, 1\}$  that evaluates to 1 if  $D(m_c, k) = \langle m, \text{valid} \rangle$ , and to 0 otherwise. To make a distinction between data origin and identity authentication protocols, we will denote the corresponding functions by  $f_D$  and  $f_I$ , respectively.

Different quantum authentication protocols can implement  $f_D$  and  $f_I$  [2–11]. Therefore, it is natural to look for ways to compare them in order to choose one that is better or more adequate to certain available resources. Despite the differences between the implementations of all these protocols, they share a common characteristic – communications are performed between the parties.

Taking the communications between the parties into account and remembering that quantum states are delicate [12] and also that the channel is subject to eavesdropping (that may affect the quantum states), a quantum authentication protocol can be considered good if it *minimizes the number of communications* between the parties but still assures a *secure authentication*. In order to meet the stated criteria, we present an approach based on the analysis of the quantum communication complexity of a quantum authentication protocol, defined as follows:

**Definition 4.1 (Quantum Communication Complexity of a Quantum Authentication Protocol)** Let  $\mathcal{P}$  be a quantum authentication protocol between two parties  $A$  and  $B$  that computes a function  $f_A : M \times K \rightarrow \{0, 1\}$  (that can be  $f_D$  or  $f_I$ ). The Quantum Communication Complexity of  $f_A$  under  $\mathcal{P}$  is the minimum number of communications between  $A$  and  $B$  to (i) allow both parties to compute  $f_A(m_c, k)$  where  $m_c$  and  $k$  are the worst case over all inputs  $M \times K$  (i.e., the cost of the protocol is maximal), and to (ii) avoid an eavesdropper Eve to create any  $m'$  such that  $f_A(m', k) = 1$  or to evaluate  $f_A(m_c, k) = 1$ .

Regarding the assumption that the computational power is unlimited, the security that avoids Eve to create any  $m'$  such that  $f_A(m', k) = 1$  or to evaluate  $f_A(m_c, k) = 1$  is desired to be unconditional. An exponentially low probability of success in the attacks is also acceptable, but there are quantum authentication protocols that still rely on unproven computational difficulties. Protocols with this last mentioned characteristic are more susceptible when compared to the two others.

It is important to emphasize that the definition of quantum communication complexity of a quantum authentication protocol used by our approach is slightly different from the original one of quantum communication complexity. In the original definition if one of the parties is able to determine the evaluation of the function, it is enough to communicate it to the other party. However, in our definition it is not allowed: the presence of the eavesdropper avoids Alice to send  $m$  directly to Bob or to perform any communication that may reveal  $k$ .

Another consideration that must be made regards the resources of Quantum Mechanics required by each protocol. In the determination of the quantum communication complexity of a quantum authentication protocol, each protocol will be evaluated according to one of the three variants – Yao, Cleve and Buhrman, or Hybrid – presented in the Section 2. Moreover, for reference, the quantum communication complexity will be denoted in function of the size of the key and of the message.

Our approach, therefore, can be described in a straightforward way considering the definitions previously presented in the Sections 2 and 3. To evaluate a quantum authentication protocol firstly it is necessary to determine the Quantum Mechanics resources required – quantum bits, classical bits and/or previously shared entangled pairs. After that, with a key of  $n$  bits and a message of  $m$  bits (if they exist), perform an execution of the protocol supposing that no impersonation nor substitution attacks occur. From this execution, it is necessary to verify how much information was exchanged between the parties to compute  $f_A$ . The information exchanged must be expressed in terms of  $n$  and  $m$ . As the final step, according to the resources identified in the initial moment, the information exchanged must be represented in accordance with the respective model, i.e., using  $Q$ ,  $C^*$  or  $Q^*$ .

Upon analyzing a quantum authentication protocol according to our approach, the final result is a concise notation of what resources it demands and how many communications are performed, considering a key and a message of a generic size. If the

exact number of communications may vary depending on certain situations, this approach also allows an asymptotic notation where the upper and lower bounds as well as best, average, and worst cases can be individually analyzed.

The asymptotic notation can also be used to measure the effort necessary so the parties can recover from an eavesdropper attack. If the attack is detectable, it is necessary to measure the resources to recover from it and to still ensure the authentication. A certain quantum authentication protocol may require the parties to discard and restart from the initial point while other can reuse the non-tampered data, saving on the number of communications. If the evaluation of a protocol will be made considering the action of an eavesdropper, its quantum communication complexity will be denoted as  $Q_E$ ,  $C_E^*$ , or  $Q_E^*$  according to the most adequate model.

The comparisons between quantum authentication protocols are also possible thanks to the proposed approach. Following the procedures previously described, the evaluation of the quantum communication complexity of each protocol must be performed independently. After that, the results obtained must be grouped according to the respective model and, then, ordered. The lower result in each group indicates the protocol that requires less communications to provide authentication, i.e., that best fits the previously state criteria. It is also important to emphasize that no comparisons between protocols classified under different groups are possible – the resources involved are of different nature and their comparison can lead to misleading conclusions.

Based on our investigation in the literature, no similar methods to analyze quantum authentication protocols were found. So, the approach presented is a seminal contribution to overcome this limitation. Pursuing this further, there are advantages of our approach that need to be highlighted: it characterizes a systematic procedure to evaluate quantum authentication protocols; its evaluation is intuitive, based only on the protocol execution; the resulting measure is a concise notation of what resources a quantum authentication protocol demands and how many communications are performed; it allows comparisons between protocols; it makes possible to analyze the communication effort when an eavesdropping occurs; and, lastly, it is likely to be applied in almost any quantum authentication protocol.

## 5 EVALUATING THE QUANTUM COMMUNICATION COMPLEXITY OF QUANTUM AUTHENTICATION PROTOCOLS

In order to illustrate the proposed approach, this section shows the evaluation of the quantum communication complexity of quantum authentication protocols existing in the literature. The results obtained and the conclusions achieved are presented in the following subsections according to the purpose of the protocol – data origin authentication or identity authentication.

### 5.1 Results for Data Origin Authentication

The first proposal of a quantum authentication protocol was made by Barnum et al. [3]. In their protocol, Alice and Bob use purity testing codes and make a prior agreement on some parameters that will be used (two keys, purity code, and syndrome). After that, they carry out the protocol that enables Bob to authenticate the message sent by Alice in a single communication to him. Considering that this protocol requires only qubits exchanges between the parties, in our approach its analysis will be made with the Yao's model. If a message has  $m$  qubits, Alice will send Bob a quantum coded message of  $m + n$  qubits, where  $n$  is the size of a security parameter as a key. Therefore, the quantum communication complexity of this protocol is  $Q(f_D) = m + n$ .

In the quantum data origin authentication protocol proposed by Yang et al. [4], Alice wants to send a message composed by a sequence of pure states. To do so, she encodes it with a Goppa code using parameters previously securely shared with Bob. The encoded message that will go through the channel has twice the qubits of the original one. When Bob receives such message he decodes it with an unitary operator built from the parameters of the Goppa code in use. The decoding procedure uses up to five registers where, in particular, the fifth (stores the original message) and the third (stores an authentication flag) must be measured. It should be noticed that this protocol only requires qubits exchanges which implies the analysis of its Quantum Complexity Communication with the Yao's model. Each message with  $m$  qubits is codified with a Goppa code using  $2 \cdot m$  qubits, therefore,  $Q(f_D) = 2 \cdot m$ . In conclusion, the security of this protocol relies on the computational hardness of building the decoding operator without the knowledge of the security parameters.

The quantum authentic protocol proposed by Curty and Santos [5] uses a code to protect the message that will be sent through the channel. Alice and Bob start the protocol already sharing a singlet state. When Alice wants to send a bit of the message to Bob she prepares two qubits in the state  $|\phi_i\rangle$ , where  $|\phi_0\rangle$  and  $|\phi_1\rangle$  are orthogonal states and represent the classical bits "0" and "1", respectively. After that Alice encodes the qubit along with her part on the singlet and send it to Bob. Upon receiving the message, Bob uses a decoding operator and is able to detect, with high probability, when a tampering occurred and when the message is authentic from Alice. In this protocol, the parties use qubits and a previously entangled pair, but no classical communication is performed between them. This implies that the Hybrid model must be used in the analysis. As explained before, to each bit of the classical message that Alice wants to send Bob, she must use a two qubits state. Hence, the quantum communication complexity of this protocol is  $Q^*(f_D) = 2 \cdot m$ .

Li and Zhang [6] present a message authentication protocol that uses previously shared EPR pairs between the parties. When Alice wants to send a bit to Bob she codifies it in a quantum system before sending to Bob. She uses a redundant coding, in which two qubits (in Bell states) codes one bit of information, and performs a CNOT operation with her half of the EPR pair. When Bob receives such state, he also performs a CNOT operation (on his half and on the received qubit) followed by a measurement. Bob is able to recover the original message sent by Alice and also to detect eavesdropping. In the described protocol the parties use entangled pairs and exchange qubits, but they don't perform classical communication. It is possible to conclude, thus, that

the model to analyze it is the Hybrid one. Moreover, Alice uses a codification where 1 bit is codified in 2 qubits. This way, the quantum communication complexity of this protocol is  $Q^*(f_D) = 2 \cdot m$ .

In the four protocols analyzed, two of them were evaluated under the Yao's variant and the other two under the Hybrid variant. Regarding the first group, the Barnum et al. [3] protocol may have smaller quantum communication complexity than the protocol of Yang et al. [4] when  $n < m$ , but the security issues must be considered. The other two protocols have equivalent quantum communication complexity. It is also important to notice that none of the protocols analyzed make use of classical communications.

## 5.2 Results for Identity Authentication

In the identity authentication quantum protocol proposed by Kanamori et al. [7, 29] Alice and Bob share a prior key  $K = \{\theta_i : 0 \leq \theta_i < \pi, i = 1, 2, \dots, n\}$  composed of a sequence of angles. Alice generates a random  $n$ -bit string  $R_A$  and encodes it into a system  $|\psi_{R_A}\rangle$  of  $n$  qubits in orthogonal states ( $|0\rangle$  or  $|1\rangle$ , for instance). In sequence, Alice rotates each qubit  $|\psi_{A,i}\rangle$  according to an angle  $\theta_i \in K$ , encrypting the original quantum state. After that, she sends the resulting state to Bob. Since Bob knows  $K$ , he decrypts the received state, performs a measurement, and, therefore, recovers  $R_A$ . Next, Bob generates a random  $n$ -bit number  $R_B$  and a session key  $K_S = \{\theta'_i : 0 \leq \theta'_i < \pi, i = 1, 2, \dots, n\}$ . In sequence, he encodes  $R_B$  in a quantum system  $|\psi_{R_B}\rangle$  and encrypts it with  $K$  and  $K_S$  before send it to Alice. Alice decrypts the state with  $K$  and performs an exclusive-OR (XOR) operation with the resulting state and  $R_A$ . She sends the resulting state to Bob who decrypts with  $K_S$  and obtains a superposition  $|\psi_{R_A \oplus R_B}\rangle$ . The last step performed by Bob is a XOR with  $R_A$ . If he retrieves  $R_B$ , he can successfully authenticate Alice's identity.

As it can be seen, the protocol proposed by Kanamori et al. just uses a quantum channel and no prior entanglement. In our approach, thus, it will be used the Yao's model to analyze it. Considering that the key  $K$  shared between the parties has  $n$  bits, and 3 quantum states of dimension  $n$  are exchanged in this protocol, the resulting complexity is  $Q(f_I) = 3 \cdot n$ . One disadvantage of this protocol is that if tampering occurs, a complete repetition of the procedures must be carried out. Despite of that, it generates a session key that can be used later by the parties of the communication.

Zeng and Guo [8] present an identity authentication quantum protocol that is based on symmetric cryptography with EPR pairs previously shared between the parties. In their protocol, Alice and Bob share a prior key  $K_1$  of  $n$  bits. From the key, they derive a serie of measurements  $M_{K_1}$  in a rectilinear or diagonal basis. Initially, Alice performs a serie of measurements in her half of the EPR par with  $M_{K_1}$ . In his turn, Bob measures his half with  $M_{K_1}$  and with a random series of measurements  $M$ . If eavesdropping occurred, Alice and Bob can detect by showing each other certain results of their measurements in common. Bob and Alice therefore change their results via classical symmetric key cryptography and can authenticate the identity of each other.

The described protocol is able to authenticate both the identities of Alice and Bob. To do so, it uses EPR pairs and classical cryptography. Regarding this last point, in particular, unconditional security cannot be guaranteed. Taking into account the resources required by this protocol, its quantum communication complexity must be evaluated with Cleve and Buhrman's variant. The communications performed between Alice and Bob are encrypted versions of their measurement results who require  $2 \cdot n + s$  bits of classical information, where  $s$  is a security parameter. Thus, according to our approach, the quantum communication complexity of this protocol is  $C^*(f_I) = \Omega(2 \cdot n)$ .

Another identity authentication quantum protocol was proposed by Li and Barnum [2]. This protocol uses EPR pairs between the parties as the identification token. In this protocol, Alice and Bob previously share  $n$  EPR pairs and create an EPR pair associated to each of them. These auxiliary pairs will be measured in the Bell basis at the end of the process. If the Alice party is legitimate and no tampering occurred, Bob will get one of the Bell states previously expected.

One interesting aspect of the protocol of Li and Barnum is that no previous key is shared between the parties, just entangled qubits. It should also be noticed that no classical communication is required although qubits exchanges occurs. Therefore, this protocol must be analyzed according the Hybrid model. The resulting quantum communication complexity is related with the numbers of communications required to produce the EPR pairs:  $Q^*(f_I) = 2 \cdot n$ .

Zhang, Li and Guo [9] present a quantum identity authentication protocol that uses previously shared EPR pairs and a quantum channel. In their protocol, Alice acts as an identifier, Bob as a verifier, and they share an angle  $\theta$  that will be helpful in the prevention of impersonation. When the protocol starts, Alice and Bob rotate  $2 \cdot k$  entangled pairs by  $\theta$ . After that, Bob creates  $k'$  ( $k' \leq k$ ) qubits in an arbitrary pure state, denoted by  $|\psi_i\rangle$ , and send it to Alice who will perform CNOT operations controlled by her half of the entangled pair. Alice sends that particles back to Bob who uses his corresponding particles of the entangled pair to do a CNOT operation, making  $|\psi_i\rangle$  turn back to the original state. Bob then performs a measurement in the basis  $\{|\psi_i\rangle, |\psi_i\rangle^\perp\}$  and checks if the results obtained are in accordance with what is expected. If the measurements passes the test, Bob can authenticate Alice.

In this protocol, the operations performed are the strength against eavesdroppers. Besides, the EPR pairs shared between the parties are intact after the execution and can be reused to help Alice authenticate Bob, for instance. To analyze this protocol, the Hybrid variant will be used since it makes use of previously entangled qubits and of a quantum channel. Considering that the state  $|\psi_i\rangle$  has  $n$  qubits and that it is sent to Alice and then back to Bob, the quantum communication complexity of this protocol is  $Q^*(f_I) = 2 \cdot n$ . It is also important to emphasize that no classical communication is carried out.

Barnum [10] proposes a quantum identity authentication protocol that exploits the phenomenon of entanglement-catalyzed transformations between pure states. Alice and Bob share a catalyst state  $|\phi\rangle$ , and there are incommensurate states  $|\phi_1\rangle$  and  $|\phi_2\rangle$  such that in the presence of the catalyst,  $|\phi_1\rangle$  can be converted to  $|\phi_2\rangle$  while retaining  $|\phi\rangle$ . When Alice wants to authenticate, Bob

prepares  $|\phi_1\rangle$  and sends half of it to her. They go through the steps, involving local measurements, one-way communication of measurement results, and local operations conditional on those measurements results, which convert  $|\phi_1\rangle$  to  $|\phi_2\rangle$ . This protocol involves qubits exchanges and classical communication and, thus, the model to analyze it is the Hybrid one. However, despite the security of this protocol, the number of communications may vary depending on the steps to transform a certain  $|\phi_1\rangle$  into a  $|\phi_2\rangle$ . For this reason, the quantum communication complexity of this protocol cannot be precisely determined. It just can be said that  $Q^*(f_I) = \Omega(n)$  and that this may not be a tight lower bound.

The protocol proposed by Zeng and Zhang [11] uses a trusted center to help the legitimate users to authenticate identity. The trusted center sets up a quantum channel between Alice and the center and between Bob and the center. The center generates the same two entangled pairs to Alice and Bob, keeping half of each. Similarly to BB84, Alice and Bob measure their particles with a randomly chosen basis (horizontal-vertical or diagonally polarized) and share the basis used for the measurements, creating a session key – so, in this protocol, both authentication and QKD are implemented. The resources used are previously entangled pairs, quantum and classical communication what implies in the analysis according to the Hybrid model. The number of communications cannot be determined precisely because it depends on the size of the key. Apart from it, a lower bound of  $Q^*(f_I) = \Omega(4n)$  can be determined. It is important to mention that this protocol is provably secure.

Once the evaluation of the quantum communication complexity of each quantum identity authentication protocol was performed, it is possible to draw some conclusions about them. A common characteristic of all of these protocols is that the number of communications performed is a polynomial in the size of the key. Regarding the models considered, just the protocols from Li and Barnum [2], Zhang et al. [9], Barnum [10] and Zeng and Zhang [11] fall in the same variant. The protocols of Li and Barnum [2] and Zhang et al. [9] have equivalent quantum communication complexity. Considering the Barnum's protocol [10], since its quantum communication complexity is highly related to the states used, it is not possible to determine its performance in contrast with the others. But, despite the security, the Zeng and Zhang's protocol [11] is the one which may perform more communications among the protocols analyzed. Additionally, just the protocol of Kanamori et al. protocol [7] makes use exclusively of qubits exchanges.

## 6 FINAL REMARKS

In this paper we presented an approach to evaluate quantum authentication protocols based on the determination of their quantum communication complexity. Our proposal characterizes a systematic procedure to analyze such protocols, allowing comparisons between them and also providing a concise notation of what resources a certain quantum authentication protocol demands.

So far to our knowledge, no similar approaches were found in the literature. The proposed approach aims to overcome this limitation and also contributes to provide a big picture of the existing quantum authentication protocols. In this context, it helps the identification of the efforts necessary to the proposition of better protocols and may lead new researches in this way.

In the attempt to illustrate the proposed approach, we surveyed the literature and analyzed ten existing quantum authentication protocols. From the quantum data origin authentication protocols, we concluded that two of them have analogous quantum communication complexity according to the Hybrid model and the other two, analyzed under the Yao's model, may distinguish according to the size of the key used in one of them. In the quantum identity authentication protocols covered, it was not possible to determine precisely the quantum communication complexity of all of them, but lower bounds were given in such cases. The resulting analysis helped in the identification of two protocols with equivalent quantum communication complexity and concluded that the Zeng and Zhang's protocol [11] may require the most communications between all of them. In both categories of quantum authentication protocols investigated, it was possible to conclude that few of them exploits classical communications. The evaluations performed helped in increase the knowledge about the existing literature.

In future works we aim to extend our research to other existing quantum authentication protocols. We also would like to increment the presented analysis, including results about the quantum communication complexity when attacks occur. An open question resultant of this work, in particular, is if it is possible to provide a secure authentication with quantum protocols approximating the Holevo bound, i.e., optimizing the number of communications performed.

## ACKNOWLEDGEMENTS

The authors gratefully acknowledge the IQuanta and the financial support rendered by the CNPq.

## REFERENCES

- [1] H. Delfs and H. Knebl. *Introduction to Cryptography – Principles and Applications*. Springer, 2007.
- [2] X. Li and H. Barnum. “Quantum authentication using entangled states”. *International Journal of Foundations of Computer Science*, vol. 15, pp. 609–617, 2004.
- [3] H. Barnum, C. Crepeau, D. Gottesman, A. Smith and A. Tapp. “Authentication of Quantum Messages”. In *43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)*, pp. 449–458. IEEE Press, 2002.
- [4] L. Yang, L. Hu and D.-G. Feng. “Quantum Message Authentication Based on Classical NP-Complete Problem”. arXiv.org: quantum-ph/0310078, 2003.

- [5] M. Curty and D. J. Santos. "Quantum authentication of classical messages". *Physical Review A*, vol. 64, pp. 062309–1–06230–5, 2001.
- [6] X. Li and D. Zhang. "Quantum Information authentication using entangled states". In *International Conference on Digital Telecommunications*, 2006.
- [7] Y. Kanamori, S.-M. Yoo, D. A. Gregory and F. T. Sheldon. "Authentication protocol using quantum superposition states". *International Journal of Networks Security*, vol. 9, pp. 101–108, 2009.
- [8] G. Zeng and G. Guo. "Quantum authentication protocol". arXiv.org :quant-ph/0001046, 2000.
- [9] Y. S. Zhang, C. F. Li and G. C. Guo. "'Quantum authentication using entangled state". arXiv.org : quant-ph/0008044, 2000.
- [10] H. N. Barnum. "Quantum secure identification using entanglement and catalysis". arXiv.org: quantum-ph/9910072, 1999.
- [11] G. Zeng and W. Zhang. "Identity verification in quantum key distribution". *Physical Review A*, vol. 61, pp. 022303–1–022303–5, 2000.
- [12] D. Gottesman. "An Introduction to Quantum Error Correction, ed. S. J. Lomonaco, Jr.,". *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, 2002. pp. 221-235 (American Mathematical Society, Providence, Rhode Island), quant-ph/0004072.
- [13] R. de Wolf. "Quantum Communication and Complexity." *Theoretical Computer Science*, vol. 287, no. 1, pp. 337–353, 2002.
- [14] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2006.
- [15] C. E. Shannon. "A Mathematical Theory of Communication". *The Bell System Tech. Journal*, vol. 27, pp. 379–423, 623–656, 1948.
- [16] A. C. Yao. "Some complexity questions related to distributive computing". In *11th ACM STOC*, pp. 209–213, 1979.
- [17] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.
- [18] A. C. Yao. "Quantum circuit complexity". In *Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science*, pp. 352–361, Washington, DC, USA, 1993. IEEE Computer Society.
- [19] I. Kremer. "Quantum Communication". Master's thesis, The Hebrew University of Jerusalem, March 1995.
- [20] R. Cleve and H. Buhrman. "Substituting quantum entanglement for communication". *Phys. Rev. A*, vol. 56, no. 2, pp. 1201–1204, Aug 1997.
- [21] G. Brassard. "Quantum Communication Complexity". *Foundations of Physics*, vol. 33, no. 11, pp. 1593–1616, 2003.
- [22] H. Klauck. "On quantum and probabilistic communications: Las Vegas and one-way protocols". In *Proceedings of 32nd ACM Symposium on Theory of Computing*, pp. 644–651, 2000.
- [23] P. Sen and S. Venkatesh. "Lower bounds in the quantum cell probe model". In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming*, volume 2076 of *Lecture Notes in Computer Science*, pp. 358–369. Springer, 2001.
- [24] M. Ben-Or, D. W. Leung and D. Mayers. "The universal composable security of quantum key distribution". In *Theory of Cryptography: Second Theory of Cryptography Conference*, volume 3378, pp. 386–406. Springer-Verlag, 2005.
- [25] W. Stallings. *Cryptography and Network Security – Principles and Practices*. Prentice Hall, 2005.
- [26] H. C. van Tilborg. *Encyclopedia Of Cryptography and Security*. Springer, 2005.
- [27] M. A. Nielsen and I. L. Chuang. *Computação Quântica e Informação Quântica*. Bookman, 2005.
- [28] R. J. Hughes, G. L. Morgan and C. G. Peterson. "Quantum Key Distribution over a 48km optical fiber network". *J. Mod. Opt.*, vol. 47, pp. 533, 2000.
- [29] Y. Kanamori, S.-M. Yoo, D. A. Gregory and F. T. Sheldon. "On Quantum Authentication Protocols". In *Proceedings of IEEE GLOBECOM*, pp. 1650–1654, 2005.

# Enhancing Quantum Protocols with the Security of Decoherence-Free Subspaces and Subsystems

Elloá B. Guedes and Francisco M. de Assis

**Abstract**—In the attempt to overcome the negative effects of the noise on quantum channels and to provide secure communications, some quantum secure direct communication protocols and deterministic secure quantum communication protocols making use of decoherence-free subspaces and subsystems have been proposed in the literature. However, recent results regarding the use of decoherence-free subspaces and subsystems show that they can be used to convey classical information through quantum channels with unconditional security. In this work, we use these results to propose enhancements into four already existing protocols. As a result, in all cases considered, (i) the encoding was simplified, requiring less gates to be implemented; (ii) the number of qubit and bit exchange was reduced, reaching a four times reduction in one of the cases; (iii) no eavesdropping check nor redundancy are further required; and (iv) the rate of information transmission was increased in all protocols. Such enhancements favor the adoption of such modified protocols in practical scenarios.

**Index Terms**—Collective Decoherence; Decoherence-Free Subspaces and Subsystems; Quantum Protocols.

## I. INTRODUCTION

THE principles of Quantum Mechanics provide novel ways for quantum information transmission and processing, such as Quantum Computation and Quantum Communication. Regarding Quantum Communication, in particular, some intrinsic properties of Quantum Mechanics enable features that do not have counterpart in Classical Communication, such as: (i) a qubit has not a definite value until the moment after it is read; (ii) every measurement in a qubit may disturb it; (iii) arbitrary states of qubits cannot be copied; (iv) qubits can be entangled; among others [1]. Thanks to these Quantum Mechanics principles, in certain scenarios unconditional security can be achieved in quantum information conveying through quantum channels.

The *Quantum Key Distribution* [2]–[5] is one of the most mature quantum information techniques nowadays. According QKD, two remote users can create a private key securely. These keys are then used to crypt the secret message into a ciphertext through a classical cryptographic scheme such as the one-time pad, and the ciphertexts are then sent from one user to another through a classical channel. However, in

a practical transmission process, the channel noise cannot be avoided completely. Noise can increase not only the error rate of the sending message, but also the difficulty of finding an eavesdropper in the process of a security check.

Recently, the *quantum secure direct communication* (QSDC) protocols have been proposed as a new technique of communication. Its objective is to transmit classical messages directly, without the help of private keys nor classical communications. In this scheme, the QKD and the classical transmission of the ciphertext are condensed into a single quantum communication. For this reason, QSDC is considered as a purely quantum mechanical technique [6].

In a similar way, in the *deterministic secure quantum communication* (DSQC) protocols, the message is deterministically sent through the quantum channel, but can only be deduced after a round of classical information transmission. In fact, this is the fundamental difference between QSDC and DSQC protocols [6].

So far, many QSDC and DSQC protocols have been proposed in the literature considering the use of different resources and methods, such as entanglement swapping [7], teleportation [8]–[10], quantum one-time pad [11], rearrangement of orders of particles [12], among others. The survey of Long et al. [6] contemplates the recent developments about both QSDC and DSQC.

In the attempt to avoid the negative effects of noise, some QSDC and DSQC protocols making use of *decoherence-free subspaces and subsystems* (DFS) have been proposed [13]–[15]. States belonging to these subspaces and subsystems exploit the dynamical symmetries existing in the quantum channel to keep their invariability against the noise [16].

However, recent results regarding codes built from states of a DFS show that they can achieve unconditional security [17], [18]. So, a question that arises is: are there any enhancements that can be made on these QSDC and DSQC protocols that use DFS aiming at simplification or at increase efficiency? This paper attempts at answering this question.

As a result, we propose changes into four already existing protocols, reducing significantly the number of qubits exchanged per communication and also avoiding redundancy and eavesdropping checking. In practical scenarios, the difficult to build completely closed systems [19] is a motivating factor for the use of such simplified protocols, specially considering the already existing results regarding the use of DFS in

Elloá B. Guedes and Francisco M. de Assis. IQanta – Institute for Studies in Quantum Computation and Information, Federal University of Campina Grande, Av. Aprígio Veloso, 882 – 58429-140, Campina Grande – Paraíba – Brazil. E-mails: {elloaguedes,fmarassis}@gmail.com. This work was supported by the Brazilian funding agencies CAPES and CNPq.

communications [20]–[22], particularly in long-distance [23].

The rest of this paper is organized as follows. Section II introduces the concepts regarding DFS; Section III shows how codes built from DFS can achieve unconditional security; Sections IV, V, and VI, show the concepts of collective dephasing, rotation and amplitude damping quantum channels, respectively, as well as QSDC and DSQC protocols to them with the corresponding suggestions for improvement. Lastly, Section VII presents the final remarks and suggestions for future work.

## II. DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

Due to decoherence, a quantum system may lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information it carries becomes lost [24]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed by the *system of interest*  $S$  defined on a Hilbert space  $\mathcal{H}$  and by the *environment*  $E$ . The Hamiltonian that describes this system is defined as follows:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE} \quad (1)$$

where  $\mathbb{1}$  is the identity operator; and  $\mathbb{H}_S$ ,  $\mathbb{H}_E$  and  $\mathbb{H}_{SE}$  denote the Hamiltonians of system, environment and system-environment interaction, respectively.

In order to prevent errors, it would be ideal that  $\mathbb{H}_{SE}$  were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians  $\mathbb{H}_S$  and  $\mathbb{H}_E$  [16]. However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system [19].

If some symmetries exist in the interaction between the system and the environment, it is possible to find a “quiet corner” in the system Hilbert space not experiencing decoherence. Let  $\{A_i(t)\}$  be a set of operators in the *operator-sum representation* (OSR) corresponding to the evolution of the system. We say that a system density matrix  $\rho_S$  is *invariant* under the OSR operators  $\{A_i(t)\}$  if  $\sum_i A_i(t)\rho_S A_i^\dagger(t) = \rho_S$ . We are now able to define the *decoherence-free subspaces* whose states are invariant despite a non-trivial coupling between the system and the environment.

**Definition 1.** (*Decoherence-Free Subspace* [25]) *A subspace  $\tilde{\mathcal{H}}$  of a Hilbert space  $\mathcal{H}$  is called decoherence-free with respect to a system-environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:*

$$\sum_i A_i(t)|\tilde{k}\rangle\langle\tilde{k}|A_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \quad (2)$$

Let the Hamiltonian of the system-environment interaction be  $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$ , where  $\mathbf{S}_j$  and  $\mathbf{E}_j$  are the system and environment operators, respectively. We consider that the environment operators  $\mathbf{E}_j$  are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations see [16, Sec. 5].

**Theorem 1.** (*DFS Conditions* [24]) *A subspace  $\tilde{\mathcal{H}}$  is a decoherence-free subspace iff the system operators  $\mathbf{S}_j$  act proportional to identity on the subspace:*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \quad (3)$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system [16]. Knill et al. [26] discovered a method for decoherence-free encoding into subsystems instead of into subspaces which is presented below.

**Definition 2.** (*Decoherence-Free Subsystem*) *Consider a decomposition of the whole Hilbert space  $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ , where  $\dim(\mathcal{H}) = \dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$ . A subspace  $\mathcal{H}^B$  of the full Hilbert space is a decoherence-free subsystem if*

$$\forall \rho^A, \forall \rho^B, \exists \tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B, \quad (4)$$

where  $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$ , and  $\rho^B \in \mathcal{B}(\mathcal{H}^B)$ .

In fact,  $B$  is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when  $\dim(\mathcal{H}^A) = 1$ ,  $B$  is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit  $\alpha|0\rangle + \beta|1\rangle$  into  $\alpha|01\rangle + \beta|10\rangle$ . In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose now that the information is encoded only into the first qubit of the two qubits, i.e.,  $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$ . Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem* [25].

In practice, identifying a useful symmetry and taking advantage of it can be very difficult. One must (i) identify the symmetry, and (ii) find the states which are invariant to the interaction. Despite these difficulties, a method for obtaining DFS was already proposed in the literature [27].

Quantum codes constructed from states of a DFS are classified as *quantum error-avoiding codes* (QEAC) and the

tasks of perturbation and recovery on them are trivial. They can be contrasted with *quantum-error correcting codes* (QECC) in some aspects. While QECCs are devised to correct errors after their occurrence, QEACs do not have the ability to correct errors since they avoid them; QECCs devised in practical circumstances belong to the class of non-degenerate codes while QEACs are highly degenerate; QEACs usually require a lower number of physical qubits to encode one logical qubit than QECCs. In particular, if the degeneracy attains the maximum, a QECC reduces to a QEAC what illustrates a circumstance in which a type of code becomes equivalent to the other [28].

The absence of decoherence in DFS has been shown as of major importance for implementations of quantum memory and quantum algorithms. Other applications of it cover encoding information in quantum dots, collective dissipation, noise reduction, among others [16], [19].

### III. UNCONDITIONAL SECURITY IN DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

Until nowadays, many works in the literature already explored the potential of DFS in Quantum Communications. All of them consist of protocols against certain types of collective noise (such as rotation, dephasing, amplitude damping, among others) and consider the use of small DFS (with two or three qubits, for instance) [13]–[15], [29], [30]. Even experimental realizations were already implemented aiming at quantum information processing [31]–[34]. In the perspective of these works, the protection of information means avoiding the loss of coherence, maintaining the fidelity of the quantum states.

The work of Guedes and de Assis [17], [18] attempted to investigate the potential of DFS in terms of *secure message exchange*. To do so, they considered the following scenario: a sender (Alice) wants to convey secret classical messages through a quantum channel to a legitimate receiver (Bob). These messages must be protected from a wiretapper (Eve) that has full access to the environment.

To exchange the messages without being deceived by Eve, Alice and Bob use a QEAC build from the states of a DFS according to the following definition.

**Definition 3.** Let  $\tilde{\mathcal{H}}$  be a DFS spanned by a set of eigenvectors  $\{|\tilde{k}\rangle\}$ , i.e.,  $\tilde{\mathcal{H}} = \text{Span}\{|\tilde{k}\rangle\}$ . A set of codewords of length  $n$  ( $n = \dim(\tilde{\mathcal{H}})$ ) for a set  $\mathcal{U}$  of classical messages is a set of input states labeled by messages in  $\mathcal{U}$ ,  $\tilde{K}(\mathcal{U}) = \{\tilde{k}(u) : u \in \mathcal{U}\} \subseteq \tilde{\mathcal{H}}$ , and a decoding measurement composed of a set of positive operators  $\tilde{\mathcal{D}}_u$ ,  $u \in \mathcal{U}$  with  $\sum_{u \in \mathcal{U}} \tilde{\mathcal{D}}_u \leq \mathbf{1}$ . The pair  $(\tilde{K}(\mathcal{U}), \{\tilde{\mathcal{D}}_u : u \in \mathcal{U}\})$  is called a QEAC of length  $n$  for the set  $\mathcal{U}$  of messages. The rate of this code is  $\frac{1}{n} \log |\mathcal{U}|$ .

Using the code defined, if Alice wants to send a classical message  $u$  over a quantum channel  $\mathcal{E}$ , now she encodes it the QEAC defined over  $\tilde{\mathcal{H}}$ , obtaining  $\tilde{k}(u)$ . When she sends

it through the communication channel, the message interacts with the environment (which is assumed to start in a pure state  $|0_E\rangle$ ). This scenario is depicted in Figure 1. Bob then receives  $\rho_{\text{Bob}}(\tilde{k}(u))$  and Eve receives  $\rho_{\text{Eve}}(\tilde{k}(u))$  which are given by:

$$\rho_{\text{Bob}}(\tilde{k}(u)) = \text{Tr}_E \left[ \mathcal{E}^{\otimes n}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|) \right], \quad (5)$$

$$\rho_{\text{Eve}}(\tilde{k}(u)) = \text{Tr}_B \left[ \mathcal{E}^{\otimes n}(\tilde{k}(u) \otimes |0_E\rangle\langle 0_E|) \right]. \quad (6)$$

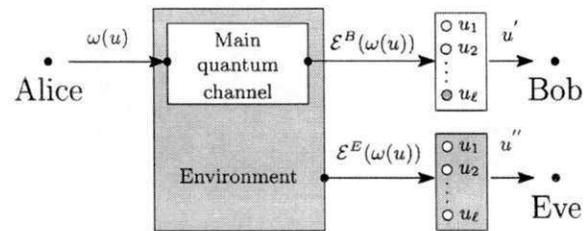


Fig. 1: General idea of the scenario described.

To analyze the security of such message exchange, Guedes and de Assis [17], [18] considered (i) the use of a QEAC; (ii) the interaction Hamiltonian of (1); (iii) the fact that Eve is restricted only to the environment; (iv) the accessible information by Bob and Eve; and (v) the theory of quantum wiretap channels [35], [36]. They established a proof that, in this scenario, the Holevo quantity of Eve is  $\chi^{\text{Eve}} = 0$ . Recalling that the Holevo quantity is an upper bound for the accessible information, it means that Eve does not gather anything from the secret message exchanged between Alice and Bob. It means that the criterion for *unconditional security* is achieved in this scenario.

On the other hand, the maximum accessible information by Bob is equal to  $\max_{\{P\}} \chi^{\text{Bob}}$  where the maximum is taken over all probability distributions  $P$  over  $\mathcal{U}$ . This coincides with the classical capacity of a quantum channel according to the Holevo-Schumacher-Westmoreland theorem [37], [38]. It means that the ability of such quantum channel to send secret information can be made as large as its capacity to send ordinary classical information.

However, not all quantum channels exhibit such properties – only those which are subject to collective noise do. In collective noise quantum channels several qubits couple identically to the same environment, while undergoing both dephasing and dissipation [16].

In the next sections, some QSDC and DSQC protocol that consider the use of collective noise quantum channels will be examined taking into account the security results regarding DFS. The main objective is to point out some simplifications or modifications that aim at their enhancement.

## IV. COLLECTIVE DEPHASING

Dephasing is a phenomenon in which the relative phase of a qubit is lost. Collective dephasing quantum channels act as follows on input qubits

$$|0\rangle \rightarrow |0\rangle, \quad (7)$$

$$|1\rangle \rightarrow e^{i\phi}|1\rangle. \quad (8)$$

where  $\phi$  is the parameter of a collective-dephasing which fluctuates with time  $t$ . A logical qubit composed of two physical qubits with an antiparallel parity is immune to the collective dephasing, i.e.

$$|0_L\rangle = |01\rangle, \quad (9)$$

$$|1_L\rangle = |10\rangle. \quad (10)$$

A qubit can, thus, be codified as  $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$ . It is interesting to see that  $|\psi_L\rangle$  does not suffer from the effects of decoherence

$$\mathcal{E}(|\psi_L\rangle) = \mathcal{E}(\alpha|0_L\rangle + \beta|1_L\rangle) \quad (11)$$

$$= \alpha e^{i\phi}|01\rangle + \beta e^{i\phi}|10\rangle \quad (12)$$

$$= e^{i\phi}(\alpha|01\rangle + \beta|10\rangle) \quad (13)$$

$$= e^{i\phi}|\psi_L\rangle \quad (14)$$

$$= |\psi_L\rangle. \quad (15)$$

because the overall phase factor  $e^{i\phi}$  acquired due to the dephasing process has no physical significance. It means that both states  $|01\rangle$  and  $|10\rangle$  belong to  $\tilde{\mathcal{H}}$ , a decoherence-free subspace of the Hilbert space  $\mathcal{H}$  in the collective dephasing quantum channel.

Gu et al. [13] proposed a DSQC over a collective dephasing quantum channel which is described as follows:

- 1) Alice prepares a sequence of quantum states in a three-photon entangled state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle|0_{B_1}1_{B_2}\rangle + |1_A\rangle|1_{B_1}0_{B_2}\rangle). \quad (16)$$

Notice that the two qubits  $B_1$  and  $B_2$  are entangled with the qubit  $A$  of Alice. Alice divides the quantum systems into two sequences  $S_A$  and  $S_B$ , where  $S_A$  is composed of the qubits  $A$ , and  $S_B$  is composed of qubits  $B_1$  and  $B_2$ , respectively. Alice keeps  $S_A$  and sends  $S_B$  to Bob;

- 2) Bob picks up some samples for eavesdropping check after he receives  $S_B$ . He measures the two qubits with one of the two measuring bases  $Z_{B_1} \otimes Z_{B_2}$  or  $X_{B_1} \otimes X_{B_2}$ , randomly. The state  $|\psi^+\rangle$  can be written as follows

$$|\psi^+\rangle = \frac{1}{2} [|+A\rangle (|+B_1+B_2\rangle - |-B_1-B_2\rangle) - |-A\rangle (|+B_1-B_2\rangle - |-B_1+B_2\rangle)]. \quad (17)$$

The outcomes obtained by Alice and Bob are correlated if they choose two corresponding measuring basis;

- 3) Bob tells Alice which qubits are chosen for eavesdropping check and the states obtained for the samples;
- 4) If Bob chooses  $Z_{B_1} \otimes Z_{B_2}$ , Alice chooses  $Z_A$  to measure her qubit; otherwise she chooses  $X_A$ ;
- 5) Alice and Bob use the correlation between their samples to analyze the error rate for eavesdropping check. They code the outcomes  $|0_A\rangle, |+A\rangle, |0_{B_1}1_{B_2}\rangle, |+B_1+B_2\rangle$ , and  $|-B_1-B_2\rangle$  as the classical bit 0; and the outcomes  $|1_A\rangle, |-A\rangle, |1_{B_1}0_{B_2}\rangle, |+B_1-B_2\rangle$ , and  $|-B_1+B_2\rangle$  as the classical bit 1. The error rate must be below a threshold;
- 6) Alice tells Bob  $C_A = O_A \oplus M_A$  where  $O_A$  is the outcome of the measurements performed by Alice;  $M_A$  is the secret classical message; and  $\oplus$  denotes a sum modulo 2;
- 7) Bob reads the message directly with his outcome  $O_B$ , i.e.,  $M_A = O_B \oplus C_A$ .

To analyze this protocol, we will estimate its Communication Complexity. The communication complexity is a measure of how many communications are necessary until two distribute parties become able to accomplish some task using as little communication as possible [39]. We will use the *hybrid variant* which takes into account the number of qubits and bits exchanged between the parties.

Let's suppose that the message  $M_A$  has  $m$  bits. First of all, Alice and Bob need to create a key with at least  $m$  bits by using the correlation between their outcomes to encode the message, that will be sent classically in the penultimate step of the protocol. If they use  $e$  qubits to eavesdropping check, the communication complexity of this protocol will be lower bounded by  $Q^*(2 \cdot m + e)$ .

Considering the results shown in Section III, the use of states of a DFS enable unconditional security. So, if Alice uses the encoding  $0 \equiv |01\rangle$  and  $1 \equiv |10\rangle$ , Bob can distinguish both states and decode the secret message sent by Alice. It results in a communication complexity of  $Q^*(m)$  and a rate of 1 bit per channel use, considering that the bits 0 and 1 are equally probable. In comparison with the protocol proposed by Gu et al. [13], this scheme requires less than the half of the amount of bits and qubits exchanged.

The simplification proposed consists in a very simplified encoding-decoding scheme since it does not require entanglement between the parties nor eavesdropping check. Given that the states used belong to a DFS, no error threshold is necessary to be imposed, because such states are immune to errors. The process of encoding-decoding is also very trivial and can be constructed using only the well-known Pauli  $X$  gates as shown in Figure 2, where Figures 2a and 2b show the encoding for  $|01\rangle$  and  $|10\rangle$ , respectively.

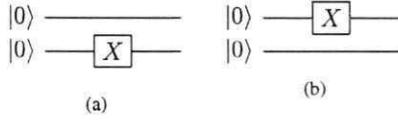


Fig. 2: Circuit for encoding the simplification suggested to the protocol of Gu et al. [13].

## V. COLLECTIVE AMPLITUDE DAMPING

The phenomenon of energy dissipation when conveying a quantum state is modeled by the *collective amplitude damping channel*. This channel has the following OSR

$$\mathcal{E}(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger, \quad (18)$$

where the operation elements  $A_0$  and  $A_1$  are as follows

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}, \quad (19)$$

where  $\gamma$  is the damping rate which can be thought of as the probability of losing a photon [40, p. 380].

A QSDC protocol over collective amplitude damping channels was proposed by Qin et al. [14]. This protocol makes use of two states from a DFS defined over this channel ( $|0_L\rangle$  and  $|1_L\rangle$ ) and also of other two states based on them ( $|+_L\rangle$  and  $|-_L\rangle$ ). These quantum states are

$$|0_L\rangle = |00\rangle, \quad (20)$$

$$|1_L\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}, \quad (21)$$

$$|+_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}}, \quad (22)$$

$$|-_L\rangle = \frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}}. \quad (23)$$

The protocol of Qin et al. [14] works as follows:

- 1) Alice generates a random sequence of the following states  $\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\}$  and sends to Bob;
- 2) Bob chooses a set of qubits to check eavesdropping. He measures them in one of the two bases randomly chosen ( $\{|0_L\rangle, |1_L\rangle\}$  or  $\{|+_L\rangle, |-_L\rangle\}$ ) and publish his outputs. Alice checks the outcomes in order judge whether there are eavesdroppers online. Bob performs certain operations on the remaining qubits, inserts some random bits, and sends back the encoded qubits to Alice;
- 3) Alice measures the received qubits in the same bases that she originally prepared. According to the relationship between her outcomes and the initial states, Alice can deterministically decode Bob's message;
- 4) Bob declares the position and values of the random bits. Alice judges the security and retrieves the message sent.

In this protocol, the number of communications required in the attempt to detect eavesdropping, besides the secret message, includes redundancy, random bits and also classical communications to publish measurement outcomes. If the message has  $m$  bits, then the communication complexity of this protocol is upper bounded by  $Q^*(4 \cdot m + e)$ . Besides that, even using a 2-qubit state, the rate achieved by this protocol is less than 0.25 bits per channel use.

A simplification in this protocol than can be suggested considers the use of a QEAC ( $\tilde{K}(\{0, 1\}) = \{\tilde{k}(0) = |0_L\rangle, \tilde{k}(1) = |1_L\rangle\}$ ,  $\{\tilde{D}_0 = |0_L\rangle\langle 0_L|, \tilde{D}_1 = |1_L\rangle\langle 1_L|\}$ ) to perform quantum secure direct communications. So, the secret message can be conveyed directly through the quantum channel without requiring random bits nor classical communications. The rate achieved is equal to 1 bit per symbol per channel use and the encoding-decoding procedures are less complex, which reduces the number of quantum gates required to implement this scheme.

Moreover, another suggestion to such scenario is to use the four states  $|0_L\rangle, |1_L\rangle, |+_L\rangle$  and  $|-_L\rangle$  from Eqs. (20)-(23) to perform QKD with the BB84 protocol [2] over a collective amplitude damping channel.

## VI. COLLECTIVE ROTATION

A collective rotation noise can be written as

$$|0\rangle \rightarrow \cos \theta |0\rangle + \sin \theta |1\rangle, \quad (24)$$

$$|1\rangle \rightarrow -\sin \theta |0\rangle + \cos \theta |1\rangle. \quad (25)$$

where  $\theta$  is the parameter of a collective-rotation noise which fluctuates with time  $t$ . Two states immune to the effects of this channels are the Bell states

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2\rangle + |1_1 1_2\rangle), \quad (26)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0_1 1_2\rangle - |1_1 0_2\rangle). \quad (27)$$

Recently, Gu et al. [13] proposed a DSQC which makes use of the existing DFS on the collective rotation quantum channel. According to these authors, the creation of a key in this protocol is made as follows:

- 1) Alice prepares a three-photon entangled state

$$|\Phi^+\rangle_{AB_1 B_2} = \frac{1}{\sqrt{2}}(|0_A\rangle|\phi_{B_1 B_2}^+\rangle + |1_A\rangle|\psi_{B_1 B_2}^-\rangle). \quad (28)$$

She keeps the qubit  $A$  and sends the qubits  $B_1$  and  $B_2$  to Bob;

- 2) After receiving the sequence sent by Alice, Bob picks up some samples for eavesdropping check. To do so, he measure some samples in three measuring bases  $Z_{B_1} \otimes Z_{B_2}$ ,  $Z_{B_1} \otimes X_{B_2}$  and  $X_{B_1} \otimes Z_{B_2}$  randomly chosen;

- 3) Bob tells Alice which qubits are chosen for eavesdropping check and the outcomes of measurements on the samples;
- 4) If Bob chooses the measuring basis  $Z_{B_1} \otimes Z_{B_2}$ , then Alice chooses  $Z_A$  to measure her corresponding photon; otherwise, she chooses  $X_A$ ;
- 5) Alice and Bob use the correlation between their samples to analyze the error rate. If the error rate is higher than the threshold, they repeat the protocol from the beginning. They code the outcomes  $|0_A\rangle$ ,  $|0_{B_1 0_{B_2}}\rangle$ ,  $|1_{B_1 1_{B_2}}\rangle$ ,  $|+_A\rangle$ ,  $|0_{B_1 + B_2}\rangle$ ,  $|1_{B_1 - B_2}\rangle$ ,  $|-_{B_1 0_{B_2}}\rangle$ , and  $|+_B 1_{B_2}\rangle$  as the classical bit 0; while the outcomes  $|1_A\rangle$ ,  $|0_{B_1 1_{B_2}}\rangle$ ,  $|1_{B_1 0_{B_2}}\rangle$ ,  $|-_A\rangle$ ,  $|0_{B_1 - B_2}\rangle$ ,  $|1_{B_1 + B_2}\rangle$ ,  $|+_B 0_{B_2}\rangle$ , and  $|-_{B_1 1_{B_2}}\rangle$  correspond to the classical bit 1;
- 6) Alice tells Bob the outcome  $C_A = O_A \oplus M_A$  where  $O_A$  is the outcome of her measurement on photon  $A$  and  $M_A$  is the secret message that she wants to send Bob privately;
- 7) Bob reads out the secret message directly, i.e.,  $M_A = C_A \oplus O_B$  where  $O_B$  is the outcome of his measurements on the photons  $B_1$  and  $B_2$ .

Before start the analysis of this protocol, we first make some considerations about it. The states of the DFS are Bell states; the existing correlation between the samples of Alice and Bob enable eavesdropping checking; and, lastly, an one-time pad encryption is made before the message is sent. This protocol is very similar to the one presented in Section IV, but considering the collective rotation scenario.

In face of the existence of a DFS, some simplifications can be applied in this protocol. If Alice and Bob want to send the message directly through the quantum channel, an appropriate encoding using only the states  $|\phi^+\rangle$  and  $|\psi^-\rangle$  can be made to send 1 bit of information per channel use. Two strategies can be used to simplify this protocol: the first one is to send the classical information directly via the quantum channel using an appropriate encoding, such as  $0 \equiv |\phi^+\rangle$  and  $1 \equiv |\psi^-\rangle$ , and Bell measurements for decoding; the second strategy uses the quantum channel to create a private classical key and the message is sent through a classical channel, using a one-time pad encryption scheme, according to the last two steps of the protocol presented.

In both suggestions, the unconditional secrecy provided by the DFS is the key ingredient to increase the simplicity of the protocols. As can also be observed, in both cases no eavesdropping checking is required – it reduces significantly the number of communications performed. In the original protocol, the communication complexity is lower bounded by  $Q^*(4 \cdot m)$  where  $m$  is the number of bits of the secret classical message to be exchanged. In contrast, the first simplification suggested has communication complexity equal to  $Q^*(m)$ , and the second is  $Q^*(2 \cdot m)$  because and additional communication

must be made to send the ciphertext through the classical channel. It is important to emphasize that, even in the second suggestion of simplification in which the number of communication is higher, there is a reduction of at least half of the number of communications performed when compared to the original protocol.

A second protocol found in the literature to collective rotation quantum channels is a DSQC proposed by Dong et al. [15] as is characterized as follows

- 1) Alice prepares a  $4 \cdot m$  two-photons sequence randomly in the state  $\{|0_L\rangle, |1_L\rangle, |+_L\rangle, |-_L\rangle\}$  where

$$|0_L\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \quad (29)$$

$$|1_L\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \quad (30)$$

$$\begin{aligned} |+_L\rangle &= \frac{1}{\sqrt{2}} (|0_L\rangle + |1_L\rangle) \\ &= \frac{1}{\sqrt{2}} (|+\rangle|1\rangle + |-\rangle|0\rangle) \end{aligned} \quad (31)$$

$$\begin{aligned} |-_L\rangle &= \frac{1}{\sqrt{2}} (|0_L\rangle - |1_L\rangle) \\ &= \frac{1}{\sqrt{2}} (|-\rangle|1\rangle + |+\rangle|0\rangle) \end{aligned} \quad (32)$$

where  $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$  and  $|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ . Alice sends it to Bob;

- 2) Bob measures the first qubit of each pair randomly in the  $Z$  or  $X$  basis, the second one in the  $Z$  basis, and records the measurement outcomes where  $\{|0\rangle, |1\rangle\}$  are two bases of  $Z$  measurement, and  $\{|+\rangle, |-\rangle\}$  are two bases of  $X$  measurement;
- 3) Alice and Bob check the security of the channel. Bob publicizes the measurements in sequence. Then they abandon the records in two situations: (i) when the state prepared by Alice is  $|+_L\rangle$  or  $|-_L\rangle$  and the measurement basis of the first qubit performed by Bob is the  $Z$  basis; and (ii) when the state prepared by Alice is  $|0_L\rangle$  and  $|1_L\rangle$  and Bob's measurement basis of the first qubit is in the  $X$  basis. After this step, about  $2 \cdot m$  qubits remain. They then use  $m$  qubits for eavesdropping check;
- 4) If the quantum channel is safe, they use the leftover  $m$  measurements records to communicate. Alice and Bob agree on the following encoding:  $0 \equiv |0_L\rangle, |+_L\rangle$  and  $1 \equiv |1_L\rangle, |-_L\rangle$ . Alice sends 0 through the classical channel if the secret message is the same as the encoding message. Otherwise 1 is sent.

The protocol of Dong et al. [15] requires  $Q^*(5 \cdot m)$  bits and qubits exchanges to be performed. Most of these communications are spent in eavesdropping check and also in making Alice learn Bob's outcomes by the publication of the basis he used. This last step is essential for the protocol execution because it makes both of them agree on the bits to

be used without communicate them directly.

When compared to the protocol of Gu et al. [13] which has communication complexity of  $Q^*(4 \cdot m)$ , we can conclude that the protocol of Dong et al. [15] is more expensive. However, it does not require entanglement between the parties as the former does. The two suggestions for simplification presented for the protocol of Gu et al. [13] can similarly be applied in this scenario, simplifying significantly the protocol, reducing the number of communications, and also providing unconditional security.

## VII. FINAL REMARKS

In this work, we proposed modifications into four already existing QSDC and DSQC protocols that make use of DFS aiming at simplification or at increase efficiency. Such modifications were motivated by a recent result of Guedes and de Assis [17], [18] that codes built with states from a DFS can achieve unconditional security. The simplifications proposed were compared with their original versions taking into account the communication complexity, a measure of how many communications a protocol performs.

In the collective dephasing quantum channel, the protocol of Gu et al. [13] was considered, which has communication complexity lower bounded by  $Q^*(2 \cdot m + e)$ . The simplification suggested does not require eavesdropping check and has communication complexity equal to  $Q^*(m)$ . Furthermore, the process of encoding-decoding becomes very trivial and can be constructed using only the well-known Pauli  $X$  gates.

To the collective amplitude damping scenario, the protocol of Qin et al. [14] was considered. The simplification proposed to it was the use of a QEAC with rate of 1 bit per channel use. The original version has communication complexity of  $Q^*(4 \cdot m + e)$  in contrast with  $Q^*(m)$  of the simplification suggested. Furthermore, we suggested how the four states of the existing DFS can be used to perform the BB84 over the collective amplitude damping quantum channel. Regarding the QKD using DFS in the collective amplitude damping quantum channel, no similar propositions were found in literature. It is in contrast with the collective rotation and dephasing quantum channels to which QKD protocols were already proposed [41], [42]

In the case of the collective rotation quantum channels, two protocols were considered: one proposed by Gu et al. [13] and another proposed by Dong et al. [15]. Two suggestions were made and are applicable to both protocols. In the best case observed, the number of communications performed was reduced in four times.

The use of DFS and its ability to send information with unconditional security can be exploited in practical scenarios of implementation of quantum channels. Since it is difficult to build completely closed systems [19], some results already consolidated considering the use of DFS in practical quantum

communications [20]–[23] favors the implementation of such simplifications suggested. They can be considered well-suited for such scenarios for requiring (i) a small number of resources (absence of entanglement between the parties, for instance); (ii) a small amount of information exchange; and (iii) simple quantum gates that are already widely use in encoding-decoding processes.

In future works, we suggest the investigation of more general conditions to the existence of perfect secrecy in quantum systems.

## ACKNOWLEDGMENTS

The authors thanks Gilson O. Santos for his valuable suggestions.

## REFERENCES

- [1] C. P. Williams, *Explorations in Quantum Computing*, 2nd ed., Springer, Ed. Springer, 2011.
- [2] C. H. Bennett and G. Brassard. "Quantum cryptography: public key distribution and coin tossing," in *Int. Conf. Computers, Systems & Signal Processing, Bangalore, India*.
- [3] A. K. Ekert. "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.
- [4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, p. 3121, 1992.
- [5] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.
- [6] G. lu Long, F. guo Deng, C. W. X. han Lo, K. Wen, and W. ying Wang. "Quantum secure direct communication and deterministic secure quantum communication," *Front. Phys. China*, vol. 2, no. 3, pp. 251–272, 2007.
- [7] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "event-ready-detectors" bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, p. 4287, 1993.
- [8] T. Gao, "Controlled and secure direct communication using ghz state and teleportation," *Z. Naturforsch.*, vol. 59, p. 597, 2004.
- [9] T. Gao, F.-L. Yan, and Z.-X. Wang, "Controlled quantum teleportation and secure direct communication," *Chinese Phys.*, vol. 14, p. 893, 2005.
- [10] F. L. Yan, and X. Q. Zhang, "A scheme for secure direct communication using EPR pairs and teleportation," *Eur. Phys. J. B*, vol. 41, pp. 75–78, 2004.
- [11] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, p. 052319, 2004.
- [12] A. D. Zhu, Y. Xia, Q. B. Fan, and S. Zhang, "Secure direct communication based on secret transmitting order of particles," *Phys. Rev. A*, vol. 73, p. 022338, 2006.
- [13] G. Bin, P. ShiXin, S. Biao, and Z. Kun. "Deterministic secure quantum communication over a collective-noise channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 12, pp. 1913–1918, 2009.
- [14] S. Qin, Q. Wen, L. Meng, and F. Zhu, "Quantum secure direct communication over the collective amplitude damping channel," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 8, pp. 1208–1212, 2009.
- [15] H.-K. Dong, L. Dong, X.-M. Xiu, and Y.-J. Gao, "A deterministic secure quantum communication protocol through a collective rotation noise channel," *Int. J. of Quantum Inf.*, vol. 8, no. 8, pp. 1389–1395, 2010.
- [16] D. A. Lidar and K. B. Whaley, "Decoherence-free subspaces and subsystems," arXiv:quant-ph/0301032v1, pp. 83–120, 2003.
- [17] E. B. Guedes and F. M. de Assis, "Unconditional security with decoherence-free subspaces," arXiv:quant-ph/1204.3000, pp. 1–6, 2012.
- [18] —, "Utilização de subespaços livres de descoerência em comunicações quânticas incondicionalmente seguras," in *XXX Simpósio Brasileiro de Telecomunicações – SBR'T'12*, 2012.

IV Workshop-school on Quantum Computation and Information (WECIQ 2012)

- [19] M. S. Byrd, L.-A. Wu, and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, no. 16-18, pp. 2449-2460, 2004.
- [20] U. Dörner, A. Klein, and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, p. 468, 2008.
- [21] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, p. 2120, 2008.
- [22] Y. Xia, J. Song, Z.-B. Yang, and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, pp. 651-656, 2010.
- [23] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, pp. 6859-6866, 2008.
- [24] A. Shabani and D. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems," *Phys. Rev. A*, vol. 72, p. 042303, 2005.
- [25] D. M. Bacon, "Decoherence, control, and symmetry in quantum computers," Ph.D. dissertation, University of California at Berkeley, 2001.
- [26] E. Knill, R. Laflamme, and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, p. 2525, 2000.
- [27] M.-D. Choi and D. W. Kribs, "A method to find quantum noiseless subsystems," *Phys. Rev. Lett.*, vol. 96, p. 050501, 2006.
- [28] L.-M. Duan and G.-C. Guo, "Quantum error avoiding codes versus quantum error correcting codes," *Phys. Lett. A*, vol. 255, pp. 209-212, 1999.
- [29] K. Majgier, H. Maassen, and K. Życzkowski, "Protected subspaces in quantum information," *Quantum Inf. Process.*, vol. 9, pp. 343-367, 2010.
- [30] M. S. Byrd, D. A. Lidar, L.-A. Wu, and P. Zanardi, "Universal leakage elimination," *Phys. Rev. A*, vol. 71, p. 052301, 2005.
- [31] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme, and D. G. Cory, "Experimental realization of noiseless subsystems for quantum information processing," *Science*, vol. 293, pp. 2059-2063, 2001.
- [32] A. Beige, D. Braun, B. Tregenna, and P. L. Knight, "Quantum computing using dissipation to remain in a decoherence-free subspace," *Phys. Rev. Lett.*, vol. 85, p. 1762, 2000.
- [33] D. Kielpinski, "A decoherence-free quantum memory using trapped ions," *Science*, vol. 291, p. 1013, 2001.
- [34] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, "Experimental verification of decoherence-free subspaces," *Science*, vol. 290, pp. 498-501, 2000.
- [35] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, pp. 318-336, 2004.
- [36] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Th.*, vol. 51, no. 1, pp. 44-55, 2005.
- [37] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Info. Theory*, vol. 4, no. 1, pp. 269-273, 1998.
- [38] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131-138, 1997.
- [39] R. de Wolf, "Quantum communication and complexity," *Theoretical Computer Science*, vol. 287, no. 1, pp. 337-353, 2002.
- [40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, C. U. Press, Ed. Bookman, 2010.
- [41] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, "Robust polarization-based quantum key distribution over a collective-noise channel," *Phys. Rev. Lett.*, vol. 92, p. 017901, 2004.
- [42] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Efficient quantum key distribution over a collective noise channel," *Phys. Rev. A*, vol. 78, p. 022321, 2008.

# Quantum Key Distribution over Collective Amplitude Damping Quantum Channels

Elloá B. Guedes and Francisco M. de Assis

Institute for Studies in Quantum Computation and Information (IQuanta)  
Post Graduation Programs in Electrical Engineering and Computer Science  
Federal University of Campina Grande (UFCG)  
Campina Grande – Paraíba – Brazil  
Email: {elloaguedes, fmarassis}@gmail.com

**Abstract**—One of the most mature quantum information techniques nowadays is Quantum Key Distribution (QKD) in which two legitimate parties make use of a protocol to create a symmetric private key using a quantum channel. The quantum channel is not secure, since there may be an eavesdropper intercepting and re-sending the quantum states that are sent through it. One of the main problems in using QKD protocols is the existence of noise which can make difficult the task of eavesdropping checking. Considering these issues, this paper presents a QKD protocol over a collective amplitude damping quantum channel that makes use of decoherence-free subspaces and subsystems. The QKD protocol proposed is noiseless despite the errors existing in the quantum channel. Moreover, it makes the probability of the eavesdropper's retrieve the secret message negligible asymptotically. Besides, the probability of eavesdropper detection is stable during the whole communication which eases the eavesdropping checking procedures.

**Keywords**—Quantum Key Distribution; One-Time Pad; Decoherence-Free Subspaces and Subsystems.

## I. INTRODUCTION

The principles of Quantum Mechanics provide novel ways for quantum information transmission and processing, such as Quantum Computation and Quantum Communication. Regarding Quantum Communication, in particular, some intrinsic properties of Quantum Mechanics enable features that do not have a counterpart in Classical Communication, such as: (i) a qubit does not have not a definite value until the moment after it is read; (ii) every measurement in a qubit may disturb it; (iii) arbitrary states of qubits cannot be copied; (iv) qubits can be entangled; among others [1]. Thanks to these Quantum Mechanics principles, in certain scenarios, unconditional security can be achieved in information conveying through quantum channels.

The *Quantum Key Distribution* (QKD) [2]–[5] is one of the most mature quantum information techniques nowadays. According to QKD, two remote users can create a private key securely. This key is then used to crypt the secret message into a ciphertext through a classical cryptographic scheme such as the one-time pad, and the ciphertexts are then sent from one user to another through a classical channel. However, in a practical transmission process, the channel noise cannot be avoided completely. Noise can increase not only the error rate of the sending message, but also the difficulty of finding an eavesdropper in the process of a security check.

In order to avoid the noise, some QKD protocols [6], [7] considered the use of quantum channels which are subject to *collective decoherence*. In this scenario, all qubits which suffer

noise are affected exactly in the same way [8]. Considering this particularity, in such quantum channels it is possible to find some symmetries that protect the information from the noise. The states which remain unaffected by the decoherence compose a *decoherence-free subspace or subsystem* (DFS) [9].

Boileau et al. [6] proposed two QKD protocols using the DFS existing in the collective rotation quantum channel. The first protocol considers a subspace and the second a subsystem, both free of decoherence. Their protocol considers also the use of singlets and the encoding is based on the parity of qubits. Thanks to that, an uncertainty is inserted about the state originally sent from the perspective of the eavesdropper. However, it does not affect the legitimate parties of the protocol, enabling them to create a private key that can be later used to encrypt a classical message. It is important to emphasize that the eavesdropper is not able to affect the qubits exchanged, nor gather information about the key. Based on similar ideas, Li et al. [7] proposed two QKD protocols using DFS and considering the collective rotation and dephasing quantum channels.

The *amplitude damping* is a type of quantum noise which can make a qubit be lost. This type of error is also subject to collective decoherence, characterizing the *collective amplitude damping quantum channels*. Although these quantum channels have a DFS, no QKD protocols have been developed for them. Hence, the main objective of the present work is to characterize a QKD protocol over collective amplitude damping quantum channels, aiming at providing a secure way to create private keys between the legitimate parties despite the existence of an eavesdropper on the channel.

The present work is organized as follows. The decoherence-free subspaces and subsystems are characterized and exemplified in Section II. The collective amplitude damping quantum channels and the decoherence-free subspaces existing on their structure are shown in Section III. The model of communication considered as well as the steps that comprise the protocol proposed are shown in Section IV. An analysis of security is discussed in Section V. Lastly, final remarks and suggestions for future work are presented in Section VI.

*Notations and Conventions* – The Dirac notation [10] will be used to denote quantum states and operations over them throughout the paper. A quantum state is said to be pure if it can be represented by a unitary vector in the Hilbert space  $\mathcal{H}$ . The *Hadamard operation*, implemented by the gate  $H$ , has the following matricial representation  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ . The symbol  $\mathbb{1}$  denotes the *identity matrix*.

## II. DECOHERENCE-FREE SUBSPACES AND SUBSYSTEMS

Due to decoherence, a quantum system may begin to lose energy into the environment and decay to a ground state, its relative phase may be erased and, thus, the information it carries may be lost [11]. In this section, we will show how to avoid these undesired effects despite the existence of decoherence.

Let a closed quantum system be composed of the *system of interest*  $S$  defined on a Hilbert space  $\mathcal{H}$  and of the *environment*  $E$ . The Hamiltonian that describes this system is defined as follows:

$$\mathbb{H} = \mathbb{H}_S \otimes \mathbb{1}_E + \mathbb{1}_S \otimes \mathbb{H}_E + \mathbb{H}_{SE}, \quad (1)$$

where  $\mathbb{1}$  is the identity operator; and  $\mathbb{H}_S$ ,  $\mathbb{H}_E$  and  $\mathbb{H}_{SE}$  denote the Hamiltonians of system, environment and system-environment interaction, respectively.

In order to prevent errors, it would be ideal that  $\mathbb{H}_{SE}$  were equal to zero, indicating that system and environment are decoupled and evolve independently and unitarily under their respective Hamiltonians  $\mathbb{H}_S$  and  $\mathbb{H}_E$  [9]. However, in practical scenarios, such an ideal situation is not possible since no system is noiseless. So, after isolating a system to the best of our ability, we should aim for the realistic goals of the identification and correction of errors when they occur and/or avoiding noises when possible and/or suppressing noise in the system [12].

If some symmetries exist in the interaction between the system and the environment, it is possible to find a “quiet corner” in the system Hilbert space not experiencing decoherence. Let  $\{E_i(t)\}$  be a set of operators in the *operator-sum representation* (OSR) corresponding to the evolution of the system. We say that a system density matrix  $\rho_S$  is *invariant* under the OSR operators  $\{E_i(t)\}$  if  $\sum_i E_i(t)\rho_S E_i^\dagger(t) = \rho_S$ . We are now able to define the decoherence-free subspaces whose states are invariant despite a non-trivial coupling between the system and the environment.

**Definition 1** (Decoherence-Free Subspace). *A subspace  $\tilde{\mathcal{H}}$  of a Hilbert space  $\mathcal{H}$  is called decoherence-free with respect to a system-environment coupling if every pure state from this subspace is invariant under the corresponding OSR evolution for any possible environment initial condition:*

$$\sum_i E_i(t)|\tilde{k}\rangle\langle\tilde{k}|E_i^\dagger(t) = |\tilde{k}\rangle\langle\tilde{k}|, \forall |\tilde{k}\rangle\langle\tilde{k}| \in \tilde{\mathcal{H}}, \forall \rho_E(0). \quad (2)$$

Let the Hamiltonian of the system-environment interaction be  $\mathbb{H}_{SE} = \sum_j \mathbf{S}_j \otimes \mathbf{E}_j$ , where  $\mathbf{S}_j$  and  $\mathbf{E}_j$  are the system and environment operators, respectively. We consider that the environment operators  $\mathbf{E}_j$  are linearly independent. The symmetries required to define a decoherence-free subspace are described in the theorem below. For a detailed proof or different formulations, see [9, Section 5].

**Theorem 1** (Decoherence-Free Subspace Conditions). *A subspace  $\tilde{\mathcal{H}}$  is decoherence-free iff the system operators  $\mathbf{S}_j$  act proportional to the identity on the subspace:*

$$\mathbf{S}_j|\tilde{k}\rangle = c_j|\tilde{k}\rangle \quad \forall j, |\tilde{k}\rangle \in \tilde{\mathcal{H}}. \quad (3)$$

The notion of a subspace which remains decoherence-free throughout the evolution of a system is not, however, the most general method for providing decoherence-free encoding of information in a quantum system [9]. Knill et al. discovered a method for decoherence-free encoding into subsystems instead of into subspaces, which is presented below [13].

**Definition 2** (Decoherence-Free Subsystem). *Consider a decomposition of the whole Hilbert space  $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ , where  $\dim(\mathcal{H}) = \dim(\mathcal{H}^A) \cdot \dim(\mathcal{H}^B) + \dim(\mathcal{K})$ . A subspace  $\mathcal{H}^B$  of the full Hilbert space is a decoherence-free subsystem if, for a quantum channel  $\mathcal{E}$ :*

$$\forall \rho^A, \forall \rho^B, \exists \tau^A : \mathcal{E}(\rho^A \otimes \rho^B) = \tau^A \otimes \rho^B, \quad (4)$$

where  $\rho^A, \tau^A \in \mathcal{B}(\mathcal{H}^A)$ , and  $\rho^B \in \mathcal{B}(\mathcal{H}^B)$ .

In fact,  $\mathcal{H}^B$  is said to encode a decoherence-free subsystem if (4) is satisfied. In particular, when  $\dim(\mathcal{H}^A) = 1$ ,  $\mathcal{H}^B$  is a decoherence-free subspace.

To make explicit the difference between decoherence-free subspaces and subsystems, consider the encoding of a generic qubit  $\alpha|0\rangle + \beta|1\rangle$  into  $\alpha|01\rangle + \beta|10\rangle$ . In this case, the information has been encoded into a *subspace* of the two qubit Hilbert space. Suppose now that the information is encoded only into the first qubit of the two qubits available, i.e.,  $\alpha|0\rangle + \beta|1\rangle \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle$ . Since this second encoding is a one-to-many mapping from the quantum information in one qubit to a two qubit Hilbert space, then it is said that the information has been encoded into a *subsystem*.

### A. Example

The *collective rotation quantum channel* acts on the input as follows:

$$|0\rangle \mapsto \cos\theta|0\rangle + \sin\theta|1\rangle, \quad (5)$$

$$|1\rangle \mapsto -\sin\theta|0\rangle + \cos\theta|1\rangle, \quad (6)$$

where  $\theta$  is the collective rotation parameter which fluctuates over time  $t$ . Two states that are immune to the decoherence caused by this quantum noisy channel are the following Bell states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (7)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (8)$$

Despite being entangled, these states are distinguishable and can be properly obtained at the channel's end using Bell measurements.

If one encodes a generic quantum state  $|\psi\rangle = a|0\rangle + b|1\rangle$  using the mentioned Bell states as logic qubits, i.e.,  $|\psi_L\rangle = a|\beta_{00}\rangle + b|\beta_{11}\rangle$ , we have that the resulting encoded state is protected from decoherence since the logic states are immune to the decoherence caused by the collective rotation quantum channel  $\mathcal{E}$  as follows:

$$\begin{aligned}\mathcal{E}(|\beta_{00}\rangle) &= \frac{1}{\sqrt{2}} [(\cos\theta|0\rangle + \sin\theta|1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle) \\ &\quad + (-\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (-\sin\theta|0\rangle + \cos\theta|1\rangle)] \\ &= |\beta_{00}\rangle,\end{aligned}\tag{9}$$

and

$$\begin{aligned}\mathcal{E}(|\beta_{11}\rangle) &= \frac{1}{\sqrt{2}} [(\cos\theta|0\rangle + \sin\theta|1\rangle) \otimes (-\sin\theta|0\rangle + \cos\theta|1\rangle) \\ &\quad + (-\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)] \\ &= |\beta_{11}\rangle.\end{aligned}\tag{11}$$

Besides the collective rotation quantum channel, the collective amplitude damping and the collective dephasing quantum channels are also examples of noisy quantum channels that have subspaces and subsystems that are immune to the existing decoherence.

### III. COLLECTIVE AMPLITUDE DAMPING QUANTUM CHANNEL

The phenomenon of energy dissipation when conveying a quantum state is modeled by the *collective amplitude damping quantum channel*. This channel has the following OSR:

$$\mathcal{E}(\rho) = A_0\rho A_0^\dagger + A_1\rho A_1^\dagger,\tag{13}$$

where the operation elements  $A_0$  and  $A_1$  are as follows:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix},\tag{14}$$

where  $\gamma$  is the damping rate which can be thought of as the probability of losing a photon [1, p. 380].

In this channel, due to its collectiveness behaviour, all qubits which suffer amplitude damping are subject to the same damping rate. Thanks to that, it is possible to find a "quiet corner" in the Hilbert space of this channel whose states do not suffer from the effects caused by this type of decoherence. Such states are said to belong to a DFS  $\tilde{\mathcal{H}}$  of the input Hilbert space  $\mathcal{H}$  of this quantum channel [9]. If a state  $\rho \in \tilde{\mathcal{H}}$ , where  $\tilde{\mathcal{H}} \subset \mathcal{H}$ , then it is not affected by the existing decoherence on the collective amplitude damping quantum channel  $\mathcal{E}$ , i.e.,  $\mathcal{E}(\rho) = \rho$ .

In this quantum channel, there are three different DFS, with dimensions 1, 2 and 3, respectively, as shown below:

$$\tilde{\mathcal{H}}_1 = \{|1\rangle\},\tag{15}$$

$$\tilde{\mathcal{H}}_2 = \left\{ |00\rangle, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\},\tag{16}$$

$$\tilde{\mathcal{H}}_3 = \left\{ \frac{1}{\sqrt{6}}(-2|001\rangle + |010\rangle + |100\rangle), \frac{1}{\sqrt{2}}(|011\rangle - |101\rangle), |000\rangle \right\}.\tag{17}$$

In particular, the DFS  $\tilde{\mathcal{H}}_2$  will be used in the quantum key distribution protocol that will be described in the next section.

## IV. PROPOSED PROTOCOL

Our protocol considers the scheme of communications showed in Figure 1. The legitimate parties (Alice and Bob) are connected through a classical channel and also through a collective amplitude damping quantum channel. Both channels are considered insecure. Despite of that, the objective of Alice and Bob is to create a private key to perform a secure classical message exchange.

The eavesdropper Eve has access to the quantum channel between Alice and Bob. She makes use of a device, which measures the quantum states sent through the channel and stores the basis used for measurement as well as the classical result obtained.

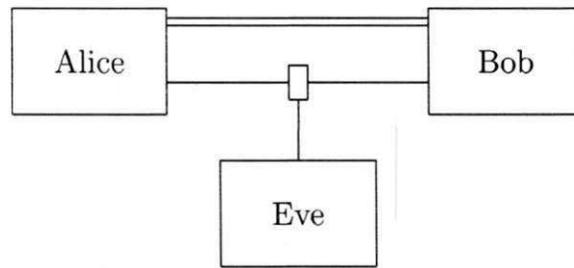


Fig. 1. Communication model considered. The single line wire represented is used for quantum communications while the double line wire is used for classical communications.

The idea of this protocol is very similar to the BB84 QKD protocol [2], but with the advantage of the noise avoidance due to the use of the DFS existing. The description of the protocol will be presented in the sections below.

### A. Protocol Description

The legitimate parties Alice and Bob makes use of the following quantum states:

$$|\rightarrow\rangle = |00\rangle,\tag{18}$$

$$|\uparrow\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},\tag{19}$$

$$|\nearrow\rangle = |++\rangle,\tag{20}$$

$$|\searrow\rangle = \frac{|+-\rangle - |-+\rangle}{\sqrt{2}},\tag{21}$$

where  $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$  and  $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ . Notice that the quantum states  $|\nearrow\rangle$  and  $|\searrow\rangle$  are obtained from  $|\rightarrow\rangle$  and  $|\uparrow\rangle$  by a Hadamard operation. Thanks to the DFS properties, none of the quantum states presented in Eqs. (18)-(21) are affected by the collective amplitude damping. The quantum circuits illustrated on Figure 2 show how to obtain such quantum states.

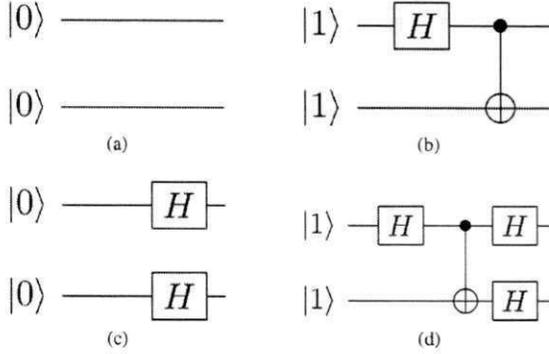


Fig. 2. Quantum circuits that implement the states  $|\rightarrow\rangle$ ,  $|\uparrow\rangle$ ,  $|\nearrow\rangle$ , and  $|\searrow\rangle$ , respectively.

Alice starts the protocol sending states randomly chosen from the set  $\{|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, |\searrow\rangle\}$ . Bob and Eve measure the states received using the bases horizontal-vertical  $+ = \{|\rightarrow\rangle, |\uparrow\rangle\}$  or diagonal  $\times = \{|\nearrow\rangle, |\searrow\rangle\}$  also randomly chosen.

Let's first consider that Eve is not affecting the communication between Alice and Bob. Table I shows some examples of the results obtained by Alice and Bob in order to create their private symmetric key. If Alice sends  $|\rightarrow\rangle$  or  $|\uparrow\rangle$  and Bob measures with  $+$ , he will obtain bits 0 and 1, respectively, with 100% of certainty. The same is true when Alice sends  $|\nearrow\rangle$  and  $|\searrow\rangle$  and Bob measures with  $\times$ . However, for instance, if Alice sends  $|\rightarrow\rangle$  and Bob measures with  $\times$ , then there is a probability of 0.5 that he will receive the bit 0 and of 0.5 regarding the bit 1.

TABLE I. RESULTS OBTAINED BY BOB AFTER MEASURING THE QUANTUM STATES SENT BY ALICE WITH THEIR RESPECTIVE PROBABILITY.

Alice sends	$ \rightarrow\rangle$	$ \uparrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$
Bob measurement	$+$	$+$	$\times$	$\times$
Bit obtained	0	1	0	1
Probability	1	1	1	1

Alice sends	$ \rightarrow\rangle$	$ \searrow\rangle$	$ \nearrow\rangle$	$ \uparrow\rangle$
Bob measurement	$\times$	$+$	$+$	$\times$
Bit obtained	0 or 1	0 or 1	0 or 1	0 or 1
Probability	0.5	0.5	0.5	0.5

In order to avoid uncertainties regarding the bits obtained by Bob, he will communicate to Alice the sequence of bases he used to measure the qubits that she sent. Alice will return to Bob a string of 0's and 1's, where 0 indicates that the respective measurement must be discarded because it leads to uncertainty. After this process, even without communicating the results of the measurements, Alice and Bob agree on the results obtained after the measurement. The bits resultant will compose the private symmetric key that they will use in an one-time pad encryption of the secret classical message sent through the classical channel.

To illustrate the protocol proposed, let's suppose that Alice sends to Bob the following sequence of qubits:  $|\nearrow\rangle, |\uparrow\rangle, |\uparrow\rangle, |\rightarrow\rangle, |\nearrow\rangle, |\searrow\rangle, |\uparrow\rangle$ . Bob uses the sequence of bases  $+, +, \times, +, \times, +, +$  and obtains the sequence of bits given by 0100011. Bob sends the sequence of bases he used

through the classical channel and Alice returns him the sequence 0011101. The sequence of bits sent by Alice indicates that the first, second and sixth bits obtained by Bob must be discarded. So, the private symmetric key between Alice and Bob will have length 5 and will be equal to 00001. With this key, Alice can send Bob a classical message in secrecy by using the one-time pad scheme.

The *one-time pad* encryption scheme requires that the message and the secret key must be of equal length. Let  $m$  be the message and  $k$  be the key, both with  $n$  bits. The encrypted version of the message  $e$  is obtained by  $e_i = m_i \oplus k_i$ , for  $i = 1, \dots, n$ , where  $\oplus$  denotes the addition modulo 2. If the key is used only a single time and if it is kept in secret, then the conditions for *perfect secrecy* in the communication are guaranteed [14].

In the considered example, let's suppose that Alice wants to send a message  $m = 10101$  to Bob. She will follow the one-time pad steps, considering the key  $k = 00001$ , and will obtain  $e = 10100$  that will be sent through the classical channel to Bob. Upon receiving  $e = 10100$ , Bob will use the key  $k = 00001$ , and will retrieve the message sent by Alice by also using the  $\oplus$  operation, which results in  $m = 10101$ . This way, the quantum key distribution protocol and the secret classical message exchange conclude successfully.

In the characterization of the protocol presented, the eavesdropper Eve makes no action during the key creation process. However, it is very unrealistic and her action on the quantum channel must be considered. The next section shows how she can gather information from the private key created by Alice and Bob and how they can use strategies in order to detect her presence and to avoid her success.

### B. Eavesdropping Checking

According to the model of communications considered, Eve can perform measurements in the state sent by Alice, recover a bit from it, and resend the resulting state to Bob. During this process, Eve can not only recover bits from the private key, but also change the quantum state originally sent to Bob.

Eve performs measurements in the state sent by Alice using the bases  $+$  and  $\times$  randomly chosen, i.e. using the same strategy than Bob. To do so, she uses a device which gets the input on the quantum channel, measures it, and resend the resulting quantum state to the channel's output. The effects on the measurements performed by her may degrade the information received by Bob. Table II synthesizes the effects of Eve on the quantum channel.

If by random choice Eve chooses the same basis that Alice used to prepare the quantum states, as shown in the first part of Table II, she will measure the same bit than Bob and will cause no disturbance on the system. However, if she measure the states using the wrong basis, as shown in the second part of Table II, she will have no certainty about the state sent by Alice and will also modify the state received by Bob. When this second situation happens, Alice and Bob can perform successfully the eavesdropper detection.

To perform the eavesdrop detection, besides the bases exchange between Bob and Alice, Bob will also reveal to Alice some bits that he obtained after the measurement. Those bits revealed are important to detect the eavesdropper but they must be discarded after that in order to not compromise the security

TABLE II. STATES SENT BY ALICE AND MEASURED BY THE EAVESDROPPER EVE.

Alice sends	$ \rightarrow\rangle$	$ \uparrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$
Eve measurement	+	+	$\times$	$\times$
Eve's resulting bit	0	1	0	1
Probability	1	1	1	1
Bob received state	$ \rightarrow\rangle$	$ \uparrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$

Alice sends	$ \rightarrow\rangle$	$ \uparrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$
Eve measurement	$\times$	$\times$	+	+
Eve's resulting bit	0 or 1	0 or 1	0 or 1	0 or 1
Probability	0.5	0.5	0.5	0.5
Bob received state	$ \nearrow\rangle$ or $ \searrow\rangle$	$ \nearrow\rangle$ or $ \searrow\rangle$	$ \rightarrow\rangle$ or $ \uparrow\rangle$	$ \rightarrow\rangle$ or $ \uparrow\rangle$

of private key. To illustrate such situation, let's suppose that Alice sent Bob the state  $|\nearrow\rangle$ , Eve measured it with the basis  $+$  and obtained the bit 1, and Bob measured with the basis  $\times$  and received the bit 1. When Bob tells Alice that he used the basis  $\times$  and obtained the bit 1, she can notice that something is wrong and can conclude that there exists an eavesdropper in the quantum channel, because the scenario considered is noiseless.

So, in order to create a private key in secrecy, they must communicate not only the bases used for measurement, but also some of the results obtained. It is essential to ensure the security in the protocol proposed as it is going to be shown in the next section.

## V. SECURITY ANALYSIS

The goal of an ideal key distribution is to allow Alice and Bob, who share no information initially, to share a secret key (a string of bits) at the end. Eve, the eavesdropper, should not obtain information about the key. Also, whatever Eve does, Alice's and Bob's key should be identical. It is assumed that all quantum and communication between Alice and Bob passes through Eve, and similarly for classical communication [5].

No quantum key distribution protocol can succeed if Eve has the power to impersonate Alice while communicating with Bob and to impersonate Bob while communicating with Alice. If Alice and Bob meet previously, there are authentication techniques which can be used to ensure unconditional security [15]. However, in a scenario where Alice and Bob have never exchanged a secret key before, one must assume that Alice and Bob have access to a faithful (classical) public channel so a third part cannot accomplish the impersonation attack without being detected.

Different from classic communication, the security of quantum communication is based on the laws of physics rather than the difficulty of computation. The eavesdropper Eve is so powerful that her ability is only limited by the principles in quantum mechanics. However, the *No-Cloning Theorem* [16] forbids Eve to eavesdrop the quantum signals freely and fully as her action will inevitably disturb the unknown states and leave a trace in the outcomes obtained by the two legitimate users [7]. These facts will help us in the characterization of the security in the proposed protocol.

The eavesdropping strategy that we will consider in the security analysis of the proposed protocol is the *intercept and resend attack* [17] in which Eve measures the quantum state sent by Alice, obtains a bit, and re-sends the resulting quantum

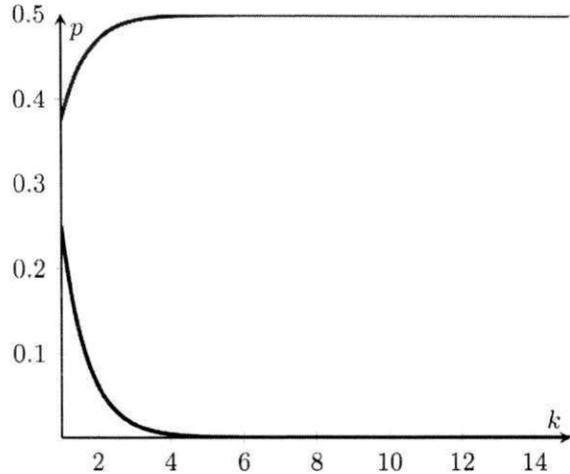


Fig. 3. Graphic showing the exponential decrease in Eve's success probability in recovering all key bits (blue line) and the probability of Alice and Bob detecting the eavesdropper per bit exchanged to create the secret key (red line).

state to Bob. This kind of attack was already depicted in Section IV, but the probability of eavesdropping detection and of Eve's success is going to be described from now on. It is important to emphasize that since this protocol is based on the BB84 QKD protocol [2], the same proofs of security are adequate to our proposition. We strongly suggest the work of Mayers [5] as a source of a more formal approach to these proofs.

If Alice wants to send a bit  $b$  to Bob, she can encode it in two different ways. Eve, upon intercepting it, can also use two options of measurement bases. Her chance of guessing the correct bit is equal to 50%. But if she uses an incorrect basis and it leads to Bob receiving a different bit than was originally sent by Alice, the chance of eavesdropping detection is also of 50% per bit sent.

Let us suppose that Alice and Bob want to create a private key of size  $k$ . Given that Eve may perform intercept and resend attacks, they will reinforce the eavesdropping checking procedure by using  $k$  additional bits. The probability of Eve measuring correctly the  $2 \cdot k$  bits exchanged between the legitimate parties is of  $p(2 \cdot k) = 0.5^{2 \cdot k}$  which decreases exponentially as the size of the key increases as shown in the blue line in Figure 3.

However, if Eve mistakes a single bit in a  $2 \cdot k$  bits sequences (probability equal to  $p_{\text{error}}(1) = 0.5$  per bit), it may result in a bit error detection by Bob and Alice (probability equal to  $p_{\text{detection}}(1) = 0.5$  per bit missed by Eve). Considering these probabilities, the chance of detecting Eve at the  $n$ -th bit goes asymptotically to 0.5, as shown in the red line of the graphic in Figure 3, i.e., it is strongly related with the probability of error detection. Differently from the probability of Eve success, the probability of eavesdropping detection is independent per bit exchanged. Since Eve can change a qubit and this alteration may not be detected, as reported in Tables I and II, there always a probability of not detecting the eavesdropper in the communication.

As it can be seen, while the success of Eve depends on guessing all bits without disturbing the communication between Alice and Bob, her detection depends on one mistake

on her measurements which disturbs the bit received by Bob used in the eavesdrop checking process. Thus, we can conclude that the ability of the protocol to detect eavesdropping is high, ensuring enough security for practical scenarios of its use. This concludes the analysis of security of the quantum key distribution protocol proposed.

## VI. CONCLUSION

The first practical demonstration of a QKD protocol took place in the early 1990s using photons over a distance of 30 km through air. After that, the next implementation over the atmosphere guaranteed a secure communication with quantum bits over a distance of 2 km. After that, QKD protocols could be implemented in distances up to 250 km [18]. Nowadays, even commercial devices are being developed and sold to perform secure quantum key distribution [19].

However, one of the main problems in practical QKD is the noise, which can not only affect the communication between the legitimate parties, but can also favor an existing eavesdropper. In the attempt to minimize such problems, we proposed a QKD protocol over a collective amplitude damping quantum channel where an eavesdropper performs intercept and resend attacks.

This protocol is mainly based on BB84 QKD protocol [2], but since it considers the existing DFS on the quantum channel taken into account, the communication is noiseless. However, we consider the existence of an eavesdropper which aims at discovering the private key in the attempt to make a breach of security in the message exchange between Alice and Bob. In order to avoid it, the legitimate parties must use extra bits, randomness and also certain procedures for eavesdropping checking. As shown in Section V, it causes a very low probability of Eve's success while the probability of eavesdropping detection is high.

This work contributes to the use of the DFS in secure communications. If the eavesdropper is passive, following the model of quantum wiretap channels [20], [21], it is possible to reach unconditional security in the communications [22], [23]. This scenario not always occurs, so it is essential to consider other protocols and techniques. Since DFS arise where collective decoherence takes place [24], other works developing QKD protocols for collective dephasing and rotation quantum channels were already considered [6], [7]. However, so far, no protocol for QKD on collective amplitude damping quantum channels were known.

In practical scenarios, some works already report the implementation of quantum channels with DFS [25]–[27] even in long distance [28]. With this already existing technology, the proposed protocol can be adopted in realistic scenarios to provide secure communications.

In future work, we aim at proposing other protocols and techniques for secure communications over eavesdropped quantum noisy channels.

## ACKNOWLEDGEMENTS

The authors acknowledge the financial support rendered by the Brazilian funding agencies CAPES and CNPq, by the Post Graduation Program in Electrical Engineering at the Federal University of Campina Grande, and by the project QUANTA/RENASIC/FINEP.

## REFERENCES

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. 2nd ed., Bookman: Cambridge University Press, 2010.
- [2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing." ICCSSP Press, 1984, pp. 175-179.
- [3] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem." *Phys. Rev. Lett.*, vol. 67, 1991, pp. 661-663.
- [4] C. H. Bennett, "Quantum Cryptography Using any Two Nonorthogonal States." *Phys. Rev. Lett.*, vol. 68, 1992, pp. 3121-3124.
- [5] D. Mayers, "Unconditional Security in Quantum Cryptography," *Journal of the ACM*, vol. 48, 2001, pp. 351-406.
- [6] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin and R. W. Spekkens, "Robust Polarization-Based Quantum Key Distribution over a Collective-Noise Channel." *Phys. Rev. Lett.*, vol. 92, 2004, pp. 017901.
- [7] X.-H. Li, F.-G. Deng and H.-Y. Zhou, "Efficient Quantum Key Distribution Over a Collective Noise Channel," *Phys. Rev. A*, vol. 78, 2008, pp. 022321.
- [8] J. Stolze and D. Suter, *Quantum Computing – A short course from theory to experiment*. Wiley: VCH Verlag, 2004.
- [9] D. A. Lidar and K. B. Whaley, "Decoherence-Free Subspaces and Subsystems", arxiv: quantum-ph/0301032v1, 2003. (Retrieved: May, 2013).
- [10] P. Dirac, *The principles of Quantum Mechanics*, 4th ed., Oxford University Press: Oxford, 1982.
- [11] A. Shabani and D. A. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems." *Phys. Rev. A*, vol. 72, 2005, pp. 042303.
- [12] M. S. Byrd, L.-A. Wu and D. A. Lidar, "Overview of quantum error prevention and leakage elimination," *Journal of Modern Optics*, vol. 51, 2004, pp. 2449-2460.
- [13] E. Knill, R. Laflamme and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, 2000, pp. 2525.
- [14] C. Paar and J. Pelzl, *Understanding Cryptography*, Springer: Springer, 2010.
- [15] M. N. Wegman and J. L. Carter, "New Hash Function and their Use in Authentication and Set Equality," *J. Comput. Syst. Sci.*, vol. 22, 1981, pp. 265-279.
- [16] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned," *J. Comput. Syst. Sci.*, vol. 299, 1982, pp. 802-803.
- [17] D. Kalamidas, "Single-Photon Quantum Error Rejection and Correction With Linear Optics," *Phys. Lett. A*, vol. 343, 2005, pp. 331-335.
- [18] J. Mullins, "Making Unbreakable Code," *IEEE Spectrum*, vol. May, 2002, pp. 40-45.
- [19] ID Quantique, "Quantum Key Distribution", <http://www.idquantique.com>, 2013. (Retrieved: May, 2013).
- [20] N. Cai, A. Winter and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, 2004, pp. 318-336.
- [21] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, 2005, pp. 44 -55.
- [22] E. B. Guedes and F. M. Assis, "Utilização de Subespaços Livres de Decoerência em Comunicações Quânticas Incondicionalmente Seguras," *Proc. Simpósio Brasileiro de Telecomunicações (SBTr'12)*, SBTr Press, 2012, pp. 1-5.
- [23] E. B. Guedes and F. M. Assis, "Unconditional Security with Decoherence-Free Subspaces", arXiv:quant-ph/1204.3000, 2012, pp. 1-6. (Retrieved: May, 2013).
- [24] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, 1997, pp. 3306.
- [25] G. Jaeger and A. Sergienko, "Constructing four-photon states for quantum communication and information processing," *Int. J. Theor. Phys.*, vol. 47, 2008, pp. 2120.
- [26] U. Dorner, A. Klein and D. Jaksch, "A quantum repeater based on decoherence free subspaces," *Quant. Inf. Comp.*, vol. 8, 2008, pp. 468-490.
- [27] Y. Xia, J. Song, Z.-B. Yang and S.-B. Zheng, "Generation of four-photon polarization-entangled decoherence-free states within a network," *Appl. Phys. B*, vol. 99, 2010, pp. 651-656.
- [28] P. Xue, "Long-distance quantum communication in a decoherence-free subspace," *Phys. Lett. A*, vol. 372, 2008, pp. 6859-6866.

# Simulating the Quantum Fourier Transform

Francisco R. Pereira<sup>1</sup>, Elloá B. Guedes<sup>1,2</sup>, Francisco M. de Assis<sup>1</sup>

<sup>1</sup>Institute for Studies in Quantum Computation and Information  
Federal University of Campina Grande  
Av. Aprígio Veloso, 882 – 58429-900 – Campina Grande – PB – Brazil

<sup>2</sup>Superior School of Technology  
University of the Amazonian State  
Av. Darcy Vargas, 1200 – 69050-020 – Manaus – AM – Brazil

{revson.ee, elloaguedes, fmarassis}@gmail.com

**Abstract.** *Quantum Computing is a computational paradigm that takes into account the laws of Quantum Physics in the steps of the computation which advantages were verified both in Computation and Communications. No scalable quantum computer was developed so far and to execute, to test, and to create new quantum algorithms the simulation of quantum computers on classical computers plays an important role. In this work, we show the design, tools and results obtained for the simulation of the Quantum Fourier Transform algorithm. As a result, we developed an open-source tool, called FT Simulator; and we could simulate up to 12 qubits according to the procedures specified by an experimental test.*

## 1. Introduction

In 1982, Feynman observed that it did not appear possible for a Turing machine to simulate certain quantum physical processes without incurring an exponential slowdown [Feynman 1982]. Considering this difficulty, years later Deutsch proposed a computing model – the quantum Turing machine – which considered the processes of Quantum Mechanics in the steps of computation [Deutsch 1985, Deutsch 1989]. With such contribution, Deutsch inaugurated the *Quantum Computing paradigm*.

The first algorithms proposed according to Quantum Computing already showed some advantages over their classical counterpart [Nielsen and Chuang 2010]. However, the first outstanding algorithm proposed according to this paradigm was the *quantum factorizing algorithm* [Shor 1997]. This algorithm has a polynomial-time complexity on the quantum Turing machine while no similar time complexity algorithm is known for classical computers. The *quantum search algorithm* is also a remarkable result [Grover 1997]. This algorithm has a quadratic speedup over classical algorithms on searching over an unsorted database.

The intrinsic properties of Quantum Mechanics such as superposition and entanglement motivated the research and proposition of quantum algorithms not only for computing, but also for communication systems [Imre and Gyongyosi 2012]. Developments made by literature updated some computing models such as automata and grammars to take into account quantum properties in their computation [Bacon and van Dam 2010]. However, a formal proof that the Quantum Computing paradigm is better or not than the Classical/Probabilistic Computing paradigm is not known yet.

Despite the already consolidated results on quantum algorithms and the advantages verified, the practical implementation of a quantum computer is still far from being scalable. Different technologies are under research and some of them are very restrictive, demanding a very low temperature, a high degree of precision, among other hard to meet requirements [Ladd et al. 2010].

Considering the practical difficulty of building a quantum computer, despite the limitations of simulating quantum systems on classical computers, sometimes it is the only way to “execute” a quantum algorithm over some input. Given the importance of simulation in the current context of Quantum Computing, this article aims at presenting a simulation of the *Quantum Fourier Transform* algorithm. This algorithm is in the heart of the quantum factorization algorithm [Shor 1997] and was applied in the development of quantum codes [Santos et al. 2013], in the design of quantum attacks to pseudorandom generators [Guedes et al. 2013], and even in other quantum algorithms [Williams 2011].

To present such simulation, this article is organized as follows. The description of the Quantum Fourier Transform algorithm, its quantum circuit and applications are described in Sec. 2. The simulation of the Quantum Fourier Transform is described in Sec. 3 and its analysis in Sec. 4. Lastly, final remarks and future work are presented in Sec. 5.

**Notations, Conventions and Suggestions** Along this paper, the Dirac notation will be used to denote quantum states and operations. Moreover,  $\mathbb{1}$  is the identity matrix and  $i$  is the imaginary unity. If the reader is not familiar with Quantum Computing, the books of Nielsen and Chuang [Nielsen and Chuang 2010, Chapter 2] and of Williams [Williams 2011, Part I] are recommended.

## 2. Quantum Fourier Transform

The *Quantum Fourier transform* (QFT) is the quantum counterpart of the well known discrete Fourier transform. The QFT takes as input a quantum state and produces a superposition of quantum states as formalized in Definition 1.

**Definition 1 (Quantum Fourier Transform).** *Let  $|j\rangle$  be an orthonormal vector in a Hilbert space  $\mathcal{H}$  with dimension  $2^m$  ( $m > 0$ ), i.e., belonging to the basis  $\{|0\rangle, |1\rangle, \dots, |2^m - 1\rangle\}$ . The quantum Fourier transform of  $|j\rangle$  is given by*

$$\text{QFT } |j\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{\frac{2\pi i k \cdot j}{2^m}} |k\rangle. \quad (1)$$

The QFT is unitary, invertible and has quadratic polynomial time over the input size. The quantum circuit which implements such transform is shown on Figure 1. The matricial expression for the gates  $H$  and  $R_k$  are given by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \quad (2)$$

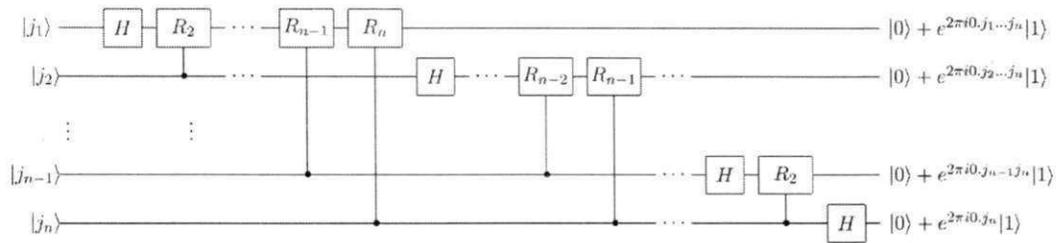


Figure 1. Quantum circuit which implements the QFT [Nielsen and Chuang 2010].

The QFT is very important for Quantum Computation and Information. Its conception enabled the development of the quantum factorizing algorithm, the first one that was identified as having a superpolynomial speedup over its best classical counterpart [Shor 1997]. The practical implementation of these algorithms may harm the security of RSA-based systems widely used nowadays [Paar and Pelzl 2010]. Besides these applications, the QFT is used to compromise the unpredictability of cryptographically secure pseudorandom generators [Guedes et al. 2013], to calculate the decoding syndrome for quantum graph codes [Santos et al. 2013], etc.

### 3. Simulation of the Quantum Fourier Transform

In order to simulate the QFT in a classical computer, we developed a C++ software called *FTSimulator*. The C++ programming language was chosen because its advantages due to be compiled which results in a better efficiency when compared to interpreted programming languages [Grune et al. 2012]. The input for the simulation is a text file which describes the density matrix of the initial quantum state. The output file is also a density matrix containing the result of the input state transformed by the QFT.

The *FTSimulator* architecture follows the Model-View-Controller design pattern [Gamma et al. 1994]. The advantages of using this pattern is to enable a clear modularization and to favor the encapsulation of the classes implemented. An overview of the architecture of *FTSimulator* is shown on Figure 2. Some elements presented in the architecture will be depicted later.

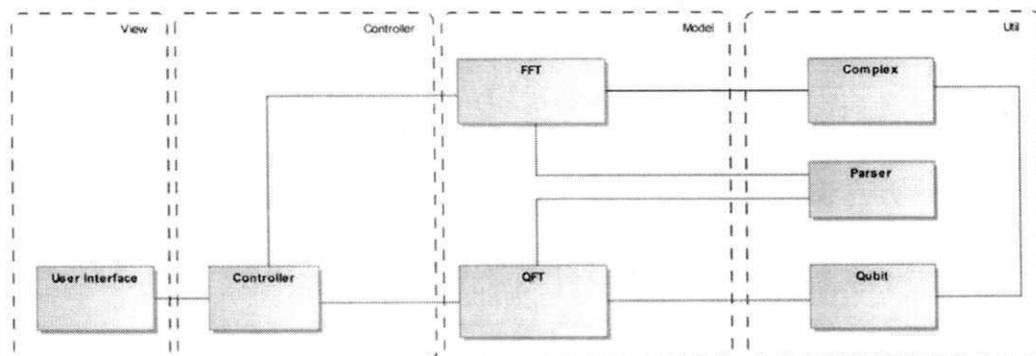


Figure 2. Architectural view of the *FTSimulator*.

The *View* part includes the textual interface with which the user interacts. The *Controller* part contains the layer that converts the user input into commands and that

presents the results to the user. The *Model* part includes the QFT module and also the FFT module, that will be explained latter. Utilities classes can also be found, such as for complex numbers and qubits representation as well as a parser that reads the input files according to their formatting.

The QFT module considers the input as being a density matrix. Such representation enables entangled and superpositioned multi-qubits input. Given a density operator  $\rho$ , the *FTSimulator* will perform the operation  $\text{QFT } \rho \text{ QFT}^\dagger$ , where  $\dagger$  denotes the transpose conjugate. The difficulty is to build and apply the QFT operator for different input dimensions. To do so, the algorithm that builds the QFT operator of Eq. (1) is shown on Figure 3.

```

function CQFT::QFTOPERATOR(complex **qftOp, int N)
  for int i = 0; i < N; i ++ do
    for int j = 0; j < N; j ++ do
      qftOp[i][j] = complex((double) (1/sqrt((float) N))*cos(2*PI*i*((float) j/((int) N))),
        (double) (1/sqrt((float) N))*sin(2*PI*i*((float) j/((int) N))))
    end for
  end for
end function

```

**Figure 3. Algorithm in C++ syntax-like style showing how the QFT operator is defined.**

Due to the inefficiency issues when simulating a quantum system on a classical computer, the *FTSimulator* tries to minimize the possible problems by disposing data structures out of the memory as long as they are not needed. The positive effects of such practice are specially important when the input considered has a considerable number of qubits.

In order to exemplify the execution of the *FTSimulator*, consider that the Bell state  $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  whose density matrix is shown on Eq. (3) is in the input file.

$$\rho_{\text{input}} = \begin{bmatrix} 0,5 & 0 & 0 & 0,5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0,5 & 0 & 0 & 0,5 \end{bmatrix}. \quad (3)$$

It must be emphasized that this 2-qubit quantum state is in superposition and is also highly entangled (mixed state), showing two unique quantum characteristics. The *FTSimulator* performs the following processing:  $\rho_{\text{output}} = \text{QFT } \rho_{\text{input}} \text{ QFT}^\dagger$ , in which the QFT operator is described in Sec. 2. As a result, the density matrix  $\rho_{\text{output}}$ , shown in Eq. (4) is stored in the output file.

$$\rho_{\text{output}} = \begin{bmatrix} 0,5 & 0,25 + 0,25\iota & 0 & 0,25 - 0,25\iota \\ 0,25 - 0,25\iota & 0,25 & 0 & -0,25\iota \\ 0 & 0 & 0 & 0 \\ 0,25 + 0,25\iota & 0,25\iota & 0 & 0,25 \end{bmatrix}. \quad (4)$$

Besides performing the QFT, the *FTSimulator* is also able to perform the *Fast Fourier transform* (FFT) [Cooley and Tukey 1965] on any matricial input. Different from the QFT, the FFT can be applied to any matrix and it specifies a transformation which is applied to numbers instead of quantum states. The FFT is very important to communications, audio and image processing, differential equations, among other applications [Rao et al. 2010]. The FFT output on *FTSimulator* can be automatically converted to  $\LaTeX$  graphics that can be used in reports, articles, etc. The FFT module and its relation with the other elements of the *FTSimulator* can be view in Figure 2.

#### 4. Analysis of the Simulation of the Quantum Fourier Transform

To analyze the simulation of the QFT performed by the *FTSimulator*, we considered an experimental approach. This approach would be helpful in the determination of the maximum number of qubits of the input able to be simulated and also the time spent by this simulation. To do so, we considered a machine with a processor with 3.2 GHz and with 15 GB of main memory.

To evaluate the *FTSimulator* regarding the QFT, it was necessary to develop two additional modules: (i) a module for generation of density matrices, respecting the properties that they are hermitian, positive and have trace equal to 1; and (ii) a test control module which receives  $n$  and  $r$  where  $n$  is the number of qubits to be tested and  $r$  is the number of repetitions necessary to reach certain significance level.

The test control module calls the module for generation of density matrices, uses them as input for the QFT and stores the time that each matrix took to be transformed with the *FTSimulator*. The organization of these modules and the data flow are illustrated in Figure 4.

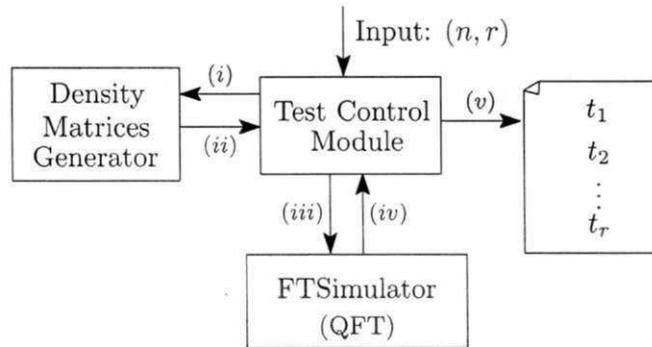
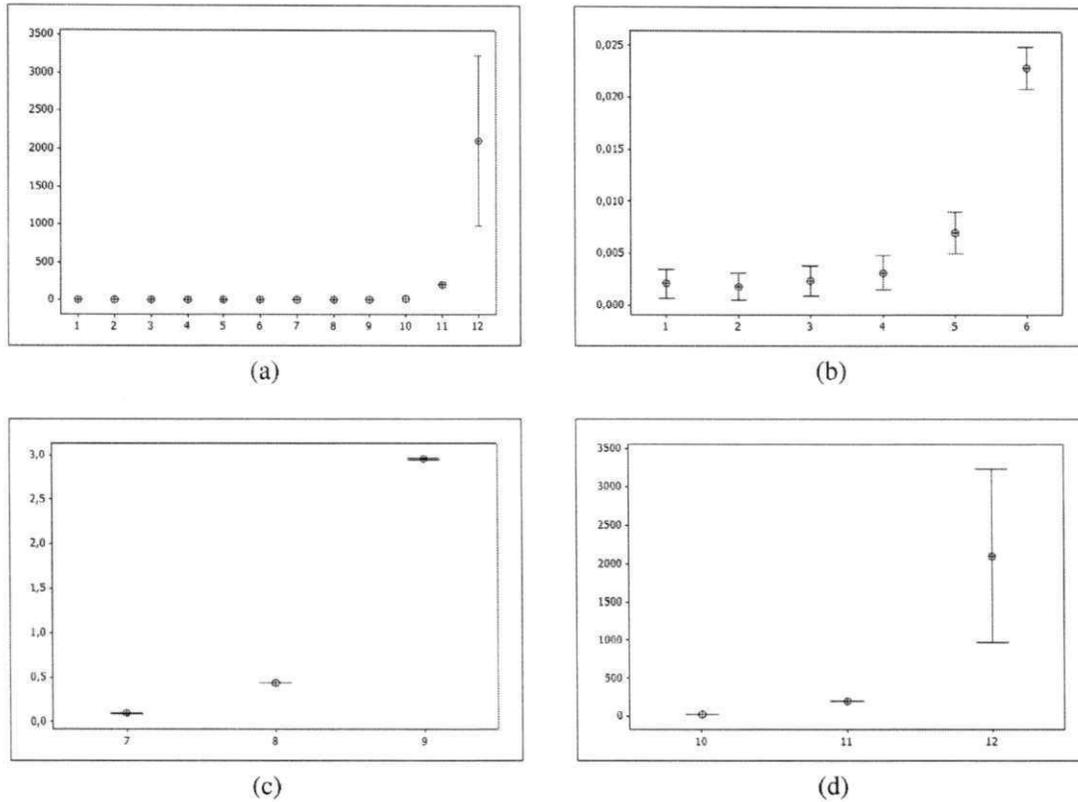


Figure 4. General idea of the evaluation of the QFT in the *FTSimulator*.

The confidence level considered was 95% for the mean and the data obtained for each  $n$  did not revealed a normal distribution tendency. The confidence interval plot of the results obtained is shown on Figure 5 and other statistics are shown on Table 1.<sup>1</sup>

<sup>1</sup>For more information regarding experimental tests and their results meaning, the books of Jain [Jain 1991] and Lilja [Lilja 2004] are recommended.



**Figure 5. Interval plots for the mean with confidence level of 95%. The  $x$  axis represents the number of qubits and the  $y$  axis represents the time in seconds.**

**Table 1. Mean and standard deviation obtained for the time of simulation per number of qubits.**

Qubits	Mean	Standard Deviation
1	0,002083	0,005359
2	0,001817	0,005044
3	0,002333	0,005605
4	0,003167	0,006389
5	0,00700	0,00781
6	0,02290	0,00792
7	0,09078	0,01274
8	0,43967	0,00884
9	2,9572	0,0358
10	22,540	0,178
11	200,52	0,774
12	2107	709

The most of confidence intervals are small as can be confirmed by the respective standard deviation. A narrow confidence interval shows an accurate result for the simulation time for the respective number of qubits. As the number of qubits increase, an exponential-like growth can also be observed. This is an expected consequence since the simulation of quantum systems by classical computers is not efficient.

The results for 12 qubits, however, were expected to be a little better, i.e., the simulation of the QFT for 12-qubit input would be desired to require less time. We strongly believe that it happened due to operating system issues where paging was required and data from main memory was moved to a lower access secondary memory.

## 5. Conclusion

In this paper we presented a simulation of the quantum Fourier transform algorithm. This simulation was performed in a classical computer due to the non-existence of a scalable implementation of a quantum computer. However, as shown previously, this kind of simulation is not efficient and issues like input size, memory management, data structure management, among others had to be considered.

Aiming at performing the proposed simulation, a software called *FTSimulator* was built. This software is able to perform the QFT on up to 12 qubits. The time required by these simulations was analyzed and narrow confidence intervals were verified, showing that the *FTSimulator* has a very similar performance on input of same size. In this analysis, the 12 qubit input revealed a high standard deviation when compared to the other number of qubits. Although we strongly believe that it is due to an operating system behavior, we are interested in performing more tests on such input size considering operating system variables in order to verify this hypothesis.

The *FTSimulator* is a multi-platform open-source application under the GNU Public License 3 which code is available on <http://ftsimulator.googlecode.com>. Besides the QFT, the *FTSimulator* is also able to perform the FFT, generating  $\LaTeX$  graphics for the output.

In future work we aim at improving the number of qubits able to be simulated with the *FTSimulator* by using more complex data structures (considering the existence of sparse matrices, for instance) and other optimization techniques for quantum circuits simulation [Viamontes et al. 2009]. These improvements would be helpful to use the *FTSimulator* as part of a simulation of the quantum factorizing algorithm. Moreover, we would like to develop didactic resources to help Computer Science and Engineering students to use *FTSimulator* as a tool to support the learning of the Quantum Computing paradigm.

## Acknowledgements

The authors acknowledge the financial support rendered by the CAPES, CNPQ, UFCG and by the project QUANTA/RENASIS/FINEP. The authors are thankful for the help and ideas provided by the Professors Aécio de Lima and Bruno Albert.

## References

- Bacon, D. and van Dam, W. (2010). Recent Progress in Quantum Algorithms. *Commun. ACM*, 53(2):84–93.
- Cooley, J. W. and Tukey, J. W. (1965). An algorithm for the machine calculation of complex fourier series. *Mathematics of Computation*, 19:297–301.
- Deutsch, D. (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London A*, 400:97–117.
- Deutsch, D. (1989). Quantum computational networks. *Proc. R. Soc. London A*, 425:73–90.
- Feynman, R. (1982). Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21:467–488.

- Gamma, E., Helm, R., Johnson, R., and Vlissides, J. (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional.
- Grover, L. K. (1997). Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters*, 79:325–328.
- Grune, D., van Reeuwijk, K., Bal, H. E., Jacobs, C. J., and Langendoen, K. (2012). *Modern Compiler Design*. Springer.
- Guedes, E. B., de Assis, F. M., and Lula Jr., B. (2013). Quantum attacks on pseudorandom generators. *Mathematical Structures in Computer Science*, 23:1–27.
- Imre, S. and Gyongyosi, L. (2012). *Advanced Quantum Communications: An Engineering Approach*. Wiley-IEEE Press.
- Jain, R. (1991). *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modeling*. John Wiley.
- Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., and O'Brien, J. L. (2010). Quantum computers. *Nature*, 464:45–53.
- Lilja, D. (2004). *Measuring Computer Performance*. Cambridge University Press.
- Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Bookman.
- Paar, C. and Pelzl, J. (2010). *Understanding Cryptography*. Springer.
- Rao, K., Kim, D., and Hwang, J. (2010). *Fast Fourier Transform: Algorithms and Applications*. Springer.
- Santos, G. O., de Assis, F. M., and de Lima, A. F. (2013). Explicit error syndrome calculation for quantum graph codes. *Quantum Information Processing*, 12(2):1269–1285.
- Shor, P. (1997). Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26:1484–1509.
- Viamontes, G. F., Markov, I. L., and Hayes, J. P. (2009). *Quantum Circuit Simulation*. Springer.
- Williams, C. P. (2011). *Explorations in Quantum Computing*. Springer.