

# ANAIS DO 7º WORKSHOP-ESCOLA DE COMPUTAÇÃO E INFORMAÇÃO QUÂNTICA

Inovações em Computação, Comunicação e Informação Quântica na Academia e na Indústria



João Terêncio Dias  
(Organizador)

1ª Edição

Rio de Janeiro  
CEFET/RJ  
2024

Para citar este trabalho, utilizando as regras da ABNT (abaixo exemplos):

A obra integral:

DIAS, J. T. (Org.). **Anais do 7º Workshop-Escola de Computação e Informação Quântica: Inovações em Computação, Comunicação e Informação Quântica na Academia e na Indústria.** Rio de Janeiro: CEFET/RJ, Agosto de 2024.

Artigo ou resumo específico:

Gomes, O. C. V.; Leite, G. F.; Aguiar, A. F.; Nóbrega, K. Z. e Silva, J. B.. Propostas de Portas Reversíveis para Obtenção de Funções Lógicas e C-NOT para Qubits de Estados Coerentes. In: 7º Workshop-Escola de Computação e Informação Quântica, 2024, Rio de Janeiro. **Anais do 7º Workshop-Escola de Computação e Informação Quântica: Inovações em Computação, Comunicação e Informação Quântica na Academia e na Indústria.** Rio de Janeiro: CEFET/RJ. p. 16-19, 2024.

Informações editoriais:

Editora: CEFET/RJ

Lançamento da 1ª Edição: Setembro de 2024, Rio de Janeiro

ISBN: 978-65-01-14237-1

Formato: E-book

Ficha catalográfica elaborada pela Biblioteca Central do CEFET/RJ

S495 7º Workshop-Escola de Computação e Informação Quântica (7. : 2024 : Rio de Janeiro, RJ)  
Anais do VII Workshop-Escola de Computação e Informação Quântica: Inovações em Computação, Comunicação e Informação Quântica na Academia e na Indústria, 21, 22 e 23 de agosto de 2024 [recurso eletrônico] / organizado por João Terêncio Dias – 1.ed. – Rio de Janeiro : CEFET/RJ, 2024. 126 [127]p. : il. (algumas color.) , graf. , tabs.

Evento realizado nos dias 21, 22 e 23 de agosto de 2024.  
Inclui bibliografias

1. Computação quântica. 2. Computação. 3. Inovações tecnológica. I. Centro Federal de Educação Tecnológica Celso Suckow da Fonseca. II. Dias, João Terêncio (Org.). III. Título.

CDD 004.1

Elaborada pela bibliotecária Tania Mello – CRB/7 nº 5507/04

## APRESENTAÇÃO

O Workshop-Escola de Computação e Informação Quântica (WECIQ) é um evento nacional com a participação de palestrantes nacionais e internacionais que contempla as áreas temáticas de Aplicações da Computação Quântica na Indústria, Computação Quântica e Grafos, Comunicação e Informação Quânticas, Internet Quântica e Aprendizado Quântico de Máquinas.

O público alvo é formado por pesquisadores, professores, alunos de graduação e pós-graduação dos cursos de Computação, Engenharia Elétrica, Física, Matemática, entre outros, além de profissionais que atuam nestas áreas e demais interessados na compreensão da utilização da Mecânica Quântica na computação, comunicação e segurança computacional.

O evento tem como objetivos principais: 1 - Incrementar o desenvolvimento da informação quântica, computação quântica e comunicação quântica no Brasil; 2 - Ampliar o intercâmbio de informações e ideias entre professores, pesquisadores, estudantes e profissionais destas áreas; 3 - Promover a integração entre universidades, centros de pesquisas e empresas; 4 - Divulgar a produção técnico-científica nacional nessas áreas; 5 - Prover minicursos para a atualização de estudantes, docentes, pesquisadores, profissionais e público não especializado.

Para cumprir esses objetivos, a comissão organizadora procurou promover espaços de apresentação de trabalhos; plenárias com pesquisadores convidados de ampla experiência; mesas-redonda com profissionais da indústria especializada e minicursos específicos sobre a temática do evento, todos com tempo para discussão e debate.

Nesse monográfico constam a descrição das atividades realizadas durante o evento, a lista de professores e pesquisadores que se envolveram na organização, bem como os trabalhos completos e resumos expandidos provenientes das apresentações de trabalho nas sessões de comunicação oral. Esperamos que o material aqui disponível seja fonte de inspiração e pesquisa para comunidade de computação, comunicação e informação quântica.

A Comissão Organizadora

## AGRADECIMENTOS

Gostaríamos de expressar os nossos agradecimentos à Direção Geral e às Diretorias Sistêmicas do CEFET/RJ por aceitarem e abraçarem a realização deste evento na instituição. Nossos sinceros agradecimentos às instituições representadas pela comissão organizadora (LNCC, UFRJ, UFF, UERJ, UFMS e UFCA) por apoiar e liberar os professores para participar da organização do WECIQ. Agradecemos também aos órgãos de fomento (FAPERJ, CNPq), colaboradores (SBMAC, INCTMat, DEAC/Cefet-rj), patrocinadores ouro (IBM, Venturus e Keysight) e patrocinadores prata (Tektronix/RioLink e Rohde&Schwarz) que acreditaram e nos ajudaram no fomento das nossas demandas. Aproveitamos para agradecer aos palestrantes que abrilhantaram esse workshop-escola. Agradecer aos autores pelos excelentes trabalhos apresentados, e a todos(as) os(as) servidores(as) e alunos que se voluntariaram e se dedicaram na realização deste evento. E, por fim, e não menos especial, agradecemos a você, participante do 7º WECIQ, que presencialmente ou virtualmente esteve conosco nesses dias de grande troca de conhecimentos.

## COMISSÕES

### **Comitê organizador**

- Clarice Dias de Albuquerque, UFCA
- Dayse Haime Pastore, CEFET-RJ
- Demerson Nunes Gonçalves, CEFET-RJ
- Franklin de Lima Marquezino, UFRJ
- João Terêncio Dias, CEFET-RJ
- Leandro Bezerra de Lima, UFMS
- Luis Antonio Brasil Kowada, UFF
- Luís Felipe Ignácio Cunha, UFF
- Renato Portugal, LNCC
- Robert Mota Oliveira, UERJ

### **Comitê de Programa**

- Amir Ordacgi Caldeira, IF/UNICAMP
- Belita Koiller, IF/UFRJ
- Benjamin Callejas Bedregal, DIMAP/UFRN
- Carlile Lavor, IMECC/UNICAMP
- Celso Villas-Boas, UFSCar
- Francisco Marcos de Assis, IQUANTA/UFCG
- Franklin de Lima Marquezino, UFRJ
- Fernando Bandeira de Melo, CBPF
- Juliana Kaizer Vizzotto, UCPel/UFRGS
- Ivan dos Santos Oliveria Júnior, CBPF
- Luiz Davidovich, IF/UFRJ
- Marcelo Terra Cunha, IMECC/UNICAMP
- Marcos Cesar de Oliveira, UNICAMP
- Miguel Angel Martin-Delgado, Complutense de Madrid
- Nelson Maculan, COPPE/UFRJ
- Rafael Chaves, IIP-UFRN
- Raul José Donangelo, UDELAR
- Renata Hax Sander Reiser, UFPel
- Renato Portugal, LNCC
- Reginaldo Palazzo Junior, UNICAMP
- Rubens Viana, UFC
- Sueli Irene Rodrigues Costa, IMECC/UNICAMP

## PROGRAMAÇÃO

HORÁRIO	21/08 (QUARTA)	22/08 (QUINTA)	23/08 (SEXTA)	24/08 (SÁBADO)
8:00 – 8:30	Credenciamento			
8:30 – 9:00	Mesa de abertura Coord. Demerson			
9:00 – 10:00	Sessão Plenária 1 <u>Francesco Petruccione</u> Coord. Francisco de Assis	Sessão Plenária 3 <u>Miguel Angel Martin-Delgado</u> Coord. Renato	Sessão Plenária 6 <u>Eduardo Inácio Duzzioni</u> Coord. Marcos Oliveira	Passeio (por adesão)
10:00 – 10:30	1ª Sessão de Pôsteres e Coffee break	3ª Sessão de Pôsteres e Coffee break	5ª Sessão de Pôsteres e Coffee break	
10:30 – 12:00	Minicurso 1* / sessão oral 1 Coord. Luis Felipe	Minicurso 2* / sessão oral 3 Coord. Dayse	Minicurso 3* / sessão oral 5 Coord. Luis Kowada	
12:00 – 14:00	Almoço	Almoço	Almoço	
14:00 – 15:00	Sessão Plenária 2	Sessão Plenária 4 <u>Marcos Cesar de Oliveira</u> Coord. Demerson	Sessão Plenária 7 <u>Salvador E. Venegas-Andraca</u> Coord. Clarice	Retorno do passeio
15:00 – 16:00	Mesa Redonda: Tecnologias quânticas na indústria  Coord. Leandro	Sessão Plenária 5 Soluções Quânticas das empresas Coord. João Dias	Sessão Plenária 8 <u>Renato Portugal</u> Coord. Leandro	
16:00 – 16:30	2ª Sessão de Pôsteres e Coffee break	4ª Sessão de Pôsteres e Coffee break	6ª Sessão de Pôsteres e Coffee break	
16:30 – 18:00	Minicurso 1* / sessão oral 2 Coord. Giuliano	Minicurso 2* / sessão oral 4 Coord. Tharso	Minicurso 3* / sessão oral 6 Coord. Robert	
18:00 – 21:00	Coquetel de boas-vindas		Encerramento 18:00 – 18:30	

**Obs1:** Os minicursos e sessões orais foram atividades paralelas, os minicursos ocorreram no auditório 5 e as sessões orais no auditório 1.

**Obs2:** Os coffee breaks e as sessões de pôsteres foram simultâneos, no mesmo espaço físico (hall onde ficaram os estandes, mesas de coffee breaks e pôsteres).

**Minicurso 1\*** - INTERNET QUÂNTICA: FUNDAMENTOS, ESTADO-DA-ARTE E PERSPECTIVAS - Guilherme Penello Temporão

**Minicurso 2\*** - CÓDIGOS QUÂNTICOS: DO CÓDIGO DE SHOR AOS CÓDIGOS TOPOLÓGICOS - Clarice Dias de Albuquerque; Giuliano G. La Guardia e Leandro Bezerra de Lima

**Minicurso 3\*** - APRENDIZADO QUÂNTICO DE MÁQUINAS: FUNDAMENTOS, ESTADO-DA-ARTE E PERSPECTIVAS - Adenilton José da Silva

## PLENÁRIAS

### **Quantum Horizons: The challenges of machine learning**

A palestra iniciou analisando a evolução da computação, sua aplicação em inteligência artificial, o consumo de energia e o mercado mundial de tecnologia. Em seguida, foi apresentada uma introdução a computação quântica, analisando o estado-da-arte e o aprendizado quântico de máquinas. Foi analisado os algoritmos quânticos, suas aplicações e complexidades. Por fim, foram detalhados e comparados os algoritmos de aprendizado de máquina clássicos e quânticos.

A íntegra desta plenária pode ser assistida em:

<https://www.youtube.com/watch?v=BiWzb0Hqda8&t=1s>



**Francesco Petruccione** é professor catedrático de Física Teórica na Universidade de KwaZulu-Natal (África do Sul), com pesquisas em Processamento e Comunicação de Informação Quântica. É diretor do Instituto Nacional de Ciências Teóricas e Computacionais (NITheCS) e Professor de Computação Quântica na Escola de Ciência de Dados e Pensamento Computacional da Universidade de Stellenbosch. É membro eleito da Academia de Ciências da África do Sul (ASSAf), membro da Royal Society of South Africa e da Academia Africana de Ciências. Possui mais de 400 artigos científicos publicados e é referência mundial em *Quantum Machine Learning* (QML).

### **An Introduction to Topological Quantum Computation**

A topologia é um dos ramos mais recentes da matemática e entrou plenamente nos aspectos mais modernos da física teórica: a computação quântica. Nesta plenária, é apresentada uma abordagem elementar ao papel da topologia na física quântica e suas implicações para estados exóticos da matéria quântica. A topologia ajuda a resolver o problema essencial da computação quântica: combater a sua fragilidade para beneficiar das suas enormes possibilidades potenciais. Após a apresentação dos códigos de cores topológicos e sua realização experimental, foram abordados desafios futuros.

A íntegra desta plenária pode ser assistida em:

[https://www.youtube.com/watch?v=RG9D\\_AtdQK4](https://www.youtube.com/watch?v=RG9D_AtdQK4)



**Miguel Angel Martin-Delgado** é professor catedrático de Física Teórica da Universidade Complutense de Madrid. Dirigiu e participou em mais de 20 projetos de pesquisa na área de informação quântica e é co-autor de centenas de publicações com milhares de citações na área de física quântica. É membro correspondente da Real Academia de Ciências da Espanha. Coordenador geral do consórcio de investigação QUITEMAD (*Quantum Information Technologies Madrid*) e editor científico da revista *Scientific Reports* (área de Física Quântica) do *Nature Publishing Group*.

## **Simulating spin biology using a digital quantum computer: Prospects on a near-term quantum hardware emulator**

Entender a intrincada dinâmica quântica de spin de reações de pares radicais é crucial para desvendar a natureza subjacente de processos químicos em diversos domínios científicos. Nesta palestra, É mostrado que a Trotterização pode ser usada para mapear a dinâmica coerente de spin de pares radicais em uma simulação quântica baseada em porta digital e que os resultados apresentam concordância entre a simulação de circuito quântico sem ruído idealizado e abordagens de equação mestre estabelecidas para recombinação homogênea de pares radicais, identificando aproximadamente 15 etapas de Trotter como suficientes para reproduzir fielmente a dinâmica de spin acoplada de um sistema prototípico. Ao utilizar esta técnica computacional para estudar a dinâmica de sistemas de spin de relevância biológica, as descobertas ressaltaram o potencial da simulação quântica digital (DQS) de reações complexas de pares radicais e construíram a base para investigações mais utilitárias em suas intrincadas dinâmicas de reação. Foi investigado ainda mais o efeito de modelos de erro realistas na abordagem DQS e fornecido um limite superior para o número de etapas de Trotter que podem ser aplicadas atualmente na ausência de técnicas de mitigação de erros antes de perder a precisão da simulação para efeitos de ruído deletérios.

A integra desta plenária pode ser assistida em:

<https://www.youtube.com/watch?v=bxO3By4oLi0&t=12807s>



**Marcos Cesar de Oliveira** é professor titular no Instituto de Física Gleb Wataghin da Universidade Estadual de Campinas e foi professor visitante do Institute for *Quantum Information Science*, na universidade de Calgary entre 2011-2012. Tem experiência na área de Física, com ênfase em Óptica Quântica, e Informação Quântica, atuando principalmente nos seguintes temas: emaranhamento de estados em variáveis contínuas, colisões controladas de átomos em condensados aprisionados em redes ópticas, aspectos fundamentais da teoria de informação quântica, e investigação de potenciais sistemas físicos para implementação de computação quântica.

## **Ket Quantum Programming Platform: Measurements and Algorithms**

A palestra iniciou com a descrição da plataforma de programação quântica *Ket*. Em seguida, foi apresentado um processo de otimização para decomposição de portas para programação quântica de alto nível. Foi definida as “sombras” clássicas e descrito o processo de quantificação genuína de emaranhamentos multipartite com sombras clássicas. Foi mostrado como melhorar o algoritmo FALQON com sombras clássicas. Por fim, foi detalhado o algoritmo de aprendizado de máquina quântico para regressão com bases Walsh.

A integra desta plenária pode ser assistida em:

<https://www.youtube.com/watch?v=Xt9IHvLYtQo&t=174s>





**Eduardo Inácio Duzzioni** é professor no Departamento de Física da Universidade Federal de Santa Catarina. Tem experiência na área de Física, com ênfase em Física Quântica; atuando principalmente nos seguintes temas: Medidas de correlação quânticas; Computação quântica contínua no tempo; Controle quântico; Algoritmos quânticos; Descrição quântica da interação entre radiação e matéria; Sistemas quânticos abertos. É co-fundador da startup QuanBy Computação Quântica.

### Quantum Thoughts from Mexico

A palestra iniciou com a descrição do ecossistema hardware e software quânticos. Em seguida, foi apresentado o cenário atual do mercado em computação quântica. Foi discutido os fundamentos de “caminhadas quânticas” e mostrado como aplicar caminhadas quânticas em redes de genótipos. Foi detalhada a conversão da caminhada quântica em circuitos quânticos e apontado um horizonte para a pesquisa em caminhadas quânticas. Por fim, foi discutido o problema de cibersegurança e a possível solução com algoritmos quânticos.

A íntegra desta plenária pode ser assistida em:

<https://www.youtube.com/watch?v=KP4qZvYs9Mo&t=3437s>



**Salvador E. Venegas-Andraca** é pesquisador chefe do Laboratório de Computação e Professor de Ciência da Computação no *Tecnológico de Monterrey*. É editor da *Quantum Information Processing*, membro da *Quantum Economy Network* do Fórum Econômico Mundial e palestrante da *Association for Computing Machinery*. Seu trabalho visa compreender os aspectos científicos e sociais da computação, bem como contribuir para o desenvolvimento da sociedade baseado na ciência e na tecnologia. Realiza pesquisas sobre algoritmos quânticos e segurança cibernética quântica. É co-fundador da área de Processamento de Imagens Quânticas e fundador da área de Computação Quântica no México.

### Quantum algorithms

A palestra iniciou com revisão dos principais algoritmos quânticos básicos. Em seguida, foi apresentado o algoritmo de distinção de elementos. Foi discutido os fundamentos do algoritmo HHL (*Harrow-Hassidim-Lloyd*) e mostrado como funcionam os algoritmos quânticos variacionais. Foi detalhado o processo de caminhada quântica, seus postulados e aplicações. Por fim, foi mostrado uma plataforma de simulação de caminhadas quânticas.

A íntegra desta plenária pode ser assistida em:

<https://www.youtube.com/watch?v=KP4qZvYs9Mo&t=3711s>



**Renato Portugal** é Pesquisador Titular do Laboratório Nacional de Computação Científica (LNCC). Suas áreas de investigação são: Computação Quântica, Algoritmos Quânticos, Caminhadas Quânticas e Criptografia. Autor de diversos livros e artigos sobre o tema, com destaque para os livros: *Códigos Quânticos Corretores de Erros*, SBMAC, 2010 e *Quantum Walks and Search Algorithms* - 2ª edição (2018). É membro do comitê temático em computação e informação quântica da Sociedade Brasileira de Matemática Aplicada a Computação (SBMAC).

## MESA REDONDA – TECNOLOGIAS QUÂNTICAS NA INDÚSTRIA

A mesa iniciou com a apresentação do Senai/Cimatec (João Marcelo) e foram feitas algumas provocações para o debate com as empresas. Em seguida, houve a apresentação da IBM (Alexandre Pfeifer), onde foram apresentados alguns problemas da computação quântica e como a IBM está trabalhando para resolvê-los. Na sequência, a Venturus (Daniel Haro) apresentou sua carteira de soluções, pesquisa e desenvolvimento, e sua visão do mercado das tecnologias quânticas. Dando continuidade, a Keysight (Rodrigo Vicentini) apresentou sua atuação na produção de equipamentos de medição para tecnologias quânticas. Por fim, foi aberto para perguntas da plateia e se iniciou o debate. A íntegra desta mesa pode ser assistida em:

<https://www.youtube.com/watch?v=fk8k64u12G4>



**João Marcelo** é pesquisador líder e coordenador do Centro de Computação Quântica e Supercomputação do SENAI CIMATEC (*Latin America Quantum Computing Center - CIMATEC LAQCC*). Trabalha no desenvolvimento de soluções de inovação e projetos da indústria que necessitam de grande poder de processamento, simulações e cálculos, com atuação em petróleo, energia, metalomecânica e saúde.



**Alexandre Pfeifer** é responsável pela unidade de negócios de Computação Quântica para a América Latina na IBM. É responsável pela comercialização e estabelecimento de acordos de colaboração relacionados a esta tecnologia. Foi responsável por gerenciar os negócios de colaboração de pesquisa e licenciamento de tecnologia da IBM *Research* no Brasil, América Latina e com clientes estratégicos globais.



**Daniel de Haro Moraes** Atualmente é head de segurança da Venturus - Centro de Inovação Tecnológica e sócio e gerente da Botunix Ltda ME. Tem experiência na área de Engenharia Elétrica, com ênfase em Telecomunicações, atuando principalmente nos seguintes temas: internet, sistemas distribuídos e segurança da informação.



**Rodrigo Vicentino** é Gerente de Engenharia de Aplicação e Consultor na Keysight Technologies, responsável pelas áreas de Pré-Vendas, Suporte, Treinamento e Entrega de Projetos abrangendo RF, Micro-ondas, Comunicações Ópticas, Veículos Elétricos e Autônomos, Tecnologias Digitais de Alta Velocidade, Defesa Aeroespacial e Computação Quântica na região da América Latina. Com mais de 20 anos de experiência na indústria de alta tecnologia, tenho trabalhado em ambientes multinacionais e culturais.

## MINICURSOS

### INTERNET QUÂNTICA: FUNDAMENTOS, ESTADO-DA-ARTE E PERSPECTIVAS

Este minicurso foi iniciado com os fundamentos da comunicação quântica e seus postulados. Em seguida, foi mostrado o estado-da-arte das redes quânticas e os experimentos de internet quântica no Brasil e no mundo. Por fim, foi apresentado o caminho de pesquisa a ser seguido, os desafios e as expectativas com esta nova tecnologia.

Parte deste minicurso pode ser assistido em:

[https://www.youtube.com/watch?v=0S-pRb9\\_ZAM](https://www.youtube.com/watch?v=0S-pRb9_ZAM)



**Guilherme Penello Temporão** é Professor e Diretor do Centro de Estudos em Telecomunicações (CETUC) da PUC-Rio, atua como pesquisador na área de comunicações quânticas via fibras ópticas. Suas áreas de interesse incluem metrologia quântica, computação quântica, instrumentação optoeletrônica e educação em engenharia. Autor de dezenas de artigos científicos sobre o tema, participa do projeto “Rede Rio Quântica”.

### CÓDIGOS QUÂNTICOS: DO CÓDIGO DE SHOR AOS CÓDIGOS TOPOLÓGICOS

Foi apresentado a base construída pelos códigos anteriores ao topológico, como o código de Shor, os códigos CSS e os códigos estabilizadores, bem como, aspectos básicos da teoria de codificação quântica. Em seguida foram estudados os códigos teóricos de Kitaev e algumas construções de códigos em superfícies compactas orientáveis com gênero  $g$  maior ou igual a 1. Em busca da computação quântica tolerante a falhas, esse curso introduziu os códigos quânticos topológicos.

A integra deste minicurso pode ser assistido em:

Parte 1: [https://www.youtube.com/watch?v=m\\_2V7ox6u9g](https://www.youtube.com/watch?v=m_2V7ox6u9g)

Parte 2: <https://www.youtube.com/watch?v=lZ9RxM1VgkE>



**Clarice Dias de Albuquerque** é professora da Universidade Federal do Cariri - UFCA. Tem experiência na área de Matemática e Engenharia Elétrica, com ênfase em Topologia e Geometria e Teoria de Informação e Codificação, atuando principalmente nos seguintes temas: Códigos Corretores de Erros Clássicos e Quânticos, Códigos Quânticos Topológicos, Computação Quântica Topológica. Participa do projeto de pesquisa “Códigos Quânticos Euclidianos e Hiperbólicos” financiado pela FAPEMIG (2021 - 2024), faz parte dos Comitês Temáticos da SBMAC de Computação Quântica e Códigos Quânticos, de Matemática Discreta: Códigos e Reticulados, e de Mulheres na Matemática Aplicada e Computacional.



**Giuliano Gadioli La Guardia** é professor adjunto da Universidade Estadual de Ponta Grossa - UEPG. Tem experiência na área de Matemática e Engenharia Elétrica, com ênfase em Teoria de Informação e Codificação, atuando principalmente nos seguintes temas: Códigos Corretores de Erros Clássicos e Quânticos, Teoria de Matróides e Teoria de Categorias. Participa do projeto de pesquisa “Códigos Quânticos Euclidianos e Hiperbólicos” financiado pela FAPEMIG (2021 - 2024), faz parte dos Comitês Temáticos da SBMAC de “Computação Quântica e Códigos Quânticos” e “Matemática Discreta: Códigos e Reticulados”. É Bolsista de Produtividade CNPq nível 2.



**Leandro Bezerra de Lima** é professor associado do Instituto de Matemática da Universidade Federal do Mato Grosso do Sul - UFMS. Tem experiência na área de Matemática e Engenharia Elétrica, com ênfase em Teoria de Informação e Codificação, atuando principalmente nos seguintes temas: Códigos Corretores de Erros Clássicos e Quânticos, Códigos Quânticos de Subespaços, Geometria de Galois. Participa do projeto de pesquisa “Códigos Quânticos Euclidianos e Hiperbólicos” financiado pela FAPEMIG (2021 - 2024), faz parte dos Comitês Temáticos da SBMAC de “Computação Quântica e Códigos Quânticos” e “Matemática Discreta: Códigos e Reticulados”. Faz parte da Comissão Especial de Comunicação da SBMAC e atualmente é 2º Vice Presidente da SBMAC.

## **APRENDIZADO QUÂNTICO DE MÁQUINAS: FUNDAMENTOS, ESTADO-DA-ARTE E PERSPECTIVAS**

Este minicurso foi iniciado com os fundamentos do aprendizado de máquinas e suas aplicações. Em seguida, foi mostrado o estado-da-arte dos algoritmos quânticos para aprendizado de máquinas, as dificuldades e as vantagens. Por fim, foi apresentado o caminho de pesquisa a ser seguido, os desafios e as expectativas com esta nova tecnologia.



**Adenilton José da Silva** é Professor da Universidade Federal de Pernambuco, Revisor de periódicos da “Engineering Applications of Artificial Intelligence”, “PLoS One”, “Mechanical Systems and Signal Processing” e “Neurocomputing”. Tem experiência na área de Ciência da Computação, com ênfase em Inteligência Artificial. Atuando principalmente nos seguintes temas: Computação Quântica, Redes Neurais Quânticas e Aprendizado quântico de máquinas.

## SUMÁRIO

### TRABALHOS COMPLETOS

Obs: os trabalhos contidos neste documento são os que atenderam os requisitos de publicação, permissão dos autores e recebimento da versão final revisada (*camera ready*). Todos artigos apresentados estão com o link para a gravação da apresentação no canal do evento no YouTube.

#### **Performance limits for the Quantum Alternating Operator Ansatz with Grover Mixer**

Guilherme Adamatti Bridi, Franklin de Lima Marquezino

<https://www.youtube.com/watch?v=KVYIHfXvafg>

#### **Propostas de Portas Reversíveis para Obtenção de Funções Lógicas e C-NOT para Qubits de Estados Coerentes** \_\_\_\_\_ **16**

Orleans Cardoso Viana Gomes, Gabriel Fonseca Leite, Antônio Francisco Aguiar, Kleber Zuza Nóbrega, João Batista Rosa Silva

<https://www.youtube.com/watch?v=KVYIHfXvafg>

#### **Uma Proposta de QPU Fotônica para Qubits de Estados Coerentes** \_\_\_\_\_ **20**

Antônio Francisco Aguiar, Orleans Cardoso Viana Gomes, Gabriel Fonseca Leite, João Batista Rosa Silva

<https://www.youtube.com/watch?v=KVYIHfXvafg>

#### **Quantum-Fuzzy Interpretations of Xor-Connectives using Overlapping and Grouping Aggregations** \_\_\_\_\_ **24**

Juliano Strelow Buss, Bruna Camilly Domingues Novack, Emerson Vieira, Cecilia Silva da Costa Botelho, Helida Salles Santos, Giancarlo Lucca, Anderson Avila, Adenauer Yamin, Anderson Cruz, Renata Hax Sander Reiser

<https://www.youtube.com/watch?v=KVYIHfXvafg>

#### **QT3GG Approach: Simulating a Quantum Game in a Game Engine Based on Graph Grammar** \_\_\_\_\_ **29**

Júlia Veiga da Silva, Júlia da Rocha Junqueira, Ricardo Coutinho Cordeiro, Renata Hax Sander Reiser, Adenauer Yamin, Bruno M. P. de Moura, Giancarlo Lucca, SIMONE ANDRE DA COSTA CAVALHEIRO, Ulisses B. Corrêa

<https://www.youtube.com/watch?v=KVYIHfXvafg>

#### **Enumeration of Circuits with $n$ Quantum Gates** \_\_\_\_\_ **33**

Andresso da Silva, Francisco Marcos de Assis

<https://www.youtube.com/watch?v=9sPGxw7RbaY&t=2897s>

#### **Using simulations to validate improvements over Shor's Algorithm** \_\_\_\_\_ **38**

Fábio Gomes dos Santos, Luis Antonio Brasil Kowada

<https://www.youtube.com/watch?v=9sPGxw7RbaY&t=2897s>

#### **Implementação de Passeios quânticos a tempo contínuo nos Computadores Quânticos da IBM** \_\_\_\_\_ **43**

Frank Henry Acasiete Quispe, Renato Portugal

<https://www.youtube.com/watch?v=9sPGxw7RbaY&t=2897s>

#### **Jogos Quânticos: Uma Análise dos Simuladores Quânticos em Jogos Interativos** \_\_\_\_\_ **47**

Gabriel Rosa de Oliveira Silva, Bruno Alexandre, Adenauer Yamin, Bruno M. P. de Moura, Renata Hax Sander Reiser, Giancarlo Lucca

<https://www.youtube.com/watch?v=9sPGxw7RbaY&t=2897s>

#### **Quantum Computing Insights into Direct Air Capture Materials**

Marco Antonio Barroca, Rodrigo Neumann, Mathias B. Steiner

<https://www.youtube.com/watch?v=9sPGxw7RbaY&t=2897s>

#### **A Fully Quantum Particle Swarm Optimization Algorithm Applied in the Realm of Robotics**

David Oliveira Santos, Francisco Marcos de Assis, Elyson Ádan Nunes Carvalho, Lucas Molina

<https://www.youtube.com/watch?v=7AnWunBiFqc&t=1880s>

<b>Simulação de Circuitos Quânticos Ópticos</b>	<b>52</b>
Vitor Ferreira Guedes, Fábio Alencar Mendonça, Rubens Viana <a href="https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s">https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s</a>	
<b>Efficient Computation of the Wave Function <math>\psi_n(x)</math> using Hermite Coefficient Matrix in Python</b>	<b>56</b>
Matheus Gomes Cordeiro, Italo Bezerra, Hilma Vasconcelos <a href="https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s">https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s</a>	
<b>HHL: Estado da Arte, Limitações e Melhorias</b>	<b>61</b>
Lucas Amaral Dos Santos Barroso Leite, Luis Antonio Brasil Kowada <a href="https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s">https://www.youtube.com/watch?v=7AnWunBiFqc&amp;t=1880s</a>	
<b>Quantum Computing VHDL Library for Hardware Synthesis</b>	<b>66</b>
Giancarlo Lucca, Igor Basilio Valerao, Luis Henrique de Freitas Brum, Renata Hax Sander Reiser, Adenauer Yamin, Edmilson Marques Batista <a href="https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s">https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s</a>	
<b>Quantum Support Vector Regression for Predicting Zeros of the Riemann Zeta Function</b>	<b>71</b>
Tharso D. Fernandes, Demerson Nunes Gonçalves, João Terêncio Dias <a href="https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s">https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s</a>	
<b>A new Euclidean framework for Quantum-Enhanced Neural Networks.</b>	<b>76</b>
Javier Roperro, Clovis Aparecido Caface Filho, Ricardo Tiosso Panassiol, Karla Vittori <a href="https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s">https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s</a>	
<b>Automation of the Quantum Algorithm HHL for implementing two-dimensional SVMs</b>	
Gabriela Pinheiro, Luis Antonio Brasil Kowada <a href="https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s">https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s</a>	
<b>Simulação do Impacto do Espalhamento Raman Espontâneo na Taxa de Transmissão em Sistemas de QKD em Redes Ópticas Passivas</b>	<b>81</b>
Joacir Soares de Andrade, Rubens Viana <a href="https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s">https://www.youtube.com/watch?v=bxO3By4oLi0&amp;t=202s</a>	
<b>Análise do Desempenho de Geradores Quânticos de Números Aleatórios usando a Disentropia</b>	<b>86</b>
Sergio Tahim, Glaucionor Lima de Oliveira, Rubens Viana <a href="https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s">https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s</a>	
<b>CVQKD Reconciliation with Slepian-Wolf LDPC Coding and Bit-Flipping Decoding</b>	<b>91</b>
Rávilla Raianni Silva Leite, Francisco Marcos de Assis <a href="https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s">https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s</a>	
<b>Exploring Non-Gaussianity Reduction in Quantum Channels</b>	<b>96</b>
Micael Andrade Dias, Francisco Marcos de Assis <a href="https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s">https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s</a>	
<b>Enhanced Channel Estimation and Data Detection in OFDM Systems without Cyclic Prefix using Quantum Machine Learning Algorithms</b>	<b>101</b>
João Terêncio Dias, Demerson Nunes Gonçalves <a href="https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s">https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s</a>	
<b>Recorrência de Cadeias de Markov Quânticas</b>	<b>107</b>
Newton Loebens <a href="https://www.youtube.com/watch?v=wOn8fouiWRs&amp;t=1826s">https://www.youtube.com/watch?v=wOn8fouiWRs&amp;t=1826s</a>	
<b>Exponential Decay for Continuous-time Open Quantum Walks</b>	<b>112</b>
Newton Loebens <a href="https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s">https://www.youtube.com/watch?v=AK2rMRM8yXc&amp;t=1506s</a>	

**A Transience Condition for Homogeneous Open Quantum Walks on the Line**

Thomas Soler Jacq

<https://www.youtube.com/watch?v=wOn8fouiWRs&t=1826s>

**Exploring the Post-Quantum NTRU Cryptography Algorithm**

Vitor Dos Santos Ponciano, Vilc Quepe Rufino, Augusto Parisot de Gusmão Neto

<https://www.youtube.com/watch?v=wOn8fouiWRs&t=1826s>

**Ensinando o Protocolo BB84 com Simulações Interativas**

Gisele B Freitas, Clovis Aparecido Caface Filho

<https://www.youtube.com/watch?v=wOn8fouiWRs&t=1826s>

**Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels** \_\_\_\_\_ **117**

Marciel Medeiros de Oliveira, Andressa da Silva, Micael Andrade Dias, Francisco M de Assis

<https://www.youtube.com/watch?v=wOn8fouiWRs&t=1826s>

**RESUMOS**

**Aplicação de Pulsos Compostos nos Computadores Quânticos da IBM**

Pedro Faria Albuquerque

**Feature Map Selection for Quantum Classifiers using Pauli Decomposition** \_\_\_\_\_ **121**

Demerson Nunes Gonçalves, Andrias Magno Miranda Cordeiro, Caio Neves Silva, Tharso D. Fernandes, João Terêncio Dias

**Integração de Redes Neurais Quânticas e aprendizado não supervisionado: A rede KLN quântica**

Clovis Aparecido Caface Filho, KARLA VITTORI, Javier Roperio

**Majorization-based benchmark of the complexity of quantum processors**

Nina Machado ONeill, Alexandre Baron Tacla, Gabriel G. Carlo, Raúl Oscar Vallejos, Fernando Bandeira de Melo

**Pilotless Channel Estimation Scheme in OFDM Systems using K-Means and Quantum K-Means** \_\_\_\_\_ **123**

Caio Neves Silva, Andrias Magno Miranda Cordeiro, Tharso D. Fernandes, DEMERSON NUNES GONÇALVES, João Terêncio Dias

**Simulação de algoritmos quânticos usando GPU** \_\_\_\_\_ **125**

Raian Pierre Cardoso Machado, Luis Antonio Brasil Kowada

**Solução de Sistemas de Equações Diferenciais em Simuladores Quânticos**

Paulo Cesar Souza Pavoletti, Daniel Yoshio Akamatsu, Celso Villas-Boas

**The Cost of Weak Simulating Quantum Circuits via Generative Adversarial Networks**

João Pedro d'El-Rey, Alexandre Baron Tacla, Raúl O. Vallejos, Fernando Bandeira de Melo

**Towards a Security Analysis for the Rio Quantum Network**

Mario Curvo, Raúl Oscar Vallejos, Fernando de Melo

# Propostas de Portas Reversíveis para Obtenção de Funções Lógicas e $C$ -NOT para Qubits de Estados Coerentes

Orleans C. V. Gomes<sup>1</sup>, Gabriel F. Leite<sup>2</sup>, Antônio F. Aguiar<sup>3</sup>, Kleber Z. Nóbrega<sup>4</sup> e João Batista R. Silva<sup>5</sup>

**Resumo**—Este trabalho propõe duas portas reversíveis inéditas de três qubits e um sistema óptico para implementá-las probabilisticamente. Usando dispositivos baseados em óptica linear, o sistema proposto para qubits de estados coerentes é capaz de implementar funções lógicas (AND, OR, NAND e/ou NOR) para dois qubits, simultaneamente, e as portas  $C$ -NOT e  $\bar{C}$ -NOT com uma eficiência de até 1/8.

**Palavras-Chave**—Portas reversíveis, óptica linear, estados coerentes,  $C$ -NOT, funções lógicas.

**Abstract**—This work proposes two gates reversible three-qubit gates and an optical system to probabilistically implement them. Using linear optics-based devices, the proposed system for coherent state qubits is able to implementing logical functions (AND, OR, NAND, and/or NOR) for two qubits simultaneously, as well as the  $C$ -NOT and  $\bar{C}$ -NOT gates, with an efficiency of up to 1/8.

**Keywords**—Reversible gates, linear optics, coherent states,  $C$ -NOT, logical functions.

## I. INTRODUÇÃO

A computação quântica é uma abordagem inovadora para processamento de informações, baseada na mecânica quântica [1]-[2]. Enquanto a computação clássica armazena informações em bits, que podem estar em um estado de 0 ou 1, a computação quântica utiliza qubits, que podem estar em uma superposição de ambos os estados simultaneamente, permitindo realizar cálculos muito mais rapidamente do que seria possível com computadores clássicos.

Apesar dos desafios para implementar portas quânticas que são essenciais para processamento quântico de informação, atualmente, existem várias tecnologias sendo utilizadas para realização de computação quântica, incluindo pontos quânticos [3]-[5], supercondutores [6]-[8], ressonância magnética nuclear (RMN) [9]-[11], íons aprisionados [12]-[14], spins eletrônicos em diamantes, entre outros. No entanto, uma das tecnologias mais promissoras é a computação quântica baseada em óptica linear e dispositivos fotônicos [15]-[25].

Este trabalho propõe um estudo teórico de duas portas reversíveis inéditas de três qubits e um sistema óptico para implementá-las probabilisticamente. O sistema, baseado em dispositivos ópticos lineares para qubits de estados coerentes, oferece flexibilidade para obtenção: de funções lógicas (AND, OR, NAND e/ou NOR) para dois qubits, simultaneamente; e das portas  $C$ -NOT e  $\bar{C}$ -NOT.

DETI<sup>1,3,4,5</sup> e DEE<sup>2</sup>, Universidade Federal do Ceará<sup>1-5</sup>, Fortaleza-CE; e-mail: orleancardoso@outlook.com<sup>1</sup>, fonsecag.leite1810@gmail.com<sup>2</sup>, antonioaguiar.etiufc@alu.ufc.br<sup>3</sup>, kznobrega@ufc.br<sup>4</sup> e joaobrs@ufc.br<sup>5</sup>.

## II. AS PORTAS REVERSÍVEIS PROPOSTAS

No presente trabalho, são propostas duas portas reversíveis para três qubits, conforme ilustrado na Figura 1. As entradas lógicas para o sistema são representadas por  $A$ ,  $B$  e  $C$ , enquanto as saídas correspondentes, determinadas pelas entradas, são indicadas por  $S_1$ ,  $S_2$  e  $S_3$ .

A porta  $C_1$ , Figura 1a, difere da porta  $C_2$ , Figura 1b, apenas na saída  $S_3$ . E as matrizes das mesmas são apresentadas, respectivamente, em (1) e (2).

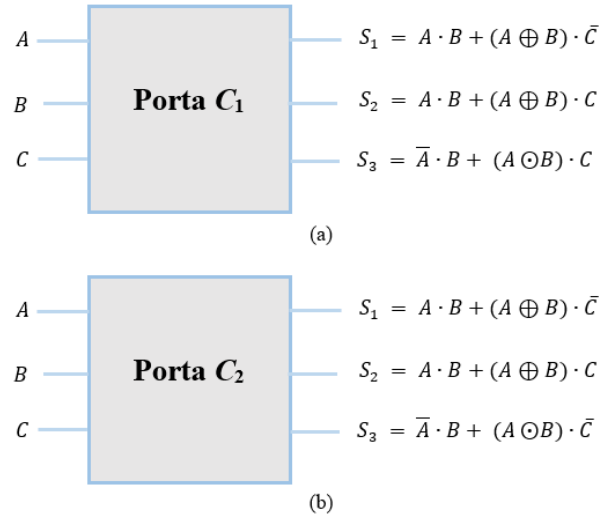


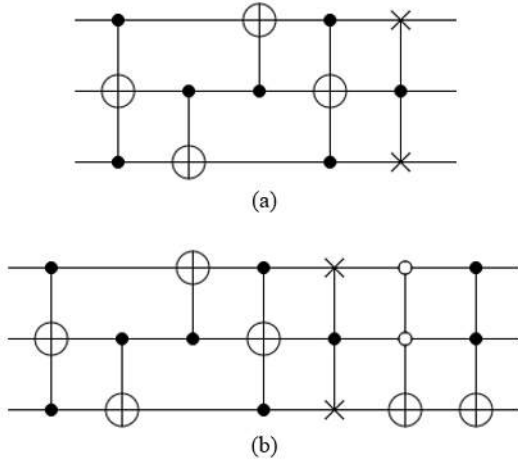
Fig. 1: Portas reversíveis propostas: (a) porta  $C_1$  e (b) porta  $C_2$ .

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (1)$$

$$C_2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (2)$$



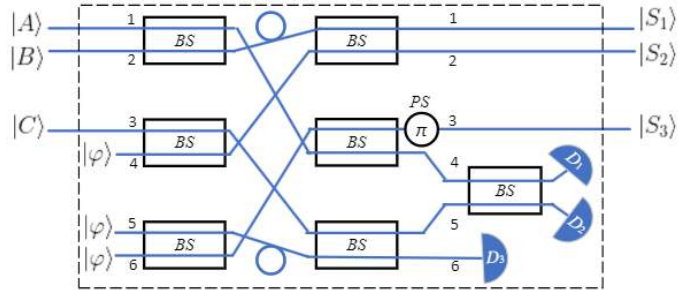
A Figura 2 apresenta os circuitos quânticos não-otimizados para implementar as portas  $C_1$  e  $C_2$ . A construção desses circuitos usa-se apenas portas  $C$ -NOT, Toffoli e Fredkin.



**Fig. 2:** Circuitos equivalentes usando apenas portas  $C$ -NOT, Toffoli e Fredkin: (a) porta  $C_1$  e (b) porta  $C_2$ .

### III. SISTEMA ÓPTICO PROPOSTO

A Figura 3 apresenta um sistema óptico inédito que é capaz de implementar as portas reversíveis  $C_1$  e  $C_2$ , probabilisticamente, usando óptica linear. O sistema óptico proposto opera através da manipulação de feixes de luz para implementar as operações lógicas mostradas na Figura 1.



**Fig. 3:** Sistema óptico que implementa as portas  $C_1$  e  $C_2$  usando apenas dispositivos ópticos lineares.

Essa manipulação é realizada por meio de componentes ópticos como divisores de feixes balanceados (BS) que direcionam e geram interferência entre feixes de luz de acordo com os princípios da óptica e modificam a fase dos mesmos por meio de um deslocador de fase (PS) de acordo com os princípios da óptica. Por fim, medições são realizadas com fotodetectores ( $D$ 's) para determinar se as operações lógicas desejadas foram obtidas.

O sistema óptico na Figura 3 utiliza-se de três estados auxiliares  $|\varphi\rangle$  além das três entradas ( $|A\rangle$ ,  $|B\rangle$  e  $|C\rangle$ ). Tais estados, tanto os de entrada quanto os auxiliares, são construídos a partir de estados coerentes da luz.

Os estados coerentes são auto-estados do operador de aniquilação  $\hat{a}$  (criação,  $\hat{a}^\dagger$ ), com autovalor complexo  $\alpha$  ( $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ ), e foram introduzidos por R. J. Glauber em 1963 [25]. Estes estados podem ser escritos na base dos estados de Fock (estados de número de fótons) como:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (3)$$

Na área da informação quântica, a ortogonalidade entre os estados que representam os qubits lógicos é fundamental. Essa propriedade garante a distinção precisa das informações armazenadas nos qubits, assegurando a confiabilidade e a precisão dos sistemas quânticos. Portanto, para estados coerentes  $|\alpha\rangle$  e  $|\beta\rangle$ , o produto interno é dado por:

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \quad (4)$$

Assim, os qubits lógicos podem ser codificados usando  $|0\rangle = |-\alpha\rangle$  e  $|1\rangle = |\alpha\rangle$ , sendo  $\alpha$  um número real e a distinguibilidade entre os mesmos é garantida para uma  $|\alpha|^2 \geq 4$  [20].

Portanto, dois estados coerentes  $|\alpha\rangle$  e  $|\beta\rangle$  passam pelo BS conforme mostrado na Figura 3 seu estado na saída será [20]:

$$|\alpha, \beta\rangle \xrightarrow{BS} \left| \frac{\alpha - \beta}{\sqrt{2}}, \frac{\alpha + \beta}{\sqrt{2}} \right\rangle. \quad (5)$$

Já o  $PS(\theta)$  adiciona uma fase  $\theta$  ao sinal óptico que o atravessa [20]. Ou seja:

$$|\alpha\rangle \xrightarrow{PS(\theta)} |e^{j\theta}\alpha\rangle. \quad (6)$$

Logo, o  $PS$  com  $\theta = \pi$  funcionará como a porta NOT ( $X$ ) para qubits de estados coerentes.

Então, conforme mostrado na Figura 3, os estados de entrada são dado por  $|A\rangle = N_A(a_0|-\alpha\rangle + a_1|\alpha\rangle)$ ,  $|B\rangle = N_B(b_0|-\alpha\rangle + b_1|\alpha\rangle)$ ,  $|C\rangle = N_C(c_0|-\alpha\rangle + c_1|\alpha\rangle)$ , e  $|\varphi\rangle = N(|-\alpha\rangle + |\alpha\rangle)$  com estado auxiliar, onde  $N$ 's são as constantes de normalização. Com isso, o estado de entrada,  $|\psi_{in}\rangle = |A\rangle_1|B\rangle_2|C\rangle_3|\varphi\rangle_4|\varphi\rangle_5|\varphi\rangle_6$ , é dado por:

$$\begin{aligned} |\psi_{in}\rangle = N^3 N_A N_B N_C [ & (a_0 b_0 c_0 |-\alpha, -\alpha, -\alpha\rangle + \\ & a_0 b_0 c_1 |-\alpha, -\alpha, \alpha\rangle + \\ & a_0 b_1 c_0 |-\alpha, \alpha, -\alpha\rangle + \\ & a_0 b_1 c_1 |-\alpha, \alpha, \alpha\rangle + \\ & a_1 b_0 c_0 |\alpha, -\alpha, -\alpha\rangle + \\ & a_1 b_0 c_1 |\alpha, -\alpha, \alpha\rangle + \\ & a_1 b_1 c_0 |\alpha, \alpha, -\alpha\rangle + \\ & a_1 b_1 c_1 |\alpha, \alpha, \alpha\rangle)_{123} |\varphi, \varphi, \varphi\rangle_{456}. \end{aligned} \quad (7)$$

Após esse estado evoluir pelo sistema óptico, obtém-se o seguinte estado na saída (antes das medições), estado  $|\psi_{out}\rangle$ , onde os três primeiros qubits (1, 2 e 3) correspondem às saídas  $S_1$ ,  $S_2$  e  $S_3$  da porta  $C_1$  ou  $C_2$ , conforme os resultados obtidos na medição dos três últimos qubits (4, 5 e 6):

$$\begin{aligned} |\psi_{out}\rangle \approx & \frac{1}{2\sqrt{2}} |\psi_1\rangle_{123} |0, \pm\sqrt{2}\alpha, \pm\alpha\rangle_{456} \\ & + \frac{1}{2\sqrt{2}} |\psi_2\rangle_{123} |\pm\sqrt{2}\alpha, 0, \pm\alpha\rangle_{456} \\ & + \frac{\sqrt{3}}{2} |\psi_u\rangle_{1-6}, \end{aligned} \quad (8)$$

onde

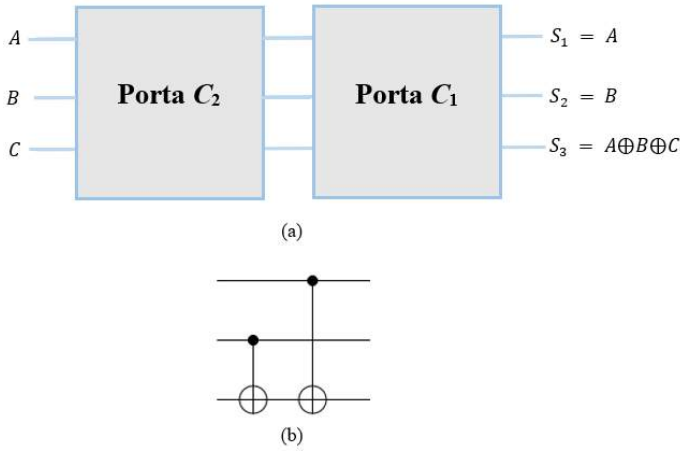
$$\begin{aligned}
 |\psi_1\rangle \approx & a_0 b_0 c_0 |-\alpha, -\alpha, -\alpha\rangle + a_0 b_0 c_1 |-\alpha, -\alpha, \alpha\rangle \\
 & + a_0 b_1 c_0 |\alpha, -\alpha, \alpha\rangle + a_0 b_1 c_1 |-\alpha, \alpha, \alpha\rangle \\
 & + a_1 b_0 c_0 |\alpha, -\alpha, -\alpha\rangle + a_1 b_0 c_1 |-\alpha, \alpha, -\alpha\rangle \\
 & + a_1 b_1 c_0 |\alpha, \alpha, -\alpha\rangle + a_1 b_1 c_1 |\alpha, \alpha, \alpha\rangle
 \end{aligned} \quad (9)$$

e

$$\begin{aligned}
 |\psi_2\rangle \approx & a_0 b_0 c_0 |-\alpha, -\alpha, \alpha\rangle + a_0 b_0 c_1 |-\alpha, -\alpha, -\alpha\rangle \\
 & + a_0 b_1 c_0 |\alpha, -\alpha, \alpha\rangle + a_0 b_1 c_1 |-\alpha, \alpha, \alpha\rangle \\
 & + a_1 b_0 c_0 |\alpha, -\alpha, -\alpha\rangle + a_1 b_0 c_1 |-\alpha, \alpha, -\alpha\rangle \\
 & + a_1 b_1 c_0 |\alpha, \alpha, \alpha\rangle + a_1 b_1 c_1 |\alpha, \alpha, -\alpha\rangle
 \end{aligned} \quad (10)$$

são os estados desejados na saída das portas  $C_1$  e  $C_2$ , respectivamente, obtidos após a medição quando o sistema funciona e o estado  $|\psi_u\rangle_{123}$  corresponde os casos que o sistema falha. Assim, em (8), quando houver detecção nos detectores  $D_2$  e  $D_3$  e nenhuma detecção em  $D_1$ , o estado na saída é (9) e quando houver apenas detecção em  $D_1$  e  $D_3$  e nenhuma detecção em  $D_2$ , o estado da saída será (10). Logo, nota-se (8) que a probabilidade de obter tanto o estado  $|\psi_1\rangle$  quanto o  $|\psi_2\rangle$  é de até  $1/8$ .

Pode-se cascatear a porta  $C_1$  seguida de uma porta  $C_2$ , conforme mostrado na Figura 4a, para obter um circuito quântico mais complexo (Circuito  $CC$ ) constituído de duas portas C-NOTs, Figura 4b.



**Fig. 4:** Circuito quântico obtido pelo (a) cascateamento das portas  $C_1$  e  $C_2$  e que corresponde a (b) duas portas C-NOTs.

#### IV. APLICAÇÕES

O sistema óptico proposto possui a capacidade de ser configurado, permitindo a obtenção de diversas funções lógicas a partir de uma única configuração inicial. Essa flexibilidade é alcançada através da pré-definição de uma das entradas do sistema, enquanto as demais entradas assumem diferentes valores para gerar as funções lógicas desejadas conforme mostrado na Tabela I.

Pode-se notar na Figura 4a que se a entrada  $C$  for pré-configurada em 0 ( $C = 0$ ), tem-se a função NXOR de  $A$  e  $B$  na saída  $S_3$ . Por outro lado, se  $C = 1$ , tem-se a função XOR de  $A$  e  $B$  conforme mostrado na Tabela II. Ou seja, o Circuito  $CC$  é capaz de implementar a porta C-NOT.

**TABELA I:** Funções lógicas obtidas a partir do circuito  $C_1$ .

Porta $C_1$	$S_1$	$S_2$	$S_3$
$C = 0$	$A + B$	$A \cdot B$	$\overline{A} \cdot \overline{B}$
$C = 1$	$A \cdot B$	$\overline{A + B}$	$A \cdot \overline{B}$

**TABELA II:** Funções lógicas obtidas a partir do circuito  $CC$ .

Circuito $CC$	$S_1$	$S_2$	$S_3$
$C = 0$	$A$	$B$	$A \odot B$
$C = 1$	$A$	$B$	$A \oplus B$

#### V. CONCLUSÕES

Este trabalho apresenta um sistema original baseado em dispositivos ópticos lineares para a realização probabilística de duas portas reversíveis,  $C_1$  e  $C_2$ , utilizando qubits de estados coerentes. O sistema demonstra a viabilidade de implementar operações lógicas reversíveis em um contexto óptico, possibilitando aplicações em áreas como computação quântica e processamento de informações.

O sistema proposto apresenta uma probabilidade de sucesso de até  $1/8$  para ambas as portas reversíveis. Além disso, o sistema permite a pré-configuração de um dos estados de entrada para a obtenção de três funções lógicas (AND, OR, NAND e/ou NOR), simultaneamente, das demais entradas por cada processamento. Essa flexibilidade possibilita a implementação da porta C-NOT por meio do cascateamento de ambas as portas.

#### AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, da Funcap e do INCT-IQ.

#### REFERÊNCIAS

- [1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, p. 45, 2010.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
- [3] A. Imamoglu, "Are quantum dots useful for quantum computation?" *Physica E: Low-dimensional Systems and Nanostructures*, vol. 16, no. 1, pp. 47–50, 2003.
- [4] D. A. Herrera-Martí, A. G. Fowler, D. Jennings, and T. Rudolph, "Photonic implementation for the topological cluster-state quantum computer," *Physical Review A*, vol. 82, no. 3, p. 032332, 2010.
- [5] G. S. Uhrig, "Keeping a quantum bit alive by optimized -pulse sequences," *Physical Review Letters*, vol. 98, no. 10, p. 100504, 2007.
- [6] You, J. Q., and Franco Nori. "Superconducting circuits and quantum information." *arXiv preprint quant-ph/0601121*, (2006).
- [7] Y. Makhlin, G. Schön, and A. Shnirman, "Josephson junction quantum logic gates," *Computer physics communications*, vol. 127, no. 1, pp. 156–164, 2000.
- [8] J. Schreier, A. A. Houck, J. Koch, D. I. Schuster, B. Johnson, J. Chow, J. M. Gambetta, J. Majer, L. Frunzio, M. H. Devoret, et al., "Suppressing charge noise decoherence in superconducting charge qubits," *Physical Review B*, vol. 77, no. 18, p. 180502, 2008.

- [9] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, "Bulk quantum computation with nuclear magnetic resonance: theory and experiment," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 454, pp. 447–467, The Royal Society, 1998.
- [10] Vandersypen, L., Steffen, M., Breyta, G. et al. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". *Nature* 414, 883–887 (2001).
- [11] L. M. K. Vandersypen, I. L. Chuang, "NMR techniques for quantum control and computation" *Reviews of Modern Physics*, January 2005.
- [12] C. Ospelkaus, C. E. Langer, J. M. Amini, K. R. Brown, D. Leibfried, and D. J. Wineland, "Trapped-ion quantum logic gates based on oscillating magnetic fields," *Physical review letters*, vol. 101, no. 9, p. 090502, 2008.
- [13] J. J. García-Ripoll, P. Zoller, and J. I. Cirac, "Speed optimized two-qubit gates with laser coherent control techniques for ion trap quantum computing," *Physical Review Letters*, vol. 91, no. 15, p. 157901, 2003.
- [14] A. Bermudez, P. O. Schmidt, M. B. Plenio, and A. Retzker, "Robust trapped-ion quantum logic gates by continuous dynamical decoupling", *Phys. Rev. A* 85, 040302(R) 2012.
- [15] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics", *nature*, vol. 409, no. 6816, p. 46, 2001.
- [16] T. C. Ralph, A. Gilchrist and G. J. Milburn, "Quantum computation with optical coherent states", *Phys. Rev. A*, 68, 042319, 2003.
- [17] H. Jeong and M. Kim, "Efficient quantum computation using coherent states", *Phys. Rev. A*, vol.65, 042305, 2002.
- [18] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Reviews of Modern Physics*, vol. 79, no. 1, p. 135, 2007.
- [19] M.S.R. Oliveira; H.M. Vasconcelos and J.B.R Silva. "A probabilistic CNOT gate for coherent-state qubits". *Phys. Lett. A*, 377, 2821-2825, 2013.
- [20] Rosa Silva, J.B., Ramos, R.V., "Smart generation of a tripartite GHZ-type state for coherent state qubit". *Opt. Commun.* 281(9), 2705 (2008).
- [21] S. Glancy, J. LoSecco, H. Vasconcelos, and C. Tanner, "Imperfect detectors in linear optical quantum computers," *Physical Review A*, vol. 65, no. 6, p. 062317, 2002.
- [22] J. B. R. Silva and R. V. Ramos, "Implementations of quantum and classical gates with linear optical devices and photon number quantum non-demolition measurement for polarization encoded qubits," *Physics Letters A*, vol. 359, no. 6, pp. 592–596, 2006.
- [23] D. Copsey, M. Oskin, F. Impens, T. Metodiev, A. Cross, F. T. Chong, I. L. Chuang, and J. Kubiatowicz, "Toward a scalable, silicon-based quantum computing architecture," *IEEE Journal of selected topics in quantum electronics*, vol. 9, no. 6, pp. 1552–1569, 2003.
- [24] J. L. O'Brien, A. Furusawa, and J. Vučković, "Photonic quantum technologies," *Nature Photonics*, vol. 3, no. 12, p. 687, 2009.
- [25] Glauber, Roy, J. The Quantum Theory of Optical Coherence. *Physical Review*, v. 130, n. 6, p. 2529, 1963.

# Uma Proposta de QPU Fotônica para Qubits de Estados Coerentes

Antônio F. Aguiar<sup>1</sup>, Orleans C. V. Gomes<sup>2</sup>, Gabriel F. Leite<sup>3</sup> e João Batista R. Silva<sup>4</sup>

**Resumo**— Este trabalho apresenta uma proposta de *QPU* fotônica versátil para qubits de estados coerentes usando dispositivos baseados em óptica linear capaz de implementar, probabilisticamente, as funções lógicas (*AND*, *OR*, *C-NOT*, *C<sup>2</sup>-NOT* e *C-SWAP*) com uma eficiência de até 1/4.

**Palavras-Chave**— *QPU* fotônica, porta Toffoli, porta Fredkin, óptica linear, estados coerentes.

**Abstract**— This work presents a versatile photonic *QPU* proposal for coherent state qubits using linear optics-based devices able to implement logical functions (*AND*, *OR*, *C-NOT*, *C<sup>2</sup>-NOT*, and *C-SWAP*) probabilistically with an efficiency of up to 1/4.

**Keywords**— Photonic *QPU*, Toffoli gate, Fredkin gate, linear optics, coherent states.

## I. INTRODUÇÃO

Em computação quântica, a busca por *QPU*'s (Unidades de Processamento Quântico) eficientes e escaláveis se intensifica. Nesse contexto, a fotônica emerge como uma plataforma promissora, com diversas propostas na literatura explorando características importantes dos fótons como sua capacidade de transportar informação quântica de baixo ruído por serem menos suscetíveis a decoerência [1]–[6]. Assim, eliminando a necessidade de temperaturas baixíssimas ou ambientes com alto vácuo. No entanto, a construção de uma *QPU* fotônica completa ainda representa um desafio significativo. Diversas propostas foram exploradas na literatura, cada uma com suas vantagens e desvantagens [7]–[11].

Os avanços em dispositivos de óptica integrada gerou uma ampla variedade de plataformas voltadas para aplicações em processamento quântico de informação (*QIP*), incluindo sílica sobre isolante [12]–[17], dentre muitos outros. A evolução do *QIP* tem sido favorável para construção de *QPU*'s que contornem obstáculos relacionados ao princípio da coerência quântica. Por tanto, trabalhos teóricos mostram que o ruído e a decoerência não são obstáculos fundamentais aos estudos com a utilização de estados coerentes no processamento de informação quântica [18]–[20]. Usando óptica linear, com o objetivo de codificar informações, os fótons únicos são substituídos por estados coerentes, abrindo a possibilidade de se obter portas lógicas com maiores probabilidades de sucesso.

Considerando que uma porta lógica reversível parte do princípio de que a informação pode ser reconstruída exclusivamente a partir de sua saída, dada sua entrada, e vice-versa, sem qualquer perda de informação. A reversibilidade é uma característica fundamental no desenvolvimento de algoritmos

DETI<sup>1,2,4</sup> e DEE<sup>3</sup>, Universidade Federal do Ceará<sup>1–4</sup>, Fortaleza-CE; e-mail: antonioaguiar.etiufc@alu.ufc.br<sup>1</sup>, orleanscardoso@outlook.com<sup>2</sup>, fonsecag.leite1810@gmail.com<sup>3</sup> e joaobrs@ufc.br<sup>4</sup>.

e circuitos quânticos que realizem operações complexas. Diante disso, o objetivo deste trabalho é apresentar um estudo teórico de um dispositivo *QPU* versátil para implementação de funções lógicas (*AND*, *OR*, *C<sup>2</sup>-NOT*, *C-NOT*, *C<sup>2</sup>-NOT* e *C-SWAP*) para qubits de estados coerentes, usando um sistema óptico proposto que irá implementá-las probabilisticamente.

## II. QUBITS FOTÔNICOS E DISPOSITIVOS BASEADOS EM ÓPTICA LINEAR

Uma forma de representar qubits fotônicos é por meio de estados coerentes da luz. Uma das características importantes dos estados coerentes é o fato de serem auto-estados do operador de aniquilação  $\hat{a}$  (criação,  $\hat{a}^\dagger$ ), com autovalor complexo  $\alpha$  ( $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ ). Tais estados foram descritos por R. J. Glauber em 1963 [21] e podem ser escritos na base dos estados de Fock,  $|n\rangle$ , também conhecidos como estados de número de fótons. Logo, o estado coerente  $|\alpha\rangle$  é dado por:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (1)$$

Na computação quântica os estados que representam os qubits lógicos precisam obedecer a uma relação fundamental de ortogonalidade entre si. Tal princípio garante a distinguibilidade e precisão das informações armazenadas usando qubits, proporcionando maior confiabilidade e precisão dos sistemas quânticos. Assim, a distinguibilidade entre dois dos estados coerentes,  $|\alpha\rangle$  e  $|\beta\rangle$ , é dado por:

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \quad (2)$$

Ou seja, quanto mais  $|\langle\alpha|\beta\rangle|^2$  tende a zero, mais distinguíveis são os estados. Portanto, em *QIP* com estados coerentes, usa-se  $|0\rangle = |-\alpha\rangle$  e  $|1\rangle = |\alpha\rangle$ , tal que  $\alpha$  é um número real e  $|\alpha|^2 \geq 4$  [22].

Então, quando dois estados coerentes  $|\alpha\rangle$  e  $|\beta\rangle$  atravessam um divisor de feixe (*BS*) balanceado, como pode ser visto na Figura 2a, seu estado na saída é dado por [22]:

$$|\alpha, \beta\rangle_{12} \xrightarrow{BS} \left| \frac{\alpha - \beta}{\sqrt{2}}, \frac{\alpha + \beta}{\sqrt{2}} \right\rangle_{1'2'}. \quad (3)$$

Quanto a interação do sinal óptico com um deslocador de fase *PS*( $\phi$ ), é adicionada uma fase  $\phi$  quando ele o atravessa, conforme mostrado na Figura 2b. Assim:

$$|\alpha\rangle_1 \xrightarrow{PS(\phi)} |e^{j\phi}\alpha\rangle_{1'}. \quad (4)$$

Com isso, um *PS* com  $\phi = \pi$  funcionará como uma porta *NOT* (*X*) para qubits de estados coerentes.

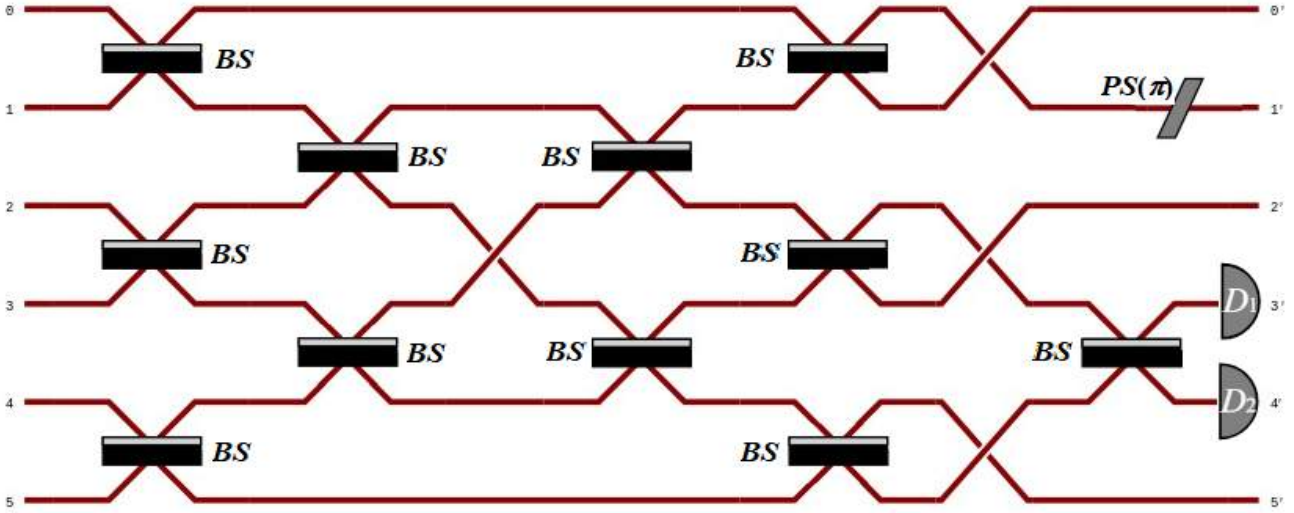


Fig. 1: *QPU X* fotônica: sistema óptico proposto usando apenas dispositivos ópticos lineares.



Fig. 2: Dispositivo ópticos: (a) divisor de feixes balanceado (*BS*) e (b) deslocador de fase (*PS*).

### III. UMA PROPOSTA DE QPU FOTÔNICA

Uma proposta *QPU* fotônica (*QPU X*) é apresentado na Figura 1. Esse sistema óptico é composto por onze *BS*'s onde ocorrem as interferências entre os feixes de luz, um *PS* e dois fotodetectores ( $D_1$  e  $D_2$ ) que permitirão, conforme as medições realizadas, deduzir se as operações lógicas entre os estados de entradas (0, 1 e 4) foram obtidas nas saídas (0', 1', 2' e 5').

Na Figura 1, as entradas enumeradas por 0, 1 e 4 são, respectivamente, as entradas de informação representadas pelos qubits de estados coerentes  $|A\rangle_0 = N_A(a_0|-\alpha\rangle + a_1|\alpha\rangle)$ ,  $|B\rangle_1 = N_B(b_0|-\alpha\rangle + b_1|\alpha\rangle)$ ,  $|C\rangle_4 = N_C(c_0|-\alpha\rangle + c_1|\alpha\rangle)$ , e as demais entradas (2, 3 e 5) são qubits auxiliares do tipo  $|\varphi\rangle = N(|-\alpha\rangle + |\alpha\rangle)$ , onde  $N$ 's são as constantes de normalização. Assim, o estado de entrada,  $|\psi_{in}\rangle = |A\rangle_0|B\rangle_1|\varphi\rangle_2|\varphi\rangle_3|C\rangle_4|\varphi\rangle_5$ , é dado por:

$$|\psi_{in}\rangle = N^3 N_A N_B N_C [(a_0 b_0 c_0 |-\alpha, -\alpha, -\alpha\rangle + a_0 b_0 c_1 |-\alpha, -\alpha, \alpha\rangle + a_0 b_1 c_0 |-\alpha, \alpha, -\alpha\rangle + a_0 b_1 c_1 |-\alpha, \alpha, \alpha\rangle + a_1 b_0 c_0 |\alpha, -\alpha, -\alpha\rangle + a_1 b_0 c_1 |\alpha, -\alpha, \alpha\rangle + a_1 b_1 c_0 |\alpha, \alpha, -\alpha\rangle + a_1 b_1 c_1 |\alpha, \alpha, \alpha\rangle)_{014} |\varphi, \varphi, \varphi\rangle_{235}]. \quad (5)$$

Após esse estado evoluir pelo sistema óptico, obtém-se o seguinte estado (não normalizado) na saída (antes das

medições), estado  $|\psi_{out}\rangle$ :

$$|\psi_{out}\rangle \approx \frac{1}{2\sqrt{2}} |\psi\rangle_{0'1'2'5'} |0, \pm\sqrt{2}\alpha\rangle_{3'4'} + \frac{1}{2} \sqrt{\frac{7}{2}} |\psi_u\rangle_{0'1'2'3'4'5'}, \quad (6)$$

onde

$$|\psi\rangle \approx a_0 b_0 c_0 |-\alpha, -\alpha, -\alpha, \alpha\rangle + a_0 b_0 c_1 |-\alpha, -\alpha, -\alpha, -\alpha\rangle + a_0 b_1 c_0 |-\alpha, \alpha, \alpha, -\alpha\rangle + a_0 b_1 c_1 |-\alpha, \alpha, -\alpha, \alpha\rangle + a_1 b_0 c_0 |\alpha, -\alpha, \alpha, -\alpha\rangle + a_1 b_0 c_1 |\alpha, -\alpha, -\alpha, \alpha\rangle + a_1 b_1 c_0 |\alpha, \alpha, \alpha, \alpha\rangle + a_1 b_1 c_1 |\alpha, \alpha, \alpha, -\alpha\rangle \quad (7)$$

é o estado desejado na saída, obtido após a medição quando houver detecção apenas no detector  $D_2$ . Caso contrário, o sistema falha e o estado na saída será  $|\psi_u\rangle_{0'1'2'5'}$ . Logo, nota-se (6) que a probabilidade de obter o estado (7) é de, aproximadamente, 1/8.

### IV. APLICAÇÕES

Uma representação da *QPU X* funcional é mostrado na Figura 3.

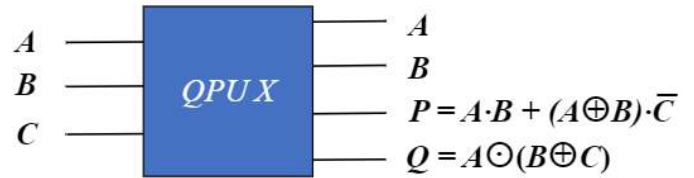


Fig. 3: Uma representação da *QPU X*.

A partir da Figura 3 obtém-se duas portas 3x3, conforme mostrado na Figura 4: a porta  $X'$  e a porta  $X''$ . A porta  $X'$  (Figura 4a), onde a saída  $Q$  é ignorada, não é reversível, mas quando a entrada  $C$  for 1 (0), tem-se a função *AND* (*OR*) de  $A$  e  $B$ . Por outro lado, a porta  $X''$  (Figura 4b), quando a saída  $P$  é descartada, é reversível e podemos obter as portas  $\bar{C}$ -NOT

(*NXOR*) e *C-NOT (XOR)* de *A* e *B* quando  $C = 0$  e  $C = 1$ , respectivamente.

As funções lógicas obtidas a partir da *QPU X* com pré-definição de uma das entradas são mostradas na Tabela I. A probabilidade de sucesso para obtenção das funções listadas na Tabela I é de até 1/4, uma vez que a entrada 3, na Figura 1, pode ser atribuída o mesmo valor da entrada *C*.

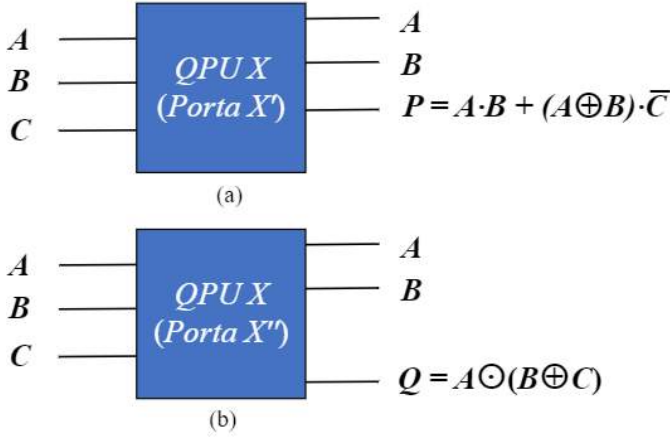


Fig. 4: Representação da (a) porta  $X'$  e da (b) porta  $X''$  obtidas a partir da *QPU X*.

TABELA I: Funções lógicas obtidas a partir de *QPU X*.

<i>QPU X</i>	<i>P</i>	<i>Q</i>
$C = 0$	$A + B$	$A \odot B$
$C = 1$	$A \cdot B$	$A \oplus B$

Pode-se obter a porta Toffoli ( $C^2$ -NOT) a partir das portas  $X'$  e  $X''$  conforme mostrado na Figura 5. Já na Figura 6, é apresentado uma proposta da porta Fredkin (*C-SWAP*) a partir de uma porta  $C^2$ -NOT (Figura 5) e de duas *C-NOT* (Figura 4b com  $C = 1$ ). Uma vez que a eficiência das portas quânticas fotônicas restringe a taxa de sucesso da porta Fredkin a  $10^{-5}$  [23], [24], as portas Toffoli e Fredkin propostas tem uma eficiência significativa de até 1/16 e 1/256, respectivamente.

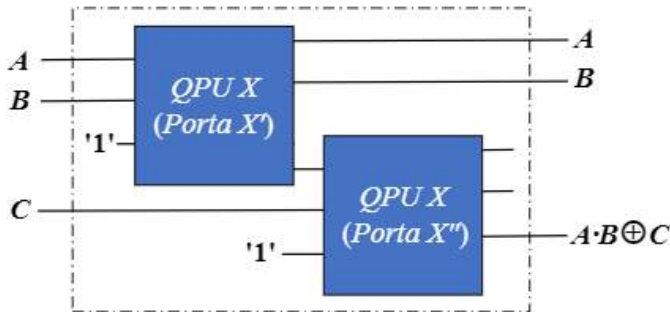


Fig. 5: Representação da porta Toffoli a partir da *QPU X*.

## V. CONCLUSÕES

A proposta de uma *QPU* fotônica (*QPU X*) para qubits de estados coerentes apresentada neste artigo demonstra a viabilidade e eficácia da utilização de estados coerentes na

implementação de funções lógicas em computação quântica. Ao explorar a óptica linear e a substituição de fótons únicos por estados coerentes, foi possível gerar funções lógicas importantes, como *AND*, *OR*, *C-NOT*,  $C^2$ -NOT e *C-SWAP*, de forma probabilística. A reversibilidade dessas funções é essencial para o desenvolvimento de algoritmos e circuitos quânticos complexos, garantindo a reconstrução da informação sem perdas.

A eficiência das funções lógicas geradas a partir da *QPU* proposta é um ponto relevante, destacando a capacidade de implementar operações complexas com estados coerentes. A porta Toffoli ( $C^2$ -NOT) e a porta Fredkin (*C-SWAP*) foram obtidas a partir das portas  $X'$  e  $X''$  propostas, demonstrando a versatilidade e potencial do sistema proposto. Apesar da eficiência do sistema diminuir a medida que se pretende obter circuitos mais complexos, o que já é esperado para esse tipo de tecnologia, o desempenho da *QPU X* proposta é promissor.

Vale ressaltar a originalidade da *QPU X* por implementar, simultaneamente, duas funções lógicas por processamento com a preservação dos estados de entradas. Portanto, a combinação de óptica linear e estados coerentes mostra-se promissora para superar desafios e alcançar resultados confiáveis no processamento de informação quântica.

## AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, da Funcap e do INCT-IQ.

## REFERÊNCIAS

- [1] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *nature*, vol. 409, no. 6816, pp. 46–52, 2001.
- [2] A. Laing, A. Peruzzo, A. Politi, M. R. Verde, M. Halder, T. C. Ralph, M. G. Thompson, and J. L. O'Brien, "High-fidelity operation of quantum photonic circuits," *Applied Physics Letters*, vol. 97, no. 21, 2010.
- [3] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical review letters*, vol. 86, no. 22, p. 5188, 2001.
- [4] M. A. Nielsen, "Optical quantum computation using cluster states," *Physical review letters*, vol. 93, no. 4, p. 040503, 2004.
- [5] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," *Nature Photonics*, vol. 14, no. 5, pp. 273–284, 2020.
- [6] S. Slussarenko and G. J. Pryde, "Photonic quantum information processing: A concise review," *Applied Physics Reviews*, vol. 6, no. 4, 2019.
- [7] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. Matthews, M. G. Thompson, and J. L. O'Brien, "Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit," *Nature Photonics*, vol. 6, no. 1, pp. 45–49, 2012.
- [8] J. Huang, Y. Chi, Z. Zhang, Y. Yang, Q. Gong, and J. Wang, "A programmable photonic chip for high-dimensional quantum computing," in *TENCON 2022-2022 IEEE Region 10 Conference (TENCON)*. IEEE, 2022, pp. 1–4.
- [9] F. Zilk, K. Staudacher, T. Guggemos, K. Furlinger, D. Kranzlmüller, and P. Walther, "A compiler for universal photonic quantum computers," in *2022 IEEE/ACM Third International Workshop on Quantum Computing Software (QCS)*. IEEE, 2022, pp. 57–67.
- [10] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," *Nature communications*, vol. 5, no. 1, p. 4213, 2014.
- [11] Y. Chi, J. Huang, Z. Zhang, J. Mao, Z. Zhou, X. Chen, C. Zhai, J. Bao, T. Dai, H. Yuan *et al.*, "A programmable qudit-based quantum processor," *Nature communications*, vol. 13, no. 1, p. 1166, 2022.

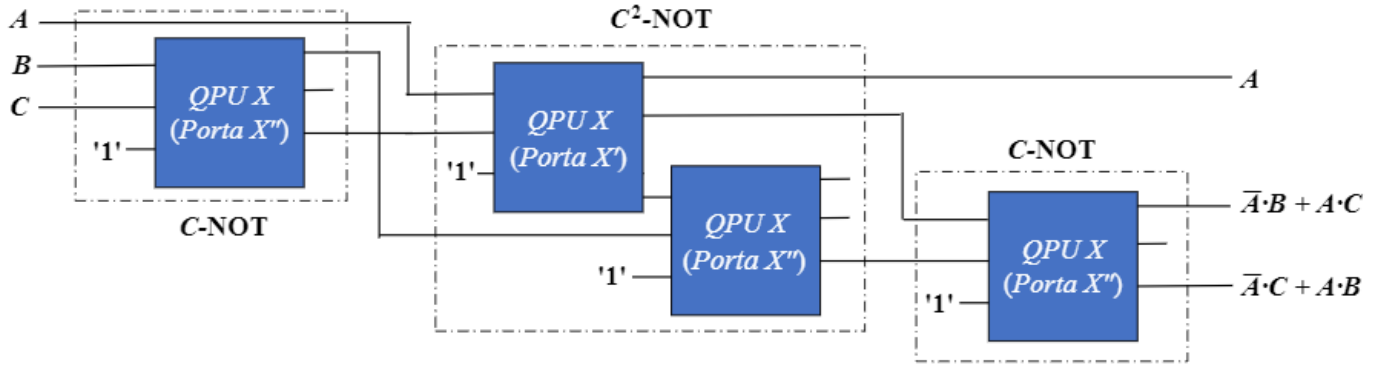


Fig. 6: Representação da porta Fredkin a partir da  $QPU X$ .

- [12] J. M. Arrazola, V. Bergholm, K. Brádler, T. R. Bromley, M. J. Collins, I. Dhand, A. Fumagalli, T. Gerrits, A. Goussev, L. G. Helt *et al.*, “Quantum circuits with many photons on a programmable nanophotonic chip,” *Nature*, vol. 591, no. 7848, pp. 54–60, 2021.
- [13] N. Maring, A. Fyrrillas, M. Pont, E. Ivanov, P. Stepanov, N. Margaria, W. Hease, A. Pishchagin, A. Lemaître, I. Sagnes *et al.*, “A versatile single-photon-based quantum computing platform,” *Nature Photonics*, vol. 18, no. 6, pp. 603–609, 2024.
- [14] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O’Brien, “Silicon-silicon waveguide quantum circuits,” *Science*, vol. 320, no. 5876, pp. 646–649, 2008.
- [15] B. J. Smith, D. Kundys, N. Thomas-Peter, P. Smith, and I. Walmsley, “Phase-controlled integrated photonic quantum circuits,” *Optics Express*, vol. 17, no. 16, pp. 13 516–13 525, 2009.
- [16] H. Takesue, Y. Tokura, H. Fukuda, T. Suchizawa, T. Watanabe, K. Yamada, and S.-i. Itabashi, “Entanglement generation using silicon wire waveguide,” *Applied Physics Letters*, vol. 91, no. 20, 2007.
- [17] D. Bonneau, E. Engin, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield *et al.*, “Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits,” *New Journal of Physics*, vol. 14, no. 4, p. 045003, 2012.
- [18] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, “Quantum computation with optical coherent states,” *Physical Review A*, vol. 68, no. 4, p. 042319, 2003.
- [19] H. Jeong and M. S. Kim, “Efficient quantum computation using coherent states,” *Physical Review A*, vol. 65, no. 4, p. 042305, 2002.
- [20] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, “Linear optical quantum computing with photonic qubits,” *Reviews of modern physics*, vol. 79, no. 1, p. 135, 2007.
- [21] R. J. Glauber, “The quantum theory of optical coherence,” *Physical Review*, vol. 130, no. 6, p. 2529, 1963.
- [22] J. B. R. Silva and R. V. Ramos, “Smart generation of a tripartite ghz-type state for coherent state qubit,” *Optics communications*, vol. 281, no. 9, pp. 2705–2709, 2008.
- [23] H. F. Hofmann and S. Takeuchi, “Quantum phase gate for photonic qubits using only beam splitters and postselection,” *Phys. Rev. A*, vol. 66, p. 024308, Aug 2002.
- [24] T. Ono, R. Okamoto, M. Tanida, H. F. Hofmann, and S. Takeuchi, “Implementation of a quantum controlled-swap gate with photonic circuits,” *Scientific reports*, vol. 7, no. 1, p. 45353, 2017.

# Quantum-Fuzzy Interpretations of Xor-Connectives using Overlapping and Grouping Aggregations

Juliano Buss<sup>1</sup>, Bruna Novack<sup>1</sup>, Emerson Vieira<sup>1</sup>, Cecilia Botelho<sup>1</sup>, Helida Santos<sup>2</sup>, Giancarlo Lucca<sup>3</sup>, Anderson Avila<sup>1</sup>, Adenauer Yamin<sup>1</sup>, Anderson Cruz<sup>4</sup>, Renata Reiser<sup>1</sup>

**Abstract**—This study aims to contribute to the broader dissemination of knowledge concerning quantum fuzzy computing. Combining characteristics and exploring fusion information by Fuzzy Logic and Quantum Computing, this work extends the quantum interpretation in the class of fuzzy Xor-connectives. Firstly, the Xor-connective is defined by aggregations as overlap and grouping functions. Additionally, the results are validated in the Qfuzzy-Analyser, a computational component providing methodologies for algebraic analysis and logical interpretation of flexible systems via quantum circuit modeling. This study considers the well-known IBM Qiskit simulator, which promotes execution and graphic representations for fuzzy Xor-connectives, including quantum circuits and many tools to observe the evolution of flexible systems and quantum-fuzzy interpretations.

**Keywords**—Quantum computing, Fuzzy Logic, Quantum Circuit, Quantum Transformations.

## I. INTRODUCTION

Currently, computing is being expanded to different branches of knowledge, and all of these areas of knowledge can benefit from computing in some way, be it automating processes, storing information or complex calculations. However, due to Moore’s law [18], classical computing may reach a physical limit, where the size of the transistors composing a processor is approaching the size of an atom. Quantum Computing (QC) [10], [16] may be a solution to this problem, as seen in [14] and [24] demonstrating the superiority of QC over classical computing.

Being one of the important areas covered in this article, QC is an interesting outlet for the continuous evolution of computing. QC expresses the inherent uncertainty in the physical environment, in the real world, where its foundations [12] are used to obtain efficiency for computation, such as state superposition and entanglement [26].

Fuzzy Logic (FL) [27] expresses the uncertainty inherent in human thought by mathematically modeling the imprecision

of natural language through the Fuzzy Set Theory [28]. Each element may belong to various sets with an associated degree of membership. Thus, FL has a greater representability capacity than classical computational logic, being able to take advantage of the  $[0, 1]$  range to represent data.

This article seeks to benefit from using such relevant areas, presenting the FL operators modeled in QC using multidimensional quantum registers and quantum bits (qubits) [1]. Several studies have already demonstrated the advantages of combining both areas of FL and QC [5], [7], [19].

In turn, Xor connectives report relevant scientific and technological applications in various areas of knowledge and computing, such as cryptography [2], generation of pseudo-random numbers [23], algorithm optimizations [4], and decision-making problems in biomedicine [15]. This large application specter motivates new studies to model the fuzzy Xor operator based on quantum computing. Such a class of logical connectives provides significant results in the development of electronic devices and the advent of new manufacturing techniques, such as *quantum-dot cellular automata* and tunneling phase logic [13]. Structures that generalize AND-XOR, such as CMOS XOR [3], require fewer terms than the traditional AND-OR structure, simplifying test architectures.

This work extends the quantum interpretation of fuzzy Xor connectives, defined by fuzzy aggregations as overlap and grouping functions. Additionally, the achieved results extend the Qfuzzy-Analyser, a computational component providing methodologies for algebraic analysis and logical interpretation of flexible systems via quantum circuit modeling (QCM).

In particular, among the various definitions of Xor fuzzy operators, we consider the fuzzy extension of the classical  $(x \wedge y) - (x \vee y)$ . However, we take (i) the grouping function [9], an aggregation combining two degrees of weak preference into a degree of information, and the dual concept, (ii) an overlap function [8], which turns two degrees of weak preference into a degree of indifference.

For the simulation of the proposed methodologies to interpret Xor connectives, this work considers IBM’s Qiskit simulator [21], promoting the graphic presentation for quantum circuits [22], [25] and many tools to observe the evolution of flexible systems via quantum-fuzzy interpretations [20].

The structure of the article is organized as follows. In Sect. II, the fundamentals of QC and FL are presented. Sect. III introduces the methods to obtain a quantum-fuzzy interpretation for Xor-connectives through quantum registers modeling membership degrees and quantum transformations (QT) to formalize the evolution of flexible systems. In addi-

<sup>1</sup>Juliano Buss, Bruna Novack, Emerson Vieira, Cecilia Botelho, Anderson Avila, Adenauer Yamin and Renata Reiser are with Federal University of Pelotas, Pelotas-RS 96010-610, Brazil, e-mail: {js-buss,bcdnovack,edvvieira,csbotelho,reiser,abdavila,adenauer}@inf.ufpel.edu.br;

<sup>2</sup>Helida Santos is with Federal University of Rio Grande, Rio Grande-RS 96203-900, Brazil, e-mail: helida@furg.br;

<sup>3</sup>Giancarlo Lucca is with Catholic University of Pelotas, Pelotas-RS 96010-000, Brazil, e-mail: giancarlo.lucca@ucpel.edu.br;

<sup>4</sup>Anderson Cruz is with Federal University of Rio Grande do Norte, Natal-RN 59078-900, Brazil, e-mail: anderson@imd.ufrn.br;

The authors would like to thank the following funding agencies: CAPES, CNPq (309160/2019-7; 311429/2020-3, 150160/2023-2), PqG/FAPERGS (21/2551-0002057-1), TechIn-FlexC3 (309559/2022-7), Q-Flex (409696/2022-6), FAPERGS/CNPq (23/2551-0000126-8) and PRONEX (16/2551-0000488-9).



tion, the development of the Qfuzzy-Analyzer is discussed, presenting simulations of fuzzy Xor-connectives generated by grouping and overlap operators. The fourth section presents the structuring and control system in the Qiskit simulator. Besides, the Xor simulation generated by grouping and overlap functions is analyzed using the Qiskit simulator. The last section discusses the results and final considerations.

## II. PRELIMINARIES

### A. Main Concepts on Quantum computing

Quantum Mechanics (QM) provides the basis for quantum computers to exist. It is possible to compute data through its postulates or rules by appropriating the properties of superposition and entanglement present in QM [17].

The qubit is the basic unit of information, composed of a unitary two-dimensional vector with complex components  $\alpha$  and  $\beta$ , such that  $|\alpha| + |\beta| = 1$ , and given as  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ , in Dirac's notation [11]. Generically, in the matrix representation, it is described as follows:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \quad (1)$$

The  $\alpha$  and  $\beta$  coefficients in Eq. (1) represent the state amplitude of  $|\phi\rangle$ , changing the probability of each of their states and expressed in a decimal notation.

The measuring on  $|\phi\rangle$  returns the probabilities  $p_0(|\phi\rangle) = \alpha$  related to  $|0\rangle$  or  $p_1(|\phi\rangle) = \beta$  related to  $|1\rangle$  [17].

Quantum transformations, or quantum gates, manipulate the information related to the qubits' coefficients, considering the matrices as the mathematical structure supported by the active physical laws and quantum mechanic postulates.

A quantum circuit model (QCM) provides a quantum model based on the composition of  $n$ -dimensional quantum gates. The execution of the  $n$ -qubits is performed by temporal evolution of the  $2^n$  horizontal lines, from left to right, while quantum operators are applied on the vertical line. At the end of the circuit computation, a measurement operation is performed as a probabilistic operation, obtaining a mixed quantum state - the new state as the  $n$ -projection and its corresponding probability  $P_n$ .

A generic one-dimensional quantum gate to manipulate a qubit can be defined based on the three parameters: theta, phi, and lambda, wherever  $\theta \in [0, \frac{\pi}{2}]$ ,  $\lambda, \phi \in [0, 2\pi]$ . Its matrix representation on IBM Qiskit<sup>1</sup> is given by Eq. (2):

$$\mu(\theta, \phi, \lambda) = \begin{pmatrix} \cos \frac{\theta}{2} & -e^{i\lambda} \sin \frac{\theta}{2} \\ e^{i\phi} \sin \frac{\theta}{2} & e^{i(\phi+\lambda)} \cos \frac{\theta}{2} \end{pmatrix}. \quad (2)$$

And, if  $\theta = \pi$ ,  $\lambda = \phi = \pi$ , we obtain the NOT or Pauli  $X$  gate, referring to the classic Not logical operator. However, for the quantum superposition, there is no reciprocal gate in classical logic. Applying  $X$  to a superposition state  $|\phi\rangle$ , the following evolution is obtained from an input  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$  to an output:  $X|\phi\rangle = \beta|0\rangle + \alpha|1\rangle$ , where  $\{\alpha, \beta\} \neq \{0, 1\}$ . It is represented in a QCM by Figure 1 [17].

The Toffoli gate ( $\mathcal{T}_{\phi_3}^{\phi_1, \phi_2}$ ) is a three-dimensional quantum transformation, where the first two ( $\phi_1, \phi_2$ ) are control qubits

and the last one ( $\phi_3$ ) is the target qubit. When the two control qubits are equal to  $|1\rangle$ , the value of the target qubit is changed by the  $NOT$  gate; otherwise, nothing happens. The representation of  $\mathcal{T}_3^{1,2}$  in a QCM is given by Figure 2.

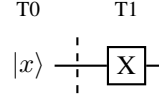


Fig. 1: NOT gate.

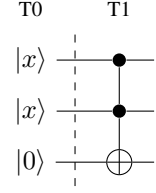


Fig. 2: Toffoli gate.

The measurement operation on the current state of a quantum system is defined by a set of linear projections,  $M_m$ , acting on quantum states [1]. For  $|\psi\rangle$ , the measured result on the probability is:

$$p(|\psi\rangle) = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}.$$

Measurement operations satisfy the completeness relation:  $\sum_m M_m^\dagger M_m = I$ . For one-dimensional systems, it holds that:

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = M_0^\dagger; \text{ and } M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = M_1^\dagger.$$

And, for the  $|\psi\rangle$  qubit, with  $\alpha, \beta \neq 0$ , observe that the probabilities for  $|0\rangle$  and  $|1\rangle$  result in:

- $p(|0\rangle) = \langle\phi|M_0^\dagger M_0|\phi\rangle = \langle\phi|M_0|\phi\rangle = |\alpha|^2$ ;
- $p(|1\rangle) = \langle\phi|M_1^\dagger M_1|\phi\rangle = \langle\phi|M_1|\phi\rangle = |\beta|^2$ .

So, after measuring  $|\psi\rangle$ , we have  $|\alpha|^2$  as the probability related to  $|0\rangle$ ; and  $|\beta|^2$  being the probability related to  $|1\rangle$ .

### B. Main Concepts on Fuzzy logic

FL has the purpose of expanding classic computational logic and its representation. Considering 0 and 1 as the possible values for a bit to assume, FL seeks to expand this notation, allowing the entire closed range of  $[0, 1]$  as possible values for data representation. Thus, it expands and makes the values more flexible. The membership function allows an element to partially belong to a set with an associated membership degree in a non-empty universe, represented by  $f_A(x)$ , with  $0 \leq f_A(x) \leq 1$ . Thus, a fuzzy set  $A$ , in a universe  $\chi \neq \emptyset$ , is given by the expression [27]:

$$A = \{(x, f_A(x)) : x \in \chi\}. \quad (3)$$

A fuzzy negation is a function  $N: [0, 1] \rightarrow [0, 1]$  satisfying:

N1: Boundary Conditions:  $N(0) = 1$  and  $N(1) = 0$ ;

N2: Monotonicity: If  $x \leq y$  then  $N(x) \geq N(y)$ ,  $\forall x, y \in [0, 1]$ .

The complement operation of a fuzzy set  $A$  is the FS  $A' = \{(x, f_{A'}(x)) : x \in \chi\}$ , where  $f_{A'}: \chi \rightarrow [0, 1]$  is given as:

$$f_{A'}(x) = N_S(f_A(x)) = 1 - f_A(x), \forall x \in \chi. \quad (4)$$

In [8], a continuous binary function  $O: [0, 1]^2 \rightarrow [0, 1]$  is an overlap function if it satisfies,  $\forall x, y \in [0, 1]$ , the conditions:

$O_1$ : If  $x \leq y$  then  $O(x, z) \leq O(y, z)$  (monotone increasing);

$O_2$ :  $O(x, y) = O(y, x)$  (symmetric);

$O_3$ :  $O(x, y) = 0$  if, and only if,  $x \cdot y = 0$ ;

$O_4$ :  $O(x, y) = 1$  if, and only if,  $x \cdot y = 1$ .

The overlap function can also satisfy an extra property:

<sup>1</sup><https://docs.quantum.ibm.com/api/qiskit/qiskit.circuit.library.U3Gate>

$O_5: O(x, 1) \leq x, \forall x \in [0, 1]$  (deflation).

Some overlap functions are reported as follows.

*Example 1:* Let  $p$  be a positive real number. So,

- $O_p(x, y) = x^p \cdot y^p$ ;
- $O_{mp}(x, y) = \min(x^p, y^p)$ ;
- $O_{Mp}(x, y) = 1 - \max((1-x)^p, (1-y)^p)$ .

See an instance of the fuzzy overlap operator  $O_p$  given by:

$$O_2(x, y) = x^2 \cdot y^2. \quad (5)$$

Thus, a standard will be maintained for modeling via quantum registers. The overlap aggregator will be used through the product between its two inputs, using  $p = 2$ .

The dual construction is the disjunctive aggregator called the grouping function. In [9], it was defined as a continuous binary function  $G: [0, 1]^2 \rightarrow [0, 1]$  known to be a grouping function if,  $\forall x, y \in [0, 1]$ , the following properties hold:

- $G_1$ : If  $y \leq z$  then  $G(x, z) \leq G(y, z)$  (monotone increasing);
- $G_2$ :  $G(x, y) = G(y, x)$  (symmetric);
- $G_3$ :  $G(x, y) = 0$  if, and only, if  $x = y = 0$  ( $x \cdot y = 0$ );
- $G_4$ :  $G(x, y) = 1$  if, and only, if,  $x = 1$  or  $y = 1$ .

*Example 2:* Let the parameter  $p$  be a positive real number.

See examples illustrating grouping functions:

- $G_{nm}(x, y) = 1 - \min(1-x, 1-y) \max((1-x)^p, (1-y)^p)$ ;
- $G_p(x, y) = 1 - (1-x)^p \cdot (1-y)^p$ ;
- $G_{mp}(x, y) = 1 - \min((1-x)^p, (1-y)^p)$ ;
- $G_{Mp}(x, y) = \max(x^p, y^p)$ .

In this work, for the interpretation via quantum computing, we consider the grouping function given by the expression:

$$G_2(x, y) = 1 - (1-x)^2 \cdot (1-y)^2. \quad (6)$$

Analogously, the grouping aggregator  $G_p$  will be used through the product between its two inputs, where  $p = 2$ .

The fuzzy connective E-Xor is a mapping  $E: [0, 1]^2 \rightarrow [0, 1]$ , holding the following properties:

- E1:  $E(1, 1) = E(0, 0) = 0$  and  $E(1, 0) = E(0, 1) = 1$ ;
- E2:  $E(x, y) = E(y, x)$ ;
- E3(a): If  $y \leq z$  then  $E(0, y) \leq E(0, z)$ ;
- E3(b): If  $y \leq z$  then  $E(1, y) \geq E(1, z)$ .

In [6], many classes of fuzzy XOR connectives are defined. Here we will consider fuzzy sets generated by the Xor operator, expressed as the difference between grouping and overlap functions.

*Proposition 1:* Consider  $G$  and  $O$  as grouping and overlap functions. The function  $E_{(G,O)}: [0, 1]^2 \rightarrow [0, 1]$  given by Eq. (7) below is an  $E_{(G,O)}$ -Xor connective:

$$E_{(G,O)}(x, y) = G(x, y) - (O(x, y)). \quad (7)$$

*Proof 1:* Straightforward.

*Example 3:* Consider the results in Eqs. (5) and (6). Then, an instance of Eq. (7) is given as

$$E_{(G_2, O_2)}(x, y) = 1 - (1-x)^2(1-y)^2 - x^2y^2. \quad (8)$$

### III. QUANTUM-FUZZY INTERPRETATION

We can interpret FSs by multidimensional quantum states and an FS operation by a quantum transformation. Let  $A$  be an FS defined by the membership function  $f_A: X \rightarrow [0, 1]$ ,

related to the universe set  $X \neq \emptyset, |X| = N$ . For each element  $x_i \in X$ ,  $A$  is interpreted by a quantum state given as:

$$|S_{f_A}\rangle = \bigotimes_{1 \leq i \leq N} [\sqrt{f_A(x_i)}|1\rangle + \sqrt{1-f_A(x_i)}|0\rangle]. \quad (9)$$

So,  $A$  is modeled based on a quantum superposition state, expressed by Eq. (9) and obtained by a tensor of the product of  $N$  qubits. The amplitude in  $|1\rangle$  interprets the membership function  $f_A(i)$ , and the other amplitude in  $|0\rangle$ , the non-membership of  $f_A(i)$ , expressed by  $1-f_A(i)$ .

The  $E_{(G_2, O_2)}$ -Xor connective, in Eq. (7), is interpreted by compositions of NOT ( $X$ ) and Toffoli ( $\mathcal{T}$ ) gates. Next, let  $|S_{f_i}\rangle$  and  $|S_{g_i}\rangle$  be quantum states for FSs  $A$  and  $B$ :

$$|x\rangle = |S_{f_i}\rangle = \sqrt{f_A(i)}|1\rangle + \sqrt{1-f_A(i)}|0\rangle; \quad (10)$$

$$|y\rangle = |S_{g_i}\rangle = \sqrt{f_B(i)}|1\rangle + \sqrt{1-f_B(i)}|0\rangle. \quad (11)$$

*Proposition 2:* Let  $|\psi_1\rangle$  and  $|\psi_2\rangle$  be expressed as follows:  $|\psi_1\rangle = \mathcal{T}_7^{5,6}(\mathcal{T}_5^{1,2}(X_1|x\rangle, X_2|x\rangle, |0\rangle), \mathcal{T}_6^{3,4}(X_3|y\rangle, X_4|y\rangle, |0\rangle), |0\rangle)$ ;  $|\psi_2\rangle = \mathcal{T}_{10}^{8,9}(\mathcal{T}_8^{1,2}(|x\rangle, |x\rangle, |0\rangle), \mathcal{T}_9^{3,4}(|y\rangle, |y\rangle, |0\rangle), |0\rangle)$ .

The quantum interpretation of  $E_{(G,O)}$ -Xor is given as:

$$E_{(G_2, O_2)}(|x\rangle, |y\rangle) = M_1^{11}(\mathcal{T}_{11}^{7,10}(X_{1,2,3,4}(X_7(|\psi_1\rangle, X_{10}|\psi_2\rangle))))).$$

*Proof 2:* Straightforward.

Figure 3 presents the quantum circuits with 11 qubits and the temporal evolution of the Xor-connective  $E_{(G_2, O_2)}$  from  $T_0$  to  $T_{12}$ , executed in the Qfuzzy-Analyser component. The measure operation is omitted in this representation.

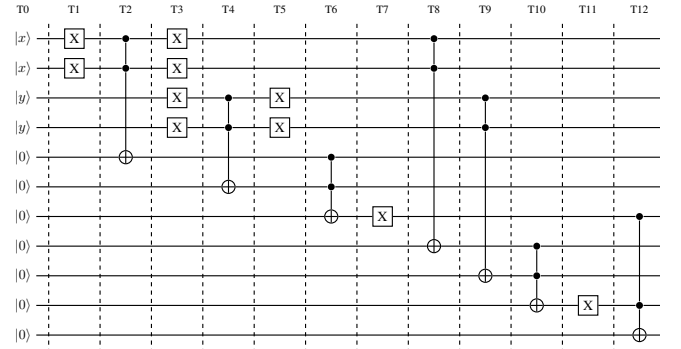


Fig. 3:  $E_{(G,O)}$  gate in a QCM on the quantum-fuzzy simulator.

Thus, a measurement operation performed on the  $11^{th}$  qubit, related to  $|1\rangle$  reaches the following final state:

$$E_{(G,O)}(|x\rangle, |y\rangle) = \frac{1}{\sqrt{1 - (1-x)^2(1-y)^2 - x^2y^2}} \left( \begin{aligned} &(1-x)\sqrt{(1-y)y}(|00011010011\rangle + |00101010011\rangle) \\ &+ (1-x)y|00111010111\rangle + \sqrt{(1-x)x(1-y)}|01000110011\rangle \\ &+ \sqrt{(1-x)xy(1-y)y}(|01010010011\rangle + |01100010011\rangle) \\ &+ \sqrt{(1-x)xy}|01110010111\rangle + \sqrt{x(1-x)(1-y)}|10000110011\rangle \\ &+ \sqrt{x(1-x)(1-y)y}(|10010010011\rangle + |10100010011\rangle) \\ &+ \sqrt{x(1-x)y}|10110010111\rangle + x(1-y)|11000111011\rangle \\ &+ x\sqrt{(1-y)y}(|11010011011\rangle + |11100011011\rangle), \end{aligned} \right) \quad (12)$$

with the probability of an element  $x_i$  being in a FS  $E_{G,O}$  given as:

$$p_1 = 1 - (1-x)^2(1-y)^2 - x^2 \cdot y^2. \quad (13)$$

Table I shows the square of non-null amplitudes of quantum states in four selected steps of temporal evolutions ( $T0$ ,  $T7$ ,  $T10$ ,  $T12$ ) given by the Qfuzzy-Analyser interface. The algebraic expressions for the non-null amplitudes, as described in column  $T12$ , precede the  $M_1^{11}$  measure operation.

TABLE I: Qfuzzy-Analyser evolution of the  $E_{(G,O)}$ -interpretation.

* Algebraic Expression (AE).				
AE	$T0$	$T7$	$T10$	$T12$
$(1-x)^2 * (1-y)^2$	0000000000	0000110000	0000110000	0000110010
$(1-x)^2 * (1-y) * y$	0001000000	0001101000	0001101000	0001101001
$(1-x)^2 * y * (1-y)$	0010000000	0010101000	0010101000	0010101001
$(1-x)^2 * y^2$	0011000000	0011101000	0011101010	0011101011
$(1-x) * x * (1-y)^2$	0100000000	0100011000	0100011000	0100011001
$(1-x) * x * (1-y) * y$	0101000000	0101001000	0101001000	0101001001
$(1-x) * x * y * (1-y)$	0110000000	0110001000	0110001000	0110001001
$(1-x) * x * y^2$	0111000000	0111001000	0111001010	0111001011
$x * (1-x) * (1-y)^2$	1000000000	1000011000	1000011000	1000011001
$x * (1-x) * (1-y) * y$	1001000000	1001001000	1001001000	1001001001
$x * (1-x) * y * (1-y)$	1010000000	1010001000	1010001000	1010001001
$x * (1-x) * y^2$	1011000000	1011001000	1011001010	1011001011
$x^2 * (1-y)^2$	1100000000	1100011000	1100011000	1100011001
$x^2 * (1-y) * y$	1101000000	1101001000	1101001000	1101001001
$x^2 * y * (1-y)$	1110000000	1110001000	1110001000	1110001001
$x^2 * y^2$	1111000000	1111001000	1111001110	1111001100

Furthermore, measuring on the last qubit, related to  $|0\rangle$ , we obtain:

$$E_{(G,O)}(|x\rangle, |y\rangle) = \frac{1}{(1-x)^2(1-y)^2 + x^2y^2} (xy|0000110010\rangle + (1-x)(1-y)|11110011100\rangle), \quad (14)$$

and the probability of element  $x_i$  not being in a FS  $E_{(G,O)}$  is given as:

$$p_0 = (1-x)^2(1-y)^2 + x^2y^2. \quad (15)$$

#### IV. CONTROL SYSTEM IN THE QISKIT-SIMULATIONS

The Qfuzzy-Analyser provides the algebraic methods to generate quantum fuzzy interpretations from the membership degree of an element in a fuzzy set, applying multidimensional quantum transformations and states. So, it integrates the uncertainty modeling from a multivalued logical approach and the quantum effects related to the generic quantum model. Being a simulator for teaching purposes, developed by researchers from Qflex-project, the mathematical expressions in the Qfuzzy-Analyser consider generic expressions for quantum data and operations.

We use the Qiskit simulator for real simulations, which allows access to real quantum processors available in the IBM cloud. Thus, running algorithms on real quantum hardware makes it possible to analyze the behavior of flexible algorithms, also considering effects and possible quantum errors.

The modeling of fuzzy connectors focuses on the Xor-connectives generated by overlap and grouping functions. Through the quantum transformations presented in Section II-A, it is possible to assign the membership degrees of FSs in quantum registers, according to the discussion in Section III.

Firstly, the algorithm that generates the expected result will be studied in relation to the membership degree to a set considering the connectives addressed by Eqs. (5) and (6). After this step, the simulation will be carried out in the Qiskit

simulator, still considering the same modeling applied in the Qfuzzy-Analyser.

Consider the following instances for the  $|x\rangle$  and  $|y\rangle$  states, which will be used to perform calculations on the amplitude of the quantum states and to model the system evolution:

$$|x\rangle = \frac{\sqrt{2}}{2}|1\rangle + \frac{\sqrt{2}}{2}|0\rangle \quad \text{and} \quad |y\rangle = \frac{\sqrt{3}}{2}|1\rangle + \frac{1}{2}|0\rangle. \quad (16)$$

These instances initializing the  $E_{(G,O)}$  connective can be expressed by taking Eq. (2):

- When  $\lambda = \pi$  rad,  $\phi = 0$  rad e  $\theta = \frac{\pi}{2}$  rad, we obtain the Hadamard QT, given as  $H = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{pmatrix}$ .

And,  $H(|0\rangle) = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$ , interpreting the membership degree  $f_A = x = \frac{1}{2}$ .

- When  $\lambda = \pi$  rad,  $\phi = 0$  rad and  $\theta = \frac{2\pi}{3}$  rad, then we obtain the QT  $J = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ . Moreover, we have that  $J(|0\rangle) = (\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle)$ , interpreting the membership degree  $f_B = y = \frac{3}{4}$ .

The amplitudes defined by Eq. (16) as inputs to Eq. (13) and Eq. (15) generate the following probabilities:

- $p_1 = 1 - (\frac{1}{2})^2(\frac{1}{4})^2 - (\frac{1}{2})^2(\frac{3}{4})^2 = 1 - \frac{10}{64} = \frac{54}{64} = 84.4\%$ ;
- $p_0 = (\frac{1}{2})^2(\frac{1}{4})^2 + (\frac{1}{2})^2(\frac{3}{4})^2 = \frac{10}{64} = 15.6\%$ .

See Fig. 4 for the graphical construction in the Qiskit simulator. It presents the steps of the algorithm related to the quantum Xor- $E_{G_2, O_2}$  in the QCM, including the  $M_1$  measure operation performed on the 11<sup>th</sup> qubit.

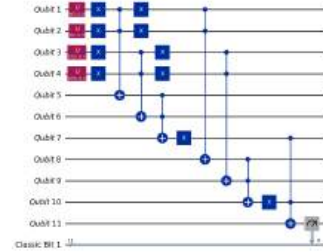


Fig. 4: Computing  $E_{(G,O)}$ -Xor QT in the Qiskit simulator.

From the simulations on the Qiskit, the probability slightly has an error associated with its execution, resulting in the approximation for the above probability distribution. The sample to obtain these results was carried out over 1.000 runs. Fig. 5 presents the final result given by the circuit in the Qiskit simulator, considering the initial states described in Eq. (16), using the  $H$  and  $J$  gates to generate such amplitudes.

#### V. CONCLUSION

This work focuses on presenting the concepts of FL and QC, simulating the operators and connectives present in FL and QC, using quantum registers, quantum transformations, and qubits. Thus, it is possible to obtain benefits from both areas of knowledge. The specifications for the class of E-connectives

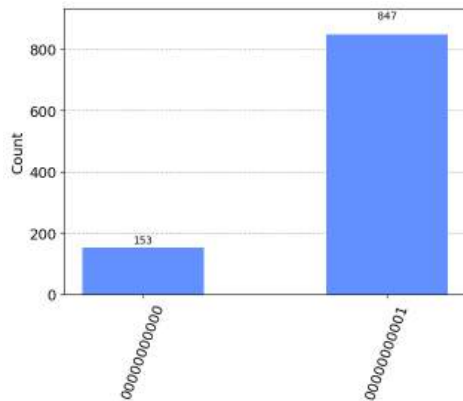


Fig. 5:  $E_{(G,O)}$  measurement results in the Qiskit simulator.

in the Qfuzzy-Analyser provide support to better understand the measurement procedures generated by the Qiskit simulator and to validate probabilities obtained by instantiating the Xor-operator in the quantum-fuzzy interpretations. It is possible to establish the relationship between the simulator built on a classical computer and the simulator running on a quantum computer. This increases the benefits of using both approaches, considering the mathematical support. It also enables a complete understanding during the Qiskit execution as a real simulation that is affected by the phenomena of QM. Furthermore, it promotes practical learning about the quantum world and improvements in the Qfuzzy-Analyser approach.

Hence, this study aims to contribute to the broader dissemination of knowledge concerning quantum computing. Specifically, our goal is to aid in its proliferation among universities, researchers, and individuals with an interest in areas where QC and FL intersect.

## REFERENCES

- [1] Nielsen, Michael A. and Chuang, I. L.: Quantum Computation and Quantum Information. Cambridge University Press (2000).
- [2] Aboughalia, R.A., Alkishriwo, O.A.S.: Color Image Encryption Based on Chaotic Block Permutation and XOR Operation. ArXiv (2018). <https://doi.org/10.48550/arXiv.1808.10198>
- [3] Aljafar, M.J., Perkowski, M.A., Acken, J.M., Tan, R.: A time-efficient cmos-memristive programmable circuit realizing logic functions in generalized and-xor structures. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **26**(1), 23–36 (2018). <https://doi.org/10.1109/TVLSI.2017.2750074>
- [4] Aslan, M., Gunduz, M., Kiran, M.S.: Jayax: Jaya algorithm with xor operator for binary optimization. Applied Soft Computing **82**, 105576 (2019). <https://doi.org/10.1016/j.asoc.2019.105576>
- [5] de Avila, A.B., Reiser, R., Pilla, M.L., Yamin, A.C.: Interpreting xor intuitionistic fuzzy connectives from quantum fuzzy computing. In: Guervós, J.J.M., Garibaldi, J.M., Linares-Barranco, A., Madani, K., Warwick, K. (eds.) Proceedings of the 11th International Joint Conference on Computational Intelligence, IJCCI 2019, Vienna, Austria, September 17–19, 2019. pp. 288–295. ScitePress (2019). <https://doi.org/10.5220/0008169702880295>
- [6] Bedregal, B.R.C., Reiser, R.H.S., Dimuro, G.P.: Revisiting XOR-Implications: Classes of fuzzy (Co)Implications Based on F-XOR (F-XNOR) Connectives. Int. J. Uncertain. Fuzziness Knowl. Based Syst. **21**(6), 899–926 (2013). <https://doi.org/10.1142/S0218488513500414>
- [7] Buss, J., Novack, B., Santos, H., Lucca, G., Avila, A., Yamin, A., Cruz, A., Reiser, R.: Conectivo fuzzy xor  $E_{\otimes}$  - interpretações quantum-fuzzy. In: Anais do VII Workshop-Escola de Informática Teórica. pp. 10–18. SBC, Porto Alegre, RS, Brasil (2023). <https://doi.org/10.5753/weit.2023.26592>
- [8] Bustince, H., Fernandez, J., Mesiar, R., Montero, J., Orduna, R.: Overlap functions. Nonlinear Analysis: Theory, Methods & Applications **72**(3), 1488–1499 (2010). <https://doi.org/10.1016/j.na.2009.08.033>
- [9] Bustince, H., Pagola, M., Mesiar, R., Hullermeier, E., Herrera, F.: Grouping, overlap, and generalized bientropic functions for fuzzy modeling of pairwise comparisons. IEEE Transactions on Fuzzy Systems **20**(3), 405–415 (2012). <https://doi.org/10.1109/TFUZZ.2011.2173581>
- [10] Deutsch, D., Ekert, A., Jozsa, R., Cirac, J.I., Zoller, P., Poyatos, J.F.: Concepts of quantum computation pp. 93–132 (2000). [https://doi.org/10.1007/978-3-662-04209-0\\_4](https://doi.org/10.1007/978-3-662-04209-0_4)
- [11] Dirac, P.A.M.: A new notation for quantum mechanics. Mathematical Proceedings of the Cambridge Philosophical Society **35**(3), 416–418 (1939). <https://doi.org/10.1017/S0305004100021162>
- [12] Gottfried, K., Yan, T.M.: Quantum mechanics: fundamentals, vol. 2. Springer (2003). <https://doi.org/10.1007/978-0-387-21623-2>
- [13] Haaswijk, W., Soeken, M., Amarù, L., Gaillardon, P.E., De Micheli, G.: A novel basis for logic rewriting. In: 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC). pp. 151–156 (2017). <https://doi.org/10.1109/ASPDAC.2017.7858312>
- [14] Harrow, A.W., Montanaro, A.: Quantum computational supremacy. Nature **549**(7671), 203–209 (Sep 2017). <https://doi.org/10.1038/nature23458>
- [15] Hocine, A., Kouaissah, N., Lozza, S.O.: XOR-analytic network process and assessing the impact of COVID-19 by sector. Computers & Industrial Engineering **177**, 109017 (2023). <https://doi.org/10.1016/j.cie.2023.109017>
- [16] Ladd, T.D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O’Brien, J.L.: Quantum computers. nature **464**(7285), 45–53 (2010). <https://doi.org/10.1038/nature08812>
- [17] Mermin, N David: Quantum computer science: An introduction. Cambridge University Press (2007). <https://doi.org/10.1017/CBO9780511813870>
- [18] Moore, G.E.: Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff. IEEE Solid-State Circuits Society Newsletter, **11**, 33–35 (2006). <https://doi.org/10.1109/N-SSC.2006.4785860>
- [19] Novack, B., Buss, J., Santos, H., Lucca, G., Avila, A., Yamin, A., Cruz, A., Reiser, R.: Modelagem quantum-fuzzy xor fuzzy  $E_{\ominus}$ . In: Anais do VII Workshop-Escola de Informática Teórica. pp. 62–70. SBC, Porto Alegre, RS, Brasil (2023). <https://doi.org/10.5753/weit.2023.26598>
- [20] qflex project, Avila, A., Cruz, A.: quantum-fuzzy (2023), <https://github.com/qflex-project/quantum-fuzzy>. Accessed: (May 14, 2024)
- [21] Qiskit contributors: Qiskit: An open-source framework for quantum computing (2023). <https://doi.org/10.5281/zenodo.2573505>
- [22] Raghuvanshi, A., Perkowski, M.: Fuzzy quantum circuits to model emotional behaviors of humanoid robots. In: IEEE Congress on Evolutionary Computation. pp. 1–8 (2010). <https://doi.org/10.1109/CEC.2010.5586038>
- [23] Sharma, M., Ranjan, R.K., Bharti, V.: A pseudo-random bit generator based on chaotic maps enhanced with a bit-XOR operation. Journal of Information Security and Applications **69**, 103299 (2022). <https://doi.org/10.1016/j.jisa.2022.103299>
- [24] Steane, A.: Quantum computing. Reports on Progress in Physics **61**(2), 117–173 (feb 1998). <https://doi.org/10.1088/0034-4885/61/2/002>
- [25] Wille, R., Chattopadhyay, A., Drechsler, R.: From reversible logic to quantum circuits: Logic design for an emerging technology. In: 2016 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS). pp. 268–274 (2016). <https://doi.org/10.1109/SAMOS.2016.7818357>
- [26] Wineland, D.J.: Nobel lecture: Superposition, entanglement, and raising schrödinger’s cat. Rev. Mod. Phys. **85**, 1103–1114 (Jul 2013). <https://doi.org/10.1103/RevModPhys.85.1103>
- [27] Zadeh, L.: Fuzzy sets. Information and Control **8**(3), 338–353 (1965). [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X)
- [28] Zimmermann, H.J.: Fuzzy Set Theory – and Its Applications, vol. 2001. Springer (01 2001). <https://doi.org/10.1007/978-94-010-0646-0>

# QT<sup>3</sup>GG Approach: Simulating a Quantum Game in a Game Engine Based on Graph Grammar

Júlia Veiga da Silva<sup>1</sup>, Júlia da Rocha Junqueira<sup>1</sup>, Ricardo Coutinho Cordeiro<sup>1</sup>, Renata Reiser<sup>1</sup>, Adenauer Yamin<sup>1</sup>, Bruno Moura<sup>2</sup>, Giancarlo Lucca<sup>3</sup>, Simone Cavalheiro<sup>1</sup>, Ulisses Corrêa<sup>1</sup>

**Abstract**— Educational games, especially those exploring quantum concepts, have gained attention for their potential to enhance learning experiences. This work introduces a simulation proposal for the Quantum Tic-Tac-Toe game, called QT<sup>3</sup>GG, implemented within the GameStation engine, which operates on Graph Grammar principles. We demonstrate that simulating quantum behavior using Graph Grammar is feasible but with some limitations. These findings suggest that, while Graph Grammar can capture certain aspects of quantum mechanics in game simulations, further development and refinement are necessary to accommodate the complexity of quantum games fully.

**Keywords**— Graph Grammar, Quantum Computing, Quantum Games

## I. INTRODUCTION

Considering quantum technologies and educational games, the integration of quantum games and game engines based on Graph Grammar (GG) offers a new path for exploration. Sekir et al. (2022) [6] delve into quantum games and interactive tools designed for quantum technologies outreach and education, highlighting the importance of such tools in engaging the target audience with quantum concepts. Additionally, Silva Junior (2021) [8] introduces GameStation, a game engine based on GG, a formal language used to describe systems and verify properties [3], showcasing the practical application of GG in game development.

GameStation allows all users to design and/or run GGs in a ludic environment while fostering Computational Thinking skills such as pattern recognition, data representation, and abstraction. Thus, it aims to support education in multiple ways: encouraging active methodologies and creative learning by turning students into game makers; enabling teachers to create educational games without coding; and developing Computational Thinking in activities not restricted to Computer Science subjects.

Synthesizing these studies, it is evident that combining quantum games with a game engine based on GG provides a promising approach to developing immersive and educational quantum gaming experiences. The use of GG enables the

modeling of quantum phenomena within the game environment, enhancing player engagement with intricate quantum concepts in an interactive and visually appealing manner. This strategy not only improves the gaming experience but also serves as a valuable educational tool for teaching individuals about quantum technologies in an accessible and engaging way.

Therefore, this work aims to simulate the quantum Tic-Tac-Toe game on GameStation, using GG to model the game's quantum interactions. Quantum Computing (QC) is a complex area, even for physicists, due to its highly mathematical nature. We believe that introducing quantum concepts through educational games can make these topics more accessible and understandable. By simulating the quantum Tic-Tac-Toe game, we seek not only to create an engaging gaming experience but also to provide an educational resource that facilitates an understanding of the fundamentals of QC.

The rest of this paper is organized as follows: Section 2 delves into the theoretical background, exploring concepts such as GG, the game engine GameStation, QC, and the Quantum Tic-Tac-Toe game; Section 3 introduces our innovative approach, detailing the integration of the QC concepts into the GameStation; Section 4 concludes the paper presenting final remarks and outlines potential paths for future research.

## II. THEORETICAL BACKGROUND

This section delves into the theoretical background of our study. It explores foundational concepts, rules, and theories that inform about the research and methodologies employed.

### A. Graph Grammar

GG is a formal language that can be seen as a generalization of Chomsky grammars, replacing strings with graphs [3]. In other words, it is a visual way of specifying systems. This language represents the states of a system as graphs and describes its events (transitions between states) with graph transformation rules. Graphs are structures essentially composed of vertices and edges, usually represented by points and arrows, respectively.

The GG definition used by GameStation specifies a type graph, which declares the types of system elements (vertices and edges); a start graph, which indicates the initial configuration from which the rules can be applied; and a set of rules that change the current state (graph). A rule is composed of two graphs, the **Left Hand Side (LHS)** and the **Right Hand Side (RHS)**, as well as a morphism that maps the LHS into the

<sup>1</sup>Júlia Veiga da Silva, Júlia da Rocha Junqueira, Ricardo Coutinho Cordeiro, Renata Reiser, Adenauer Yamin, Simone Cavalheiro, Ulisses Corrêa, Technological Development Center, Federal University of Pelotas, Pelotas-RS, e-mail: {jvsilva,julia.rjunqueira,ricardo.ccordeiro,reiser,adenauer,simone.costa,ulisses}@inf.ufpel.edu.br; <sup>2</sup>Bruno Moura, Directorate of Information Technology and Communication, Federal University of Pampa, Bagé-RS, e-mail: brunomoura@unipampa.edu.br; <sup>3</sup>Giancarlo Lucca, Center for Social and Technological Sciences, Catholic University of Pelotas, Pelotas-RS, e-mail: giancarlo.lucca@ucpel.edu.br. This study was financed in parts by CAPES, CNPq, PqG/FAPERGS, FAPERGS/CNPq, and PRONEX. Also financed this work the projects: QFlex 409696/2022-6 and TechIn-FlexC3: 309559/2022-7.

RHS, defining what should be deleted, preserved, or created during the rule application. Elements on the LHS that are related by the morphism must be preserved, while those that are not related must be deleted. On the other hand, elements on the RHS that are not in the morphism image must be created.

The LHS expresses a condition for applying a rule, while the RHS expresses a consequence of its application. For a rule to be applied in a state graph, its condition must be satisfied, meaning that it must be possible to map each element on the LHS of the rule to an element of the state graph. This mapping is called match and must respect the type of elements as well as the source and target of each edge. Thus, applying a rule changes the state graph by removing the elements in the match image associated with the deleted elements and adding the elements that must be created by the rule.

Figure 1 illustrates the type graph and the start graph of the Pac-Man game as a GG. The type graph (shown on the left of the figure) declares the existence of Pac-Man, ghosts, fruits, places (grey dots), a counter (pink triangle), and the relations between these elements. The start graph (depicted on the right of the figure) shows one Pac-Man, one ghost, and three fruits in a 3x4 map of places, while the counter indicates that no fruits have been eaten yet.



Fig. 1. Type graph (left) and start graph (right) for the Pac-Man game.

The set of rules (Figure 2) includes: Pac Move, Ghost Move, Pac Eat, and Ghost Eat. The rules are represented by a pair of graphs linked by an arrow. For instance, in the Pac Move rule, the LHS defines the condition for applying the rule: having a Pac-Man in a place that has a way to another one. The RHS defines the consequence of this rule: the Pac-Man’s connection is removed from its original place and it is restored at the next one.

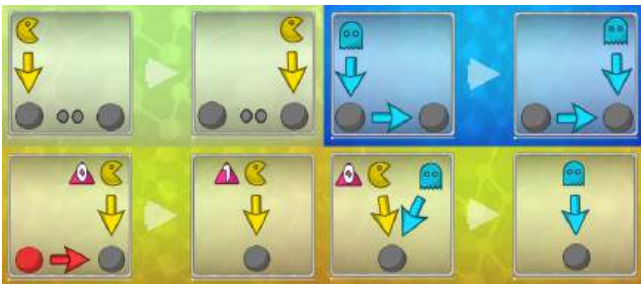


Fig. 2. Rules *Pac Move* (left, top), *Ghost Move* (right, top), *Pac Eat* (left, bottom), and *Ghost Eat* (right, bottom).

### B. GameStation

GameStation [1] is a GG-based tool used for creating and running games modeled according to this formal language.

Since games are represented as GG, the tool also promotes the development of skills related to Computational Thinking [10], a problem-solving technique based on Computer Science. These skills are developed both by those who create a game (specifies a GG) and those who run a game (simulates a GG). Silva Junior (2020) [8] detailed how concepts such as data representation, problem decomposition, abstraction, algorithms and processes, and parallelism are developed through the creation and simulation of a game (GG). GameStation is divided into three modules: Game Builder, Game Player, and Game Explorer. These modules allow users to create, run, and find games, respectively.

When specifying a GG in GameStation, users can import external resources such as images or use the original resources available within the tool. The user should also create the type graph, which corresponds to a declaration area in the platform, and the start graph, which represents the initial organization of the game. Finally, the rules which define the actions of the game’s actions must be created. All games begin with an empty type graph and an empty start graph. To specify elements in the type graph, users must define properties such as name, appearance, color, width, height, and rotation (on the  $x$ ,  $y$ , and  $z$  axis). In the start graph, users can create new elements by instantiating those defined in the type graph, specifying the type and name of each element. To specify rules, users must indicate whether an element will be preserved, created, or deleted by the rule, as well as its type and name. Additionally, if the element is an edge, the source and target must be specified; if it is a vertex, its position (coordinates) must be defined.

To play a game (using the Game Player module), the user can select, map, and apply the specified rules during the execution. When a rule is selected, the LHS and RHS graphs are shown, and the user should find a match by clicking on elements in the LHS and then selecting their corresponding elements in the state graph. Additionally, GameStation provides feedback by indicating whether the match is correct or incorrect.

### C. Quantum Computing

QC represents a paradigm shift in the world of computing. It offers an unconventional approach to processing information when compared to classical computing and its bits. Instead of relying on bits that can either be a 0 or a 1, QC harnesses the power of quantum bits (or qubits).

One of the most exciting aspects of QC is its potential to solve complex problems significantly faster than classical computers. Quantum computers, with their inherent ability to explore vast numbers of possible solutions simultaneously, could revolutionize fields such as cryptography, optimization, and artificial intelligence [2].

The first quantum computer was described in 1985 by David Deutsch and is known as the Quantum Turing Machine. This abstract machine is designed to replicate the effects of quantum mechanics in a computational context. This Turing Machine would be able to read, write, and perform displacement operations according to the behavior described by

quantum mechanics and then the tape could exist in non-classical states [9].

Unlike a conventional computer, the quantum computer performs its calculations using the properties of quantum mechanics. While a classical computer uses its base from electronic circuits and bits, the quantum computer is based on electron spins, energy levels of atoms, and has as its fundamental unit, instead of bits, the quantum bits (qubits) [7]. Some of the quantum mechanical theories that are applied in quantum computers are superposition, entanglement, interference, and parallelism. These theories are used to model the algebraic behaviors of the machine.

### III. QT<sup>3</sup>GG: APPROACH

This section introduces our proposal, starting with a description of the Quantum Tic-Tac-Toe game. Subsequently, we outline the QT<sup>3</sup>GG, our approach for implementing the game exploring GG, leveraging the GameStation engine for this purpose. After a review of the literature, we found out that there are no works directly related to our study. Although there are approaches that address partial aspects of our topic, we did not find publications that specifically address the combination of methods and objectives presented in our investigation. The absence of directly comparable previous studies shows the innovative contribution of this study to the field.

#### A. Quantum Tic-Tac-Toe Game

Introducing the concept of quantum, this version of Tic-Tac-Toe was created to demonstrate the events of QC in a more simplified way. This new version of the game was invented by Allan Goff, who developed this game as a gateway to the universe of quantum physics, offering an intuitive grasp of the essence of quantum mechanics without delving into complex mathematics [5]. In our work, we will use the online version of the game.

The quantum Tic-Tac-Toe game illustrates, through its rules, three phenomena of QC:

- **Superposition:** this refers to the ability of quantum entities to exist simultaneously in two or more states. In the context of Tic-Tac-Toe, a quantum state can simultaneously represent both “X” and “O” until it is observed or measured.
- **Entanglement:** this is a phenomenon where distant portions of a quantum system show correlations that cannot be accounted for by conventional causal relationships or common causes.
- **Collapse:** the process by which a system’s quantum states are narrowed down to classical states.

During the game, at every turn, a player must place two marks on the board. These two marks are then labeled with the corresponding turn number. The player using “X” begins with odd-numbered turns (e.g.,  $X_1, X_3$ ), while the player using “O” starts with even-numbered turns (e.g.,  $O_2, O_4$ ). These marks, which quantize the turns, are called “spooky” marks, named this way as a reference to Einstein’s comment about particles in a quantum state system that he famously described as “spooky action at a distance” [4]. Each pair of moves is a

mixed state, distributed between two squares where the true location of each move is only revealed later in the game.

When mixed states or mixed marks share one square, the move becomes entangled. There is no limit to how many states can be in one square, but at some point, it will cause a cyclical entanglement requiring a collapse to happen, which will define the true mark of the square [4].

#### B. Quantum Tic-Tac-Toe Game Exploring GG

Figure 3 illustrates part of the specification of the Tic-Tac-Toe game in GameStation. In the type graph (depicted on the left of the figure), all elements related to the game and their relations are defined. The “blue X” and the “red O” vertices represent the markings of the two players in the game, while the “white square” vertex corresponds to the subdivisions of the board – called “places” – in which the players place their respective markings. The “gray sphere” vertex, in turn, represents the empty space, used to indicate when a certain place is not marked by a vertex. The blue, red, and gray edges indicate, respectively, the relations of the vertices “X”, “O”, and “sphere” with a particular place.



Fig. 3. Type graph (left) and start graph (right) for the Tic-Tac-Toe game.

Finally, the other edges represent the relation between places in the directions established by the game: horizontal (green), vertical (yellow), main diagonal (purple), and secondary diagonal (pink). The initial graph - or state graph - (depicted on the right of the figure) indicates the arrangement of the game elements at the beginning of the game. Since Tic-Tac-Toe must start with a board composed of nine unoccupied places, each one is assigned a relation with the empty element, as well as relations between the places in the established directions.

The states of the game can be changed by applying rules. In Figure 4, the rules *PutX* (top, left) and *PutO* (top, right) specify possible actions for the players in their respective turns. For the application of these rules, a condition must be met (LHS): the presence of an unoccupied place on the board. After application, an effect is produced (RHS): the vertex “X” or the vertex “O” is marked in this place, and the sphere vertex is deleted. The rest of the defined rules are the victory conditions of the game. To win in Tic-Tac-Toe, the player needs to get a sequence of three identical elements in one of the four allowed directions.

Thus, eight rules were defined: two possibilities of vertices (“X” and “O”) for four possibilities of directions (horizontal, vertical, main diagonal, and secondary diagonal). Figure 4 illustrates two of the eight rules: *XHor*, which indicates the victory of the player who is playing with the vertex “X”, horizontally; and *OMainDiag*, which indicates the victory of the player who is playing with the vertex “O”, in the main diagonal.

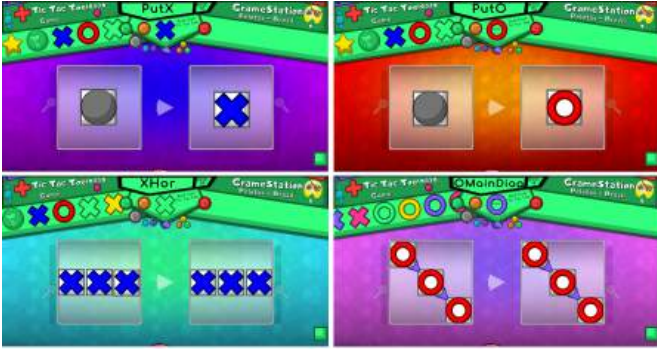


Fig. 4. Rules *PutX* (left, top), *PutO* (right, top), *XHor* (left, bottom), and *OMainDiag* (right, bottom).

To simulate the behavior of quantum Tic-Tac-Toe on GameStation, adaptations to the original rules were made. Due to the quantum nature of the board’s squares, they can be in a superposition of states, including being both empty and marked simultaneously. Therefore, the condition of a square being empty for a player to mark their symbol no longer applies, as the square can be in a quantum state that allows multiple markings at the same time. This implies the need to update the game rules to deal with this quantum characteristic. Thus, the relation between the empty space vertex and the place vertex was deleted in the LHS (Figure 5).



Fig. 5. Rules *PutQuantumX* (left) and *PutQuantumO* (right).

Quantum Tic-Tac-Toe allows mixed states, that is, now more than one “X”/“O” can be related to the same place. There is no limit to how many states can be related to a place, but considering that at some point this will cause a cyclical tangle, requiring a collapse to occur, the true mark of the square is set. Figure 6 presents two examples of mixed states followed by their true mark in the RHS.



Fig. 6. Rules *BigX* (left) and *BigO* (right).

#### IV. FINAL REMARKS

In conclusion, the integration of quantum games within GameStation represents a significant advancement in the educational gaming and quantum technologies areas. Mixing the capabilities of GG with quantum games, users can create engaging and educational experiences that simulate complex

quantum phenomena in a ludic way. This approach not only enhances player engagement with intricate quantum concepts but also serves as a valuable tool for teaching individuals about quantum technologies in an accessible and engaging way.

While it is indeed possible to simulate quantum Tic-Tac-Toe in GameStation using GG, it would require a significant number of rules to cover all possibilities. The original Tic-Tac-Toe game already needs a considerable number of rules, and introducing the quantum aspect would further increase the complexity. This could potentially be a limitation as the game may become challenging.

Additionally, the quantum nature of the game board introduces a level of uncertainty and superposition that may complicate gameplay and decision-making processes for players. Therefore, careful consideration must be given to balancing the quantum elements with the gameplay mechanics to ensure an enjoyable and comprehensible gaming experience.

#### ACKNOWLEDGEMENTS

The authors would like to thank the following funding agencies: CAPES, CNPq (309160/2019-7; 311429/2020-3, 150160/2023-2), PqG/FAPERGS (21/2551-0002057-1) and FAPERGS/CNPq (23/2551-0000126-8) PRONEX (16/2551-0000488-9). A thank also to the Federal University of Pelotas (UFPEL), the Federal Foundation University of Rio Grande (FURG), the Catholic University of Pelotas (UCPEL), the Federal University of Pampa (UNIPAMPA), as well as the Laboratory of Ubiquitous and Parallel Systems (LUPS), the Fundamentals of Computing Laboratory, and the UFPEL HUB in Artificial Intelligence Innovation (HUB2IA).

#### REFERÊNCIAS

- [1] Braz Araujo da Silva Junior, Simone André da Costa Cavaleiro, and Luciana Foss. *Gamestation: Specifying games with graphs*. In *Anais do XXXII Simpósio Brasileiro de Informática na Educação*, pages 499–511. SBC, 2021.
- [2] MI Dyakonov. *State of the art and prospects for quantum computing*. *Future Trends in Microelectronics: frontiers and innovations*, pages 266–285, 2013.
- [3] Hartmut Ehrig, Reiko Heckel, Martin Korff, Michael Löwe, Leila Ribeiro, Annika Wagner, and Andrea Corradini. *Algebraic approaches to graph transformation—part ii: Single pushout approach and comparison with double pushout approach*. In *Handbook Of Graph Grammars And Computing By Graph Transformation: Volume 1: Foundations*, pages 247–312. World Scientific, 1997.
- [4] Allan Goff. *Quantum tic-tac-toe: A teaching metaphor for superposition in quantum mechanics*. *American Journal of Physics*, 74(11):962–973, 2006.
- [5] Allan Goff, Dale Lehmann, and Joel Siegel. *Quantum tic-tac-toe, spooky-coins & magic-envelopes, as metaphors for relativistic quantum physics*. In *38th AIAA/ASME/SAE/ASEE joint propulsion conference & exhibit*, page 3763, 2002.
- [6] Zeki C Seskir, Piotr Migdał, Carrie Weidner, Aditya Anupam, Nicky Case, Noah Davis, Chiara Decaroli, Ilke Ercan, Caterina Foti, Pawel Gora, et al. *Quantum games and interactive tools for quantum technologies outreach and education: A review and experiences from the field*.
- [7] WJN da Silva. *Uma introdução à computação quântica*. *Universidade de São Paulo, Monografia*, 2018.
- [8] Braz Araujo da Silva Júnior. *Ggaset: bringing formal methods to the computational thinking*. Master’s thesis, Universidade Federal de Pelotas, 2020.
- [9] Colin P Williams. *Explorations in quantum computing*. Springer Science & Business Media, 2010.
- [10] Jeannette M Wing. *Computational thinking*. *Communications of the ACM*, 49(3):33–35, 2006.



# Enumeration of Circuits with $n$ Quantum Gates

Andresso da Silva and Francisco M. de Assis

**Abstract**—Commutativity relations between quantum gates have recently been studied to improve quantum compilers. On the other hand, partially commutative monoids were initially proposed for modeling concurrent systems, providing tools for analyzing and representing sequences of sequential and parallel events. This article investigates the relationship between quantum circuits and partially commutative monoids. By applying partially commutative monoid enumeration techniques, we obtain the exact number of distinct circuits with  $n$  gates, taking into account the commutativity relations between the gates. This result has potential applications in circuit optimization and obtaining bounds in a quantum circuit compression context.

**Keywords**—Quantum circuits, Partially Commutative Monoid, Quantum Gates, Commutator.

## I. INTRODUCTION

Commutativity and non-commutativity relations play a fundamental role in quantum mechanics, one example being Heisenberg’s uncertainty principle [1]. In the quantum circuits context, commutativity relations between quantum gates have recently been studied to improve quantum compilers [2], [3], [4], [5], [6], [7].

Quantum compilers are responsible for receiving an algorithm at the input and providing a circuit that implements this algorithm using a series of basic operations on qubits. The compilers must obtain the circuits according to certain constraints, such as the coherence time, which is directly related to the number of gates and the depth of the circuit [4], [5], [7].

The depth of some circuits can be reduced using the commutativity relation between quantum gates [8], [9]. Gates that commute generate the same result for any order they are applied. By carrying out a search among the circuit orderings, one can select the configuration in which more gates can be applied in parallel [10], [11]. In addition, commutativity can be used to approximate operations and thus facilitate the simulation of quantum circuits [12], [13].

Partially commutative monoids provide the theoretical foundation for modeling commutativity relations between set elements. Commutativity relations are represented by a graph having the set elements as vertices. Two vertices are connected by an edge in this graph if there is a commutativity relation between them. Originally, partially commutative monoids were proposed to model concurrent systems since it is possible to represent the occurrence of events that happen sequentially or in parallel [14], [15].

Andresso da Silva, Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande - PB, e-mail: andresso.silva@ee.ufcg.edu.br; Francisco M. de Assis, Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande - PB, e-mail: fmarcos@dee.ufcg.edu.br. This work was partially support by CNPq (311680/2022-4 and 140327/2023-1).

In this paper, we investigate the relationship between partially commutative monoids and quantum circuits. The relationship occurs through the representation of commutativity relations between gates using graphs. In this way, we demonstrated how to obtain the exact number of distinct circuits with  $n$  gates by means of the commutativity relations between the gates used in the circuit construction. In this context, potential applications for the results obtained in this article involve the compression and optimization of quantum circuits. The authors of this article have not found any papers in the literature that relate quantum circuits to partially commutative monoids.

The rest of the article is structured as follows. Section II presents the fundamental concepts for understanding this work. The first topic covered in this section is quantum circuits, where we present the adopted conventions. The second topic refers to graph theory, which serves as the foundation for the topic of partially commutative monoids. With regard to partially commutative monoids, we present the definitions needed to address the enumeration techniques adopted in this paper. Section III presents the results obtained by applying the concepts of partially commutative monoids in the context of quantum circuits. Section IV presents the conclusion and future work.

## II. FUNDAMENTALS

### A. Quantum Circuits

Quantum circuits are graphical representations of a sequence of applications of unitary operators in an initial input state. In this way, each operation is represented as a quantum gate, and the horizontal lines represent qubits on which the gates act. Suppose you want to represent the operations described by

$$\begin{aligned} \text{CNOT} \cdot (R_z(\theta) \otimes I) &= \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \left( \begin{bmatrix} e^{-j\theta/2} & 0 \\ 0 & e^{j\theta/2} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \end{aligned} \quad (1)$$

in the state  $|00\rangle = [1 \ 0 \ 0 \ 0]^T$ , then the circuit shown in Fig. 1 would be obtained.

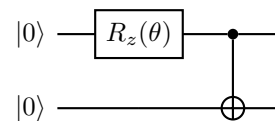


Fig. 1: Quantum circuit equivalent to Eq. 1.

The temporal order in which the operators are applied is from left to right, so first  $R_z(\theta) \otimes I$  is applied to the input

state  $|00\rangle$ . Note that  $R_z(\theta)$  is applied to the first qubit, and the second is preserved. Subsequently, the CNOT gate is applied to the result of the first operation.

In some cases, changing the order in which the gates occur does not alter the final result of the circuit. To check this, one can use the concept of a commutator.

*Definition 1 (Commutator):* Given two operators  $A$  and  $B$ , the commutator is defined as

$$[A, B] = AB - BA. \quad (3)$$

Thus, if  $AB = BA$ , then  $[A, B] = 0$  and  $A$  is said to commute with  $B$ . If  $[A, B] \neq 0$ , then  $A$  does not commute with  $B$ .

In the case of the circuit in Fig. 1, the gates CNOT and  $R_z(\theta)$  can be interchanged, since  $[\text{CNOT}, R_z(\theta)] = 0$ . Thus, CNOT and  $R_z(\theta)$  commute.

### B. Graph Theory

A simple undirected graph is a pair  $G = (V, E)$  where  $V$  is called the set of vertices and  $E \subset V \times V$  is called the set of edges. Two vertices  $a, b \in V$  are adjacent if  $(a, b) \in E$  and are called non-adjacent otherwise. In  $G$ , multiple edges connecting two vertices are not allowed, nor are edges leaving and arriving at the same vertex. The complement of a graph  $G = (V, E)$  is the graph with the same set of vertices  $V$ , where any two distinct vertices in  $V$  are adjacent in  $G$  if and only if they are not adjacent in  $G$ . A complete graph is one in which all vertices are connected pairwise and is commonly denoted as  $K_q$ , where  $q$  is the number of vertices. An empty graph is one that has no edges.

The *clique* of a graph  $G$  is a set of mutually adjacent vertices  $C \subseteq V$ . A clique is maximal if it is not a subset of another clique. The cardinality of the largest clique is called the *clique number*, denoted by  $\omega(G)$ . For a complete graph  $K_q$ , the clique number is the number of vertices,  $q$ . Finding the clique number is an NP-complete problem.

### C. Partially Commutative Monoids

Let  $\Sigma$  be a finite alphabet. The set  $\Sigma^*$  is called a free monoid and is the set of all finite words formed by the elements of  $\Sigma$ , including the empty word  $\varepsilon$ . The set  $\Sigma^n$  is constituted of all the words of length  $n$  defined in the alphabet  $\Sigma$ .

Two  $\Sigma$  symbols commute when there are two words  $\mathbf{u} = \mathbf{l}x\mathbf{y}\mathbf{m}$  and  $\mathbf{v} = \mathbf{l}y\mathbf{x}\mathbf{m}$ , with  $\mathbf{l}, \mathbf{m} \in \Sigma^*$  and  $x, y \in \Sigma$ . These types of words are known as Mazurkiewicz traces [15].

The *commutativity graph*  $G = (V, E)$  is a simple undirected graph, in which  $V$  is the set of vertices and  $E$  is the set of edges. The elements of  $V$  are associated with a finite alphabet  $\Sigma$  by means of a bijective function, so the set  $V$  and  $\Sigma$  will be treated as equivalent without loss of generality.

If the symbols  $x, y \in \Sigma$  commute, then the vertices  $x, y \in V$  are connected by an edge,  $(x, y) \in E$  in the commutativity graph. Two vertices are adjacent if they are connected on the commutativity graph. The complement of the commutativity graph,  $\overline{G} = (V, \overline{E})$ , is called the non-commutativity graph, in which vertices connected by an edge are associated with symbols that *do not* commute.

If the symbols  $x$  and  $y$  commute, then the relationship is represented by  $xy \equiv_G yx$ . If they don't commute, the relation is represented by  $xy \not\equiv_G yx$ . For example, if the *commutativity graph* is the one in Fig. 2, then  $a$  commutes with  $c$  and  $b$  commutes with  $c$ , but  $a$  does not commute with  $b$ . Therefore, in this case,  $ac \equiv_G ca$ ,  $bc \equiv_G cb$  and  $ab \not\equiv_G ba$ .

Two words  $\mathbf{u}, \mathbf{v} \in \mathcal{M}(\Sigma, G)$  are equivalent according to the relation  $\equiv_G$  if it is possible to obtain one from the other by swapping the positions of the consecutive symbols that commute.

*Definition 2 (Equivalence Class):* Let  $\mathcal{E}_G(\mathbf{u})$  be the set of words equivalent to a word  $\mathbf{u} \in \Sigma^n$ , according to the relation  $\equiv_G$ . The set  $\mathcal{E}_G(\mathbf{u})$  is called the equivalence class of  $\mathbf{u}$ .

Based on the definition of equivalence class, we can now define partially commutative monoids. A partially commutative monoid  $\mathcal{M}(\Sigma, G)$  is the set of all equivalence classes defined by the alphabet  $\Sigma$  and the commutativity relations represented by the commutativity graph  $G$ .

If two words belong to the same equivalence class, they are said to be congruent. For a given length, there will be a number of equivalence classes. The number of classes is denoted by  $\tau_G(n)$ , where  $G$  is the commutativity graph and  $n$  is the length of the words. Thus,  $\tau_G(n)$  represents the number of words of length  $n$  that *are not equivalent* to each other and can be understood as the number of possible processes in a concurrent system.

*Example 1:* In this example, we will consider the commutativity graph in Fig. 2, where  $\Sigma = \{a, b, c\}$ .

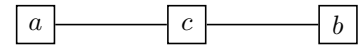


Fig. 2: Commutativity Graph  $G$ .

The equivalence classes of length  $n = 1$  will be  $\{a, b, c\}$ , totaling 3 equivalence classes. For a length of  $n = 2$ , the classes will be  $\{aa, ab, \{ac, ca\}, ba, bb, \{bc, cb\}, cc\}$ , with a total of 7 classes. For a length of  $n = 3$ , the number of distinct classes is 15 (see Table I). The braces have been removed for classes with only one element. So instead of using  $\{\{aaa\}, \{aab\}, \dots\}$ , we use  $\{aaa, aab, \dots\}$  to avoid making the presentation of the classes excessively complicated.

The number  $\tau_G(n)$  of equivalence classes  $\mathcal{E}(\mathbf{u}_i)$ , corresponds to the maximum number of words  $\mathbf{u}_i$  of length  $n$  that are pairwise non-congruent,  $i = 1, 2, \dots, \tau_G(n)$ . Thus,  $\mathcal{M}^n(\Sigma, G)$  represents the subsets of equivalence classes of the monoid  $\mathcal{M}(\Sigma, G)$  that are formed by words of length  $n$ ,

$$\mathcal{M}^n(\Sigma, G) = \mathcal{E}_G(\mathbf{u}_1) \cup \mathcal{E}_G(\mathbf{u}_2) \cup \dots \cup \mathcal{E}_G(\mathbf{u}_{\tau_G(n)}), \quad (4)$$

in which  $\mathcal{E}_G(\mathbf{u}_i) \cap \mathcal{E}_G(\mathbf{u}_j) = \emptyset$  for  $i \neq j$ ,  $|\mathbf{u}_i| = n, i = 1, 2, \dots, \tau_G(n)$  and  $\tau_G(n) = |\mathcal{M}^n(\Sigma, G)|$ .

*Example 2:* Considering, as an example, the commutativity graph of Example 1, we know that  $ac \equiv_G ca$ ,  $cb \equiv_G bc$  and  $ab \not\equiv_G ba$ . The classes  $\mathcal{M}^n(\Sigma, G)$  for  $n = 1, 2, 3$  are presented in Table I.

Fisher [16], [17] has developed methods for determining the number  $\tau_G(n)$  of equivalence classes of length  $n$  based on the theory of partially commutative monoids presented by Cartier and Foata [14]. The main tools for determining  $\tau_G(n)$

n	$\mathcal{M}^n(\Sigma, G)$	$\tau_G(n)$
1	$\{a, b, c\}$	3
2	$\{aa, ab, \{ac, ca\}, ba, bb, \{bc, cb\}, cc\}$	7
3	$\{aaa, aab, \{aac, aca, caa\}, aba, abb, \{abc, acb, cab\}, \{acc, cac, cca\}, baa, bab, \{bac, bca, cba\}, bba, bbb, \{bbc, bcb, cbb\}, \{bcc, bcb, ccb\}, ccc\}$	15

TABLE I: Equivalence classes for the graph shown in Fig. 2.

are the dependence polynomial of a commutativity graph  $G$  and generating function of the monoid [17].

*Definition 3:* (Dependence Polynomial [17]) The dependence polynomial of the commutativity graph  $G$  is defined by

$$D(G, z) = \sum_{k=0}^{\omega} (-1)^k c_k z^k, \quad (5)$$

where  $c_k$  denotes the number cliques of size  $k$  in the graph  $G$  and  $\omega$  is the clique number of  $G$ .

It is worth mentioning that, since determining  $c_k$  is an NP-complete problem, determining  $D(G, z)$  is also NP-complete.

*Definition 4 (Monoid Generating Function):* The generating function of a monoid  $\mathcal{M}(\Sigma, G)$  is defined as

$$\zeta_{\mathcal{M}}(z) = \sum_{n=0}^{\infty} \tau_G(n) z^n. \quad (6)$$

The generating function  $\zeta_{\mathcal{M}}$  of the monoid  $\mathcal{M}(\Sigma, G)$  can be used to obtain an expression for  $\tau_G(n)$  by using Corollary 1.

*Corollary 1:* [17, p.251] The generating function  $\zeta_{\mathcal{M}}(z)$  of the monoid is equal to the inverse of the dependence polynomial of the commutativity graph,

$$\zeta_{\mathcal{M}}(z) D(G, z) = 1. \quad (7)$$

*Example 3:* Using the graph in Fig. 2 once again, we obtain that  $c_1 = 3$  and  $c_2 = 3$ . Thus, the dependence polynomial is

$$D(G, z) = 1 - 3z + 2z^2. \quad (8)$$

By applying the Corollary 1, one can calculate the generating function as

$$\zeta_{\mathcal{M}}(z) = \frac{1}{D(G, z)} = \frac{1}{1 - 3z + 2z^2} \quad (9)$$

$$= \sum_{n=0}^{\infty} (2^{n+1} - 1) z^n. \quad (10)$$

Comparing the result of Eq. (10) with Definition 4, we obtain that  $\tau_G(n) = 2^{n+1} - 1$ . With this expression, one can now calculate the number of equivalence classes without having to obtain all the equivalent words and classes.

### III. ENUMERATION OF QUANTUM CIRCUITS

The first step in applying partially commutative monoids to quantum circuits is to find the relationship between these two topics. It is possible to associate commutativity between operators with the concept of congruence of partially commutative monoids. This association is formalized in Definition 5.

*Definition 5:* The congruence relation between two operators  $A$  and  $B$  is defined as

$$AB \equiv_G BA \iff [A, B] = 0, A \neq B. \quad (11)$$

In this way, Definition 5 provides a connection between partial order and commutator algebra. The condition  $A \neq B$  is necessary because a symbol, an operator in this case, does not commute with itself, by definition, in the theory of partially commutative monoids.

In this context, given a set of gates and the commutativity relations between them, how many distinct results can we obtain by applying  $n$  of these gates? Answering this question can indicate the optimum limit for compressing quantum circuits. If all the gates in the set do not commute, the number of combinations of gates will be  $q^n$ , and there will also be  $q^n$  distinct results, where  $q$  is the number of gates. When any pair of ports commute, the number of combinations is still  $q^n$ , but the number of distinct results from applying  $n$  ports will be less than  $q^n$ . In general, it will be shown using Definition 5 that it is possible to obtain  $\tau_G(n)$  distinct results,  $\tau_G(n) \leq q^n$ . In this way, the main result of this article can be stated.

*Theorem 1:* Let  $\mathcal{Q} = \{Q_1, \dots, Q_q\}$  be a set of quantum gates with commutativity relations given by a commutativity graph  $G$ , the number of distinct circuits with  $n$  gates is equal to  $\tau_G(n)$ .

*Proof:* Let  $\mathcal{Q} = \{Q_1, \dots, Q_q\}$  be a set of quantum gates defined on a Hilbert space  $\mathcal{H}^d$ . If two gates  $Q_i$  and  $Q_j$  respect  $[Q_i, Q_j] = 0$ , then  $Q_i Q_j$  and  $Q_j Q_i$  produce the same result when applied. The question is: how many distinct combinations of gates are possible when the circuit has  $n$  gates? Using the Definition 5, the problem can be treated in the language of partially commutative monoids, making it possible to treat the circuits as sequences of symbols representing the gates. By applying Corollary 1, taking  $\mathcal{Q}$  as the set of symbols and considering the commutativity graph  $G$ , the number of distinct sequences considering the commutativity relations is given exactly by  $\tau_G(n)$ . ■

*Example 4:* As an example, consider the set of gates

$$\mathcal{Q} = \{\text{CNOT}_1, \text{CNOT}_2, \text{CNOT}_3, R_z, R_x\}, \quad (12)$$

so that  $q = 5$ . The angles of  $R_z$  and  $R_x$  are suppressed because the commutativity relations in this example will not depend on their values.

The gates in  $\mathcal{Q}$  and some of the equivalence relations between the order of application of these gates are shown in Fig. 3. The gates  $R_z$  and  $R_x$  are always applied to the first qubit and the third qubit, respectively.

The gates  $\text{CNOT}_2$  and  $\text{CNOT}_3$  can be obtained by inspecting Fig. 3 as  $\text{CNOT}_2 = \text{CNOT} \otimes \text{I}$  and  $\text{CNOT}_3 = \text{I} \otimes \text{CNOT}$ . By using the definition of commutator (see Definition 1), it is possible to conclude that  $\text{CNOT}_2$  and  $\text{CNOT}_3$  do not commute, because

$$\begin{aligned} [\text{CNOT}_2, \text{CNOT}_3] &= (\text{CNOT} \otimes \text{I})(\text{I} \otimes \text{CNOT}) \\ &\quad - (\text{I} \otimes \text{CNOT})(\text{CNOT} \otimes \text{I}) \\ &\neq 0, \end{aligned}$$

since  $\text{I}$  and  $\text{CNOT}$  have different dimensions.

Since  $R_x$  and  $R_z$  are applied to different qubits, then they commute. Both  $R_z$  and  $R_x$  commute with  $\text{CNOT}_2$  and  $\text{CNOT}_3$ . Thus, only  $\text{CNOT}_2$  and  $\text{CNOT}_3$  do not commute

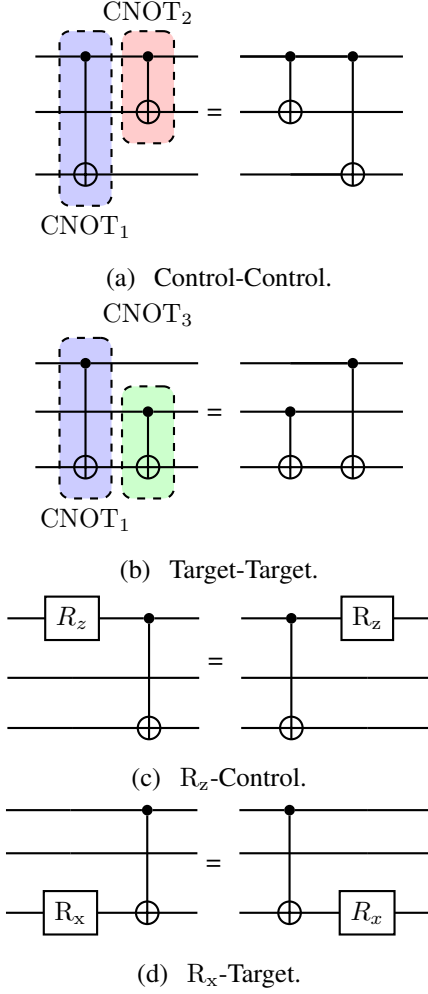


Fig. 3: Commutativity relationship between some quantum gates.

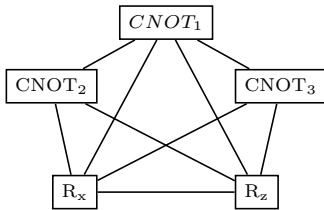


Fig. 4: Commutativity graph of the quantum gates in the set  $\mathcal{Q}$ .

with each other. From these commutativity relations, it is possible to obtain the commutativity graph shown in Fig. 4.

Using the definition of the dependence polynomial (see Definition 3), we can check that  $c_0 = 1, c_1 = 5, c_2 = 9, c_3 = 7, c_4 = 2, c_5 = 0$  and

$$D(G, z) = 1 - 5z + 9z^2 - 7z^3 + 2z^4. \quad (13)$$

Calculating the generating function of the monoid, one can

obtain

$$\zeta_{\mathcal{M}}(z) = \frac{1}{D(G, z)} = \frac{1}{1 - 5z + 9z^2 - 7z^3 + 2z^4} \quad (14)$$

$$= \sum_{n=1}^{\infty} \left( 2^{n+3} - \frac{n^2}{2} - \frac{7n}{2} - 7 \right) z^n. \quad (15)$$

Therefore, the  $\tau_G(n)$  for this case is equal to

$$\tau_G(n) = 2^{n+3} - \frac{n^2}{2} - \frac{7n}{2} - 7. \quad (16)$$

Whereas there are  $5^n$  possible combinations of circuits with  $n$  gates, only  $\tau_G(n) = 2^{n+3} - \frac{n^2}{2} - \frac{7n}{2} - 7$  of these circuits are effectively distinct. For  $n = 5$ , the number of combinations is  $5^5 = 3125$ , while  $\tau_G(5) = 219$ . In other words, the number of distinct circuits is about 7% of the value obtained without considering the commutativity relations between the gates for a circuit of length  $n = 5$ . Fig. 5 shows the number of distinct circuits calculated considering and not considering the commutativity between the gates.

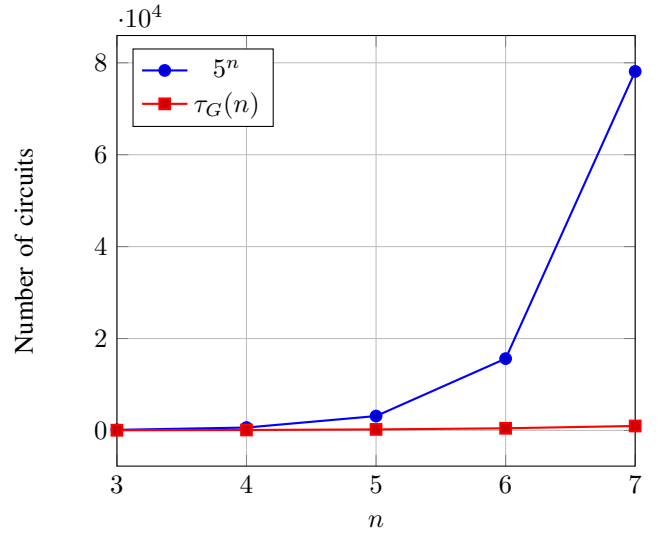


Fig. 5: Numbers of distinct circuits with  $n$  gates using the set  $\mathcal{Q} = \{\text{CNOT}_1, \text{CNOT}_2, \text{CNOT}_3, R_z, R_x\}$ .

There is a lower limit to the number of distinct circuits. This limit is obtained when the commutativity graph is complete, i.e., all the gates in the circuit commute. In Example 4, one edge is missing for the commutativity graph to be complete, so the number of circuits is close to the minimum value possible.

The lower limit for the number of circuits corresponds to the number of type classes, common in the context of information theory [18]. To calculate  $\tau_G(n)$  for a complete graph with  $q$  edges, we again use the dependence polynomial, obtaining

$$D(K_q, z) = \sum_{k=0}^q (-1)^k \binom{q}{k} z^k = -(z-1)^q \quad (17)$$

and then apply Corollary 1, obtaining

$$\tau_{K_q}(n) = \binom{q+n-1}{n}. \quad (18)$$

For the case of  $q = 5$ , one can calculate  $D(K_5, z) = -(z - 1)^5$  and

$$\tau_{K_5}(n) = \binom{5+n-1}{n}, \quad (19)$$

is the minimum number of distinct circuits with  $n$  gates obtained using  $q = 5$  distinct gates that commute mutually ( $G$  is a complete graph).

Similarly, there is an upper limit for the number of distinct circuits that is obtained when the commutativity graph is empty. In this case,  $D(G, z) = 1 - qz$  and therefore  $\tau_G(n) = q^n$ . If the graph is not empty,  $\tau_G(n)$  is strictly less than  $q^n$ , i.e.,  $\tau_G(n) < q^n$ .

Some of the possible applications of these results involve the optimization and compression of quantum circuits. Using the concept of equivalence classes reduces the search space compared to the search space without considering commutativity relations. Similarly, elements of the same equivalence class can be represented as such, and this can be used to compress circuits.

#### IV. CONCLUSIONS

In this paper, we presented the connections between partially commutative monoids and quantum circuits. From the definition of the commutator between two operators, it was possible to define a congruence relation used in the formalism of partially commutative monoids. This approach allows us to use counting methods to enumerate distinct quantum circuits with a certain number of gates.

The counting methods we used involve defining a commutativity graph that encodes commutativity relations as edges. In this way, it was possible to observe that considering the commutativity relations between operators makes it possible to obtain the exact number of distinct circuits.

Without considering commutativity relations, the number of circuits is  $q^n$ , where  $q$  is the number of available gates and  $n$  is the number of gates used in the circuit. In this work, we showed that the exact number of distinct circuits gets smaller and smaller concerning  $q^n$  as the commutativity graph approaches a complete graph.

In future work, the aim is to estimate the number of equivalent circuits according to the commutativity relations. In addition, the results obtained can be used to define limits for the optimal compression of quantum circuits.

#### ACKNOWLEDGMENTS

The authors would like to thank CNPq and COPELE for their financial support.

#### REFERENCES

- [1] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift für Physik*, vol. 33, pp. 879–893, 1925.
- [2] A. Abdollahi and M. Pedram, "Analysis and synthesis of quantum circuits by using quantum decision diagrams," in *Proceedings of the Conference on Design, Automation and Test in Europe: Proceedings, DATE '06*, (Leuven, BEL), p. 317–322, European Design and Automation Association, 2006.
- [3] X. Ni and M. Van Den Nest, "Commuting quantum circuits: Efficient classical simulations versus hardness results," *Quantum Info. Comput.*, vol. 13, p. 54–72, jan 2013.
- [4] T. Itoko, R. Raymond, T. Imamichi, A. Matsuo, and A. W. Cross, "Quantum circuit compilers using gate commutation rules," in *Proceedings of the 24th Asia and South Pacific Design Automation Conference, ASPDAC '19*, (New York, NY, USA), p. 191–196, Association for Computing Machinery, 2019.
- [5] T. Itoko, R. Raymond, T. Imamichi, and A. Matsuo, "Optimization of quantum circuit mapping using gate transformation and commutation," *Integration*, vol. 70, pp. 43–50, 2020.
- [6] J. Paykin, A. T. Schmitz, M. Ibrahim, X. Wu, and A. Y. Matsuura, "Pcoast: A pauli-based quantum circuit optimization framework," in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, (Los Alamitos, CA, USA), pp. 715–726, IEEE Computer Society, sep 2023.
- [7] S. Zhang, K. Huang, and L. Li, "Depth-optimized quantum circuit synthesis for diagonal unitary operators with asymptotically optimal gate count," *Phys. Rev. A*, vol. 109, p. 042601, Apr 2024.
- [8] D. Camps, E. Kökcü, L. Bassman Otelie, W. A. de Jong, A. F. Kemper, and R. Van Beeumen, "An algebraic quantum circuit compression algorithm for hamiltonian simulation," *SIAM Journal on Matrix Analysis and Applications*, vol. 43, no. 3, pp. 1084–1108, 2022.
- [9] N. Mariella and S. Zhuk, "A doubly stochastic matrices-based approach to optimal qubit routing," *Quantum Information Processing*, vol. 22, June 2023.
- [10] M. Alam, A. Ash-Saki, and S. Ghosh, "Circuit compilation methodologies for quantum approximate optimization algorithm," in *2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 215–228, 2020.
- [11] M. Alam, A. Ash-Saki, J. Li, A. Chattopadhyay, and S. Ghosh, "Noise resilient compilation policies for quantum approximate optimization algorithm," in *2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pp. 1–7, 2020.
- [12] Y.-A. Chen, A. M. Childs, M. Hafezi, Z. Jiang, H. Kim, and Y. Xu, "Efficient product formulas for commutators and applications to quantum simulation," *Phys. Rev. Res.*, vol. 4, p. 013191, Mar 2022.
- [13] V. Slynko and V. Bivziuk, "Influence of the commutator properties of hamiltonians on the robustness of quantum circuits," *Physics Letters A*, vol. 491, p. 129208, 2023.
- [14] C. Pierre and D. Foata, *Problèmes combinatoires de commutation et réarrangements*. Lecture notes in mathematics, Berlin Heidelberg New York: Springer-Verlag, 1969.
- [15] A. Mazurkiewicz, "Concurrent program schemes and their interpretations," *DAIMI Report Series*, vol. 6, Jul. 1977.
- [16] D. Fisher, "The number of words of length  $n$  in a graph monoid," *Am. Math. Monthly*, vol. 96, p. 610–614, Aug. 1989.
- [17] D. Fisher and A. Solow, "Dependence polynomials," *Discrete Mathematics*, vol. 82, no. 3, pp. 251 – 258, 1990.
- [18] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. USA: Wiley-Interscience, 2006.

# Using simulations to validate improvements over Shor's Algorithm

Fábio Santos and Luis Kowada

**Abstract**—There are already a bunch of works presenting a simulation of Shor's algorithm. However, the great majority lacks when it is run against large integers. It happens because the exponential characteristic of the problem requires a huge amount of resources. We propose an approach where we execute all steps of Shor's algorithm. Some steps are adapted to run faster in classical environment. This enabled us to execute a simulation against large integers and being able to get a relevant information. Through simulations, we could validate that using Jacobi symbol improves the Shor's algorithm to require only one order finding execution for some cases.

**Keywords**—Number Theory, Quantum computing, Shor's algorithm.

## I. INTRODUCTION

Shor's algorithm [1] for factoring integers was a breakthrough in computer science as it showed how a quantum computer could be used to factor integers in polynomial time. This algorithm to factor an integer  $N$  is based on a quantum routine to find the order  $r$  of an element that belongs to a group  $Z_N^*$ . Even after almost 30 years, some aspects of the algorithm are still not perfectly understood. Shor proposes some approaches to estimate  $r$  from the results measured in the quantum routine, but testing the algorithm is not an easy task because the access to quantum computers is still scant nowadays. To solve this issue, simulations can be carried out on classical computers.

A simulation is more realistic when it presents the closest circumstances of what is intended to be simulated. If it was not possible to distinguish the simulated situation in relation to the real situation in all its details we would have a perfect simulation. In the context of algorithms, you may want to simulate its execution to check if it works or to extract information regarding its use. Simulating an algorithm is especially useful when it is not possible (or difficult) to execute it in a real situation. This happens, for example, for quantum algorithms. The difficulty of quantum simulations is that, in general, they require exponential time and space, which brings challenges to the simulation process. Some very relevant information can be obtained, for example, the success rate of probabilistic algorithms in the average case. Theoretical results show that Shor's algorithm [1] for factoring integers (QIFA - Quantum Integer Factorization Algorithm) has at least a 50% chance of success if the quantum routine returns the order  $r$  of an integer  $x$  modulo  $N$ , where  $r$  is a smaller natural number such that:

$$x^r \equiv 1 \pmod{N} \quad (1)$$

Fábio Santos, IC, Universidade Federal Fluminense. Este trabalho foi parcialmente financiado por FAPERJ (260003/015313/2021).

However, through some simulations executed in [2], we see different results for probability of success when testing prime numbers with close size and randomly chosen. Simulations can also be very useful not only to corroborate theoretical estimates or extract some information about the execution, but also to refine the algorithm in some cases where details of it have not been well defined or if there is more than one possible approach. In the case of the quantum factorization algorithm, Shor suggests some techniques to estimate the order from the data returned by the quantum routine [1]. The 1<sup>st</sup> technique is to verify the observed state. If the observed state is  $|c\rangle$ , he suggests testing also the values  $c \pm 1$ ,  $c \pm 2$ , and so on. For each possibility,  $r$  is estimated by approximating the fraction  $c/q \approx d/r$ , where  $q$  is the total number of possible states. If the quantum routine returns a peak or a position near to a peak, we should be able to estimate the value for  $r$ . We can also test as candidates for  $r$ , small multiples  $2r'$ ,  $3r'$ , ... This is the 2<sup>nd</sup> technique. As the 3<sup>rd</sup> and last technique, given two candidates  $r_1$  and  $r_2$ , we take  $\text{lcm}(r_1, r_2)$  as a candidate for  $r$ . Having the  $r$  value in hands, we can obtain the factors for a number  $N$ . Simulations could provide us with interesting information like that there is no need to try  $c$  values greater than 1 in the 1<sup>st</sup> technique or that the 3<sup>rd</sup> technique is something so rare to happen that it could be disregarded. Having this kind of information, customized versions of the algorithm can be proposed.

As we can see, simulations can be very helpful. Some works [3], [6] have already proposed simulations for Shor's algorithm, however, they have used few bits. Other works, as [2], have already run simulations against large numbers, but did not execute the simulation as close to the real scenario as we would like. In this work, we propose a simulation able to factoring large numbers executing the steps as closer as possible to the steps proposed in [1]. We also propose a theorem about using Jacobi symbol to achieve a similar result of [8] with a wider set of numbers.

The rest of this work is divided in three more sections. In the second section, we will show different kinds of simulations to test Shor's algorithm, one more fine-grained and other more coarse-grained, the third shows the details of the proposed simulation by this work and its results. Finally, in the last section, we conclude this work with insights and results obtained.

## II. SIMULATIONS APPROACHES

As we saw in the introduction section, simulations can be very helpful to understand and study some classes of algorithms, including quantum algorithms. A simulation of a

quantum program would be more realistic when it reproduces all steps executed by an algorithm in a quantum computer and stores all the necessary information. This type of simulation is possible only for programs involving a few bits, as this type of simulation has an exponential cost. If the purpose of the simulation is to verify whether the program quantum is correct, it would be enough to be able to reproduce its outputs along with the expected probabilities, regardless of the simulation steps. In this context, a more perfect simulation would pass through each intermediate state until reaching the final state and, if possible, spend the same processing time at each step and store all information generated by these steps (fine-grained simulation). But instead of storing all information generated by the algorithm steps, like using a matrix representing these data, we could go from the initial to the final state without going through all the states and even so we would have a satisfactory simulation (coarse-grained). We can say that there are several granularity levels of simulation for a procedure. If the purpose of the simulation was to analyze the propagation of noise in the system, the states intermediaries are important in this case, a simulation that goes from first to the last state (widest level of granularity) might not be useful.

In the case of Shor's algorithm [1] for factorization, we can consider the routine of order estimation (QOFA - Quantum Order Finding Algorithm) as a black box, as was done in [2] or simulate smaller steps of the algorithm. Considering the quantum routine as a black box that returns the order of a number, we can obtain simulation results of arbitrarily large numbers as those used in RSA, for instance, 1024 bits or more. In this way, we can get an estimate of how many successful QOFA executions are necessary, but not how many executions would actually be necessary, since some QOFA executions may not bring relevant information to the problem.

Shor's algorithm simulations that include the QOFA simulation have very few bits. See, for example, [3], [4] with  $N$  being a number with few bits. There is also [6] where they could execute QOFA with numbers about 70/80 bits but they had to provide a large hardware to accomplish their results. The simulation of the algorithm with small numbers may not be realistic in the sense of being a degenerate situation. For example, if the number is very small, there is a high chance of finding a factor randomly. In addition to the level of granularity, another important property is the set of information that simulations use. In general, the strictest simulations, with finer granularity, do not use information other than the inputs of the problem. But there are situations where other information can help with the simulation. For example, it is only possible to simulate factorization for arbitrary wide numbers, knowing their factors in advance, as happens in simulations in [2]. Knowing and using this information does not invalidate the simulation, if the results obtained are similar to those in the real situation.

The purpose of this work is the simulation of Shor's factorization algorithm including the QOFA simulation, so that the values obtained are similar to the values obtained if this routine were executed on an ideal quantum computer. The advantage of this simulation in relation to existing simulations of the finer-grained Shor algorithm is that it allows the simulation of

factoring larger numbers and in relation to the simulations in [2], it is more realistic. The objective of these simulations is to show the behavior of the algorithm of factoring and estimate the number of necessary executions of the QOFA, using different strategies.

### III. PROPOSED SIMULATION

As we mentioned in earlier sections, when we are simulating some algorithm, we can go from a fine-grained approach to another coarse-grained one. There will be pros and cons of choosing one of them. This is certainly also true when applying some simulation for Shor's algorithm. A simulation should try to reproduce the steps as closely as possible from the real ones. The list below shows how we simulate Shor's algorithm step-by-step:

- 1) Check if number  $N$  is a prime or prime power;
- 2) If it isn't, go to step 4;
- 3) Return the prime number and its power;
- 4) Pick a random number  $x$ , where  $x$  must be  $0 < x < N$ ;
- 5) Check if  $\gcd(x, N)$  result is 1;
- 6) If it is 1, go to step 8;
- 7) Return  $\gcd(x, N)$  and  $N/\gcd(x, N)$ ;
- 8) Execute quantum routine to find the order  $r$  (quantum order finding);
- 9) Execute post-processing and validate  $r$  as the order value for  $x$ ;
- 10) If order finding has failed, go back to step 4;
- 11) Return  $\gcd((x^{r/2} - 1), N)$  and  $\gcd((x^{r/2} + 1), N)$ ;

In our work, we are more interested in analyzing what happens in post-processing depending in what  $x$  value is randomly picked in step 4. At this point, it should be clear that we want to execute simulations for values  $N$  where  $N$  is a large integer (at least greater than 128 bits). In this way, if we can suppress some steps or even make them less detailed to accomplish our goal, we should do that. However, suppressing some steps or simplifying them should not compromise the results. Therefore, we would like to show that using the coarse-grained approach will not lose quality when compared to a more fine-grained one. To accomplish this, we created a configurable simulation where we can switch on/off the fine-grained option and, after that, compare results.

Both simulations, coarse-grained and fine-grained, execute the steps as shown in the step-by-step list. The differences between them are isolated in step 8. When we switch on the fine-grained simulation, the first thing we do in this step is build a structure data, such as an array, where we set period markers. The period is defined by the  $x$  element's order calculated during this step. Each position of this structure represents a quantum state and these position values should be between  $N^2$  and  $2N^2$  [1]. After this, we execute a Fast Fourier Transform on these data. The Fast Fourier Transform will set amplitudes for each of these quantum states and we can then calculate the probabilities. We use the calculated probabilities to pick one of these simulated quantum state positions and execute the post-processing step.

Executing step 8 as described before in a fine-grained approach requires a great amount of memory and processing

time. It requires a great amount of memory because as the number  $N$  becomes greater, the number of states grows exponentially. This also happens with processing time to find the  $x$  element's order. There is no known polynomial algorithm to do that. Because of this, if we also want to execute simulations for large integers, we have to switch off the fine-grained option.

In our coarse-grained approach, we do not use a data structure to store information about period markers and we also do not execute Fast Fourier Transform aiming to get amplitudes. We, instead, calculate directly some simulated quantum state position related to a peak. As Shor describes in his work [1], when a Quantum Fast Fourier Transform is executed over a register in superposition, the output generated by this procedure is a set of amplitude data with some points with higher amplitudes (peaks). The number of peaks is equal to  $r$ , where  $r$  is the  $x$  element's order. We can establish a relation between the number of states and the number of peaks. We are going to call this offset. If we know the number states and the  $r$  value, we can calculate the quantum states that correspond to a peak. This way, we replace the quantum order finding routine and calculate some peak values randomly. It solves the problem related to memory space (memory) but not the processing time one (order algorithm). The solution for the order problem is based on restrictions we set in our simulation. We use only safe primes during our simulations. This restriction should not be a problem as we are going to see in simulation results. Through simulation results, we could see that the chance of success when running the test of Shor, for  $x$  chosen at random and  $N$  being a product of two safe primes, is approximately 50%. This is equal to the lower bound described by Shor when finding the nontrivial factors of  $N$  [1]. In other words, this would be the worst case for the Shor's algorithm. Another work we can mention is [8]. In this work, the author improves the Shor's algorithm to require approximately only one execution of QOFA when using safe primes as factors of  $N$ .

The number  $N$  used in our simulation is composed of two safe primes. A safe prime is a number in the format  $p = 2p' + 1$ , where  $p'$  is also a prime number. By Lagrange's theorem, when we get an element  $x$  from a multiplicative group  $Z_N^*$ , the element's order must divide the group's order. A group's order is the number of elements of a group. It can be calculated by Euler's Totient Function. The value of Euler's Totient Function for a prime number  $p$  is  $p - 1$  in  $Z_p$ . If we combine these two definitions, safe primes and group's order, we can see that 2 divides the group's order when the group is generated modulo a safe prime ( $p' = (p - 1)/2$ ). It makes the possible values for these group's order the small set of values  $1, 2, p', 2p'$ . To finish the approach, we need one last additional information. When we have a number  $N = p \cdot q$ , the order  $r$  of some group  $Z_N$  is  $\text{lcm}(rp, rq)$ , where  $rp$  is the order for a element  $x$  in a group  $Z_p^*$  and  $rq$  is the order for a element  $x$  in a group  $Z_q$ . It makes our possible group's order values go from  $1, 2, p', 2p'$  to  $1, 2, p', q', 2p', 2q', 2p'q'$ . So, instead of executing an algorithm to find the element's order, we only check the values in this group.

### A. Comparing fine-grained against coarse-grained

As we mentioned before in the section 3, we want to execute the simulation for large values and to do that, we should execute the coarse-grained option. It implies suppressing some steps or simplifying them without compromising the results. To check if the coarse-grained option does not compromise the results, we must execute both simulations and compare them. To help us making these comparisons, we defined some classifications for simulation results:

TABLE I  
Classification kinds.

Kind	Description
LUCKY-RANDOM-VALUE	The $x$ random value obtained is factor of $N$
GOOD-ROUNDING	The value returned by quantum order find simulation (peaks) was used to get factors without adjustments
SHOR-1	The value returned by quantum order find simulation (peaks) had to be adjusted for close values to get factors
SHOR-2	The value returned by quantum order find simulation (peaks) divides the $x$ element's order
SHOR-3	The $x$ element's order is obtained from lcm between two quantum order find executions
NO-SOLUTION-FOUND	The simulation was not able to get factors of $N$

We arrange the set of values 23, 47, 59, 83, 179 and create composite numbers through combinations of 2 elements of this set. After that, we execute both simulations. We chose this set for two reasons. The first one is because they are safe primes and even though this is not mandatory for the fine-grained approach, we must execute the coarse-grained option only with numbers composed of safe primes. The second one is because as the fine-grained option requires a lot of computing resources, we must avoid large integers in this situation.

After defining a way to compare both simulations, we executed them and get the following results: GOOD-ROUNDING - 48% of results were classified as GOOD-ROUNDING in coarse-grained against 46% in fine-grained simulation - LUCKY-RANDOM-VALUE - 11% of results were classified as LUCKY-RANDOM-VALUE in coarse-grained against 6% in fine-grained simulation - SHOR-2 - 40% of results were classified as SHOR-2 in coarse-grained against 46% in fine-grained simulation - SHOR-1 and SHOR-3 - 1% of results were classified as combination of SHOR-1 and SHOR-3 in coarse-grained and 2% were classified as SHOR-3 in fine-grained simulation - NO-SOLUTION-FOUND - There was no result classified as NO-SOLUTION-FOUND.

Analyzing the results of both simulations, we can see that there is no great qualitative differences between them and both were able to find the factors for all inputs. Therefore, we can consider that coarse-grained option does not compromise the results and we can use it to execute simulation for large numbers.



TABLE II

Classification results when running simulation. The input set is a combination of 2 elements of numbers 23, 47, 59, 83, 179.

classification kind	fine-grained	coarse-grained
GOOD-ROUNDING	46%	48%
LUCKY-RANDOM-VALUE	6%	11%
SHOR-2	46%	40%
SHOR-3	2%	0%
SHOR-1 and SHOR-3	0%	1%

### B. Executing against large numbers

Besides the qualitative results, we also generated a set of large numbers with 128, 512 and 1024 bits, where factors are safe primes. Using the openssl application [5], we could generate these safe primes through the command `openssl prime -bits number-of-desired-bits -safe -generate`. The parameter *number-of-desired-bits* was set with values 64, 256 and 512 respectively. We generated 820 composed numbers with these safe prime factors. For all composed number in the list, we executed the simulation until it returns the factors for the current composed number.

TABLE III

Large numbers factoring for  $x$  randomly chosen. SAA STANDS FOR SUCCESSFULLY ATTEMPTS AVERAGE AND MSA STANDS FOR MAX SUCCESSFULLY ATTEMPTS.

bits	SAA	MSA
128 bits	2.01	10
512 bits	2.00	9
1024 bits	2.07	10

Through simulation results, we can see that they are totally compliant with the theoretical results [1] and other simulation results [2]. Using the original Shor's proposal [1], it is necessary run, in average, twice to get the factors of some composed number  $N$ . Another interesting result we can see is that the maximum number of tries is closer to 10 as in [2].

It is important to emphasize that our simulation simplify some steps from Shor's algorithm. However, the entire post-processing procedure is executed as expected in a real situation. This way, we can focus in the order estimation and how the choice of the random value can influence in results for large numbers with until 1024 bits.

### C. Using Jacobi Symbol approach

Jacobi Symbol is a generalization of Legendre symbol. Both belongs to the field of number theory. Jacobi Symbol is also known as quadratic residue. The concept behind quadratic residues is that given two co-prime integers  $x$  and  $p$ ,  $x$  is a quadratic residue modulo  $p$  if there is some  $y$  value that satisfies  $y^2 \equiv x \pmod{p}$  (Jacobi Symbol = 1). Au contrair, if there is no  $y$  value that satisfies this congruence, we say  $x$  is a quadratic non-residue modulo  $p$  (Jacobi Symbol = -1).

*Theorem 1:* Let  $N = p \cdot q$ , where  $p$  and  $q$  are prime numbers. Further, let  $p = 2^c \cdot u + 1$  and  $q = 2^c \cdot v + 1$ , where

$u$  and  $v$  are integers and  $c$  is a constant. For all  $x \in \mathbb{Z}_N^*$ , where  $\gcd(x, N) = 1$  with  $x > 1$ , we have:

$$\text{If Jacobi Symbol}(x, N) = -1 \text{ then} \\ 1 < \gcd(x^{r/2} - 1, N) < N$$

*Proof:* The Jacobi Symbol (JS) of  $x$  with  $N = p \cdot q$  can be represented as a product of two Legendre Symbol (LS) of  $x$  with  $p$  and  $y$  with  $q$ . In this way, given any integer  $x$  and any positive odd integer  $N$ , we can substitute  $JS(x, N)$  for  $LS(x, p) \cdot LS(x, q)$ , where  $N = p \cdot q$  with  $p$  and  $q$  being odd primes. By definition of Legendre Symbol, we know that the result of  $LS(a, b) \in \{-1, 0, 1\}$ . So, if we have  $JS(x, N) = -1$ , then  $\{LS(x, p) = 1 \text{ and } LS(x, q) = -1\}$  or  $\{LS(x, p) = -1 \text{ and } LS(x, q) = 1\}$ .

Without loss of generality, we suppose  $LS(x, p) = 1$  and  $LS(x, q) = -1$ . In this case, with  $LS(x, p) = 1$  we have  $r_p = \text{ord}(x, p)$  divides  $\frac{p-1}{2} = 2^{c-1}u$ , where  $\text{ord}(x, p)$  is the order of  $x$  modulo  $p$ . Then  $2^c \nmid r_p$  and  $\gcd(2^c, r_p) < 2^c$ .

On the other hand,  $LS(x, q) = -1$  implies that  $r_q = \text{ord}(x, q)$  does not divide  $\frac{q-1}{2} = 2^{c-1}v$ . It means  $2^c \mid r_q$ . In other words,  $\gcd(2^c, r_q) = 2^c$ .

Taking into account that  $r = \text{ord}(x, N) = \text{lcm}(r_p, r_q)$  (see Lemma 2.3 in [2]), so we have  $\gcd(r, 2^c) = 2^c$ . Therefore,  $r/2$  is multiple of  $r_p$ , but  $r/2$  is not multiple of  $r_q$ . In this way,  $x^{r/2} \equiv 1 \pmod{p}$  but  $x^{r/2} \not\equiv 1 \pmod{q}$ . It means that  $x^{r/2} - 1$  is multiple of  $p$  but is not multiple of  $q$ . As  $N = p \cdot q$  then  $\gcd(x^{r/2} - 1, N) = p$ . ■

TABLE IV

Large numbers factoring for  $x$  randomly chosen but using Jacobi Symbol to select them. SAA STANDS FOR SUCCESSFULLY ATTEMPTS AVERAGE AND MSA STANDS FOR MAX SUCCESSFULLY ATTEMPTS.

bits	SAA	MSA
128 bits	1.00	1
512 bits	1.00	1
1024 bits	1.00	1

Taking into account this theorem, if we test the random value used in QOFA routine and call the QOFA only when this random value has Jacobi Symbol = -1, we should always be able to get factor for some  $N$  value. In [7], the author proposes a improvement in Shor's algorithm using Jacobi Symbol to evaluate the random value that is used by QOFA. Through our simulation approach, we can verify this behavior for large numbers. In fact, we can see there is an improvement in the success rate. The success rate is even better than that mentioned by this work (from 3/4 to 1). However, as we have already mentioned, we used only safe primes in our simulations.

## IV. CONCLUSIONS

Our target was to build a simulation where we could test Shor's algorithm executions for large numbers and also trying to verify some already known assumptions and get new information. In fact, we were able to verify some already known results such as the average number of executions

necessary to obtain the factors of a composite number and also verify new stuff. For instance, we could verify that using Jacobi symbol to select the  $x$  random value in Shor's algorithm makes a improvement in the QOFA's success rate. When we do that, the procedure requires the QOFA routine be executed only once. It is a really good result. This result is very similar the result achieved by [8]. However, based on theorem 1, our proposal is wider because it is not restricted to  $N = p_1 \cdot p_2 = (2q_1 + 1)(2q_2 + 1)$ , with  $q_1 \neq q_2$  and  $q_1, q_2 > 2$ . Instead, our result proposes  $N = p \cdot q = (2^c \cdot u + 1)(2^c \cdot v + 1)$ , where  $u$  and  $v$  are integers, with  $c$  being a constant.

#### REFERENCES

- [1] Shor, Peter W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM review, 41, 2, 303–332, 1999, SIAM
- [2] Chicayban Bastos, Daniel and Kowada, Luis Antonio, How to detect whether Shor's algorithm succeeds against large integers without a quantum computer, Procedia Computer Science, 195, 145–151, 2021, Elsevier
- [3] David S Wang, Charles D Hill, and Lloyd CL Hollenberg. Simulations of Shor's algorithm using matrix product states. Quantum Information Processing, 16:1–13, 2017.5
- [4] Tankasala A, Ilatikhameneh H. Quantum-kit: simulating shor's factorization of 24-bit number on desktop. arXiv preprint arXiv:1908.07187. 2019 Aug 20.
- [5] OpenSSL Homepage, <https://www.openssl.org>. Last accessed 22 Oct 2023
- [6] Willsch D, Willsch M, Jin F, De Raedt H, Michielsens K. Large-Scale Simulation of Shor's Quantum Factoring Algorithm. Mathematics. 2023 Oct 9;11(19):4222.
- [7] Leander G. Improving the Success Probability for Shor's Factoring Algorithm. arXiv preprint quant-ph/0208183. 2002 Aug 29.
- [8] Grosshans F, Lawson T, Morain F, Smith B. Factoring safe semiprimes with a single quantum query (2015).

# Implementação de Passeios quânticos a tempo contínuo nos Computadores Quânticos da IBM

Frank Acasiete e Renato Portugal

**Resumo**—Neste trabalho, descrevemos a implementação de caminhadas quânticas a tempo contínuo em um grafo bipartido completo com um vértice marcado usando computadores quânticos da IBM. Comparamos os resultados obtidos do simulador quântico com aqueles do computador quântico. Nosso estudo não só contribui para o crescente corpo de pesquisa em algoritmos quânticos, mas também destaca a importância da otimização cuidadosa ao nível de portas para a computação quântica prática.

**Palavras-Chave**—Passeios Quânticos, Computação Quântica, Qiskit, Grafos, Circuito Quântico.

**Abstract**—In this work, we describe the implementation of continuous-time quantum walks on a complete bipartite graph with a marked vertex using IBM quantum computers. We compare the results obtained from the quantum simulator with those from the quantum computer. Our study not only contributes to the growing body of research in quantum algorithms but also highlights the importance of careful gate-level optimization for practical quantum computing.

**Keywords**—Quantum Walks, Quantum Computing, Qiskit, Graphs, Quantum Circuit.

## I. INTRODUÇÃO

Nos últimos anos, observou-se um crescimento significativo nas pesquisas relacionadas à computação quântica. Embora os computadores quânticos ofereçam uma vantagem exponencial para certos problemas, é importante notar que eles apresentam ruídos, sendo conhecidos pela sigla em inglês "NISQ" (Noise Intermediate-Scale Quantum - Escala Intermediária de Ruído Quântico). Esses computadores ainda não atingiram um estágio suficientemente avançado para alcançar a supremacia quântica e serem tolerantes a erros. Estudos em diversas áreas já foram conduzidos utilizando esses computadores, como exemplificado por [1] na área da química e [2] na área da medicina.

No campo da pesquisa sobre passeios quânticos a tempo discreto, destacamos os trabalhos utilizando o modelo de passeios quânticos escalonados ("SQW", Staggered Quantum Walks em inglês) [3]. Na abordagem de tempo contínuo, destacam-se estudos como o de [5], que explora passeios com busca para um elemento marcado. Além disso, [6] realiza um estudo sobre passeios quânticos a tempo contínuo usando a base da distribuição de momentos. Em [7], é apresentado um estudo utilizando o Qiskit para a implementação de passeio quântico a tempo contínuo em um grafo completo com um elemento marcado.

Frank Acasiete, Senai-Cimatec, Salvador-BA, e-mail: frank.quispe@fbter.org.br; Renato Portugal, COMAC, LNCC, Petrópolis-RJ, e-mail: portugal@lncc.br.

Este trabalho está estruturado da seguinte forma: na Seção I-A, apresentamos conceitos básicos relacionados ao estudo; na Seção II, abordamos a parte teórica da implementação do circuito quântico em um grafo bipartido completo com elemento marcado; na Seção III, exibimos os resultados obtidos usando o Qiskit para o caso de 3 qubits nos computadores quânticos da IBM; e, por fim, na Seção IV, apresentamos algumas conclusões derivadas deste trabalho.

### A. Grafos

Nesta seção, apresentamos algumas definições da teoria de grafos para melhor compreensão do tema. Para outras definições, consulte [8], [9].

**Definição 1.1 (Grafo):** Um **grafo** é representado pelo par ordenado  $G = (V, E)$ , onde:

- $V$  é o conjunto não vazio de objetos chamados vértices.
- $E \subseteq \{\{x, y\} \mid x, y \in V, x \neq y\}$  é o conjunto de arestas.

**Definição 1.2 (Grafo completo):** Um **grafo completo** é um grafo não direcionado simples no qual cada par de vértices distintos é conectado por uma única aresta.

Isso significa que, para um grafo completo com  $n$  vértices, cada vértice está ligado diretamente a todos os outros  $n - 1$  vértices.

**Definição 1.3 (Grafo bipartido):** Um grafo  $G = (V, E)$  é **bipartido** se o conjunto de vértices  $V$  pode ser separado em dois conjuntos disjuntos  $U$  e  $V$  tais que:

- $U \cup W = V$
- $U \cap W = \emptyset$

Além disso, as arestas só podem conectar vértices de um conjunto com vértices do outro. Isso significa que, para todo  $u_1, u_2 \in U$  e  $w_1, w_2 \in W$ , não existem arestas  $(u_1, u_2)$  ou  $(w_1, w_2)$  no grafo  $G$ .

**Definição 1.4 (Grafo bipartido completo):** Um **grafo bipartido completo**  $G = (V_1 \cup V_2, E)$  é um grafo bipartido tal que, para todo  $v_1 \in V_1$  e  $v_2 \in V_2$ ,  $v_1 v_2$  é uma aresta em  $G$ . Em outras palavras, um grafo bipartido completo é formado por dois conjuntos disjuntos de vértices, e todas as arestas possíveis que conectam esses vértices estão presentes no grafo. Este grafo, com partições de tamanho  $|V_1| = m$  e  $|V_2| = n$ , é denotado por  $K_{m,n}$ .

Na Fig. 1 temos um exemplo deste tipo de grafo que é o objeto de nosso estudo. O conjunto  $U$  seriam os vértices rotulados por 1, 2, 3, 4, 5 e  $V$  é formado por A, B, C e D.

**Definição 1.5 (Matriz de adjacência):** A **matriz de adjacência**  $A(G)$  de um grafo  $G = (V, E)$  com  $n$  vértices é uma matriz  $n \times n$  definida da seguinte forma:  $A(G)_{ij} = 1$  se  $(v_i, v_j) \in E$  e  $A(G)_{ij} = 0$  caso contrário.

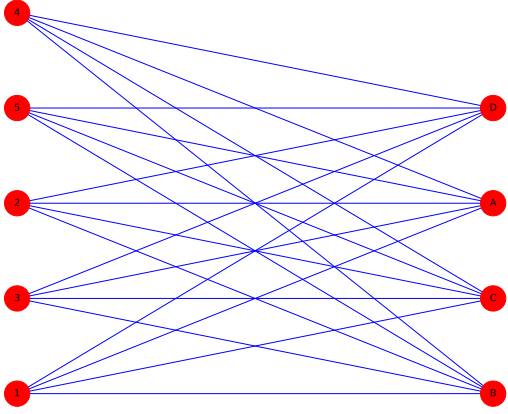


Fig. 1. Grafo bipartido completo. Fonte: gerada pelo autor.

Uma matriz de adjacência é uma das formas de representar um grafo. Dado um grafo  $G$  com  $n$  vértices, podemos representá-lo em uma matriz  $n \times n$ , denotada por  $A(G) = [a_{ij}]$  ou simplesmente  $A$ . A definição precisa das entradas da matriz varia de acordo com as propriedades do grafo que se deseja representar. Em geral, o valor  $a_{ij}$  contém informações sobre como os vértices  $v_i$  e  $v_j$  estão relacionados, ou seja, informações sobre a adjacência entre  $v_i$  e  $v_j$ .

## II. PASSEIOS QUÂNTICOS A TEMPO CONTÍNUO

Os algoritmos para passeios quânticos a tempo contínuo (CTQW, Continuous Time Quantum Walk) são uma classe de passeios quânticos projetados para localizar rapidamente um vértice marcado  $\omega \in V$  a partir de um estado inicial. Em nosso contexto, consideramos um grafo bipartido completo, onde um vértice específico é designado como marcado. A taxa de transição quântica é representada por  $\gamma$ .

Para este cenário, empregamos o Hamiltoniano

$$\mathcal{H} = -\gamma A - |\omega\rangle\langle\omega|. \quad (1)$$

proposto em [5], que descreve os níveis de energia do passeio e consequentemente gera a evolução temporal do passeio. Esse Hamiltoniano é fundamental para modelar as transições entre os vértices do grafo e incorporar os efeitos quânticos que permitem ao passeio encontrar eficientemente o vértice marcado.

Denotamos o tempo de execução ideal por  $t_{\text{opt}}$ , que serve para o cálculo da eficiência do algoritmo. Nosso objetivo é minimizar  $t_{\text{opt}}$  e maximizar a probabilidade de sucesso  $p_{\text{succ}} = |\langle\omega|\psi(t_{\text{opt}})\rangle|^2$ . Nesse contexto,  $|\psi(t)\rangle$  é calculado através da equação

$$|\psi(t)\rangle = (e^{-i\mathcal{H}t})|\psi(0)\rangle, \quad (2)$$

onde  $\mathcal{H}$  é o hamiltoniano modificado mostrado na Eq. (2) e  $|\psi(0)\rangle$  é a condição inicial definida como segue

$$|\psi(0)\rangle = |s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle, \quad (3)$$

onde  $N$  é o número de vértices do grafo. Lembrando que nos CTQW o tempo é contínuo e o espaço é discreto.

### A. Passeio quântico em um grafo bipartido completo

Esse passeio quântico pode ser referido como um modelo teórico que descreve como uma partícula quântica se propaga ou evolui em um grafo bipartido completo. Tal modelo tem potenciais aplicações em problemas que envolvem a exploração de relações ou conexões entre elementos de dois conjuntos distintos. Ao aproveitar as propriedades quânticas, esse tipo de modelo pode ser utilizado para realizar cálculos de maneira eficiente ou para resolver problemas específicos em contextos bipartidos.

Dado um grafo completo bipartido  $K_{n,n}$  com  $N = 2n$  vértices, rotulamos os vértices de uma partição de  $0, \dots, (N/2) - 1$  e, na outra partição, de  $N/2, \dots, N - 1$ . Definindo  $\hat{A}$  como

$$\hat{A} = H^{\otimes m} A H^{\otimes m}, \quad (4)$$

onde  $H$  é a matriz de Hadamard,  $m$  a quantidade de qubits usados e  $A$  a matriz adjacência, obtemos

$$\hat{A} = n|0\rangle\langle 0| - n|n\rangle\langle n|, \quad (5)$$

os autovalores, representados por  $\lambda^\pm = \pm n \neq 0$ , correspondem aos autovetores  $|\lambda^+\rangle = |0\rangle$  e  $|\lambda^-\rangle = |n\rangle$ . Vamos adotar o mesmo valor de  $\gamma$  usado na referência [10], dado por  $\gamma = \frac{1}{n}$ . O operador de evolução é neste caso

$$U_{K_{n,n}}(t) = e^{i\gamma\hat{A}t} = H^{\otimes m} e^{it|0\rangle\langle 0|} e^{-it|n\rangle\langle n|} H^{\otimes m}. \quad (6)$$

No caso de um vértice marcado o Hamiltoniano modificado é

$$\bar{\mathcal{H}}_{K_{n,n}} = -H^{\otimes m}(|0\rangle\langle 0| - |n\rangle\langle n|)H^{\otimes m} - |\omega\rangle\langle\omega|, \quad (7)$$

onde  $\omega$  é o vértice marcado. Este Hamiltoniano tem três autovalores,  $\lambda^-, \lambda^+, \lambda_0 \neq 0$ , que são as soluções da equação

$$\lambda^3 + \lambda^2 - \lambda - \left(1 - \frac{1}{n}\right) = 0, \quad (8)$$

cumprindo o seguinte:  $\lambda^- < \lambda^+ < \lambda_0$ .

Os projetores  $|\lambda^+\rangle\langle\lambda^+|$ ,  $|\lambda^-\rangle\langle\lambda^-|$  e  $|\lambda_0\rangle\langle\lambda_0|$  comutam, com isto o operador de evolução  $\bar{U}_{K_{n,n}}(t)$  deste passeio quântico com um vértice marcado se reduz a [10]

$$\bar{U}_{K_{n,n}}(t) = e^{-it\lambda_0|\lambda_0\rangle\langle\lambda_0|} e^{-it\lambda^+|\lambda^+\rangle\langle\lambda^+|} e^{-it\lambda^-|\lambda^-\rangle\langle\lambda^-|}. \quad (9)$$

O tempo ótimo de execução para  $m$  qubits é

$$t_{\text{opt}}^{K_{n,n}} = \left\lfloor \frac{\pi}{2} \sqrt{N} \right\rfloor, \quad (10)$$

onde  $N = 2n = 2^m$ .

Usamos a identidade

$$e^{itP} = I + (e^{it} - 1)P, \quad (11)$$

para qualquer projetor ortogonal  $P$ , com isto obtemos:

$$\bar{U}_{K_{n,n}}(t) = e^{-it/N} A_{\lambda_0} R_{\lambda_0} A_{\lambda_0}^\dagger A_{\lambda^+} R_{\lambda^+} A_{\lambda^+}^\dagger A_{\lambda^-} R_{\lambda^-} A_{\lambda^-}^\dagger, \quad (12)$$

onde

$$R_\lambda = I + (e^{-it\lambda} - 1)|0\rangle\langle 0|, \quad (13)$$

e

$$A_\lambda|0\rangle = |\lambda\rangle, \quad (14)$$

onde  $\lambda$  é a raiz da Eq. (9) e  $|\lambda\rangle$  é o autovetor associado.

### III. IMPLEMENTAÇÃO NOS COMPUTADORES QUÂNTICOS DA IBM

Apresentamos os resultados de um passeio quântico a tempo contínuo em um grafo bipartido completo de 8 vértices, com um elemento marcado e um estado inicial  $|0\rangle$ . Para o caso específico de  $m = 3$  qubits, o tempo ótimo de execução,  $t_{\text{opt}}$ , é aproximadamente 4.44.

A Eq. (13) descreve a decomposição do operador de evolução  $\bar{U}_{K_{n,n}}(t)$  em uma sequência de operadores mais simples que podem ser decompostas em portas elementares. Os operadores  $A_\lambda$  têm o propósito de projetar o estado inicial da partícula no autovetor associado ao autovalor  $\lambda$ . Esses autovalores  $\lambda$  são soluções da Eq. (9). No contexto de um passeio quântico contínuo em um grafo bipartido completo, os autovalores  $\lambda^\pm$  são dados por  $\lambda^\pm = \pm n$ , onde  $n$  é o número de qubits utilizados.

Para o caso específico de  $m = 3$  qubits, o tempo ótimo de execução,  $t_{\text{opt}}$ , é aproximadamente 4.44. Este tempo é crucial para que a partícula alcance uma superposição uniforme entre os dois autovetores associados aos autovalores  $\lambda^\pm$ .

A Fig. 2 mostra o circuito da Eq. (13) com  $U_1 = e^{-it\lambda^-/2}R_z(-t\lambda^-)$ ,  $U_2 = e^{-it\lambda^+/2}R_z(-t\lambda^+)$  e  $U_3 = e^{-it\lambda_0/2}R_z(-t\lambda_0)$ . Os ângulos  $\theta$  descritos na figura 3 relativos aos operadores  $R_y(\theta)$ , quando  $\omega = 0$  são dados em [10].

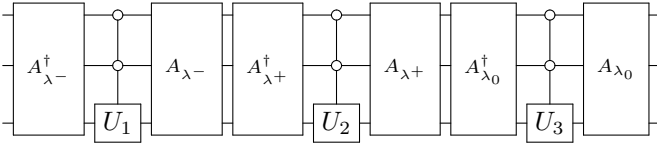


Fig. 2. Circuito do operador evolução  $\bar{U}_{K_{n,n}}(t)$  para um grafo bipartido completo  $K_{n,n}$  com elemento marcado, para  $n = 4$ .

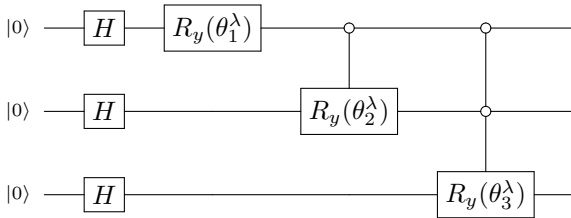


Fig. 3. Circuito que implementa  $A_\lambda$  para  $m = 3$ .

A Fig. 4 mostra os resultados da nossa implementação para a evolução do passeio quântico para os tempos  $t = 1, 2, 3$  e a Tabela I mostra as respectivas fidelidades, onde  $h^2 = \frac{1}{2} \sum_x (\sqrt{p_x} - \sqrt{q_x})^2$  é a distância de Hellinger, sendo  $p$  a distribuição de probabilidades da simulação e  $q$  do computador quântico.

Na Fig. 4, podemos observar que os resultados até o segundo passo mostram o elemento marcado localizado na posição 0. No entanto, no terceiro passo, observamos uma redução significativa na fidelidade, devido ao tamanho do circuito e à sua profundidade. Essa redução na fidelidade é uma característica comum em computadores quânticos do tipo NISQ, devido à sua natureza limitada.

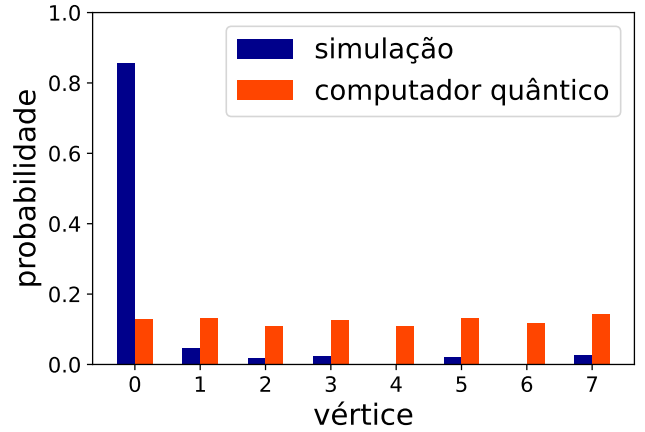
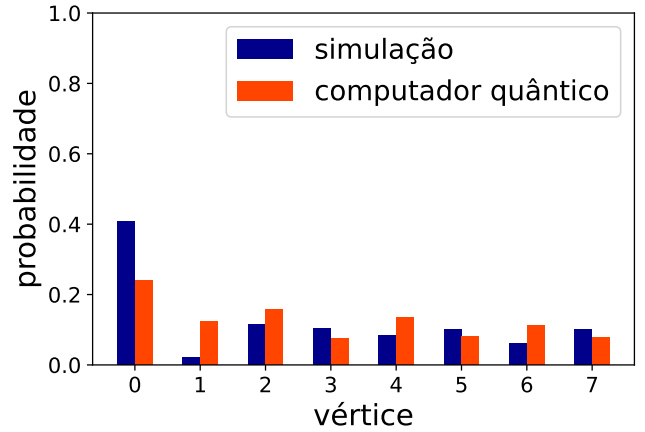
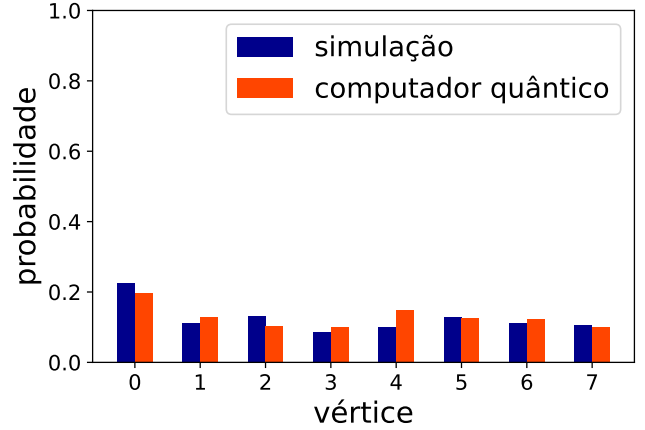


Fig. 4. Evolução de um passeio quântico a tempo contínuo com elemento marcado em um grafo bipartido completo de 8 vértices.

### IV. CONCLUSÕES

- No caso da implementação para o cenário contínuo, procedemos de forma semelhante ao caso a tempo discreto, conforme foi feito em [3], uma vez que o espaço também é discreto nos passeios quânticos a tempo contínuo. Ou seja, discretizamos o tempo e repetimos sistematicamente a aplicação do operador de evolução. Decidimos implementar desta forma porque é essencial acompanhar a evolução ao longo do tempo.
- Realizamos a implementação do operador de evolução de um passeio quântico contínuo em um grafo bipartido

TABELA I

FIDELIDADES DE UM PASSEIO QUÂNTICO A TEMPO CONTÍNUO COM ELEMENTO MARCADO EM UM GRAFO BIPARTIDO COMPLETO DE 8 VÉRTICES.

Fidelidade	Passo 1	Passo 2	Passo 3
$1 - h$	0.993	0.973	0.657

completo com oito vértices, alcançando uma fidelidade superior a 90% nos dois primeiros passos. No entanto, observamos uma considerável diminuição na fidelidade nos passos seguintes.

## REFERÊNCIAS

- [1] I. Miháliková, M. Friák, M. Pivoluska, M. Plesch, M. Saip e M. Sob *Best-Practice Aspects of Quantum-Computer Calculations: A Case Study of the Hydrogen Molecule*. *Molecules*, v. 27(3), 597, 2022.
- [2] S. Moradi, C. Brandner, C. Spielvogel e et al., *Clinical data classification with noisy intermediate scale quantum computers*. *Sci Rep*, v. 12, 1851 2022.
- [3] F. Acasiete, F.P. Agostini, J.K. Moqadam e R. Portugal, *Implementation of quantum walks on IBM quantum computers*. *Quantum Inf Process*, v. 19, 426, 2020. 1986.
- [4] R. Portugal, *Quantum Walks and Search Algorithms*. Springer, 2018.
- [5] A. M. Childs e J. Goldstone, *Spatial search by quantum walk*. *Phys. Rev. A*, v. 70, 022314, 1986.
- [6] M. Delvecchio, C. Groiseau, F. Petiziol, G. Summy e S. Wimberger, *Quantum search with a continuous-time quantum walk in momentum space*. *Phys. B: At. Mol. Opt. Phys*, v. 53, 065301, 2020.
- [7] F. Acasiete e R. Portugal, *Poster: Passeios Quânticos Contínuos usando Qiskit*. 1º Encontro Regional de Grupos de Pesquisa em Computação e Informação Quântica (1º EGPCIQ), 2023.
- [8] J. Trudeau, *Introduction to Graph Theory*. Dover Publications, v. 2, 1994.
- [9] D. West, *Introduction to graph theory*. Rashtriya Printers, v. 2, 2001.
- [10] R. Portugal e J. Khatibi, *Implementation of Continuous-Time Quantum Walks on Quantum Computers*. ArXiv abs/2212.08889, 2022.

# Jogos Quânticos: Uma Análise dos Simuladores Quânticos em Jogos Interativos

**Resumo**— Este estudo tem o objetivo de entender como a computação quântica pode influenciar o desenvolvimento de jogos, sejam eles com foco educativo ou não. Foram selecionados 7 jogos que tiveram uma alta aparição em outros artigos e discussões sobre o tema. Cada jogo abrangeu um ou mais conceitos da computação quântica, tais como a superposição, o emaranhamento, a medida e a ideia de circuitos quânticos. Ao final realizamos uma análise dos principais focos de cada jogo e de seu desenvolvimento.

**Palavras-Chave**— Computação Quântica, Jogos Quânticos, Tecnologia Educacional, Soluções de Jogos Inovadoras.

**Abstract**— This study aims to understand how quantum computing can influence the development of games, whether they have an educational focus or not. WE have selected 7 games that had a high appearance in other articles and discussions on the topic. Each game covered one or more quantum computing concepts, such as superposition, entanglement, measurement, and the idea of quantum circuits. At the end, we carried out an analysis of the main focuses of each game and its development.

**Keywords**— Quantum Computing, Quantum Games, Educational Technology, Innovative Game Solutions.

## I. INTRODUÇÃO

A computação quântica (CQ) [6] é uma área que se baseia em conceitos da física quântica, possibilitando solucionar cálculos/problemas complexos de maneira mais rápida e eficaz que a computação clássica. Na CQ temos como unidade base de informação os qbits, os quais diferentemente dos bits clássicos, conseguem assumir os valores binários de 0 ou 1 simultaneamente [14]. Através dessa definição, é possível aumentar o desempenho das operações via paralelismo. Porém, um custo de maior complexidade espacial é exigido ao adicionar novos qbits [4].

O mercado de computação quântica será provavelmente o maior contribuinte para o mercado de tecnologias quânticas, já que previsões otimistas sugerem que a receita do mercado tem potencial para atingir 93 bilhões de dólares americanos até 2040. Outros segmentos no mercado de tecnologias quânticas incluem detecção e comunicações quânticas. A seguir, é apresentado na Figura 1, um gráfico mostrando a evolução do mercado<sup>1</sup>.

A CQ tem expandido suas aplicações, alcançando diversas áreas do conhecimento, incluindo os jogos eletrônicos. Essa tecnologia tem potencial para revolucionar o desenvolvimento de jogos, seja na melhoria gráfica com placas de vídeo que incorporam princípios quânticos para realçar efeitos visuais [13], ou no uso direto da CQ para criar jogos que introduzam conceitos fundamentais aos ingressantes da área.

<sup>1</sup>FONTE: <https://www.statista.com/topics/9647/quantum-computing/>

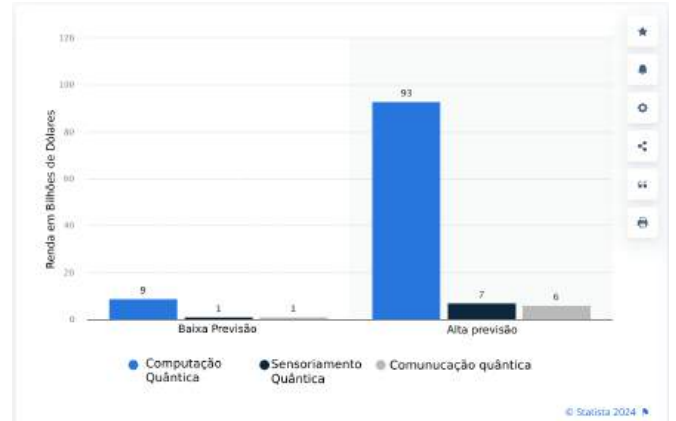


Fig. 1: Evolução do investimento em CQ.

Nessa linha de pensamento, esse estudo tem a intenção de apresentar e analisar alguns jogos que abordem a CQ seja de maneira educativa ou não [8]. Com isso visamos entender como esses jogos podem influenciar o nosso entendimento sobre o desenvolvimento de jogos eletrônicos, em uma área tão recente e de extrema importância atual.

O trabalho está organizado da seguinte forma: Na Seção II os conceitos-base são introduzidos. Em seguida, na Seção III, os jogos analisados são apresentados e discutidos. A Seção IV mostra uma comparação geral dos jogos analisado. Por fim, na Seção V, as conclusões do trabalho são feitas.

## II. PRELIMINARES EM COMPUTAÇÃO QUÂNTICA

Para a compreensão dos jogos que serão apresentados é preciso entender alguns conceitos e termos da CQ, sendo eles a medida, a superposição, o emaranhamento e, em conjunto com esses conceitos, as portas lógicas quânticas que também serão fundamentais para os jogos. É importante mencionar que cada jogo abrangeu um ou mais dos termos citados em sua mecânica de jogabilidade.

- **Superposição:** Um conceito relevante da CQ [14], que diferentemente da computação clássica onde bits podem assumir apenas dois estados, "0" ou "1", na CQ temos os qbits ou bits quânticos. Esses qbits permitem, além dos estados citados, entrar em superposição de estados, podendo assumir os valores "0" e "1", simultaneamente. Dada essa propriedade dos computadores quânticos, uma das principais vantagens deles é o processamento inerentemente paralelo, dado que os próprios qbits operam em paralelo através deste conceito.
- **Emaranhamento:** Um fenômeno da teoria quântica em que se duas partículas interagem e, em seguida, são separadas, então a medição de uma das partículas determina

os valores os quais as propriedades (como o momento e a posição) da outra partícula devam assumir. Este fenômeno foi observado por Einstein, Podolsky e Rosen em 1935 [2]. Este fato ocorre mesmo quando as partículas são separadas espacialmente ou não estão interagindo no momento da medição [16]. Este conceito de estados emaranhados desempenham um papel relevante na CQ e na informação quântica [7], [10] e [5].

- **Medida:** é a base para o funcionamento de todo o e qualquer circuito quântico, por ser com ela que podemos trazer o mundo quântico ao mundo clássico. Através da medida que é possível adquirir a informação sobre qualquer qubit, o resultado desse processo é sempre probabilístico, então o resultado será dado mediante uma probabilidade de o qubit estar naquele determinado estado medido [11].
- **Portas lógicas:** As portas lógicas (controlada, densas, de projeções e de medidas) viabilizam a manipulação dos qbits e formalizam muitos parâmetros para construção de circuitos quânticos [1], viabilizando a resolução de problemas e até mesmo construção de algoritmos quânticos.

### III. JOGOS ANALISADOS

Para este estudo, selecionamos 7 jogos que tem notável aparição e presença em artigos e discussões sobre o tema [9]. Discutimos também os que continham uma jogabilidade boa e simples, em conjunto com uma maior clareza nos conceitos utilizados da computação quântica nas mecânicas dos jogos. Os jogos utilizados nesse estudo foram retirados pelos endereços de duas coletâneas de jogos quânticos que podem ser acessadas no repositório do GitHub<sup>2</sup> e em List of Quantum Games<sup>3</sup>.

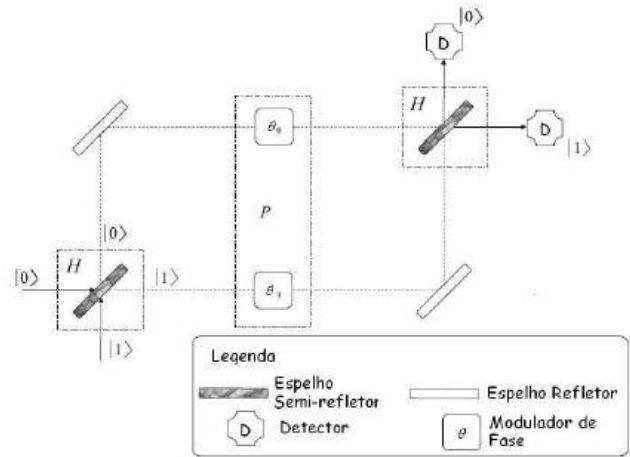
#### A. Quantum FlyTrap

O *Quantum FlyTrap* (qFT) é um *webgame*, composto por 33 fases que abordam os conceitos básicos da mecânica quântica, como a interferência e emaranhamento via polarização de cargas e variação de fases [14].

Cada fase dispõe de elementos que podem ser movimentados e/ou rotacionados em uma grade de  $13 \times 10$  quadrados. O objetivo de todas as fases é disparar 20 fótons até um detector de fótons, representado pelos *PAC-MAN*'s. Todos os componentes que aparecem nas fases são componentes reais utilizados nas construções de circuitos quânticos, como moduladores de fases ou divisores de feixes, polarizadores e não polarizadores. O jogo disponibiliza uma seção chamada VIRTUAL LAB, apresentando os componentes de todas as fases do jogo em conjunto, incluindo alguns extras, tais como portas quânticas, para criar seus próprios circuitos quânticos ou testar circuitos importantes para a comunidade.

O qFT tem como seu principal foco no ensino da ótica e funcionamento de um circuito quântico, utilizando até mesmo como representação de seus componentes uma incrível semelhança com a representação dos mesmos componentes em

circuitos reais. Veja o caso do modelo na Figura 2(A) em que se baseia o jogo, apresentando um interface na Figura 2(B), para o interferômetro de Mach-Zehnder [15] em que os retângulos do meio representam espelhos e divisores de feixe não polarizados e os robôs Pac-Man são os receptores de fótons. Tem-se uma comparação entre componentes de modelagem de circuito para o interferômetro de Mach-Zehnder real e sua



(A)



(B)

Fig. 2: O interferômetro de Max-Zehnder real no qFT

#### B. Quantum Chess

O *Quantum Chess* (qC) se baseia em utilizar das regras do xadrez conhecidas, no caso do movimento das peças, entretanto acrescentar os conceitos da mecânica quântica em seus movimentos. O objetivo do jogo, tal qual o original é capturar o rei adversário, cada peça tem um movimento único (por exemplo, cavalo se move em formato de "L"), porém, nesta versão cada peça pode se "dividir" em duas partes, entrando os conceitos quânticos. Cada peça, ao se dividir em duas, entrará em um estado de sobreposição, em que, as duas partes constituem a peça completa, sendo possível assim retornar a peça original. A principal mecânica introduzida no jogo é o fato de se perder uma dessas peças e ela continuar em jogo, como na Figura 3.

Nessa imagem é possível observar dois cavalos, aos quais são oriundos de um único cavalo das peças brancas, este

<sup>2</sup><https://github.com/HuangJunye/Awesome-Quantum-Games>

<sup>3</sup><https://kiedos.art/quantum-games-list/>



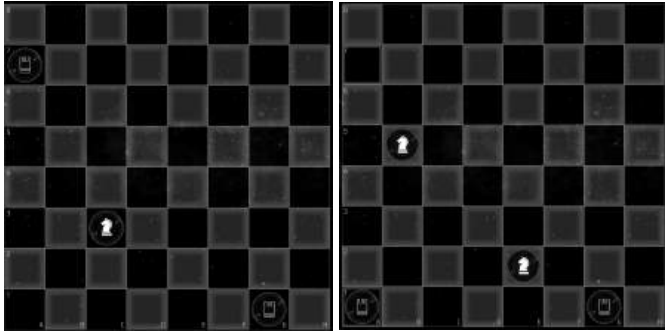


Fig. 3: Movimentação do cavalo usando superposição no ataque

cavalo está em superposição. Dessa maneira, a peça que está neste estado consegue se movimentar normalmente, entretanto, por estarem emaranhadas, se alguma das duas torres capturar qualquer um dos dois cavalos, a peça completa continuará podendo ser salva ao capturar alguma outra peça. Caso algum dos cavalos consiga capturar qualquer torre, ele colapsará e voltará a seu estado clássico novamente.

### C. Quantum Tic-tac-toe

A ideia do *Quantum Tic-tac-toe* (qTTT) é expandir a simplicidade do jogo da velha, introduzindo a mecânica quântica em sua jogabilidade[12]. O jogo funciona como o jogo da velha original, dois jogadores colocam os símbolos de "O" e "X" alternadamente e quem fizer 3 iguais em uma coluna, linha ou em alguma diagonal ganha. Ao inserir a ideia de superposição e emaranhamentos quânticos, o jogo aumenta a sua dificuldade. Nesta versão do jogo os "X" são representados pelas bolinhas ímpares e os "O" pelas bolinhas pares.

O objetivo de cada jogador será criar um loop emaranhado, formado por pelo menos 4 partículas, ou dois pares de bolinhas. Ao ser criado, o jogador terá que decidir em qual quadrado a última partícula inserida será posicionada, essa escolha irá causar um efeito em cadeia nas outras partículas que estão nos quadrados envolvidos.

Na ideia do emaranhamento um resultado que se torna possível é de que os dois jogadores consigam criar uma situação que os dois obtenham um empate, mas que os dois saiam vitoriosos por completarem o conjunto de 3 símbolos em sequência, ou seja, os dois jogadores ganham, sendo demonstrado esse caso na esquerda da Figura 4 em que, após uma sequência de jogadas, o jogador terá que decidir onde irá inserir o número 8, e ao selecionar o segundo quadrado da primeira coluna, faz com que o jogo resulte na imagem da direita na Figura 4. O jogador 2, acabou ficando com  $\frac{1}{2}$  de pontuação, pois quem fez a última jogada foi o jogador 1.

### D. QPong

Sendo um dos primeiros jogos desenvolvidos com a plataforma Qiskit o *QPong* (qP), é a versão quântica do pioneiro dos jogos eletrônicos, o Pong. Neste jogo é necessário utilizar dos conhecimentos das portas quânticas, tais como a CNOT, Pauli-X, Pauli-Y, Pauli-Z e Hadamard para conseguir realizar alguma

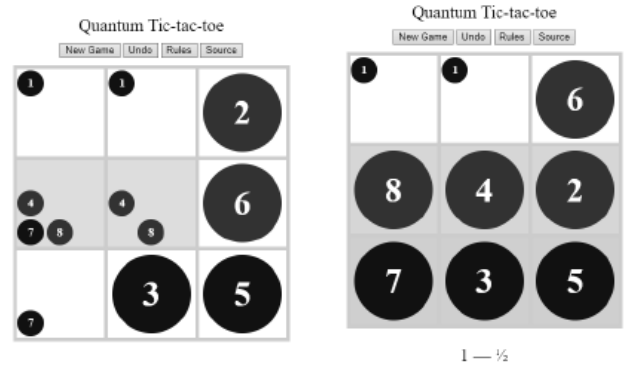


Fig. 4: Caso de empate com 2 vitoriosos

movimentação, podendo criar situações de sobreposição nas diferentes posições. As posições que se pode assumir são fixas, sendo elas todos os valores possíveis para os 3 qbits utilizados na construção dos circuitos.

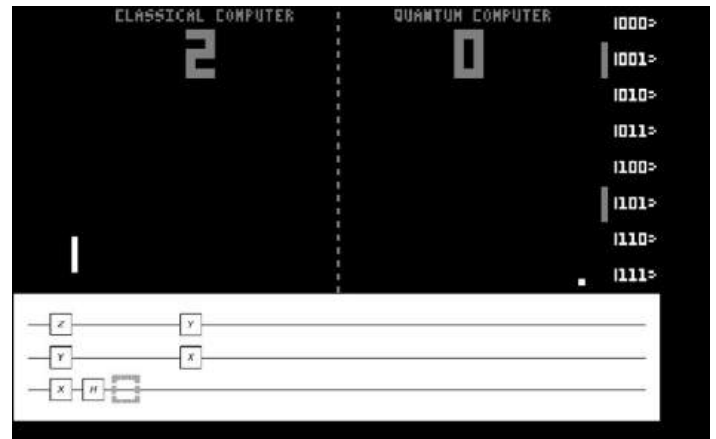


Fig. 5: Jogo QPong com diferentes portas lógicas.

Na Figura 5 temos a representação da jogabilidade do qP no qual o circuito construído, com as portas "Z", "Y", "H" e "X" nos 3 qbits indicados pelas linhas na parte inferior, gera o estado onde a barra de defesa se posiciona nos estados  $|001\rangle$  e  $|101\rangle$ . Quando a bolinha chegar na área em que a barra de defesa deveria estar, a barra irá colapsar para uma desses dois estados. Sendo assim, possível criar vários circuitos diferentes para defender o seu lado.

### E. The Qubit Game

Este jogo, desenvolvido pela Google, foi criado na intenção de ser um jogo a ensinar de uma maneira mais lúdica o funcionamento do computador quântico da empresa. O jogo tem uma jogabilidade simples de jogos incrementais, que se baseiam em uma execução de ações simples como clicar em algo na tela e aprimorar seus recursos ganhando a moeda específica do jogo, no caso *Qubit Game* (QuG). Nesse jogo a ideia é ir ganhando mais e mais informação dos qbits e ir desenvolvendo gradualmente o seu computador quântico, lembrando sempre de afastar qualquer coisa que atrapalhe o processamento das informações dos qbits.

Na Figura 6 está a tela principal, conforme se avança mais no jogo são liberadas outras funções, tais como manuseio de algoritmos quânticos. Na esquerda da imagem está a loja em que é possível comprar os upgrades para seu computador, tais como aumento do número de qbits ou capacidade de resfriamento. Abaixo da imagem está o regulador de frequência. Na direita dos qbits, no caso as bolinhas no centro, está um computador que efetuará a regulação da frequência sozinho e fará um algoritmo criado pelo próprio jogador.

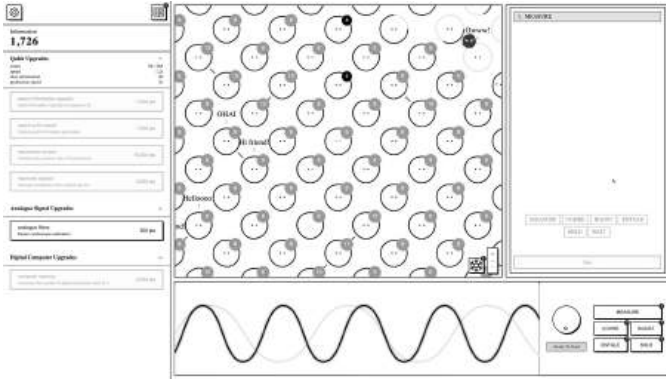


Fig. 6: The Qubit Game

F. *Minecraft - QCraft*

Uma modificação para o jogo *Minecraft*, o *QCraft* (QCr) visa adicionar conceitos de superposição e emaranhamento. O ambiente do jogo é composto por blocos, como: terra, madeira, pedra, minério (que ao serem destruídos, soltam o minério no chão para o jogador coletar) e outros. A modificação adiciona um minério quântico, que o jogador pode destruir e usar o minério para construir blocos que mudam o seu tipo quando o jogador o observa, ou conforme a posição, ou de maneira aleatória. Também é possível emaranhar dois blocos quânticos iguais, assim quando um bloco for observado, o outro cujo primeiro está emaranhado se transformará também para o mesmo tipo.

Na Figura 7, demonstra-se a construção de um bloco nesse *mod*, em que cada uma das letras indica uma direção, no caso ao colocar um bloco de pedra no local indicado pelo "N", toda vez que algum jogador olhar esse bloco quântico pelo norte, ele terá a aparência de um bloco de pedra, sendo o mesmo para o sul "S", leste "E", oeste "W", cima "U" e baixo "D" e o item no meio sendo o item quântico que faz com que o bloco seja criado. Ainda na Figura 7 temos um exemplo de construção desse bloco quântico com variados outros tipos de blocos.



Fig. 7: Exemplo de *crafting* de um bloco quântico

G. *Quantum Go*

O *Quantum Go* (qGO) se baseia no jogo de estratégia chinês Go, funcionando da mesma forma, com exceção de como os

jogadores colocam as peças. Possui dois jogadores, um com as peças pretas, que faz a primeira jogada, e outro com as peças brancas. O tabuleiro é quadriculado, e as peças são colocadas nos cruzamentos entre as linhas.

No turno do jogador, ele pode passar seu turno ou colocar uma peça, onde ele escolhe 2 ou 3 cruzamentos nos quais a peça terá uma probabilidade de cair, gerando "realidades" para cada resultado possível. Depois o outro jogador fará o mesmo, gerando novas realidades possíveis para qualquer uma já existente e assim por diante até chegar a um limite, assim resolvendo as probabilidades, resultando em uma única realidade. Se um cruzamento for ocupado pela mesma cor em todas as realidades, o número de realidades será diminuído de acordo.

Veja na Figura 8, mostrando um exemplo de jogada com as peças pretas, gerando 2 realidades, com 50% de chance de acontecer cada uma. Em seguida, as peças brancas realizam uma jogada escolhendo 3 cruzamentos, gerando 3 realidades para cada realidade pré-existente, porém como uma delas é impossível, uma peça preta caindo no mesmo lugar da peça branca, essa possibilidade é descartada, totalizando 5 possíveis realidades.

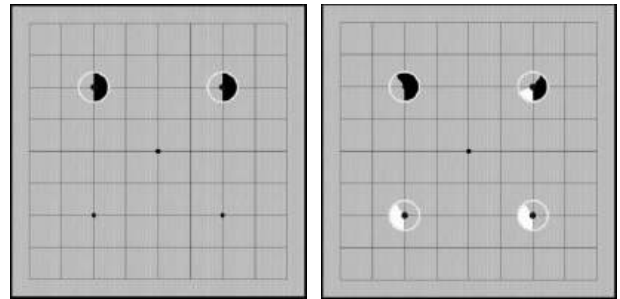


Fig. 8: Jogada das peças com dois e três cruzamentos.

Os jogadores podem capturar as peças adversárias ao colocar peças em todos os cruzamentos adjacentes, seja um grupo ou uma única peça, removendo-as do tabuleiro. Realizar uma jogada repetida, além dos movimentos ilegais do Go clássico que ocorre em todas as realidades como, colocar uma peça onde os 4 cruzamentos adjacentes já estejam ocupados por peças adversárias, com exceção que seja para captura, colocar uma peça em uma posição que voltaria o jogo ao último estado ou colocar em cima de outra peça, fará com que o turno do jogador seja passado.

O jogo acaba os dois jogadores passarem seu turno e pelo menos um deles foi intencional, ou um jogador passar e os últimos 4 turnos também foram passados. Os pontos de cada jogador são o total de peças que eles têm em campo, com as brancas ganhando 4 pontos adicionais.

IV. ANÁLISE DOS JOGOS E OBSERVAÇÕES

Observando os jogos é notável como o principal foco dos desenvolvedores é tentar explicar e tornar mais lúdico a maneira com que a mecânica quântica e aprendida, afinal neles todos apesar de alguns terem uma jogabilidade mais avançada, como o qC, nenhum apresenta maneiras de jogabilidade muito

TABELA I: Relação das características dos jogos analisados.

Jogo	Plataforma	Foco	Gênero	Conceito chave
qFT	Browser	Educacional / Original	Puzzle Game	Física Óptica / Circuitos Quântico
qC	Windows / Linux / macOS	Nova interpretação	Tabuleiro / Estratégia	Superposição
qTTT	Windows	Nova interpretação	Tabuleiro / Estratégia	Superposição / Emaranhamento
qP	Windows / macOS	Nova interpretação	Arcade	Circuitos Quânticos
QuG	Browser	Educacional / Original	Incremental/Idle	Funcionamento de Computador Quântico
QCr	Windows	Original	Sandbox / Sobrevivência	Superposição / Emaranhamento
qGo	Mobile / Tabuleiro	Nova interpretação	Estratégia	Superposição

complexas além de mover peças e/ou movimentação simples no espaço como no qE.

Para entendermos melhor as características de cada jogo foi elaborada a seguinte Tabela I, visando um detalhamento maior sobre o foco de cada um dos jogos apresentados.

Algo a ser notado é a que muitos dos jogos tem um grande foco em trazer uma nova interpretação de algo já consolidado, como o qTTT e o qC. Acreditamos que tal fato se deve a visar demonstrar como a CQ afetaria de maneira drástica a jogabilidade de tais jogos. Outro fator apontado durante o estudo é o uso de simuladores quânticos, em específico o Qiskit, para o desenvolvimento desses jogos. Por se tratar de uma ferramenta OPEN-SOURCE é compreensível que os desenvolvedores foquem em seu uso, além de que, ela baseia-se na linguagem de programação Python que é uma linguagem de alto nível, logo mais prática e acessível a todos que desejam tentar desenvolver qualquer jogo quântico.

## V. CONCLUSÃO

O estudo apresentado neste trabalho observou características que marcam a sinergia entre a CQ e os área de gamificação, e mostram como interagem conceitos e complementam abordagens mais tradicionais. As ideias da teoria quântica se mostram muito promissora na modelagem de jogos, seja em uma releitura ou em ideias originais. Ressaltamos também que apesar da existência de jogos específicos para computadores quânticos, por exemplo, o Cats/Box/Scissors<sup>4</sup>, ainda são muito escassos e de difícil acesso e compreensão, podendo ser áreas de pesquisa a serem incentivadas na atualidade.

Como trabalhos futuros destacamos o desenvolvimento de um jogo que consiga explorar de maneira eficaz todos os conceitos-chave da mecânica quântica e gerar um entretenimento ao jogador que não necessariamente tenha algum conhecimento sobre a CQ. Outro possível esforço de pesquisa foca na utilização de outros simuladores quânticos como o Q# para o desenvolvimento de jogos quânticos.

## AGRADECIMENTOS

Os autores gostariam de agradecer à Universidade Católica de Pelotas (UCPEL), Universidade Federal de Pelotas (UFPEL), à Universidade Federal do Rio Grande (FURG), à Universidade Federal do Pampa (UNIPAMPA), assim como ao Laboratório de Sistemas Ubíquos e Paralelos (LUPS).

<sup>4</sup><https://decodoku.medium.com/introducing-the-worlds-first-game-for-a-quantum-computer-50640e3c22e4>

## REFERÊNCIAS

- [1] Chuang, I. (2004). Course 1 - principles of quantum computation. In Estève, D., Raimond, J.-M., and Dalibard, J., editors, *Quantum Entanglement and Information Processing*, volume 79 of *Les Houches*, pages 1–54. Elsevier.
- [2] Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777.
- [3] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *STOC*, pages 212–219.
- [4] Lu, Y., Sigov, A., Ratkin, L., Ivanov, L. A., and Zuo, M. (2023). Quantum computing and industrial information integration: A review. *Journal of Industrial Information Integration*, page 100511.
- [5] McMahon, D. (2000). *Quantum Mechanics Demystified*. McGraw Hill, Cambridge University Press.
- [6] Mermin, N. D. (2007) *Quantum computer science: An introduction*. Cambridge University Press (2007). 10.1017/CBO9780511813870
- [7] Nielsen, M. and Knill, E. (1998). Complete quantum teleportation by nuclear magnetic resonance. (disponível via WWW em [cite-seer.ist.psu.edu/595490.html](http://cite-seer.ist.psu.edu/595490.html)).
- [8] Piispanen, L., Pfaffhauser, M., Wootton, J. R., Togelius, J., and Kultima, A. (2024). Defining quantum games.
- [9] Piispanen, L. J., Morrell, E., Park, S., Pfaffhauser, M., and Kultima, A. (2023). The history of quantum games. In *2023 IEEE Conference on Games (CoG)*, pages 1–8. IEEE.
- [10] Preskill, J. (2002). Lecture notes - course information for physics/computer science/quantum computation. Caltech Particle Theory Group - California Institute of Technology - USA.
- [11] Rieffel, E. and Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys (CSUR)*, 32(3):300–335.
- [12] Sagole, S., Dey, A., Behera, B. K., and Panigrahi, P. K. (2019). Quantum tic-tac-toe: A hybrid of quantum and classical computing.
- [13] Santos, L. P., Bashford-Rogers, T., Barbosa, J., and Navrátil, P. (2022). Towards quantum ray tracing.
- [14] Sigov, A., Ratkin, L., and Ivanov, L. A. (2022a). Quantum information technology. *Journal of Industrial Information Integration*, 28:100365.
- [15] Soares-Pinto, D. and Naves, C. (2021). O interferômetro de mach-zehnder e a escolha retardada quântica. *Revista Brasileira de Ensino de Física*, 43:e20210085.
- [16] Steeb, W. H. and Hardy, Y. (2004). *Problems and solutions in Quantum Computing and Quantum Information*. World Scientific, New Jersey.

# Simulação de Circuitos Quânticos Ópticos

V. F. Guedes, F. A. Mendonça e R. V. Ramos

**Resumo** — Neste trabalho apresentamos os resultados de um simulador de circuitos quânticos ópticos. Os circuitos quânticos considerados são compostos por divisores de feixes, moduladores de fase e contadores de fótons. Além disso, estados coerentes, estados de Fock e estados comprimidos da luz são utilizados. Os resultados apresentados demonstram que o simulador produzido é uma ferramenta útil na análise de circuitos para geração condicional de estados quânticos e de circuitos de amostragem Gaussiana de bósons.

**Palavras-Chave** — *Computação quântica, óptica quântica, simulação numérica, amostragem Gaussiana de bósons.*

**Abstract** — In this work we present the results of an optical quantum circuit simulator. The quantum circuits considered are composed by beam splitters, phase modulators and photon counters. Furthermore, coherent, Fock and squeezed states are used. The presented results demonstrate that the simulator is a useful tool for analysis of conditional quantum state generation

**Keywords** — *Quantum computing, quantum optics, numerical simulation, Gaussian boson sampling.*

## I. INTRODUÇÃO

Computadores quânticos ainda estão em estágio inicial de desenvolvimento, muitos desafios tecnológicos ainda não foram superados e, por isso, computadores quânticos ainda não estão disponíveis em larga escala. Assim, a computação quântica ainda conta com simuladores para o estudo, desenvolvimento e análise de algoritmos quânticos. De fato, há atualmente um número significativo simuladores disponíveis como o QISKIT, Cirq, QUIRK, QUBIT4MATLAB dentre muitos outros [1]. A maioria destes simuladores lida com qubits, ou seja, dois estados quânticos ortogonais representam os bits lógicos ‘0’ e ‘1’. As portas quânticas como CNOT e portas de um qubit processam esses qubits. Outra forma de computação quântica sem a utilização de bits lógicos é possível. Nesta, a distribuição de números de fótons ou os valores das quadraturas são utilizados para computação. É uma forma menos convencional, mas ainda útil e poderosa. Um exemplo é a amostragem Gaussiana de bósons [2-4]. Neste caso, circuitos ópticos construídos com divisores de feixes, moduladores de fase e contadores de fótons são utilizados. Um exemplo de simulador de circuitos quântico-ópticos é o *strawberry fields*, da empresa Xanadu, disponível em <https://strawberryfields.ai/>.

Nesta direção, o presente trabalho apresenta resultados de um simulador de circuitos quânticos ópticos. A geração

condicional de estados quânticos da luz e a amostragem Gaussiana de bósons são considerados.

Este trabalho está dividido da seguinte forma: na Seção II é feita uma revisão dos conceitos de óptica quântica necessários ao entendimento do trabalho; Na Seção III, o simulador de circuitos quânticos ópticos é utilizado na análise de circuitos quânticos com dois, três e quatro estados. Por fim as conclusões são descritas na Seção IV.

## II. CONCEITOS BÁSICOS DE ÓPTICA QUÂNTICA EM DIMENSÃO FINITA

Um estado coerente pode ser expandido na base de estados número  $\{|0\rangle \dots |s\rangle\}$ , como sendo

$$|\alpha\rangle = \sum_{n=0}^s c_n |n\rangle \quad (1)$$

sendo  $s + 1$  a dimensão do espaço finito de Hilbert. Usando o operador deslocamento de Glauber tem-se que:

$$|\alpha\rangle = e^{\alpha a^\dagger - \alpha^* a} |0\rangle. \quad (2)$$

O estado número é representado pelo vetor

$$|n\rangle = (0 \dots 1 \dots 0)^T \quad (3)$$

no qual somente um elemento não nulo ocorre na posição  $(n+1)$ . Os operadores aniquilação e criação, neste espaço finito, são dados, respectivamente, por:

$$\hat{a} = \sum_{n=1}^s \sqrt{n} |n-1\rangle \langle n| \text{ e } \hat{a}^\dagger = \sum_{n=1}^s \sqrt{n} |n\rangle \langle n-1|, \quad (4)$$

com limites inferior e superior dados por  $\hat{a}|0\rangle = 0$  e  $\hat{a}^\dagger|s\rangle = 0$ . Os estados comprimidos, por sua vez, são obtidos através da operação  $|S\rangle = S_{r,\phi}|0\rangle$  sendo  $S_{r,\phi}$  operador dado por

$$S_{r,\phi} = e^{\frac{1}{2}[\alpha^*(a)^2 - \alpha(a^\dagger)^2]} \quad (5)$$

com  $\alpha = r e^{i\phi}$ . Por fim, divisores de feixes e modulador de fase são matematicamente descritos, respectivamente, pelos operadores

$$U_{BS} = e^{\theta(a^\dagger b - ab^\dagger)} \quad (6)$$

$$U_\phi = e^{i\phi a^\dagger a} \quad (7)$$

Vitor Ferreira Guedes, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce e-mail: [vitorfergue@gmail.com](mailto:vitorfergue@gmail.com); Fábio Alencar Mendonça, Departamento de Telemática, IFCE, Fortaleza-Ce email: [fabioalencar@ifce.edu.br](mailto:fabioalencar@ifce.edu.br); Rubens Viana Ramos, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce, e-mail: [rubens.ramos@ufc.br](mailto:rubens.ramos@ufc.br).

### III. SIMULAÇÃO DE CIRCUITOS QUÂNTICOS ÓPTICOS

O primeiro circuito a ser considerado é o interferômetro de Mach-Zehnder mostrado na Fig. 1.

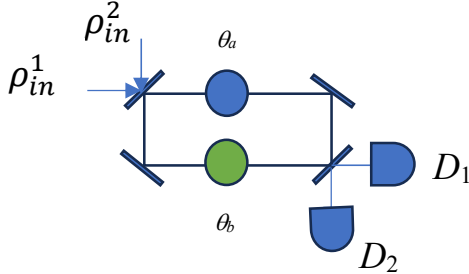


Fig. 1. Interferômetro de Mach-Zehnder.  $D_1$  e  $D_2$  são detectores.

Na primeira simulação, mostrada na Fig. 2, tem-se  $\rho_{in}^1 = |\alpha\rangle\langle\alpha|$  (estado coerente) com  $\alpha = 3$  e  $\rho_{in}^2 = |0\rangle\langle 0|$ . Na segunda simulação, mostrada na Fig. 3, tem-se  $\rho_{in}^1 = |S\rangle\langle S|$  (estado comprimido) com  $r = 3$ ,  $\phi = 0$  rad,  $\rho_{in}^2 = |0\rangle\langle 0|$ . Três situações são consideradas:  $\theta_a - \theta_b \in \{0, \pi/2, \pi\}$  rad.

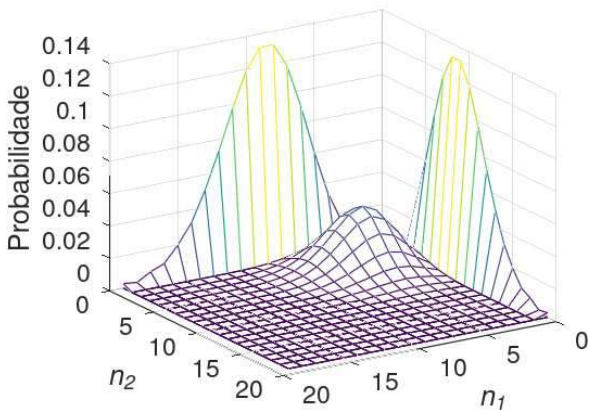


Fig. 2. Distribuições do número de fótons nas saídas do Mach-Zehnder da Fig. 1 quando  $\rho_{in}^1 = |\alpha\rangle\langle\alpha|$  com  $\alpha = 3$ ,  $\rho_{in}^2 = |0\rangle\langle 0|$  e  $\theta_a - \theta_b \in \{0, \pi/2, \pi\}$  rad.

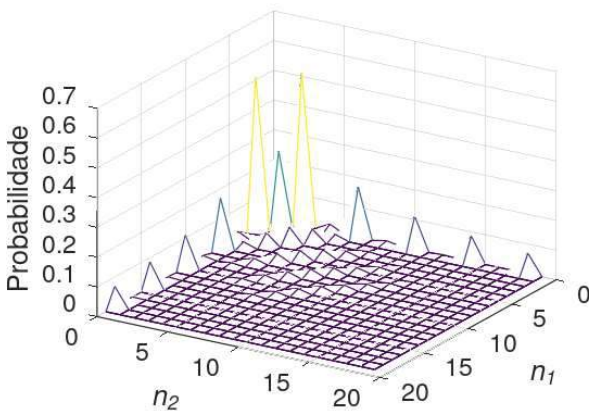


Fig. 3. Distribuições do número de fótons nas saídas do Mach-Zehnder da Fig. 1 quando  $\rho_{in}^1 = |S\rangle\langle S|$  com  $r = 3$ ,  $\phi = 0$  rad,  $\rho_{in}^2 = |0\rangle\langle 0|$  e  $\theta_a - \theta_b \in \{0, \pi/2, \pi\}$  rad.

As distribuições do número de fótons podem ser vistas nas Fig. 2 e 3, respectivamente. Como esperado, nas situações em que  $\theta_a - \theta_b \in \{0, \pi\}$  rad tem-se perfeita interferência construtiva em uma saída e destrutiva ( $n_1 = 0$  ou  $n_2 = 0$ ) na outra. Quando  $\theta_a - \theta_b = \pi/2$  rad os fótons se distribuem com a mesma probabilidade pelas duas saídas (curva que passa pela reta diagonal do piso do gráfico).

Um esquema óptico muito útil na geração de estados quânticos é mostrado na Fig. 4 [5-8].

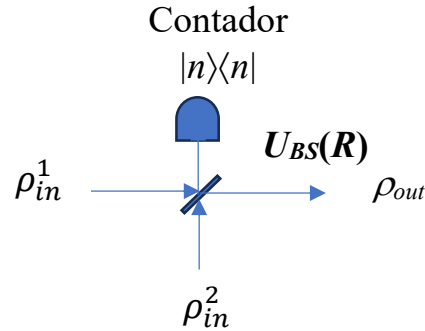


Fig. 4. Esquema básico para a geração de estados quânticos condicionado ao número de fótons medido em uma das saídas.

Basicamente, o estado quântico na saída ( $\rho_{out}$ ) depende do estado quântico na entrada ( $\rho_{in}$ ), da reflectância do divisor de feixes e do número de fótons medidos na outra saída. Aqui, consideramos uma versão ampliada do esquema na Fig. 4. Como mostrado na Fig. 5, dois divisores de feixes são utilizados, além de um modulador de fase. Uma das saídas é medida.

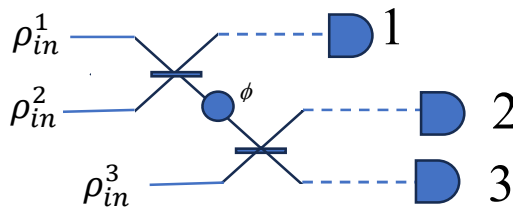


Fig. 5. Esquema ampliado com dois divisores de feixes para geração condicional de um estado quântico bipartite.

A Fig. 6 (7 e 8) a seguir mostra a distribuição do número de fótons nas saídas 2 e 3 (1 e 3, 1 e 2) condicionada à medição de um fóton na saída 1 (2, 3). Os parâmetros utilizados são:  $\theta = \pi/4$  (eq. 6 – divisores balanceados),  $\phi = 0$  (sem modulação de fase),  $\rho_{in}^1 = \rho_{in}^3 = |\alpha\rangle\langle\alpha|$  com  $\alpha = 2$  e  $\rho_{in}^2 = |1\rangle\langle 1|$ .

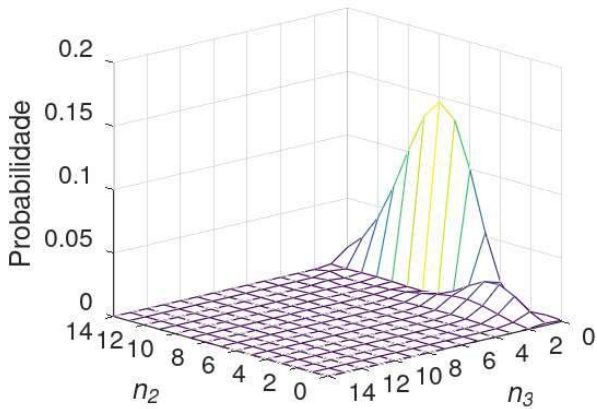


Fig. 6. Distribuição do número de fótons das saídas 2 e 3 do circuito da Fig. 5 condicionada à medição de um fóton na saída 1.

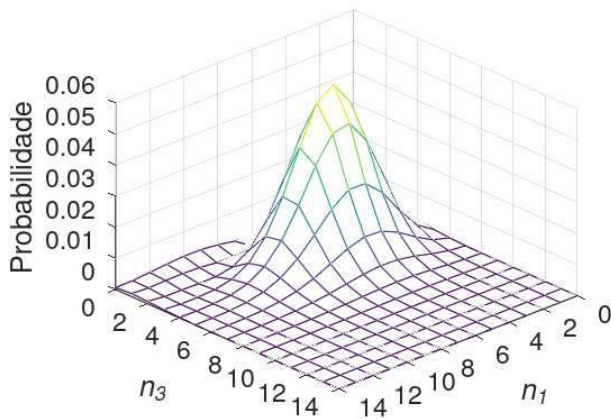


Fig. 7. Distribuição do número de fótons das saídas 1 e 3 do circuito da Fig. 5 condicionada à medição de um fóton na saída 2.

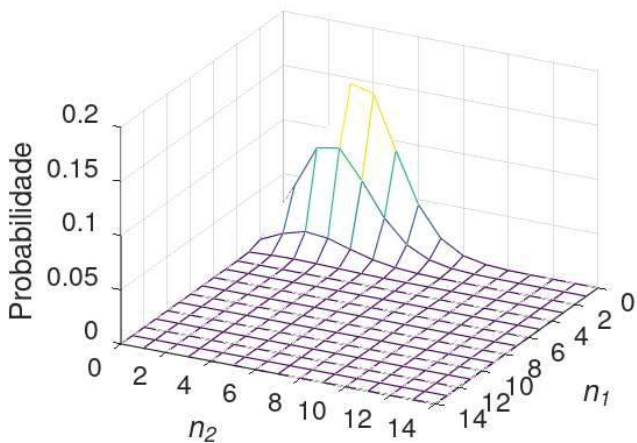


Fig. 8. Distribuição do número de fótons das saídas 1 e 2 do circuito da Fig. 5 condicionada à medição de um fóton na saída 3.

Por fim, a Fig. 9 mostra um circuito com seis divisores de feixes balanceados ( $\theta = \pi/4$ ) e 8 moduladores de fase (os dois primeiros com  $\phi = \pi/2$  e os demais com  $\phi = \pi/4$ ). Os estados de entrada são quatro estados comprimidos com  $r = 1$  e fase zero.

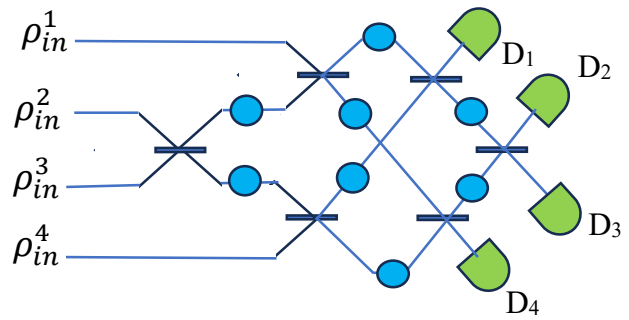


Fig. 9. Circuito óptico para amostragem Gaussiana de bósons com seis divisores de feixes, oito moduladores de fase e quatro contadores de fótons.

Os detectores  $D_1$ ,  $D_2$ ,  $D_3$  e  $D_4$  são contadores de fótons. O número de fótons em cada saída pode variar de zero a oito. Portanto, existem 6561 seqüências possíveis, sendo a primeira (seqüência #1) ‘0000’ (zero fótons medidos nas quatro saídas) e a última (seqüência #6561) ‘8888’ (oito fótons medidos nas quatro saídas). A distribuição de probabilidade dessas seqüências está mostrada na Fig. 10.

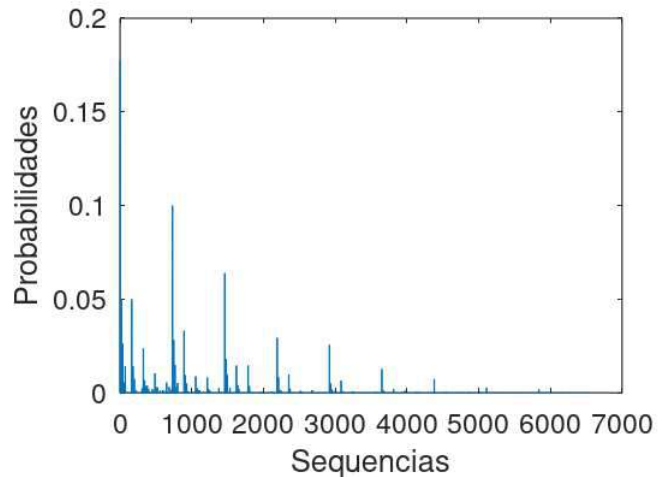


Fig. 10. Distribuição de probabilidade de ocorrência das 6561 seqüências obtidas nas saídas do circuito amostrador de bósons da Fig. 9.

Na Fig. 10 pode-se notar o caráter nada suave da distribuição obtida, o que está em acordo com a dificuldade de calculá-la em um computador clássico.

#### IV. CONCLUSÕES

Fugindo do lugar comum de simulações de circuitos quânticos utilizando portas quânticas de qubits, mostramos que um simulador que considere estado quânticos da luz e componentes ópticos simples, é uma ferramenta útil que pode explorar a rica dinâmica da geração de estados quânticos condicionados ao resultado de uma medição e investigar a amostragem Gaussiana de bósons. Além disso, embora não tenhamos discutido nesse trabalho, certamente o simulador

apresentado é útil no desenvolvimento de computação quântica com variáveis contínuas se ao invés da contagem de fótons, detecções homódinas forem utilizadas.

#### AGRADECIMENTOS

Este trabalho foi parcialmente financiado pelas agências CNPq (309374/2021-9) e CAPES (001).

#### REFERÊNCIAS

- [1] <https://thequantuminsider.com/2022/06/14/top-63-quantum-computer-simulators-for-2022/> and references there in.
- [2] T. R. Bromley, J. M. Arrazola, S. Jahangiri, J. Izaac, N. Quesada, A. D. Gran, M. Schuld, J. Swinerton, Z. Zabaneh, N. Killoran, “Applications of near-term photonic quantum computers: software and algorithms”, *Quantum Sci Tech.*, v. 5, pp. 034010, 2020.
- [3] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, F. Sciarrino, “Photonic implementation of boson sampling: a review”, *Adv Photon*, v. 1, no. 3, pp. 034001, 2019.
- [4] F. V. Mendes, C. Lima, R. V. Ramos, “Applications of the Lambert–Tsallis  $W_q$  function in quantum photonic Gaussian boson sampling”, *Quant. Inf. Process.*, v. 21, pp. 215, 2022.
- [5] M. Dakna, L. Knoll, D.-G. Welsch, “Quantum state engineering using conditional measurement on a beam splitter”, *The European Phys. J. D - Atomic, Molecular, Optical and Plasma Physics*, v. 3, pp. 295, 1998.
- [6] C. Yang, F.-L. Li, “Nonclassicality of photon-subtracted and photon-added- then-subtracted Gaussian states”, *J. Opt. Soc. Am. B*, v. 26, no. 4, pp. 830, 2009.
- [7] V. Parigi, A. Zavatta, M. Bellini, “Manipulating thermal light states by the controlled addition and subtraction of single photons”, *Laser Phys. Lett.*, v. 5, no. 3, pp. 246, 2008.
- [8] P. V. P. Pinheiro, R. V. Ramos, “Quantum communication with photon-added coherent states”, *Quant. Inf. Process.*, v. 12, pp. 537–547, 2013.

# Efficient Computation of the Wave Function $\psi_n(x)$ using Hermite Coefficient Matrix in Python

Matheus Cordeiro, Italo Bezerra, and Hilma Vasconcelos

**Abstract**—With the acceleration of quantum hardware development each year, the demand for fast and accurate Quantum Computing Simulation tools has grown significantly. This growth is largely due to the challenges in accessing real quantum hardware. In this context, our work aims to gain a computational advantage in calculating the wave function of a Quantum Harmonic Oscillator. We achieve this through a hybrid strategy that relies partially on the efficient and precise calculation of the Hermite polynomial using a coefficient matrix, combined with the use of a Python Just-In-Time (JIT) compilation optimizer.

**Keywords**—Wave Function, Hermite Polynomials, Quantum Harmonic Oscillator, JIT, Python.

## I. MOTIVATION AND THEORETICAL FOUNDATIONS

The simplicity and convenience offered by the Python programming language [1] have established it as a standard tool for Classical Quantum Computing Simulation. Python excels in building highly abstract ideas due to its high-level nature. Open access to source code promotes reproducibility of computational projects and a greater exchange of ideas.

The development of specific libraries for quantum computing has facilitated the use of Python language in research in this field. For example, *Piquasso* [2] is an open-source Python library developed by the Budapest Quantum Computing Group, which focuses on the simulation of photonic quantum computers. This library differs from the others because it offers simulations that use the *TensorFlow* and the *JAX* libraries on the backend. These are two Python libraries specifically designed for Deep Learning applications. The use of these two Python libraries by *Piquasso* is related to matrix differentiation in problems involving Continuous-Variable Quantum Neural Networks (CVQNN). In addition to the library for direct use in Python, *Piquasso* also provides a drag-and-drop interface, that is code-free and easy to handle, for simulating photonic circuits: *Piquasso* Dashboard.

*Spinsim* [3] is a simulation package for spin-1/2 and spin-1 quantum systems under time-dependent control. Developed in Python, this package has been optimized for GPU to handle geometric integration calculations, which demand substantial computational resources due to the magnitude of the calculations. This optimization is achieved using the *Numba* library [4] in Python. *Numba* has a Just-In-Time (JIT) optimizer based on the LLVM compilation infrastructure, which was developed in

C++ and was specifically designed to enhance both compilation and execution times. With *Numba*, we can get runtime translation of Python code into optimized machine code. The geometric integration provided by this package outperforms *sesolve* from *QuTip*, *NDSolve* from *Mathematica* and *ivp\_solve* from *Scipy* [5].

The use of compilation optimizers like the JIT (Just-In-Time) compiler from *Numba*, mentioned in the previous paragraph, is being explored in the field of Classical Quantum Computing Simulation. Unlike traditional compilation optimizers like the one found in *Numba*, quantum compilation optimizations are already being developed, such as Quantum Just-In-Time Compilation (QJIT) [6]. These optimizations help maintain computational performance in hybrid CPU-QPU models. Additionally, the Quingo quantum compiler [7], which is a Python framework designed for working with heterogeneous quantum computing in Noisy Intermediate-Scale Quantum (NISQ) systems, is also being developed.

### A. The Wave Function of a Quantum Harmonic Oscillator

Solving the Schrödinger Equation is a fundamental task in the field of Quantum Mechanics, as its solution, the wave function, mathematically describes the quantum state of one or more particles. The wave function provides a non-deterministic description of the physical system, which implies the need to deal with probabilities [8].

From the same perspective, the quantum harmonic oscillator is one of the most relevant models in Quantum Mechanics. Its wave function describes all harmonic potentials, which is essential for representing vibrational states of varying energies [8]. This model is applied to the description of systems in Quantum Optics, where each vibrational state is associated with a quantum number  $n$ , corresponding to the number of photons in that state. For instance, for  $n = 0$ , we have the vacuum state, representing the absence of photons [9].

For the one-dimensional harmonic oscillator, the wave function can be derived from the time-independent Schrödinger Equation, where  $V(x) = (m\omega^2 x^2/2)$  represents the potential energy of the quantum harmonic oscillator [10]:

$$E\psi(x) = -\frac{\hbar^2}{2m} \frac{d^2}{dx^2} \psi(x) + \frac{m\omega^2 x^2 \psi(x)}{2}, \quad (1)$$

where  $E$  represents the total energy of the system,  $\hbar$  is the reduced Planck constant,  $m$  is the particle's mass,  $x$  is the position,  $\omega$  is the angular frequency of the harmonic potential, and  $\psi$  is the one-dimensional, time-independent wave function to be found. Solving this equation yields the following result [11]:

Matheus Cordeiro, Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará (UFC), Fortaleza-CE, e-mail: matheus-cord@alu.ufc.br; Italo Bezerra, Universidade Estadual do Ceará (UECE), Iguatu-CE, e-mail: italop@hotmail.com; Hilma Vasconcelos, Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará (UFC), Fortaleza-CE, e-mail: hilma@ufc.br.



$$\psi_n(x) = \frac{1}{\sqrt{2^n n!}} \left( \frac{m\omega}{\pi\hbar} \right)^{\frac{1}{4}} e^{-\frac{m\omega x^2}{2\hbar}} H_n \left( \sqrt{\frac{m\omega}{\hbar}} x \right),$$

$$n = 0, 1, 2, 3, \dots \quad (2)$$

In Eq. (2),  $H_n$  is the Hermite polynomial of degree  $n$ . Thus,  $\psi_n(x)$  is considered a Hermite function. This wave function, like any other wave function, has the following properties: it is a solution to the Schrödinger Equation, it is normalizable ( $\int_{-\infty}^{\infty} |\psi_n(x)|^2 dx = 1$ ), and it is continuous in  $x$ , as well as its derivative [8].

Fig. 1 gives a better understanding of the behavior of the wave function for different values of  $n$ . In this graph, we can see the energy levels of the system changing in discrete energy increments as  $n$  increases [10]. In Quantum Optics, this change in energy levels is linked to the absorption or emission of photons in a system, altering the value of  $n$  and consequently the degree of the Hermite polynomial in Eq. (2) [9].

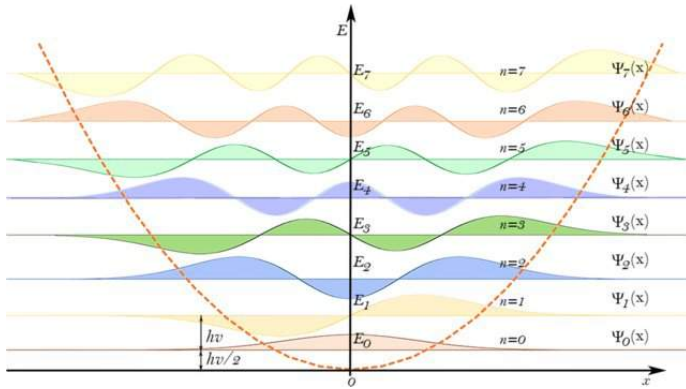


Fig. 1

WAVE FUNCTIONS AND ENERGIES FOR DIFFERENT  $n$  [12].

For large values of  $n$  and  $x$ , achieving efficient and accurate computation of the Hermite polynomial becomes essential for a reliable modeling of a Quantum Harmonic Oscillator. This work aims to present a solution to enhance the efficiency of Hermite polynomial calculations. In the next section, we will discuss the methods used for computing the Hermite polynomial, as well as well-known Python libraries for performing this task.

### B. Calculating the Hermite Polynomial

The Hermite polynomial can be explicitly defined by Rodrigues' formula as follows [13]:

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}. \quad (3)$$

These polynomials obey the following recurrence relations [13]:

$$\begin{cases} H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x), \\ H_0(x) = 1, \\ H_1(x) = 2x. \end{cases} \quad (4)$$

We can also represent the Hermite polynomial as a sum in the following manner [13]:

$$H_n(x) = n! \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \frac{(-1)^l (2x)^{n-2l}}{l!(n-2l)!}. \quad (5)$$

We can also work with calculations for the multidimensional Hermite polynomial  $G_A^k(b)$  [14], expanding the exponential function of a quadratic polynomial into a Taylor series:

$$K_A(x, b) = \exp(x^T b + \frac{1}{2} x^T A x) = \sum_{k \geq 0} \frac{G_A^k(b)}{k!} x^k. \quad (6)$$

Where  $K_A(x, b)$  is called the generating function for multidimensional Hermite polynomials,  $A$  is a  $h \times h$  symmetric matrix,  $b$  is a vector of dimension  $h$  containing values,  $x$  is a vector of dimension  $h$  containing variables, and  $k$  is a vector of dimension  $h$  containing indices.

The approaches mentioned before (Rodrigues' formula - Eq. (3), recurrence - Eq. (4), and finite power series - Eq. (5)), have their drawbacks when calculating Hermite polynomials for large values of  $n$ . Some may be too slow, while others might be too inaccurate. In this context, programmers often employ different strategies to overcome these challenges, even within the programming language itself. For example, Python's *Scipy* library offers two libraries for computing the Hermite polynomial: `scipy.special.hermite` and `scipy.special.eval_hermite`. You can find the source code for each of them at: **hermite** and **eval\_hermite**. The first function uses Eq. (3), working with a code that finds the roots of the Hermite polynomial. The second implements an iterative form of the recurrence defining the probabilistic Hermite polynomial, similar to Eq. (4), and relies on the following relationship to obtain the Hermite polynomial [13]:

$$H_n(x) = 2^{\frac{n}{2}} He_n(\sqrt{2}x), \quad (7)$$

where  $He_n$  is the probabilistic Hermite polynomial. This function is implemented in *Cython* [15], which is a hybrid language between C and Python, and is more efficient than a function implemented in standard Python.

On the other hand, *Numpy* [16] offers a function called `numpy.polynomial.hermite.hermval`, whose source code can be found at **hermval**. This function returns a Hermite series defined as follows:

$$p(x) = c_0 H_0(x) + c_1 H_1(x) + \dots + c_n H_n(x). \quad (8)$$

With this function, it's possible to obtain only the value of  $H_n(x)$  by setting the following coefficient vector as the input to the function:  $c_n = [0, 0, \dots, 1]$ . The calculation of this sum is performed using an iterative algorithm for the recurrence in Eq. (4), where the recursive nature of using previous values to obtain current values is exploited.

The *Mr Mustard* library [17], developed by the photonic quantum computing company Xanadu, uses a strategy that is currently regarded as one of the most efficient available. This strategy is utilized in the `oscillator_eigenstate`

function. This library adapts Eq. (6) so efficiently in its implementation that the execution time of this function remains virtually unchanged even with an increase in the number of photons  $n$ .

In this work we implement two strategies to compute the wave function: one using `eval_hermite` from *Scipy* and a hybrid strategy that uses Hermite coefficient matrix in conjunction with `eval_hermite`. The resulting wave functions computed using these two strategies are compared to the wave functions calculated using `oscillator_eigenstate` from *Mr Mustard*. The runtime efficiency of our two implementations is then compared to demonstrate the computational advantage of using the Hermite coefficient matrix.

## II. METHODOLOGY: WAVE FUNCTION WITH HERMITE COEFFICIENT MATRIX

The increase in efficiency when using our hybrid strategy arises from storing the coefficients of the Hermite polynomials in a pre-fixed matrix for use during the calculation. Thus, the Hermite polynomial is calculated with just a simple linear algebra operation. The Hermite polynomials varies with  $n$  according to Table I [13].

$n$	$H_n(x)$
0	1
1	$2x$
2	$4x^2 - 2$
3	$4x^3 - 12x$
4	$16x^4 - 48x^2 + 12$
5	$32x^5 - 160x^3 + 120x$
6	$64x^6 - 480x^4 + 720x^2 - 120$

TABLE I  
HERMITE POLYNOMIALS UP TO  $n = 6$ .

The coefficient matrix for  $n = 6$  is defined as follows:

$$C_6 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & -2 \\ 0 & 0 & 0 & 4 & 0 & -12 & 0 \\ 0 & 0 & 16 & 0 & -48 & 0 & 12 \\ 0 & 32 & 0 & -160 & 0 & 120 & 0 \\ 64 & 0 & -480 & 0 & 720 & 0 & -120 \end{bmatrix}$$

The  $i$ -th row of this coefficient matrix has the coefficients related to Hermite polynomials of degree  $i$ , which are obtained by taking the inner product of this row with a vector  $x_i^p$ :  $H_i(x) = x_i^p \cdot C_n[i]$ . Fig. 2 illustrates the idea just described. In this illustration, to calculate the Hermite polynomial of degree  $i$ , where  $i < n+1$ , we must construct a coefficient matrix with a degree always greater than the intended working degree.

Initially, the coefficient matrix was constructed using *Sympy* library from Python. This approach failed to outperform the efficiency of the *Scipy* strategy implemented in the `eval_hermite` function in terms of speed. However, by using *Numba*, the computation of the wave function that uses the coefficient matrix to calculate the Hermite polynomial was faster compared to using *Scipy*'s `eval_hermite`.

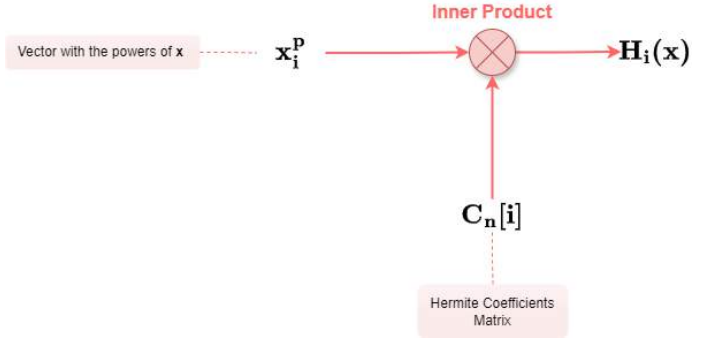


Fig. 2  
COMPUTING THE HERMITE POLYNOMIAL USING THE COEFFICIENT MATRIX.

However, it was necessary to replace the factorial in the wave function by the gamma function, where  $n! = \Gamma(n + 1)$ . Using the factorial in *Numba* introduces inaccuracy from  $n$  equal to 21 onwards. Additionally, the use of *Numba*, through the `@jit` decorator, on the wave function calculation, introduced inaccuracy for values of  $n$  greater than 60 when compared with the strategy using *Scipy* to calculate of the Hermite polynomial.

So, the best strategy we found was a hybrid calculation for the wave function that combines speed and accuracy:

- For  $n \leq 60$ , we make use of the coefficient matrix for computing the Hermite polynomial along with the *Numba* library optimization -  $\psi_{C_{matrix}}(x)$ .
- For  $n > 60$ , we make use of the `eval_hermite` function from *Scipy* for computing the Hermite polynomial -  $\psi_{scipy}(x)$ .

The complete implementation of this algorithm can be found in the following GitHub repository: CoEfficients-Matrix-Wavefunction.

## III. RESULTS AND DISCUSSIONS

In order to compare the efficiency of this hybrid strategy, several speed tests were conducted, comparing this strategy with one that solely utilizes *Scipy* and with the *Mr Mustard* strategy, used as a reference.

Initially, the execution times of the three strategies were calculated, in milliseconds, over the course of 1,000 tests. This is the time it takes to fill out a matrix  $\Psi_{n \times x}$ , with  $n = 50$  and  $x = 20$ . This experiment evaluates only the portion of the hybrid algorithm where  $\psi_{hybrid} = \psi_{C_{matrix}}$ . The result of this initial experiment is shown in Fig. 3, where  $t_{avg}$  is the average execution time. From Fig. 3 we can see that the hybrid algorithm (orange) takes less time when compared to the algorithm that uses only *Scipy* (blue). It is clear that our hybrid strategy has better performance than using solely *Scipy*.

We highlight the difference in time levels between the algorithm belonging to the *Mr Mustard* library (green) and both the hybrid algorithm and the algorithm that solely employs *Scipy*. On average, *Mr Mustard* manages to be around 40 times faster than the hybrid algorithm and about 60 times faster than the algorithm using only *Scipy*.

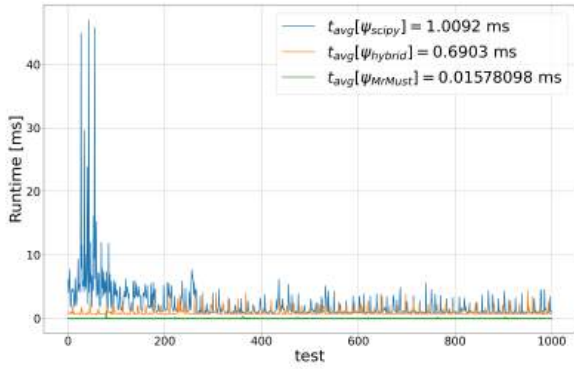


Fig. 3

SPEED TEST OF FILLING OUT THE MATRIX  $\Psi_{n,x}$ , WHERE  $n = 50$  AND  $x = 20$ .

The second experiment was identical to the previous one, but for  $n = 100$ . And now, we also evaluate the hybrid algorithm in its entirety. The outcome of this second experiment is shown in Fig. 4. As we can see, the hybrid algorithm consistently maintains a lower time level compared to the algorithm that relies only on *Scipy*. This observation is confirmed by the average execution times of each strategy over 1,000 tests, as indicated in the figure.

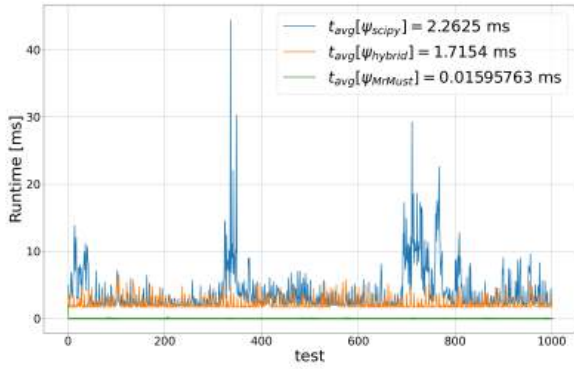


Fig. 4

SPEED TEST OF FILLING OUT THE MATRIX  $\Psi_{n,x}$ , WHERE  $n = 100$  AND  $x = 20$ , EVALUATING THE HYBRID ALGORITHM IN ITS ENTIRETY.

In Fig. 5, we have a speed experiment for a fixed value of  $x$ , set at 50.0, aiming to evaluate how the execution time of each function evolves when  $n$  increases. In this experiment, we compare the smallest execution times among all the strategies, in milliseconds, for 100 tests conducted at each  $n$ . We opt for the smallest execution time because the operating system often interferes with the execution time with some random requests that affect the average execution time, despite using filters based on the median to remove outliers.

This behavior is clearly evident in the high peaks present in the previous graphs. Therefore, in this experiment, we seek

to analyze, at least, how much time each strategy takes for each value of  $n$ , thereby also smoothing out the execution time curve. As we can observe in Fig. 5, the hybrid algorithm (orange) has higher efficiency compared to the algorithm using only *Scipy* (blue), showing an increase in the area of runtime efficiency with increasing values of  $n$ . This area is a graphical representation of the computational advantage that the hybrid algorithm holds over the one relying on *Scipy*.

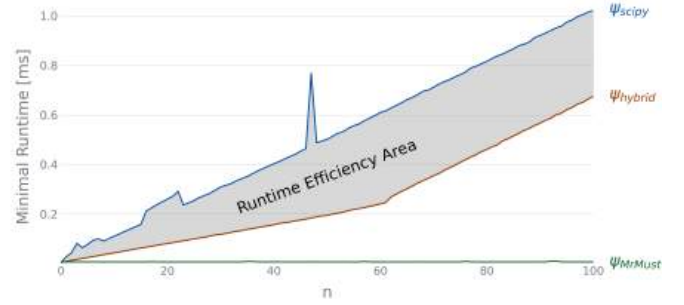


Fig. 5

SPEED TEST OF FILLING OUT THE MATRIX  $\Psi_{n,x}$  FOR A FIXED VALUE OF  $x = 50.0$  AND VARYING  $n$ .

In Fig. 6, 1,000 tests are performed for populating the matrix  $\Psi_{n|20}$  for each value of  $n$ . In other words, the number of columns in the matrix is fixed and equal to 20, while the number of rows is incremented from 0 to  $n$ , consistently conducting 1,000 tests for each  $n$ . Furthermore, the version of the hybrid strategy that accepts a vector instead of a numerical value was utilized. The runtime efficiency region is also visible in Fig. 6, demonstrating that the hybrid algorithm once again outperforms the algorithm solely utilizing *Scipy*.

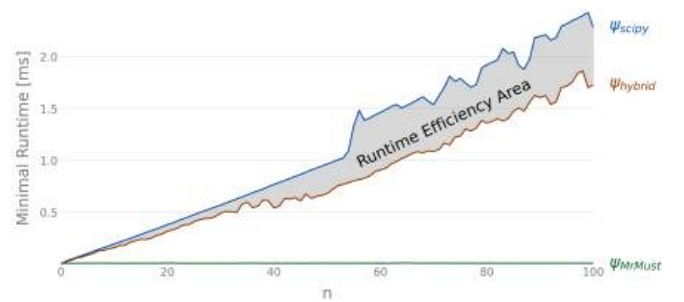


Fig. 6

SPEED TEST OF FILLING OUT THE MATRIX  $\Psi_{n,x}$ .

#### IV. CONCLUSION

The development of a precise and efficient method for calculating a wave function is highly valuable for modeling quantum systems and for executing quantum algorithms on classical computers. This was the purpose of this work, where a hybrid technique was implemented to provide both accuracy and speed.

This approach could be quite useful for well-established tools, should they choose to make use of it. For instance, it could enhance platforms like the Virtual Lab of *Quantum Flytrap* [18], an IDE for Quantum Computing without the use of code, or even *Strawberry Fields* [19], a Python library for designing, optimizing, and utilizing photonic quantum computers.

In a future work, this module currently available on GitHub will be converted into a Python package, bringing greater ease of use for its resources through package managers like *Pip* or *Conda*.

#### ACKNOWLEDGMENTS

We thank S. G. for his invaluable contributions to this project. M. C. thanks Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) and Programa de Pós-graduação em Engenharia de Teleinformática (PPGETI) for financial support.

#### REFERÊNCIAS

- [1] Python Software Foundation, *Python 3.9.1 Documentation*, available at: <https://docs.python.org/3.9/>
- [2] Budapest Quantum Computing Group, *Piquasso*, [Software]. Available at: <https://github.com/Budapest-Quantum-Computing-Group/piquasso>
- [3] A. Tritt, J. Morris, J. Hochstetter, R.P. Anderson, J. Saunderson, and L.D. Turner, *Spinsim: A GPU optimized python package for simulating spin-half and spin-one quantum systems*, *Computer Physics Communications*, vol. 287, p. 108701, 2023. DOI:10.1016/j.cpc.2023.108701
- [4] Lam, S. K., Pitrou, A., & Seibert, S. (2015). Numba: A llvm-based python jit compiler. In *Proceedings of the Second Workshop on the LLVM Compiler Infrastructure in HPC* (pp. 1–6).
- [5] P. Virtanen, R. Gommers, T. E. Oliphant, M. Haberland, T. Reddy, D. Cournapeau, et al., *SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python*, *Nature Methods*, vol. 17, pp. 261–272, 2020. DOI:10.1038/s41592-019-0686-2
- [6] T. Nguyen and A. J. McCaskey, *Extending Python for Quantum-classical Computing via Quantum Just-in-time Compilation*, *ACM Transactions on Quantum Computing*, vol. 3, no. 4, Art. no. 24, Jul. 2022. DOI:10.1145/3544496
- [7] X. Fu et al., *Quingo: A Programming Framework for Heterogeneous Quantum-Classical Computing with NISQ Features*, *ACM Trans. Quant. Comput.*, vol. 2, no. 4, p. 19, 2021. DOI:10.1145/3483528
- [8] Beiser, A. (2003). *Concepts of Modern Physics*. 6th ed. McGraw Hill.
- [9] Leonhardt, U. (2010). *Essential Quantum Optics: From Quantum Measurements to Black Holes*. 1st ed. Cambridge University Press. ISBN: 978-0-521-86978-2, 978-0-521-14505-3.
- [10] Basdevant, J.-L. (2023). *Lectures on Quantum Mechanics. With Problems, Exercises and Solutions*. 3rd ed. Springer, Graduate Texts in Physics. ISBN: 9783031176340, 9783031176357.
- [11] Bowers, P. L. (2020). *Lectures on Quantum Mechanics: A Primer for Mathematicians*. Cambridge University Press. ISBN: 1108429769, 9781108429764.
- [12] Aerts, D., & Beltran, L. (2019). Quantum Structure in Cognition: Human Language as a Boson Gas of Entangled Words. *Foundations of Science*, 25, 755–802. Available at: <https://api.semanticscholar.org/CorpusID:203838565>
- [13] Olver, F., Lozier, D., Boisvert, R., & Clark, C. (2010). *The NIST Handbook of Mathematical Functions*. Cambridge University Press, New York, NY.
- [14] Y. Yao, *Automated design of photonic quantum circuits*, PhD dissertation, Institut Polytechnique de Paris, Feb. 2023. Available at: <https://theses.hal.science/tel-04071095> PDF da tese
- [15] S. Behnel, R. Bradshaw, C. Citro, L. Dalcin, D. S. Seljebotn, e K. Smith, “Cython: The best of both worlds,” *Computing in Science & Engineering*, vol. 13, no. 2, pp. 31–39, 2011.
- [16] C. R. Harris, K. J. Millman, S. J. van der Walt, R. Gommers, P. Virtanen, D. Cournapeau, et al., *Array Programming with NumPy*, *Nature*, vol. 585, no. 7825, pp. 357–362, Sep. 2020. DOI:10.1038/s41586-020-2649-2
- [17] Xanadu Quantum Technologies, *Mr Mustard*, versão 0.7.3, 2023. [Software]. Available at: <https://github.com/XanaduAI/MrMustard>
- [18] Jankiewicz, K., Migdal, P., & Grabarz, P. (2022). Virtual Lab by Quantum Flytrap: Interactive simulation of quantum mechanics. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*, New Orleans, LA, USA. Association for Computing Machinery, New York, NY, USA, Article 175, 1–4. DOI: 10.1145/3491101.3519885. Available at: <https://lab.quantumflytrap.com/>.
- [19] N. Killoran, J. Izaac, N. Quesada, V. Bergholm, M. Amy, and C. Weedbrook, *Strawberry Fields: A Software Platform for Photonic Quantum Computing*, *Quantum*, vol. 3, p. 129, 2019. DOI:10.22331/q-2019-03-11-129

# HHL: Estado da Arte, Limitações e Melhorias

Lucas Amaral e Luis Kowada

**Resumo**— Este trabalho apresenta um algoritmo para solucionar a versão quântica de sistemas de equações lineares chamado *HHL*, salientando suas limitações quanto a sua praticidade. Será introduzido o tipo de problema e descrita as partes do algoritmo. Em seguida, será discutida algumas das restrições que tem que ser levada em consideração para que o ganho computacional se concretize. Por último, expomos melhorias na complexidade que houveram desde então. Dessa forma, este trabalho se apresenta como uma breve revisão da literatura do *HHL*.

**Palavras-Chave**— *HHL*, Problema de Sistema Linear Quântico, Simulação hamiltoniano.

**Abstract**— This work presents an algorithm to solve the quantum version of systems of linear equations called *HHL*, highlighting its limitations in terms of its practicality. The type of problem will be introduced and each part of the algorithm will be described. Next, we will discuss some of the restrictions that have to be taken into consideration for the computational gain to materialize. Finally, we expose improvements in complexity that have occurred since then. With this, this work present itself as a brief literature review on *HHL*.

**Keywords**— *HHL*, Quantum Linear System Problem, Hamiltonian simulation.

## I. INTRODUÇÃO

Sistemas de equações lineares são ferramentas importantes em diversas áreas da ciência. O melhor algoritmo clássico para solucionar este tipo de problema é o Método de Gauss com  $\mathcal{O}(n^3)$ , o qual nos é retornada a solução exata, e o método do Gradiente Descendente com número de operações crescendo linearmente em  $n$ , o qual devolve uma solução aproximada. Em 2009, foi apresentado o algoritmo *HHL* para a solução de um problema *QLSP* (*Quantum Linear System Problem*) que retorna um estado quântico cuja solução é normalizada e codificada nas amplitudes de um registrador, com *speedup* exponencial em relação aos algoritmos clássicos [1].

O *HHL* tem complexidade  $\mathcal{O}(\log ns^2\kappa^2/\epsilon)$ , isto é, logarítmico em função de  $n$ . A melhora da eficiência na solução do problema não é obtida sem ressalvas. Algumas restrições são requeridas para a obtenção do *speedup*. Por exemplo, a matriz de coeficientes deve ser esparsa – o  $s$  da complexidade mencionada acima é a esparcidade da matriz – e o número condicional  $\kappa$  dever ser mínimo –  $\kappa$  é a razão entre o maior e o menor autovalores da matriz de coeficientes [1].

Nas próximas seções, será explorado mais aprofundadamente o algoritmo *HHL*. Na Seção II, será apresentado cada parte do algoritmo. Na Seção III, iremos analisar, brevemente, algumas restrições do algoritmo e como estas se relacionam com a reivindicação de ganho exponencial em eficiência. Na Seção IV, atualizaremos algumas melhoras do algoritmo *HHL* original que foram formuladas ao longo dos anos desde a sua invenção.

Lucas Amaral, IC-UFF, Niterói-RJ, e-mail: amarallucas@id.uff.br; Luis Kowada, IC-UFF, Niterói-RJ, e-mail: luis@ic.uff.br.

## II. O ALGORITMO *HHL*

O problema, essencialmente, consiste em obter a solução de um sistema de equações lineares na forma:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases} \quad (1)$$

O mesmo sistema de equações também pode ser representado pela forma matricial. Neste caso, temos, como entrada, uma matriz, por exemplo,  $A$ , e um vetor  $b$ . Dessa maneira, temos as seguintes representações:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} |b\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \quad (2)$$

A ideia geral do algoritmo é a seguinte:

**Entrada:** A entrada do algoritmo é um sistema de equações lineares representada por um operador hermitiano  $A$ , isto é, ( $A = A^\dagger$ ) e um vetor representado pelas amplitudes de um estado quântico  $|b\rangle$ . Visto que não é provável que sistemas de equações lineares tenha tal configuração, é apresentado um truque que flexibiliza essa restrição. Caso  $A$  não seja uma matriz hermitiana, é possível transformá-la expandindo a matriz e os vetores de entrada com o seguinte truque [1]:

$$C = \begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix} \quad (3)$$

o qual  $C$  seria a nova matriz hermitiana que poderia ser resolvida na nova forma  $Cy = \begin{pmatrix} \vec{b} \\ 0 \end{pmatrix}$  para obter  $y = \begin{pmatrix} 0 \\ \vec{x} \end{pmatrix}$ . Vamos assumir que  $A$ , neste trabalho, já seja hermitiana ou transformada pelo método acima. Assim, queremos resolver o sistema de equações lineares na forma:

$$A|x\rangle = |b\rangle \quad (4)$$

Almejamos aplicar operadores quânticos até chegar a configuração:

$$|x\rangle = A^{-1}|b\rangle \quad (5)$$

A razão da matriz  $A$  ser representada como uma matriz hermitiana é porque sua decomposição espectral poder ser representada como em 6.

$$\sum_{i=0}^{2^{n_b}-1} \lambda_i |u_i\rangle \langle u_i| \quad (6)$$

sendo  $\lambda_i$  e  $|u_i\rangle$ , respectivamente, o  $i$ -ésimo autovalor e autovetor de  $A$ . Assim,  $A$  é composta por uma matriz diagonal na forma:

$$\begin{pmatrix} \lambda_0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_{2^{n_b}-1} \end{pmatrix} \quad (7)$$

multiplicados pelos autovetores.

Para conseguir  $A^{-1}$ , basta inverter os autovalores:

$$A^{-1} = \sum_{i=0}^{2^{n_b}-1} \frac{1}{\lambda_i} |u_i\rangle\langle u_i| \quad (8)$$

**Passo 1:** Para encontrar a inversa de  $A$ , primeiro é usado o *Quantum Phase Estimation (QPE)*, um algoritmo com o qual podemos extrair os autovalores de uma matriz codificando-os nos *qubits*.

**Passo 2:** Em seguida aplicamos as rotações de inversão com a ajuda de um *qubit* de *ancilla*, esta é a inversão do autovalor mencionada anteriormente.

**Passo 3:** Por último, aplicamos a computação inversa do *QPE*. A solução é codificada pelas amplitudes do estado quântico não podendo ser obtido através de uma medição. No entanto, conforme explicam os autores, podem ser usados como sub-rotina de outros problemas.

#### A. Quantum Fourier Transform

A *Quantum Fourier Transform*, ou *QFT*, é uma ferramenta útil na computação quântica, visto que, pode ser efetuada exponencialmente mais rápida quanticamente. A *QFT* pode ser vista como uma transformação do estado inicial, mais especificamente, como uma mudança de base. A base obtida como saída é chamada base de *Fourier*, oposta a base computacional, a que efetuamos medições [6].

A *QFT* transforma a base ortonormal  $|0\rangle \cdots |N-1\rangle$  em uma base resultada da transformação linear do seguinte operador [6]:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |N\rangle \quad (9)$$

sendo o estado  $|j\rangle$ , a representação binária dos estados da base computacional e  $k$ , múltiplos de 2 que representam a posição de cada *qubit*.

É conveniente, para este trabalho, apresentar a *QFT* a partir do produto de cada *qubit*. Esta representação é mostrada na equação 10.

$$|j_1, \dots, j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) \cdots (|0\rangle + e^{2\pi i 0 \cdot j_1 \cdots j_n} |1\rangle)}{2^{n/2}} \quad (10)$$

A partir desta representação é fácil notar que a *QFT* pode ser aplicada a partir de uma sequência de rotações, sendo que, para o primeiro termo, é aplicada uma rotação, e no último termo,  $n$  rotações. Cada rotação pode ser aplicada a partir da porta unitária em 11.

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^{2^k}} \end{bmatrix} \quad (11)$$

#### B. Quantum Phase Estimation

Sabe-se, pelo Teorema Espectral, que matrizes hermitianas podem ser diagonalizáveis, isto é, podem ser decomposta em  $VDV^\dagger$ . Dessa forma, a partir da matriz hermitiana dada como entrada do algoritmo, podemos construir um unitário  $U$  que tenha autovetor  $|u\rangle$  a partir  $V$  e autovalor  $e^{2\pi i \varphi}$  a partir de  $D$  [5][6].

A construção de  $U$  e  $|u\rangle$  não é tratado pelo procedimento, portanto, muitas vezes, o *QPE* é classificado como uma sub-rotina. A propósito, a preparação da matriz de coeficientes e do estado  $|b\rangle$  para o próprio *QLSP*, também é delegado a um oráculo assumindo que há um algoritmo que o construa eficientemente (esta questão será abordada na Seção III).

Para o *QPE*, é utilizado dois registradores: o primeiro registrador possui  $t$  *qubits* sendo  $t$  o número de dígitos para acurácia almejada. É preparado um estado inicial  $|v\rangle$  com tantos *qubits* quanto seja necessário. O algoritmo se dá a partir da aplicação de portas *Hadamard* dos  $t$  *qubits* do primeiro registrador e, em seguida, a aplicação controlada das portas controladas  $U$  a cada *qubit* elevado à potências de 2. Isso produz  $|c\rangle_t |v\rangle \rightarrow |c\rangle_t U^c |v\rangle$  [6].

Essa construção, na verdade, é análoga ao conceito clássico de auto-estado o qual, ao multiplicarmos uma matriz tantas vezes a um vetor, em certo momento, não há mais rotação do vetor. No caso quântico, aplicamos  $U$  a cada *qubit* elevado a potência de dois de acordo com a casa binária de cada dígito.

O estado final é dado pela equação 12.

$$\frac{1}{2^{t/2}} (|0\rangle + e^{2\pi i 2^{t-1} \varphi} |1\rangle) \cdots (|0\rangle + e^{2\pi i 2^0 \varphi} |1\rangle) |v\rangle \quad (12)$$

Perceba que cada expoente  $2^i$  se refere ao casa binária (análoga a casa decimal de base 2) de  $\varphi$  e que o estado  $|v\rangle$  continuou o mesmo durante o procedimento.

O importante de notar, para completar o procedimento, é que, comparando 10 e 12, podemos extrair  $|\varphi_0 \varphi_1 \cdots \varphi_t\rangle$  ao aplicar a *QFT* após a *QPE*. Dessa forma, obtemos os autovalores de  $U$  codificados no primeiro registrador.

#### C. Rotações Controladas

Neste ponto, utilizamos o *qubit* auxiliar para aplicar as rotações necessárias para inverter os autovalores [1]. Para rotacionar os autovalores, aplicamos  $RY(\theta)$  multi-controlada de maneira que os autovalores sejam codificados pelos *qubits*. A porta  $RY(\theta)$  é mostrada na equação 13.

$$RY(\theta) = \begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix} \quad (13)$$

O que almejamos é seguinte transformação:

$$|0\rangle \rightarrow \sqrt{1 - \frac{1}{\lambda_j^2}} |0\rangle + \frac{1}{\lambda_j} |1\rangle \quad (14)$$

A partir desta equação podemos ver que, se o *qubit* auxiliar é  $|1\rangle$ , obtemos uma inversão do autovalor. Para preparar este estado definimos  $\theta = 2 \arcsin \frac{1}{\lambda}$ .

Após essas etapas, aplicamos a computação inversa (*un-computation*). Utilizamos a  $QPE^{-1}$  para obter o resultado da multiplicação entre  $\lambda_i^{-1} |u_i\rangle\langle u_i|$  no primeiro registrador,

e  $|b\rangle$  codificado no segundo, resultando em  $|x\rangle$  no segundo registrador.

### III. LIMITAÇÕES DO ALGORITMO

Apesar de, atualmente, o *HHL* ser reconhecido como um dos algoritmos recentes mais promissores da computação quântica, tal reputação não chega sem desconfiança. Em [2], é apontado alguns problemas do *HHL* que podem influenciar no ganho vultoso de rapidez do algoritmo.

As primeiras limitações do *HHL* são as preparações da porta unitária  $U$  e do estado  $|b\rangle$  de maneira que a sua preparação não afete o ganho obtido. Isto pode ser feito para casos específicos o qual exploraremos nesta Seção. A preparação de  $U$  é feita a partir da simulação hamiltoniana de [3], enquanto a preparação de  $|b\rangle$  é feita a partir de um algoritmo apresentado por [4] para criar estados a partir de uma lista que forma uma distribuição de probabilidade. Por outro lado, os autores aventam a possibilidade do *HHL* ser usado como uma subrotina de outros problemas que já entregam os estados prontos.

#### A. Simulação Hamiltoniana

1) *O Hamiltoniano*: Na mecânica quântica, representamos um procedimento a partir de matrizes unitárias. As matrizes unitárias são transformações lineares de um estado quântico de tempo discreto. A evolução do sistema pode ser representado como:

$$|\psi\rangle \rightarrow U|\psi\rangle \quad (15)$$

Na física, no entanto, o tempo é tratado como um aspecto contínuo, isto é, ao invés de pularmos de um estado  $|\psi\rangle$  para um estado  $U|\psi\rangle$ , esse "pulo" é tratado como um processo contínuo feito em um intervalo de tempo. Assim, definimos o **hamiltoniano** como gerador de operadores unitários a partir de um tempo instantâneo. Os hamiltonianos são sempre representados como matrizes hermitianas, isto é, dado um hamiltoniano  $H$ , temos que  $H = H^\dagger$ . O hamiltoniano não é, necessariamente, uma matriz positiva semi-definida, ou seja, pode ter autovalores negativos [5].

A equação de *Schrödinger* é apresentada em 16:

$$i\hbar \frac{d}{dx} |\psi\rangle = H |\psi\rangle \quad (16)$$

em que  $H$  é um hamiltoniano. Ao assumirmos que  $H$  independe do tempo, podemos derivar, a partir da equação 16, que o estado do sistema, após o tempo  $t$ , é:

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle \quad (17)$$

Dessa forma, transformamos uma equação diferencial, a qual solucionaríamos para cada coordenada do vetor  $|\psi\rangle$ , em uma equação a qual exponenciamos uma matriz como se fosse um escalar [5].

Exponenciar uma matriz pode ser um conceito não usual, mas podemos verificar que, para qualquer matriz diagonal, a solução é a exponenciação dos termos da diagonal. Isto é:

$$\exp\left(\begin{bmatrix} \lambda_0 & & \\ & \ddots & \\ & & \lambda_{n-1} \end{bmatrix}\right) = \begin{bmatrix} e^{\lambda_0} & & \\ & \ddots & \\ & & e^{\lambda_{n-1}} \end{bmatrix} \quad (18)$$

Então, o problema se torna representar o hamiltoniano como uma matriz diagonal. Sabemos que qualquer matriz hermitiana pode ser decomposta em  $VDV^\dagger$  pelo Teorema Espectral. Dessa forma, podemos escrever  $e^H$  como  $Ve^DV^\dagger$ . Com isso, para exponenciar a matriz, é preciso, primeiramente, decompô-la [5].

No entanto, no contexto do *HHL*, decompor a matriz para codificar o hamiltoniano se torna inviável visto que almejamos uma complexidade de  $\mathcal{O}(\log n)$ . Como podemos melhorar isso? Existe métodos de simular esse hamiltoniano eficientemente?

2) *O Problema da Simulação*: Então, como visto na Seção anterior, representamos a dinâmica de um sistema quântico a partir da equação de *Schrödinger* e a solução do sistema, dada uma matriz hermitiana independente do tempo, é  $e^{iHt} |\psi_{inicial}\rangle$ .

$$i\hbar \frac{d}{dx} |\psi\rangle = H |\psi\rangle \quad \Rightarrow \quad |\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle \quad (19)$$

O problema é que exponenciar uma matriz como  $e^{-iHt}$  pode ser computacionalmente difícil, mesmo com a matriz sendo esparsa, o cálculo pode ser exponencial. No entanto, há instâncias às quais o hamiltoniano pode ser escrito como uma combinação linear de termos locais o qual cada termo atua sobre parte do sistema [6][7].

$$H = \sum_{l=1}^L H_l \quad (20)$$

O hamiltoniano é chamado  $k$ -local quando  $H$  atua sobre  $m$  qubits e cada  $H_l$  atua, não trivialmente, em, no máximo,  $k$  qubits. É assumido que, cada  $H_l$  também é hermitiano e pode ser exponenciado diretamente, isto é, é uma evolução que pode ser construída como um circuito quântico e executar em um computador quântico [7]. Fisicamente, este conceito também é muito importante, pois a maioria dos hamiltonianos que ocorrem na natureza são  $k$ -local.

Daí, podemos concluir que é possível decompor um hamiltoniano em um produto das evoluções dos termos locais. Além disso, como cada expoente pode ser representado como um circuito quântico, o problema é resolvido para todo sistema.

$$e^{-iHt} = e^{-iH_1t} e^{-iH_2t} \dots e^{-iH_Lt} \quad (21)$$

$$\text{se } [H_i, H_j] = 0$$

Sendo a restrição  $[H_i, H_j] = H_i H_j - H_j H_i = 0$ , ou seja, se todos os termos locais comutam entre si. Isso ocorre pois esta equação é derivada da fórmula binomial que gera produtos como  $H_1 H_2 H_1$  que é diferente de  $H_1^2 H_2$  [6].

Assim, o problema de simular um hamiltoniano pode ser descrito da seguinte maneira:

**Problema 1.1.** Dado um hamiltoniano  $H$ , uma matriz quadrada hermitiana  $2^n \times 2^n$ , agindo sobre sobre  $n$  qubits no tempo  $t$ , com erro  $\epsilon$ . O objetivo é encontrar a sequência de portas quânticas que implementam uma evolução em função do tempo  $U$  cuja norma da diferença entre a simulação e a evolução ideal seja, no máximo,  $\epsilon$  [6]. Ou seja:

$$\|U - e^{iHt}\| \leq \epsilon \quad (22)$$

Se  $[H_i, H_j] \neq 0$ , o produto de termos locais não se mantém. Neste caso, é usada outra ferramenta mostrada a seguir.

3) *Trotterização*: Para o caso geral, quando os termos locais não são comutativos entre si, pode ser utilizada a *Trotterização*. A fórmula de *Trotter* dá um limite de quantas exponenciações são possíveis para termos locais não comutativos. A fórmula é dada em 23.

$$e^{A+B} = \lim_{m \rightarrow \infty} (e^{A/m} e^{B/m})^m \quad (23)$$

neste caso,  $m$  é o número de iterações. Esse valor deve ser atribuído visando o número de iterações necessárias para que o erro da simulação atinja o valor desejado de  $\epsilon$ , dado em 22.  $A$  e  $B$  são matrizes hermitianas que atuam sobre  $k$  qubits com  $k < n$ . Dessa maneira, a simulação hamiltoniana que, a partir da decomposição em hamiltonianos locais  $A$  e  $B$ , pode ser feita em  $m$  iterações. É importante salientar que existe variações de 23, aqui é mostrada a fórmula de *Trotter* de 1ª ordem.

4) *Decomposição de Hamiltoniano*: Sabe-se que as matrizes de *Pauli* formam uma base ortonormal de matrizes hermitianas cujas dimensões são potências de 2. Consequentemente, dado um hamiltoniano, podemos decompô-lo em matrizes de *Pauli*. Dessa maneira, o problema de simular o hamiltoniano se resume a capacidade de conseguirmos decompor eficientemente um hamiltoniano em termos locais, o que incluem matrizes de *Pauli*.

Uma maneira imediata de obter a decomposição de hamiltonianos é testando todas as possibilidades de produtos entre as matrizes de *Pauli*. Assim, podemos identificar a composição do hamiltoniano, mas há um custo exponencial de comparações que torna o ganho do *HHL* dispensável.

O que queremos é um método de decomposição que seja, pelo menos, tão bom quanto o custo do *HHL* em função da dimensão do hamiltoniano, isto é, uma função logarítmica com o tamanho número de colunas da matriz de entrada.

Muitos trabalhos apostam na representação do hamiltoniano como um grafo para fazer a decomposição em hamiltonianos locais. A ideia é decompor este grafo em múltiplos grafos mais simples a partir da coloração de arestas [3][8].

Em [3] é apresentado um método para decompor eficientemente hamiltonianos representados por matrizes hermitianas esparsas. O procedimento decompõe a matriz de entrada em  $6s$  matrizes 1-esparsa. De [9] sabe-se que podemos aplicar  $e^{-iH_j t}$  diretamente para matrizes 1-esparsa. Daí, podemos utilizar essa informação como *black-box* para implementar a decomposição do hamiltoniano, pelo método mostrado em [3], com custo  $\mathcal{O}(\log^* n)$ .

Mais especificamente, o algoritmo consiste em representar o hamiltoniano como um grafo não direcionado e construir coloração de arestas de maneira que arestas incidentes ao mesmo vértice tenham cores distintas. A coloração é feita diretamente a partir de um ordenação das arestas incidentes aos vértices, isto é, se o vértice  $a$  é o  $i$ -ésimo vizinho de  $b$  e  $b$ , o  $j$ -ésimo vizinho de  $a$ , a cor da aresta é tida, provisoriamente, como o par  $(i, j)$ . Haverá casos em que a associação dos pares desmantelará a coloração de arestas, por isso, também é usado um índice  $v$ , construída a partir de um procedimento que define  $v$  a partir da comparação dos índices dos vértices baseado em [11].

Esse tipo de decomposição, no entanto, adiciona uma restrição ao algoritmo. Da sua execução, é adicionada a dependência de  $s$  na complexidade do *HHL*. A decomposição em termos locais apenas será feita eficientemente se o hamiltoniano for representado como uma matriz esparsa.

Outros procedimentos foram apresentados, posteriormente ao *HHL*, que melhoram a dependência de  $s$  na complexidade. Há uma redução, apresentada por [10], que permite generalizar o problema de qualquer hamiltoniano para grafos bipartidos e aplicar a coloração de arestas para este caso. Outra maneira de fazer isso é dada por [8]. Este consiste em decompor o hamiltoniano em  $6s$  galáxias, a partir da decomposição de  $s$  florestas, para isso, se utiliza do algoritmo dado em [12], que constrói uma floresta a partir da coloração, não necessariamente própria, das arestas.

## B. Preparação de $|b\rangle$

Outra limitação do algoritmo diz respeito a preparação eficiente de  $|b\rangle$ . Como transformar de maneira eficiente  $\bar{b}$  em um estado quântico cujas amplitudes codificam cada  $b_i$  normalizado. Assim, como a simulação da forma  $e^{-iHt}$  descrita anteriormente, [2] aponta a preparação de  $|b\rangle$  como uma ressalva da alegação "*HHL* soluciona  $Ax = b$  em tempo logarítmico".

Em [2], é apontado que  $b$  precisa ser rapidamente carregado na memória de um computador quântico e que, em teoria, isso poderia ser feito através de um *QRAM*, ou *Quantum RAM*, i.e., uma memória que armazena valores clássicos e os possibilita serem lidos uma vez, em superposição. Outra alternativa seria se  $\bar{b}$  fosse descrito por uma fórmula explícita, então, o computador quântico poderia calculá-lo para o próprio utilizá-lo.

No artigo original [1], a preparação de  $|b\rangle$  é terceirizada para o trabalho de [4]. Neste trabalho, é apresentado um procedimento para gerar uma superposição de estados quânticos a partir de uma distribuição de probabilidades com a restrição de que esta distribuição seja eficientemente integrável.

A ideia é gerar eficientemente uma superposição quântica a partir da distribuição de probabilidade  $p_i$ . Tal superposição é mostrada em 24.

$$|\psi(\{p_i\})\rangle = \sum_i \sqrt{p_i} |i\rangle \quad (24)$$

Perceba que, na mecânica quântica, o quadrado da amplitude é tido como a probabilidade daquele estado ser medido,



sendo assim, o procedimento prepara  $\sqrt{p_i}$ . Dessa maneira, o estado  $|i\rangle$  será medido com probabilidade  $p_i$ .

No entanto, [4] não resolve o problema genérico de eficientemente preparar um estado na forma de 24.

Em linhas gerais, o algoritmo ocorre da seguinte maneira. Seja  $n = \log N$ , o qual  $N$  é o número total de uma lista que representa uma distribuição total de probabilidade. Inicialmente, dividimos a distribuição em  $2^m$  regiões com  $m = 0$ . O algoritmo é executado iterativamente construindo 25.

$$|\psi_{(m)}\rangle = \sum_{i=0}^{2^m-1} \sqrt{p_i^{(m)}} |i\rangle \quad (25)$$

Note que  $p_i^{(m)}$  é a probabilidade de uma variável aleatória qualquer  $x$  – ou melhor, a probabilidade de medição – estar na região  $|i\rangle$ . Seguindo a iteração, adicionamos um novo *qubit* ao estado 25 e alcançamos a evolução de 26.

$$\sqrt{p_i^{(m)}} |i\rangle \rightarrow \sqrt{\alpha_i} |i\rangle |0\rangle + \sqrt{\beta_i} |i\rangle |1\rangle \quad (26)$$

o qual  $\alpha$  é a probabilidade de medição na região  $|i, 0\rangle$  e  $\beta$ , a probabilidade de medição na região  $|i, 1\rangle$ . Deste jeito, ajustamos as probabilidades de medição das  $m + 1$  regiões atuais como mostrado em 27.

$$|\psi_{(m+1)}\rangle = \sum_{i=0}^{2^{m+1}-1} \sqrt{p_i^{(m+1)}} |i\rangle \quad (27)$$

Esse processo é repetido até que  $m = n$ , isto é, até que seja obtida a superposição desejada.

#### IV. ESTADO DA ARTE DO HHL

Desde que o *HHL* foi apresentado, em 2009, melhoras na complexidade foram trabalhadas. Houveram melhoras que reduziram a complexidade para um crescimento linear de  $\kappa$  [13], logarítmico em  $\frac{1}{\epsilon}$  e independente da esparsidade  $s$ .

Em [13] é definido uma variação do conhecido *Amplitude Amplification* chamado *Variable Time Amplitude Amplification*, de maneira resumida, consiste em repetir um algoritmo  $t_m$  vezes. À cada iteração, é atualizado um registrador auxiliar que tem como saída: 0, se o algoritmo parou sem a saída desejada; 1, se deveria ser amplificado; e 2, se a computação ainda não parou. A ideia é aplicar a *Variable Time Amplitude Amplification* no *QPE*, isto é, permitir a estimação dos autovalores até a precisão alcance  $\mathcal{O}(\epsilon \tilde{\lambda}_i)$ . O algoritmo diminui a complexidade do algoritmo de  $\mathcal{O}(\kappa^2 \log n)$  para  $\mathcal{O}(\kappa \log^3 \kappa \log n)$ .

Em [14] foi apresentado uma melhora na precisão do *HHL* pela evitação da utilização do *QPE*. Em linhas gerais, a proposta baseia-se em uma técnica genérica de implementar qualquer operador a partir de uma representação de uma série de *Fourier*. A proposta diminui a dependência em  $\text{poly}(\frac{1}{\epsilon})$  para  $\text{poly}(\log \frac{1}{\epsilon})$ .

Em [15], por sua vez, há uma melhora no requisito de esparsidade  $s$  da matriz de entrada. O algoritmo original tinha crescimento quadrático com em função de  $s$ , com a melhora, o algoritmo se torna independente de  $s$ , o que abre caminho para aplicação do *HHL* em matrizes densas. O algoritmo é baseado na execução de uma sub-rotina apresentada de

estimação do valor singular que, por sua vez, utiliza o próprio *QPE* como sub-rotina. Ao final, a complexidade total fica  $\mathcal{O}(\kappa^2 \sqrt{n} \log^* n)$ .

A Tabela I mostra a diferença na complexidade dos diversos algoritmos citados comparados com *HHL* original e com o algoritmo clássico do gradiente descendente.

TABELA I

COMPARAÇÃO DE COMPLEXIDADES DO GRADIENTE DESCENDENTE COM VERSÕES DO *HHL*.

Problema	Algoritmo	Complexidade
LSP	GD	$\mathcal{O}(ns\kappa \log 1/\epsilon)$
QLSP	HHL	$\mathcal{O}(\log ns^2 \kappa^2/\epsilon)$
QLSP	VTAA HHL	$\mathcal{O}(\log ns^2 \kappa/\epsilon)$
QLSP	Childs et al. 2017	$\mathcal{O}(sk \log^*(sk/\epsilon))$
QLSP	QLSA	$\mathcal{O}(k^2 \log^*(n) \ H\ /\epsilon)$

#### V. CONCLUSÕES

Neste trabalho, fazemos uma descrição do algoritmo *HHL* tentando focar em suas limitações. Fornecemos uma intuição do algoritmo e descrevemos as partes. Em seguida, analisamos dificuldades da aplicação do algoritmo de maneira que realmente se extraia a eficiência. Por último, procuramos mostrar o estado da arte com melhorias que ocorreram desde a criação do algoritmo.

#### AGRADECIMENTOS

Agradecimento a coordenação do WECIQ por permitir um ambiente de troca de conhecimento.

#### REFERÊNCIAS

- [1] A. W. Harrow, A. Hassidim e S. Lloyd, *Quantum algorithm for linear systems of equations*. Physical review letters, 2009.
- [2] S. Aaronson *Quantum Machine Learning Algorithms: Read the Fine Print*, Nature Physics, 2014.
- [3] D. W. Berry et al. *Efficient quantum algorithms for simulating sparse Hamiltonians*, Communications in Mathematical Physics, 2007.
- [4] L. Grover e T. Rudolph. *Creating superpositions that correspond to efficiently integrable probability distributions*. 2002.
- [5] S. Aaronson. *Introduction to Quantum Information Science: Lecture Notes* (2018). Communications in Mathematical Physics, 2007.
- [6] M. A. Nielsen e I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2010.
- [7] S. Lloyd. *Universal Quantum Simulators*. Science, 1996.
- [8] R. Kothari. *Efficient simulation of Hamiltonians*. MS thesis. University of Waterloo, 2010.
- [9] A. M. Childs et al. *Exponential algorithmic speedup by a quantum walk*. Proc. 35th ACM Symposium on Foundations of Computer Science, 2003.
- [10] D. W. Berry et al. *Exponential improvement in precision for simulating sparse Hamiltonians*. Proceedings of the forty-sixth annual ACM symposium on Theory of computing, 2014.
- [11] R. Cole e U. Vishkin. *Deterministic coin tossing with applications to optimal parallel list ranking*. Inform. and Control, 1986.
- [12] A. Panconesi e R. Rizzi. *Some simple distributed algorithms for sparse networks*. Distributed computing, 2001.
- [13] A. Ambainis. *Variable time amplitude amplification and quantum algorithms for linear algebra problems*. 29th Symposium on Theoretical Aspects of Computer Science, 2012.
- [14] A. M. Childs et al. *Quantum algorithm for systems of linear equations with exponentially improved dependence on precision*. SIAM Journal on Computing, 2017.
- [15] L. Wossing, Z. Zhao e A. Prakash. *Quantum Linear System for Dense Matrices*. Phys. Rev. Let., 2018.

# Quantum Computing VHDL Library for Hardware Synthesis

Igor Basilio, Luis H. F. Brum, Edmilson M. Batista, Renata H. S. Reiser, Adenauer C. Yamin, Giancarlo Lucca

**Resumo**—Este artigo apresenta o desenvolvimento de uma biblioteca em VHDL para computação quântica visando a síntese em hardware. A biblioteca facilita a implementação de algoritmos quânticos, abordando desafios como a representação de portas quânticas, inicialização de estado e processos de medição. A abordagem baseada em VHDL permite aproveitar as metodologias existentes de design e verificação de hardware para computação quântica, reduzindo assim a lacuna entre o desenvolvimento de algoritmos quânticos e a realização prática em hardware, para validar a biblioteca a implementação do algoritmo de Bernstein-Vazirani foi realizada.

**Palavras-Chave**— Computação Quântica, VHDL, Algoritmo de Bernstein-Vazirani, Portas Quânticas.

**Abstract**—This article presents the development of a VHDL library for quantum computing aimed at hardware synthesis. The library facilitates the implementation of quantum algorithms, addressing challenges such as the representation of quantum gates, state initialization and measurement processes. The VHDL-based approach makes it possible to take advantage of existing hardware design and verification methodologies for quantum computing, thus reducing the gap between the development of quantum algorithms and their practical realization in hardware. To validate the library, the Bernstein-Vazirani algorithm was implemented.

**Keywords**— Quantum Computing, VHDL, Bernstein-Vazirani Algorithm, Quantum Gates.

## I. INTRODUÇÃO

A computação quântica [1] representa uma das fronteiras mais promissoras e desafiadoras da ciência e tecnologia contemporâneas. Diferenciando-se fundamentalmente da computação clássica por basear-se nos princípios da mecânica quântica [7].

Utilizando conceitos como superposição e entrelaçamento, essa linha de pesquisa tenta revolucionar diversos campos, desde a criptografia até o desenvolvimento de novos medicamentos, pela sua capacidade de processar informações em uma escala e velocidade inatingíveis para computadores clássicos [3]. A habilidade única de um computador quântico de analisar uma vasta quantidade de possibilidades simultaneamente abre portas para a solução de problemas complexos considerados impraticáveis ou extremamente demorados

Igor Basilio, Luis Henrique de Freitas Brum, Renata Reiser e Adenauer Yamin. Universidade Federal de Pelotas (UFPEL), Pelotas-Rio Grande do Sul, Pelotas-RS 96010-610, Brazil, e-mail: {ibvalerao, lhdfbrum, edmilson, reiser, adenauer}@inf.ufpel.edu.br; Giancarlo Lucca, Centro de Ciências Sociais e Tecnológicas, Universidade Católica de Pelotas (UCPel), Pelotas-Rio Grande do Sul, e-mail: giancarlo.lucca@ucpel.edu.br. Os autores gostariam de agradecer as seguintes agências de fomento: CAPES, CNPq (309160/2019-7; 311429/2020-3, 150160/2023-2), PqG/FAPERGS (21/2551-0002057-1), FAPERGS/CNPq (23/2551-0000126-8), Projeto TechIn-FlexC3: 309559/2022-7 e Projeto Q-Flex: 409696/2022-6

para a tecnologia atual. No entanto, apesar de seu potencial transformador, a realização prática da computação quântica enfrenta obstáculos significativos, tais como a limitação de recursos computacionais, desafiando cientistas e engenheiros a encontrar soluções inovadoras para tornar essa tecnologia acessível e eficaz.

Dentre os diversos modelos computacionais para a computação quântica, o Modelo de Circuitos Quânticos [3] destaca-se como o mais conhecido e utilizado para interação com o hardware quântico atual. A implementação prática de computadores quânticos é um campo de pesquisa bastante ativo. Apesar dos avanços, o acesso a computadores quânticos físicos ainda é bastante restrito. Além disso, as máquinas existentes estão sujeitas a erros aleatórios devido à decoerência quântica, além de serem limitadas em número de qubits, conectividade e correção de erros integrada. Assim, a simulação em hardware clássico torna-se fundamental para permitir que pesquisadores de algoritmos quânticos testem e validem novos algoritmos em um ambiente com simulação de erros.

Os sistemas de computação estão se tornando cada vez mais heterogêneos, utilizando uma variedade de aceleradores de hardware para aumentar a velocidade das tarefas computacionais. Um desses aceleradores, os *Arrays* de Portas Programáveis em Campo (FPGAs) [5] permitem criar circuitos altamente paralelos especializados capazes de imitar as propriedades de paralelismo quântico das portas quânticas, particularmente para a classe de algoritmos quânticos onde muitos cálculos diferentes podem ser realizados simultaneamente ou como parte de um pipeline profundo.

Diante dos desafios enfrentados pela computação quântica, como, por exemplo, a limitação de recursos, este artigo propõe uma abordagem utilizando FPGAs, programados via VHDL (Very high speed integrated circuit Hardware Description Language) [4], para simular algoritmos quânticos. Apresentamos uma biblioteca desenvolvida especificamente para esse fim, validando-a com a implementação do algoritmo de Bernstein-Vazirani [8].

Exploraremos inicialmente os conceitos fundamentais da computação quântica, essenciais para a compreensão das possibilidades e limitações dessa tecnologia emergente na Seção II. Em seguida, na Seção III, detalharemos como a linguagem VHDL pode ser aplicada na programação de FPGAs para criar simulações eficientes e flexíveis. Os resultados obtidos na implementação da biblioteca são postos na Seção IV e, por fim, as conclusões são postas na Seção V.

## II. FUNDAMENTOS DA COMPUTAÇÃO CLÁSSICA

A computação clássica, tal como a conhecemos hoje, é fundamentada nos princípios da lógica booleana e na manipulação de bits, sendo a unidade básica de informação, representando dois estados possíveis: 0 ou 1. Essa dualidade reflete a natureza binária do hardware computacional, onde transistores — os blocos construtivos dos circuitos integrados — operam como interruptores que podem estar em um de dois estados: ligado ou desligado [11]. A seguir, na Figura 1 está a representação do número binário 87 no gráfico de tensão contra tempo onde 1 é alto, e 0 é baixo.

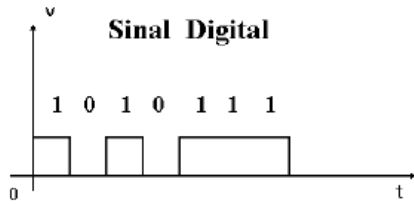


Fig. 1. Representação binária do número 87.

A lógica booleana, com suas operações fundamentais de AND, OR e NOT, é empregada no design de circuitos digitais para processar informações binárias. Os circuitos lógicos construídos a partir dessas operações básicas podem ser combinados em estruturas mais complexas, como somadores, multiplicadores, e registradores, permitindo a realização de todas as operações computacionais fundamentais, a porta NAND sendo uma porta universal capaz de realizar tudo que é computável. Na Figura 2 está a representação de um circuito clássico de duas entradas e uma saída, circuito puramente combinacional.

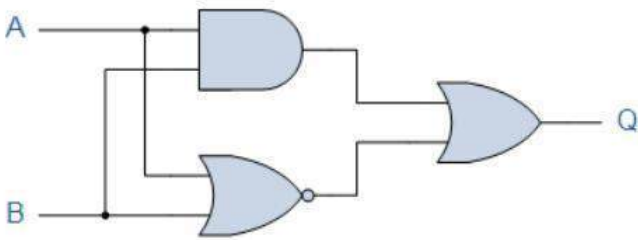


Fig. 2. Ilustração de circuito de duas entradas (A, B) e uma saída Q.

A complexidade e a eficiência dos circuitos lógicos modernos são o resultado direto da inovação contínua em tecnologias de semicondutores, permitindo uma miniaturização sem precedentes e um poder de processamento exponencialmente crescente. No entanto, à medida que nos aproximamos dos limites físicos da miniaturização, enfrentamos desafios crescentes relacionados à eficiência energética e à dissipação de calor, pressionando a indústria a buscar alternativas inovadoras. Uma dessas alternativas é a computação quântica, que, ao contrário da computação clássica, explora os princípios da mecânica quântica [7] para processar informações de maneiras radicalmente novas e mais eficientes para certos tipos de problemas.

### A. Fundamentos Da Computação Quântica

A computação quântica é um campo científico dedicado ao estudo e aplicação das teorias e propriedades da mecânica quântica na área da computação. Ao contrário dos computadores clássicos, os computadores quânticos operam conforme as leis probabilísticas da física quântica, oferecendo o potencial de resolver certos tipos de problemas de forma mais eficiente que os computadores tradicionais. Os computadores quânticos, assim como seus equivalentes clássicos, consistem em hardware e software, utilizando qubits como sua unidade fundamental de informação. Os qubits, diferentemente dos bits clássicos, aproveitam propriedades únicas da mecânica quântica, como superposição e emaranhamento, permitindo processamento de informações de maneira paralela e eficiente. [3]

A Esfera de Bloch é uma representação geométrica de um qubit no espaço, fornecendo uma maneira intuitiva de visualizar o estado de um qubit como um ponto na superfície de uma esfera [13]. Diferentemente dos bits clássicos, cujos estados são binários e lineares, a natureza multidimensional dos qubits e sua capacidade de existir em qualquer superposição de estados exigem uma representação que possa capturar essa complexidade. O emaranhamento quântico, também conhecido como entrelaçamento quântico, é um fenômeno intrigante da mecânica quântica no qual duas ou mais partículas se tornam interdependentes de tal maneira que as propriedades de uma estão intrinsecamente ligadas às propriedades da outra, independentemente da distância entre elas. Esse fenômeno é crucial para o desenvolvimento de tecnologias quânticas, como computação e criptografia quântica, pois permite a correlação instantânea entre qubits, independentemente da distância entre eles, na 3 é retratado a esfera de bloch para um qbit.

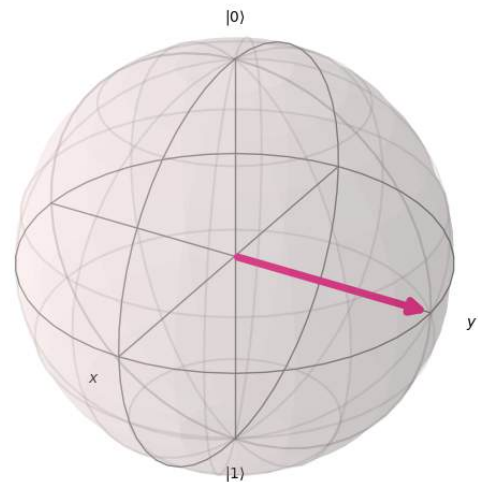


Fig. 3. Representação geométrica de um qubit utilizando a esfera de Bloch, onde o qubit representado é  $|\phi\rangle = \frac{\sqrt{2}}{2}(|0\rangle + i|1\rangle)$

As portas quânticas, operadores matriciais unitários que atuam nos qubits, desempenham um papel central na computação quântica. Analogamente às portas lógicas em computação clássica, as portas quânticas são usadas para realizar diversas

operações, incluindo transformações de estado quântico, rotações e emaranhamento. Elas são os componentes essenciais dos circuitos quânticos, responsáveis pela implementação de algoritmos quânticos e pela realização de cálculos em computadores quânticos. Veja um *framework* para simulação de portas lógicas quânticas em [9].

Na Figura 4 é mostrado como o circuito já apresentado pode ser simulado por portas quânticas.

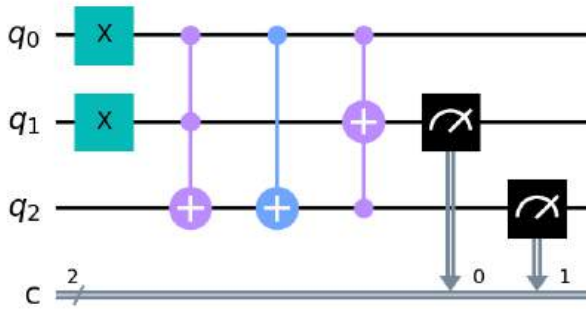
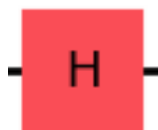


Fig. 4. Circuito quântico que simula o circuito clássico da segunda seção.

Similar aos sistemas clássicos, existe um conjunto de portas quânticas universais que aproxima qualquer porta quântica para uma precisão desejada. Alguns exemplos de conjuntos universais são: {CNOT, Todas portas de 1 qbit}, { CNOT, H, T }, ... , { CNOT,  $R_y(\pi/4)$ , S}.

### B. Portas Lógicas Quânticas

O operador Hadamard [2], denotado pela letra ‘H’, é um operador autoadjunto que pode ser usado para transformar estados não superpostos em estados superpostos (e vice-versa), uma das portas mais importantes de toda a computação quântica. A Figura 5 apresenta a relação entre dessa porta com a matriz equivalente.



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$$

Fig. 5. Relação entre a porta Hadamard (esquerda) e a matriz equivalente (direita).

A porta quântica X [1] frequentemente referida como a porta NOT quântica, é uma das operações fundamentais na computação quântica, análoga à operação NOT da lógica clássica, mas aplicada a qubits. Ela atua sobre um único qubit e tem o efeito de inverter seu estado: transformando o estado base  $|0\rangle$  em  $|1\rangle$  e vice-versa, a Figura 6 mostra a sua representação gráfica e matricial Pauli-X.

A porta Controlled-NOT (CNOT) [14], apresentada na Figura 7 é o mais básico dos operadores de múltiplos qubits. Este possui dois operandos: um qubit de controle e um qubit alvo. Em termos de bases computacionais, seu comportamento pode ser definido da seguinte forma:



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$


$$X|0\rangle = |1\rangle$$

Fig. 6. Porta X (esquerda) e a Matriz Pauli-X (direita).

$|c\rangle|t\rangle \rightarrow |c\rangle|c \oplus t\rangle$  onde  $c$  e  $t$  são, respectivamente, *control* (controle) e *target* (alvo), e " $\oplus$ " é uma adição módulo 2, equivalente ao operador booleano XOR .

Basicamente, o operador Controlled-NOT inverte o estado do qubit alvo quando o qubit de controle é definido como  $|1\rangle$ . Quando o qubit de controle é definido como  $|0\rangle$ , o estado do qubit alvo não sofre alteração. Em ambos os casos, o estado do qubit de controle não sofre alteração.

No geral, o operador Controlled-NOT tende a apresentar o comportamento de um operador Pauli-X aplicado ao qubit alvo quando o qubit de controle colapsa em  $|1\rangle$ .



$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Fig. 7. Porta CNOT (esquerda) e a Matriz da porta CNOT equivalente (direita).

Em suma, as portas de Hadamard e CNOT são fundamentais para a computação quântica devido à sua capacidade de criar superposições, entrelaçar qubits e interferir estados quânticos de maneira que facilita a exploração das propriedades quânticas para a solução eficiente de problemas específicos, existem muitas outras portas quânticas, o mais importante de se lembrar é que uma porta quântica de um Qbit é apenas uma rotação que pode ser vista na esfera de bloch, damos ênfase nestas duas por serem as únicas portas utilizadas para a implementação do algoritmo de Bernstein-Vazirani.

### III. VHDL PARA COMPUTAÇÃO QUÂNTICA

A abordagem de projeto para o desenvolvimento de dispositivos lógicos programáveis com auxílio computacional, conhecida como PLDs (Programmable Logic Device), oferece uma metodologia para conceber e descrever circuitos digitais por meio de ferramentas de descrição de hardware (HDL). Essas linguagens de programação são fundamentadas nas estruturas e comportamentos de seus componentes, manipulando equações booleanas, tabelas verdade e operações complexas de maneira direta. Na descrição estrutural, é detalhada a arquitetura dos componentes e suas interconexões dentro do circuito, enquanto na descrição comportamental [4], modela-se o comportamento dos componentes do circuito.

Utilizando-se as bibliotecas {fixed\_float\_types, fixed\_pkg\_c, float\_pkg\_c, math\_utility\_pkg} podemos

representar um qbit como uma tupla de dois números complexos (c1, c2) [12]. A seguir, é mostrada a representação VHDL para a representação de um número complexo e um qbit nas Figuras 8 e 9, respectivamente.

```
type qcomplex is
record
r : float32;
i : float32;
end record;
```

Fig. 8. Tipo VHDL para representação de um número complexo.

```
type matrix2 is
record
c0: qcomplex;
c1: qcomplex;
end record;
```

Fig. 9. Tipo VHDL para representação de um qbit.

Similarmente conseguimos representar uma porta quântica como uma matriz de dimensão  $2^N \times 2^N$ , composta por números complexos, onde N representa para qual quantidade de qubits a porta será usada, por exemplo, N = 1 {Hadamard, X, Y}. Para exemplificar, é apresentado na Figura 10 a representação em VHDL para uma porta quântica.

```
type matrix4 is
record
c0: qcomplex;
c1: qcomplex;
c2: qcomplex;
c3: qcomplex;
end record;
```

Fig. 10. Tipo VHDL para representação de uma porta quântica 2x2 unitária.

Utilizando síntese comportamental no VHDL, podemos definir a implementação de uma função que recebe um qbit (*matrix2*) e retorna o mesmo qbit depois da aplicação ou multiplicação de matrizes  $H \times Q$  onde:  $H = matrix4$ ,  $Q = matrix2$ , H é predefinida como uma constante ou como argumento de função, a Figura 11 mostra a implementação da constante da porta Hadamard.

Similarmente conseguimos definir a porta CNOT, mas como o entrelaçamento de qubits é inero com tal porta quântica precisamos definir a operação tensorial entre dois qubits de mesmo tamanho, definido no pacote<sup>1</sup>.

#### IV. RESULTADOS

<sup>1</sup>Toda a implementação do trabalho está disponível em um repositório público, disponível em – [https://github.com/Igor-Basilio/TB\\_CQHW](https://github.com/Igor-Basilio/TB_CQHW)

```
constant hadamard_m : matrix4 := ((r => to_float(0.707106), i => to_float(0)),
(r => to_float(0.707106), i => to_float(0)),
(r => to_float(0.707106), i => to_float(0)),
(r => to_float(-0.707106), i => to_float(0)));
```

Fig. 11. Exemplo de constante para a porta quântica Hadamard.

O algoritmo Bernstein-Vazirani é usado para encontrar um número escondido (ou "secreto") em uma função implementada por um oráculo. Em termos simples, o algoritmo resolve um problema de paridade de um número binário secreto, revelando esse número com apenas uma única consulta ao oráculo, sendo uma extensão do problema de Deutsch-Josza para funções de paridade de cadeias de bits secretas. [8] Ele demonstra a capacidade dos computadores quânticos de resolver certos problemas de forma mais eficiente do que os computadores clássicos. Além disso, o algoritmo é um exemplo de como a computação quântica pode superar a computação clássica em termos de complexidade computacional.

Na Figura 12 é mostrado o algoritmo para 8 qubits, subsequentemente na Figura 13 é mostrado a implementação de inicialização dos qubits em  $|0\rangle$  em código VHDL.

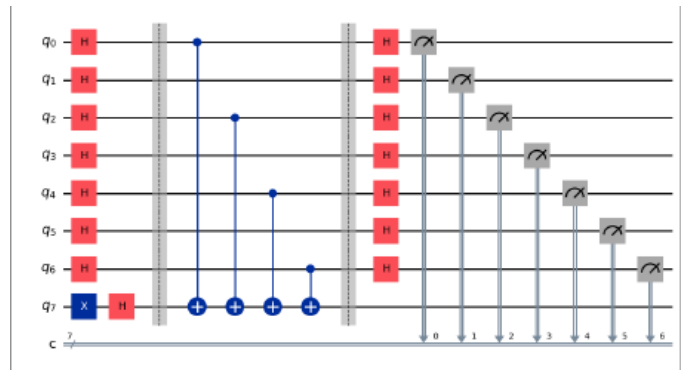


Fig. 12. Algoritmo de Bernstein-Vazirani para 8 qubits, retratado na imagem os bits { q0, q2, q4, q6 } originais estarão ao nível alto lógico, contudo o código representa uma implementação geral para qualquer palavra.

```
-- Initialize all qbits ( length of the secret_number + 1 )
-- To start state | Phi > = | 0 > = ( 1, 0 )
main : process( clk )
begin
if rising_edge( clk ) then
if ctrl = "0000" then
for i in matrix_array'range loop
matrix_array(i).c0.r <= to_float(1);
matrix_array(i).c0.i <= to_float(0);
matrix_array(i).c1.r <= to_float(0);
matrix_array(i).c1.i <= to_float(0);
end loop;
```

Fig. 13. Código VHDL para inicialização de 8 qubits com a palavra secreta sendo de tamanho 8.

No algoritmo Bernstein-Vazirani, são aplicadas as seguintes portas quânticas:

- Porta Hadamard (H)      Porta X (Inversora)
- Porta CNOT (Controlled-NOT)

Essas portas são essenciais para a implementação do algoritmo Bernstein-Vazirani e são utilizadas para manipular os qubits e realizar cálculos quânticos.

O caminho de dados foi testado realizando uma *testbench* com o controle já embutido, depois das imagens de inicialização. A Figura 12 mostrada a aplicação da porta Hadamard em todos os  $(n - 1)$  primeiros qubits e, as portas X e H, aplicadas em sequência, no último qubit  $(n)$ .

Após é aplicada a porta Not Controlada em todos os qubits ao nível alto, é subsequentemente aplicada a porta Hadamard em todos os bits independente do nível. Ao final o resultado é mensurado passando os qubits para uma representação de matriz densidade para a mais fácil realização.

Na Figura 14 é mostrado as portas CNOT e Hadamard sendo aplicadas. Através das figuras apresentadas, fica evidente a sequência de operações necessárias para a execução do algoritmo Bernstein-Vazirani, desde a inicialização dos qubits até a aplicação das portas Hadamard e CNOT, culminando na medição final.

```

elsif ctrl = '0010' then
  -- Applyin Controlled Not on all active Bits on the
  -- Secret number
  for i in q'length - 1 downto 0 loop
    if q(i) = '1' then
      matrix_array4(t) <=
        cx_gate( matrix_array(t), matrix_array( q'length ) );
    end if;
  end loop;

  for i in q'length - 1 downto 0 loop
    if q(i) = '1' then
      matrix_array4(t) <= hadamard4( matrix_array4(t) );
    end if;
  end loop;

  for t in q'length - 1 downto 0 loop
    matrix_array(t) <= hadamard( matrix_array(t) );
  end loop;

```

Fig. 14. Aplicação das portas CNOT e Hadamard, a CNOT sendo aplicada somente aos bits em nível alto.

## V. CONCLUSÕES

A computação quântica enfrenta desafios significativos, como a limitação de recursos e a necessidade de correção de erros. No entanto, a simulação em hardware clássico, especialmente utilizando FPGAs, surge como uma solução viável para testar e validar novos algoritmos quânticos em um ambiente controlado. Isso é crucial para o avanço da área, proporcionando uma plataforma robusta para o desenvolvimento de tecnologias quânticas futuras.

Neste artigo, desenvolvemos uma biblioteca VHDL para a computação quântica, focada na síntese em hardware, que facilita a implementação de algoritmos quânticos. A biblioteca aborda desafios como a representação de portas quânticas, inicialização de estados e processos de medição. Com isso, buscamos reduzir a lacuna entre o desenvolvimento de algoritmos quânticos e a sua realização prática em hardware, aproveitando metodologias existentes de design e verificação de hardware.

Em trabalhos futuros, para validar a biblioteca, implementaremos o algoritmo de Bernstein-Vazirani, um exemplo clássico que demonstra a eficiência da computação quântica na resolução de problemas específicos. Utilizaremos FPGAs programados via VHDL para simular o algoritmo, destacando a aplicação das portas Hadamard e CNOT, essenciais para a manipulação de qubits e realização de cálculos quânticos.

Esta extensão da proposta permitirá uma simulação eficiente e flexível do circuito quântico, provendo uma descrição do paralelismo via hardware em FPGA. E assim, viabilizando análise de resultados empíricos e estatísticos, agregando novas expectativas de níveis de desempenho do algoritmo considerado.

## AGRADECIMENTOS

Os autores gostariam de agradecer à Universidade Católica de Pelotas (UCPEL), Universidade Federal de Pelotas (UFPEL), à Universidade Federal do Rio Grande (FURG), à Universidade Federal do Pampa (UNIPAMPA), assim como ao Laboratório de Sistemas Ubíquos e Paralelos (LUPS).

## REFERÊNCIAS

- [1] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007. 233 pages.
- [2] M. Hirvensalo. *Quantum Computing*. Springer, New York, 2001.
- [3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition, 2010.
- [4] Douglas L. Perry. *VHDL: Programming by Example*. McGraw-Hill, 4th edition, 2002.
- [5] Pong P. Chu. *FPGA Prototyping by VHDL Examples: Xilinx Spartan-3 Version*. John Wiley & Sons, 2008.
- [6] Preskill, J. (2018). *Quantum computing in the NISQ era and beyond*. Quantum, 2, 79.
- [7] R. Shankar, *Principles of Quantum Mechanics*. Springer, 2011
- [8] Ethan Bernstein and Umesh Vazirani. *Quantum complexity theory*. SIAM Journal on Computing, 26(5):1411–1473, 1997.
- [9] Anderson Avila, Helida Santos, Anderson Cruz, Samuel Xavier-de-Souza, Giancarlo Lucca, Bruno Moura, Adenauer Yamin, and Renata Reiser. *Hybrid-GM: A Framework for Quantum Computing Simulation Targeted to Hybrid Parallel Architectures*. Entropy, 25(3):503, 2023.
- [10] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.
- [11] M. Morris Mano e Michael D. Ciletti, *Digital Design: With an Introduction to the Verilog HDL, VHDL, and SystemVerilog*, 6th ed., Prentice Hall, 2017.
- [12] Eduarda R. Monteiro, Diego P. Jaccottet, Antônio C. da Rocha Costa, Eduardo A. C. da Costa, Renata H. S. Reiser, "Aplicando VHDL na Descrição de Circuitos Quânticos", Universidade Católica de Pelotas - Centro Politécnico, Rua Félix da Cunha, 412 - 96010-000 - Pelotas, Brasil.
- [13] L. M. Carvalho, C. Lavor, and V. S. Motta. Caracterização Matemática e Visualização da Esfera de Bloch: Ferramentas para Computação Quântica. *Trends in Computational and Applied Mathematics*, 8(3):351–360, 2007.
- [14] A. U. Khalid, Zeljko Zilic, and K. Radecka. FPGA emulation of quantum circuits. In *Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD 2004)*, pages 310–315, Nov. 2004.

# Quantum Support Vector Regression for Predicting Zeros of the Riemann Zeta Function

Tharso D. Fernandes, Demerson N. Gonçalves and João T. Dias

**Abstract**—The Riemann hypothesis is one of the seven Millennium Prize Problems to be solved. It conjectures that the zeros of the Riemann Zeta function consist solely of negative even integers and complex numbers with real part equal to  $1/2$ . Several numerical studies have been conducted to find new zeros of the zeta function with real part equal to  $1/2$ . Evaluating the zeta function for large values involves time-consuming calculations. In this context, it is highly valuable to have accurate predictions about the zeros of the zeta function to avoid a large number of function evaluations needed to locate them. In this work, we apply the Quantum Support Vector Regression as a tool to assist in empirical studies of zero locations. We also compare it with classical versions of the regressor.

**Keywords**—Zeta Riemann Function, Quantum Machine Learning, Quantum Support Vector Regressor.

## I. INTRODUCTION

The Riemann hypothesis has intrigued mathematicians for centuries, standing as one of the most profound unsolved problems in the field [1]. Its significance lies in its intricate connection to the distribution of prime numbers. The Riemann Zeta Function ( $\zeta$ -function) serves as the cornerstone of this hypothesis. Defined for complex numbers, it plays a pivotal role in understanding the distribution of prime numbers along the real number line. The non-trivial zeros of the  $\zeta$ -function hold the key to unraveling the mysteries of prime numbers [2].

Researchers have explored various approaches to understand the properties of the  $\zeta$ -function. Ref. [3] investigates the connection between scattering amplitudes and  $\zeta$ -function, emphasizing locality and meromorphicity. Another study introduces a novel generalization of the  $\zeta$ -function that converges locally and approximates both trivial and non-trivial zeros [4], while a different work presents efficient methods for computing the  $\zeta$ -function on the critical line, each with varying complexities [5]. On the other hand, regression techniques, coupled with non-parametric machine learning models, offer a fresh perspective. Among these models, Support Vector Regression (SVR) stand out. These algorithms analyze extensive sequences of system parameters or relevant variables, providing insights into the behavior of the  $\zeta$ -function. Surprisingly, despite the growing interest in SVRs, only a few known applications exist for modeling the  $\zeta$ -function [6], [7].

Several recent studies have made significant contributions in exploring the connection between the Riemann  $\zeta$ -function

and quantum computing. Ref. [8] utilizes a Floquet method to identify the first nontrivial zero of the Riemann  $\zeta$ -function and the first two zeros of Pólya's function through periodically driving a single qubit. This experiment successfully characterizes the zeros of these functions by observing crossings of quasi-energies, providing experimental insight into the connection between those two areas. Additionally, quantum computation has been proposed for prime number functions, leveraging Grover's algorithm and the quantum Fourier transform to estimate the prime counting function and verify the Riemann hypothesis efficiently [9]. Another study applied the quantum Fourier transform to analyze functions related to the Riemann hypothesis using quantum computations, highlighting the potential of quantum computing in this domain [10]. Furthermore, a proposed connection between quantum computing and Zeta functions of finite field equations suggests that quantum circuits could approximate the number of solutions of these equations with unparalleled accuracy [11]. These advancements underscore the promising avenues for research at the intersection of quantum computing and the Riemann hypothesis, emphasizing the need for further exploration in this intriguing field.

In this article, we delve into the Riemann hypothesis and explore its implications within the field of quantum computing, shedding light on an area where the intersection of quantum computing and  $\zeta$ -functions remains largely unexplored. Quantum Support Vector Regression (QSVR) opens up an exciting possibility for this examination. Here, we introduce a novel approach by employing QSVR for estimating  $\zeta$ -functions, contributing to the ongoing quest for deeper insights into the connection between quantum mechanics and number theory.

The article is organized as follows: in Section II, we present the Riemann zeta function. Section III introduces the classical version of the SVR, while Section IV discusses the quantum version of the regressor. In Section V, we detail the data selection process for applying the regressors in predicting the zeros of the zeta function. Section VI presents the results obtained by the algorithms in predicting the zeros of the zeta function. Finally, Section VII provides the concluding remarks on the work conducted.

## II. RIEMANN ZETA FUNCTION

In the 1730s, Leonhard Euler delved into the study of the series

$$\sum_{n=1}^{\infty} \frac{1}{n^s}, \quad (1)$$

Tharso D. Fernandes is professor at Department of Pure and Applied Mathematics, UFES, Alegre, ES, E-mail: tharso.fernandes@ufes.br. Demerson N. Gonçalves is professor at Collegiate of Mathematics, CEFET/RJ, Petrópolis, RJ, E-mail: demerson.goncalves@cefet-rj.br. João T. Dias is professor at the Department of Telecommunications, CEFET/RJ, Maracanã, RJ, E-mail: joao.dias@cefet-rj.br.

discovering that  $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \frac{\pi^2}{6}$ , and subsequently deriving expressions for other positive even integers. In 1748, Euler made another significant discovery, famously known as Euler's product:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \quad (2)$$

where the product is taken over all prime numbers  $p$ . In 1859, Bernhard Riemann defined the function known as the zeta function ( $\zeta$ -function) as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad (3)$$

where  $s$  is a complex variable. This series converges absolutely for complex numbers  $s$  with real part of  $s$  ( $\mathcal{R}(s)$ ) greater than 1. Riemann extended the domain of the zeta function, via the process of analytic continuation, to all complex  $s$ , except at the pole  $s = 1$ . The newly extended  $\zeta$ -function [2].

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s), \quad (4)$$

where  $\Gamma$  is the Gamma function, a factorial extension defined as  $\Gamma(s) = \int_0^{\infty} x^{s-1} e^{-x} dx$ . From equation (4), we observe that the  $\zeta$ -function vanishes at negative even integers, which Riemann referred to as trivial zeros. Later, Riemann hypothesized that all other (non-trivial) zeros lie on a critical line ( $\mathcal{R}(s) = \frac{1}{2}$ ). This conjecture is widely known as the Riemann Hypothesis and is now among Hilbert's unsolved problems.

To date, all computations support the Riemann hypothesis. Furthermore, it has been rigorously demonstrated that no non-trivial zeros of the  $\zeta$ -function lie outside of a critical strip, defined by  $s \in \mathbb{C} : 0 < \mathcal{R}(s) < 1$  [12]. On the critical line, we define the Riemann-Siegel  $Z$ -function:

$$Z(t) := \zeta\left(\frac{1}{2} + it\right) \pi^{-it/2} e^{i \arg(\Gamma(\frac{1}{4} + \frac{it}{2}))}. \quad (5)$$

By using the fact that for any complex number  $z$ ,  $\arg(z) = \frac{1}{i} \ln \sqrt{\frac{z}{\bar{z}}}$ , the equation (5) can be simplified to:

$$Z(t) = \zeta\left(\frac{1}{2} + it\right) e^{i\theta(t)}, \quad (6)$$

where  $\theta(t)$  is the Riemann-Siegel  $\theta$ -function:

$$\theta(t) = \arg\left(\Gamma\left(\frac{1}{4} + \frac{it}{2}\right)\right) - \frac{\ln \pi}{2} t. \quad (7)$$

Then, the representation for  $\zeta$ -function on the critical line is:

$$\zeta\left(\frac{1}{2} + it\right) = Z(t) e^{-i\theta(t)}. \quad (8)$$

One advantage of working with the  $Z$ -function over the  $\zeta$ -function is that its values are easier to compute. Carl Siegel developed the asymptotic expansion of the  $Z$ -function in 1932, which is defined as

$$Z(t) = 2 \sum_{n=1}^N \frac{\cos(\theta(t) - t \ln(n))}{\sqrt{n}} + R, \quad (9)$$

where  $N = \lfloor \sqrt{t/2\pi} \rfloor$  and  $R$  is a remainder term. If we separate the  $\zeta$ -function, on critical line into, its real and imaginary parts, we obtain:

$$\zeta(1/2 + it) = Z(t) \cos(\theta(t)) - iZ(t) \sin(\theta(t)), \quad (10)$$

$$A(t) := Z(t) \cos(\theta(t)), \quad (11)$$

$$B(t) := -Z(t) \sin(\theta(t)). \quad (12)$$

Locating zeros of the  $\zeta$ -function on the critical line is equivalent to identifying values of  $t$  where both  $A(t)$  and  $B(t)$  are equal to zero. With this insight, the mathematician Jørgen Gram defined the points bearing his name,  $g_n$ , such that  $\theta(g_n) = (n-1)\pi$ . The existence and uniqueness of such solutions are guaranteed by the monotonicity of the  $\theta$ -function. Regarding the Gram points, it's important to note that:

$$\zeta(1/2 + ig_n) = (-1)^{n-1} Z(g_n). \quad (13)$$

In accordance with the aforementioned equation, if  $g_n$  and  $g_{n+1}$  are two Gram points where  $A(g_n)$  and  $A(g_{n+1})$  share the same sign, then  $Z(g_n)Z(g_{n+1}) < 0$ . Consequently,  $Z(t)$  vanishes at least once within the interval  $(g_n, g_{n+1})$ . Thus, Gram points serve as indicators of intervals containing roots of the Riemann-Siegel  $Z$ -function and, by extension, nontrivial zeros of the Riemann function within the critical strip. By employing this technique, Jørgen Gram demonstrated that the first 15 imaginary parts ( $\gamma_n$ ) of the nontrivial zeros are located between Gram points, specifically  $g_{n-1} < \gamma_n < g_n$ . While this result cannot be generalized [13], it inspired the demonstration that Gram points and the imaginary part of nontrivial zeros are asymptotically equivalent, namely

$$g_n \sim \gamma_n \sim \frac{2n\pi}{\ln(n)}, \quad (14)$$

for large  $n$  [14].

In this study, we will harness this equivalence by computing the Gram points and training both classical (SVR) and quantum (QSVR) algorithms using information about the Gram points. Our objective is to forecast the differences between the Gram points and the imaginary part of the nontrivial zeros of the  $\zeta$ -function ( $\gamma_n - g_{n-1}$ ).

### III. SUPPORT VECTOR REGRESSION

SVR is a potent tool in machine learning, offering a flexible approach to modeling complex relationships in data. In our investigation to predict the zeros of the Riemann  $\zeta$ -function, SVR emerges as a promising technique. Specifically, we will use SVR to predict time-series obtained by taking differences  $\gamma_n - g_{n-1}$ , where  $\gamma_n$  is the imaginary part of the  $n$ -th zero located on the critical line and  $g_{n-1}$  is the  $(n-1)$ -th Gram point.

SVR belongs to the class of supervised learning algorithms and excels at handling nonlinear relationships between input and output variables. By employing kernel functions, SVR can efficiently transform data into a higher dimensional feature space where linear separation becomes feasible. This transformation enables the technique to capture intricate patterns and nuances in the data that may not be discernible in the original feature space [15], [16].



Mathematically, SVR aims to learn a function  $f(x)$  that predicts the output  $y$  for a given input  $x$ :

$$y = f(x) = \langle w, \phi(x) \rangle + b, \quad (15)$$

where  $w$  represents the weight vector,  $b$  is the bias term, and  $\phi(x)$  denotes the feature mapping function that transforms the input data  $x$  into a higher-dimensional space. The angle brackets denote the inner product between  $w$  and  $\phi(x)$ , which is defined as:

$$\langle w, \phi(x) \rangle = \sum_{i=1}^N w_i \phi_i(x). \quad (16)$$

In SVR, the goal is to find the optimal values of  $w$  and  $b$  that minimize the error between the predicted output  $f(x)$  and the true output  $y$ , subject to a specified tolerance margin  $\epsilon$ . This leads to the following optimization problem:

$$\min_{w, b, \xi, \xi^*} \frac{1}{2} \|w\|^2 + C \sum_{i=1}^N (\xi_i + \xi_i^*), \quad (17)$$

subject to the constraints:

$$y_i - \langle w, \phi(x_i) \rangle - b \leq \epsilon + \xi_i, \quad (18)$$

$$\langle w, \phi(x_i) \rangle + b - y_i \leq \epsilon + \xi_i^* \quad (19)$$

$$\xi_i, \xi_i^* \geq 0. \quad (20)$$

$C$  is the regularization parameter that controls the trade-off between minimizing the error and maximizing the margin,  $\xi_i$  and  $\xi_i^*$  are slack variables that measure the deviation of the predicted output from the true output, and  $\epsilon$  is the tolerance margin that determines the acceptable deviation.

To further enhance our analysis, we will also explore the use of Quantum QSVM in addition to classical SVR. This will allow us to compare the performance of both approaches and evaluate their effectiveness in predicting the zeros of the Riemann  $\zeta$ -function.

#### IV. QUANTUM SUPPORT VECTOR REGRESSION

##### A. Quantum kernels

To exploit the power of quantum computing and make use of its advantages, we must encode classical data  $\mathbf{x} \in \mathcal{X} \subset \mathbb{R}^n$  into a quantum state  $|\psi\rangle$  [17]. In quantum computing, the quantum state  $|\psi\rangle$ , which fully describes the qubit, resides in the Hilbert space  $\mathcal{H}$ , providing a natural framework for defining a quantum kernel. The process of mapping classical data  $\mathbf{x}$  to the quantum state  $|\psi\rangle$  is achieved through the map function  $\phi: \mathcal{X} \rightarrow \mathcal{H}$ . Then, the quantum kernel is formulated as:

$$k(\mathbf{x}, \mathbf{x}') = |\langle \phi(\mathbf{x}) | \phi(\mathbf{x}') \rangle|^2, \quad (21)$$

where  $|\phi(\mathbf{x})\rangle = \mathcal{U}_{\phi(\mathbf{x})}|0\rangle$ , and the circuit  $\mathcal{U}_{\phi(\mathbf{x})}$  encodes the classical data  $\mathbf{x}$  into the quantum state  $|\phi(\mathbf{x})\rangle$  using a unitary operator  $\mathcal{U}$ . The state  $\langle \phi(\mathbf{x})|$  represents the dual vector of  $|\phi(\mathbf{x})\rangle$ , obtained by taking the adjoint of  $|\phi(\mathbf{x})\rangle$ , denoted as  $\langle \phi(\mathbf{x})| = |\phi(\mathbf{x})\rangle^\dagger$ . The kernel defined in Eq. (21) can be efficiently estimated by a quantum computer using the well known SWAP Test [18].

In our research, a classical data vector  $\mathbf{x}$  consists of features containing the Riemann-Siegel Z-function and terms of the Riemann-Siegel series applied to two successive Gram points. To obtain a quantum representation of  $\mathbf{x}$ , we employ the feature map defined in [19]:

$$\mathcal{U}_{\phi(\mathbf{x})} = \prod_d \mathcal{U}_{\phi(\mathbf{x})} H^{\otimes n}, \quad (22)$$

where

$$\mathcal{U}_{\phi(\mathbf{x})} = \exp \left( i \sum_{S \subseteq [n]} \phi_S(\mathbf{x}) \prod_{k \in S} Z_k \right). \quad (23)$$

The number  $n$  of qubits is equal to the dimensionality of the classical data  $\mathbf{x}$ . The symbols are encoded through the coefficients  $\phi_S(\mathbf{x})$ , where  $S \subseteq [n] = \{1, \dots, n\}$  describes all possible connections of qubits in the quantum circuit. The encoding function is given by

$$\phi_S : x \mapsto \begin{cases} x_i & \text{if } S = \{i\} \\ (\pi - x_i)(\pi - x_j) & \text{if } S = \{i, j\} \end{cases} \quad (24)$$

and  $Z_k$  is the  $Z$  Pauli matrix acting on the  $k$ -th qubit.

For instance, a quantum circuit that implements  $\mathcal{U}_{\phi(\mathbf{x})}$  using a single-qubit  $Z$  rotation, two-qubit  $ZZ$  rotation and interactions between all qubit pairs will produce blocks of the form

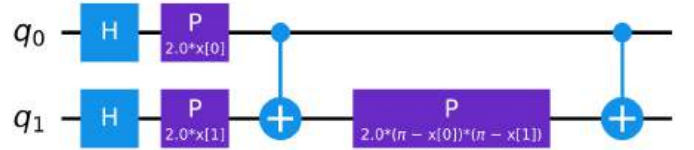


Fig. 1. Quantum circuit of  $\mathcal{U}_{\phi(\mathbf{x})}$  with  $n = 2$  qubits, depth  $d = 1$  and Pauli rotation  $P = R_Z$ .

Finally, it's worth mentioning that the main distinction between SVR and QSVM lies in the origin of the kernel. When the kernel is computed using quantum algorithms, known as a quantum kernel, it pertains to QSVM. Conversely, if the kernel is derived using classical methods, it relates to SVR.

#### V. DATA SET

##### A. Features data

While compiling our initial feature set, we drew inspiration from a relevant study by Shanker [6]. Our selected features for training the algorithms encompass the values of the Riemann-Siegel Z-function, along with the first ten terms of the Riemann-Siegel series (Eq. (9)), and nine terms where the cosine function is replaced by its corresponding sine function for consecutive pairs of Gram points. The exclusion of the initial sine term is justified by its consistent evaluation to zero at Gram points. Thus, the resulting size of our input feature set totals 40. Out of the 40 characteristics available for our simulations, we opted to utilize 10, as the selection of the quantum kernel for the algorithm limited us to no more than 10 features. The chosen features include the values of the Riemann-Siegel Z-function, the first two terms of the Riemann-Siegel series, and 2 terms where the cosine function is replaced

by its corresponding sine function for consecutive pairs of Gram points. The features were computed and arranged in the order described above.

### B. Training and test data

For training and testing the algorithm, we utilized 500 data points corresponding to the Gram points and the zeros of the Riemann zeta function. The primary objective of machine learning regression is prediction, making predictive performance the key metric in evaluating machine learning models. To assess a model's generalizability and identify potential overfitting, it's crucial to evaluate the model using independent data, distinct from the training set. This process, known as data splitting, involves dividing the dataset into separate test and training sets. In our experiments, we employed an 80%/20% data split: 80% of the shuffled data was allocated for training, while the remaining 20% was reserved for testing purposes. The evaluation of the test data was based on the mean squared error (MSE), defined as:

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2, \quad (25)$$

where  $y_i$  represents the true values of the dependent variable and  $\hat{y}_i$  represents the corresponding model predictions. To obtain accurate data on the zeros of the  $\zeta$ -function, we accessed the dataset provided by Odlyzko [21]. This dataset includes over 2 million zeros of the Riemann zeta function, each measured with an accuracy of  $4 \times 10^{-9}$ .

## VI. PREDICTED ZEROS

After training and testing the SVR with 10 features in its classical and quantum versions, we selected 50 random points from the test data to plot a graph showing the algorithm's predictions alongside the known distances of the  $\zeta$ -function to Gram points. The results can be seen in the Fig. 2 and Fig. 3.

The algorithms, in their quantum and classical versions, were trained and tested. The features used were incremented according to what is described in subsection V-A, and the performances of both versions were compared, as can be seen in Fig. 4. We can see that the algorithm using the quantum kernel performed worse than its classical version. However, it's worth noting that the quantum algorithm shows considerable potential for improvement, given the vast possibilities for variations in entanglement gates. Other possibilities should be considered as well. Additionally, an asymptotic analysis of the algorithm's behavior as the dataset size grows was not conducted. An improvement in the performance of the quantum algorithm could be expected in this regard.

## VII. FINAL REMARKS

As can be seen throughout the development this work, the quantum version of SVR can be viewed as an alternative for predicting the zeros of the  $\zeta$ -function on the critical line. Despite exhibiting a relatively inferior performance compared to the classical version, the quantum version offers a greater

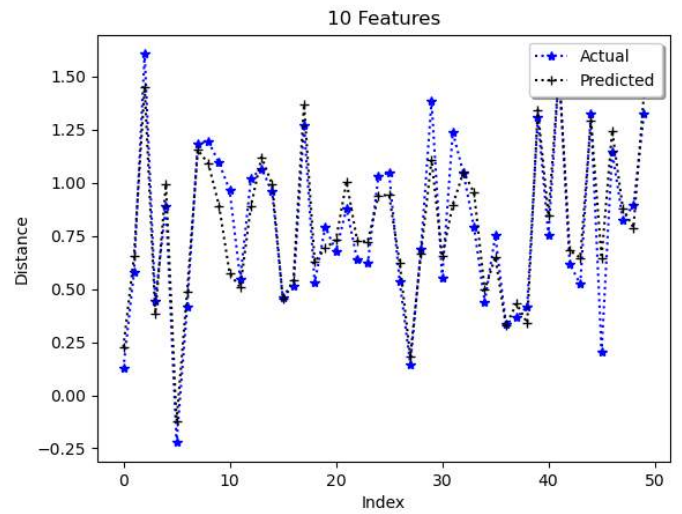


Fig. 2. Using 10 features, SVR predictions versus the actual distance  $\gamma_n - g_{n-1}$  for 50 randomly selected observations from the test data.

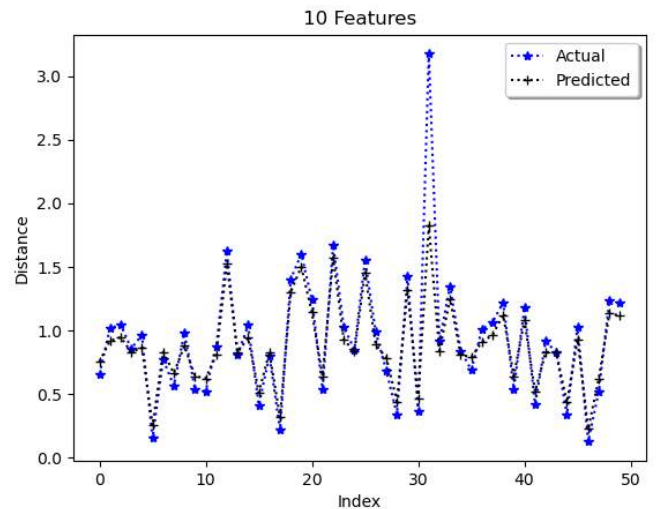


Fig. 3. Using 10 features, QSVR predictions versus the actual distance  $\gamma_n - g_{n-1}$  for 50 randomly selected observations from the test data.

number of possibilities and variations. The challenges arising from the high complexities of the quantum version hinder the investigation of the problem but also provide a range of options for improving the version. A statistical analysis can be conducted on the features used by the quantum version, aiming to select the variables that offer better accuracy for the algorithm. Additionally, studies should be undertaken to enhance the performance of quantum algorithm simulations, as the simulations of quantum algorithms adopted for solving the problem make it impractical to conduct asymptotic analyses on the determination of the zeros of the zeta function.

## REFERENCES

- [1] E. Bombieri. *The Riemann Hypothesis—official problem description*. Clay Mathematics Institute, 2000.

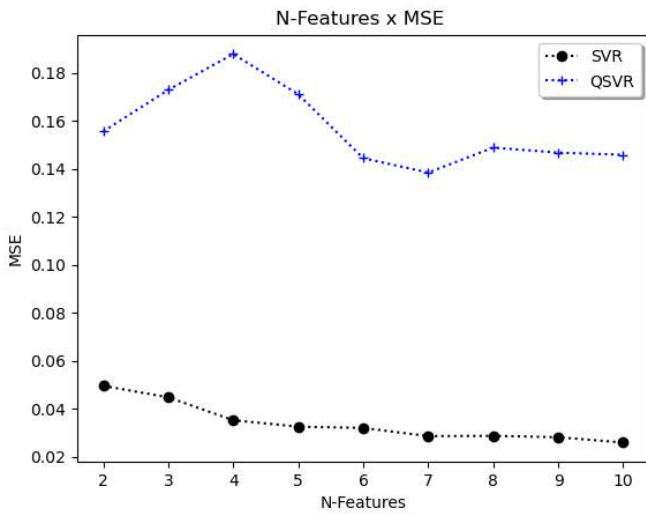


Fig. 4. The MSE decreases with the addition of features to the system.

- [2] A. Awan. *On the Theory of Zeta-functions and L-functions*. Electronic Theses and Dissertations. 53. 2015. Available in <https://stars.library.ucf.edu/etd/5>
- [3] G. N. Remmen. *Amplitudes and the Riemann Zeta Function*. Phys. Rev. Lett. 127, 241602 – Published 8 December 2021.
- [4] M. A. Chaudhry, A. Tassaddiq. *A new generalization of the Riemann zeta function and its difference equation*. Adv Differ Equ 2011. Available in <https://doi.org/10.1186/1687-1847-2011-20>
- [5] G. A. Hiary. *Fast methods to compute the Riemann zeta function*. Pages 891-946 from Volume 174, Issue 2, 2011.
- [6] O. Shanker. *Neural Network prediction of Riemann zeta zeros*. Advanced Modeling and Optimization, 14(3), 717-728, 2012.
- [7] J. Kampe, A. Vysogorets. *Predicting zeros of the riemann zeta function using machine learning: A comparative analysis*. 2018, available online: <https://www.sci.sdsu.edu/math-reu/2018-2.pdf>.
- [8] Ran He, Ming-Zhong Ai, Jin-Ming Cui, Yun-Feng Huang, Yong-Jian Han, Chuan-Feng Li, Tao Tu, C. E. Creffield, G. Sierra, and Guang-Can Guo. *Identifying the Riemann zeros by periodically driving a single qubit*. Phys. Rev. A 101, 043402, 2020.
- [9] J. Latorre, G. Sierra. *Quantum computation of prime number functions*. in Quantum information and Computation, 2014.
- [10] M. McGuigan. *Quantum Computing and the Riemann Hypothesis*. arXiv2303.04602, 2023.
- [11] W. van Dam. *Quantum Computing and Zeroes of Zeta Functions*. quant-ph/0405081, 2004.
- [12] Stein, E. M., & Shakarchi, R. (2010). *Complex analysis (Vol. 2)*. Princeton University Press.
- [13] Hutchinson, J. I. (1925). *On the roots of the Riemann zeta function*. Transactions of the American Mathematical Society, 27(1), 49-60.
- [14] Korolev, M. A. (2014). *On small values of the Riemann zeta-function at Gram points*. Sbornik: Mathematics, 205(1), 63.
- [15] Smola, A.J., Schölkopf, B. *A tutorial on support vector regression*. Statistics and Computing 14, 199–222 (2004).
- [16] Nello C., John N. S. *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*. Cambridge University Press; 2000:i-iv.
- [17] Schuld, M.; Petruccione, F. *Supervised learning with quantum computers*. Cham: Springer, 2018.
- [18] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf. *Quantum fingerprinting*. Phys. Rev. Lett. v. 87, 2001.
- [19] Havlíček, V., Córcoles, A.D., Temme, K. et al. *Supervised learning with quantum-enhanced feature spaces*. Nature 567, 209–212 (2019).
- [20] M. Nielsen, and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [21] A. Odlyzko. *Tables of zeros of the Riemann zeta function*. Available in [https://www-users.cse.umn.edu/~odlyzko/zeta\\_tables/index.html](https://www-users.cse.umn.edu/~odlyzko/zeta_tables/index.html)

# A new Euclidean framework for Quantum-Enhanced Neural Networks.

Francisco Javier Roper Peláez, Ricardo Tiosso Panassiol, Clovis Caface, Karla Vittori

**Abstract**—This paper proposes a novel mathematical framework based on Euclidean algebra that seamlessly integrates the principles of neural and quantum computing. We introduce a method for calculating synaptic weights through vectorial summations, an approach that is naturally aligned with quantum operations. By drawing parallels between the operational mechanisms of biological synapses and quantum systems, we illustrate how principal component analysis can be effectively implemented in the synaptic weights of a standard neuron so that biology is able to mimic processes akin to quantum computation. This integration paves the way for brain-inspired neural architectures that could potentially outperform current ANNs in both speed and cognitive capabilities.

**Keywords**—Quantum Computing, Neural Networks, Euclidean Algebra, Synaptic Weights Principal Component Analysis.

## I. INTRODUCTION

Artificial neural networks, initially conceptualized in the mid-20th century, have undergone significant transformations through the advent of robust algorithms like AlexNet [1] and Generative Pre-trained Transformers, GPTs [2], and advancements in hardware technologies such as GPUs. These innovations have catalyzed remarkable improvements in model performance, managing complex computations across billions of parameters at unprecedented speeds. However, despite these technological strides, the scalability of neural networks continues to be hindered by substantial latency issues, particularly as server demands escalate due to increasing client interactions.

This bottleneck, primarily caused by the extensive computational requirements of contemporary neural network algorithms, presents a critical challenge: achieving real-time processing speeds. Quantum computing emerges as a promising solution with its potential to perform calculations nearly instantaneously, especially for algebraic operations integral to neural networks like summation and matrix multiplication.

Furthermore, traditional neural network training methodologies, such as error back-propagation, are not only time-intensive, often extending over weeks or months, but also prone to converging to local minima rather than global optima. This method also distributes learned information across numerous synaptic weights, making it difficult to pinpoint specific synapses' contributions to learned behaviors.

In contrast, the human brain exhibits a remarkable capacity for continuous, real-time learning, avoiding the pitfalls of

suboptimal local minima and providing a clearer traceability of information across synapses. Despite the relatively slow signal transmission speeds in biological neurons, the brain's efficiency in processing and interpreting complex stimuli remains superior to artificial systems.

Looking ahead, there is a compelling vision where brain-inspired neural networks could gradually replace purely artificial constructs. This transition is supported by the foundational use of vector algebra in both domains, which facilitates operations such as vector projection, normalization, and orthogonalization. The intrinsic alignment between the operational principles of real neuron synapses, whose weight adjustment is governed by Hebbian learning rules equivalent to conditional probabilities [3], and the mathematical underpinnings of quantum computing provides a robust framework for this integration.

Our proposed mathematical foundation aims to unify the principles of Euclidean algebra underpinning both neural and quantum computations, offering a streamlined approach to calculating synaptic weights through simple vectorial summations—ideally suited for quantum processing. Moreover, this framework aligns with principal components analysis a process used by quantum physics to pinpoint the relevant variables associated with a physic phenomenon that we demonstrate is calculated easily under our framework by biological neurons, further illustrating our central nervous system's capability to identify and utilize crucial orthogonal features, a process that quantum systems can parallel.

## II. FROM VECTORS TO PROBABILISTIC CONCEPTS.

$N$ -tuples of real numbers are an ordered collection of numbers. The  $n$ -tuple  $[3, 1, 2]$  may, for example, indicate the number of presynaptic spikes that reach each one of the three synapses of a neuron during a certain period of time.  $N$ -tuples are vectors because they have all the properties of linear spaces.

Although many types of bases are possible, in the  $n$ -tuple linear space we will use a special type of basis called “universal basis”, which is calculated in the following way: having a finite set of  $m$   $n$ -tuples  $\vec{A}^1, \vec{A}^2, \dots, \vec{A}^m$  each of the  $n$  orthogonal axes  $\vec{Y}_i$  of this universal basis is selected so that it has only one component whose value,  $K_i$ , is different from zero.

This component is chosen to be the sum of the absolute values of the corresponding components among the set of  $n$ -tuples:

$$\forall i = 1, 2, \dots, n; j = 1, 2, \dots, m, \vec{Y}_i = [0, 0, \dots, K_i, \dots, 0]$$

Francisco Javier Roper Peláez, CMCC, UFABC, Santo André-SP, francisco.pelaez@ufabc.edu.br; Ricardo Tiosso Panassiol, NBPIP, USP, ricardo.tiosso@usp.com.br; Clovis Caface, CCENT, UEMASUL, Imperatriz-MA e CMCC, UFABC, Santo André-SP, clovis.caface@uemasul.edu.br; Karla Vittori, CMCC, UFABC, Santo André-SP, karla.vittori@ufabc.edu.br.

such that

$$K_i = \sum_{j=1}^m |A_i^j|$$

For example, in the case of the set of n-tuples:

$$\vec{W}^1 = [3, 1, 2]; \vec{W}^2 = [2, 1, 1]; \vec{W}^3 = [3, 5, 1]$$

the first axis  $Y_1$  is the one whose first component is  $3 + 2 + 3 = 8$  with the other components equal to zero. Then,  $\vec{Y}_1 = [8, 0, 0]$ .

Following this criterion, the universal basis is:

$$\vec{Y}_1 = [8, 0, 0]; \vec{Y}_2 = [0, 7, 0]; \vec{Y}_3 = [0, 0, 4]$$

Notice that the universal basis is not normalized (we use the  $l_1$ -norm as we will explain).

Here we define an specific vector,  $U$ , that we call universe or universal vector defined as:

$$\vec{U} = [Y_1, Y_2, Y_3] = [8, 7, 4] \quad (1)$$

Redefinition of universe,  $\vec{U}$ , occurs each time a new vector is placed in it, either as a result of an arbitrary decision, like “let us create a certain vector in  $\vec{U}$ ”, or as a result of an algorithm involving  $\vec{U}$  vectors.

In order to define an Euclidean space, besides selecting an orthogonal basis, we need to define an inner product. According to linear algebra, an inner product is an operation between vectors accomplishing four specific axioms. In the Appendix we show that the following operation between two vectors  $\vec{A} = [A_1, A_2, \dots, A_n]$  and  $\vec{B} = [B_1, B_2, \dots, B_n]$  accomplishes all the axioms that defines any inner product:

$$\vec{A} \cdot \vec{B} = \frac{A_1 B_1}{Y_1} + \frac{A_2 B_2}{Y_2} + \dots + \frac{A_n B_n}{Y_n} = \sum_{i=1}^n \frac{A_i B_i}{Y_i} \quad (2)$$

Where each of the  $Y_i$ s corresponds to each universal basis vectors. In terms of a norm we have chosen the, so called, sum norm (or  $l_1$  norm) that finds the magnitude of vectors as follows

$$\|\vec{A}\| = \sum_{i=1}^n \|A_i Y_i\| = \sum |A_i| |Y_i| \quad (3)$$

The axioms defining this type of norm are shown in the second part of the Appendix. A generic  $n$ -tuple  $\vec{W}$  is, according to the classical treatise from Apostol [4], expressed in terms of its basis as:

$$\begin{aligned} \vec{W} &= C_1 \vec{Y}_1 + C_2 \vec{Y}_2 + \dots + C_n \vec{Y}_n = \\ & \frac{\vec{W} \cdot \vec{Y}_1}{\vec{Y}_1 \cdot \vec{Y}_1} \vec{Y}_1 + \frac{\vec{W} \cdot \vec{Y}_2}{\vec{Y}_2 \cdot \vec{Y}_2} \vec{Y}_2 + \dots + \frac{\vec{W} \cdot \vec{Y}_n}{\vec{Y}_n \cdot \vec{Y}_n} \vec{Y}_n, \end{aligned} \quad (4)$$

The dots represent inner products, being each coefficient  $C_i$  the  $i^{\text{th}}$  component relative to the basis element  $\vec{Y}_i$

$$C_i = \frac{\vec{W} \cdot \vec{Y}_i}{\vec{Y}_i \cdot \vec{Y}_i} \quad (5)$$

For example, a specific  $n$ -tuple  $\vec{W}^1 = [3, 1, 2]$  can be expressed as:

$$\begin{aligned} \vec{W}^1 &= \frac{[3, 1, 2] \cdot [8, 0, 0]}{[8, 0, 0] \cdot [8, 0, 0]} \vec{Y}_1 + \frac{[3, 1, 2] \cdot [0, 7, 0]}{[0, 7, 0] \cdot [0, 7, 0]} \vec{Y}_2 + \\ & \frac{[3, 1, 2] \cdot [0, 0, 4]}{[0, 0, 4] \cdot [0, 0, 4]} \vec{Y}_3 = \\ & \frac{3 \times 8}{8 \times 8} \vec{Y}_1 + \frac{1 \times 7}{7 \times 7} \vec{Y}_2 + \frac{2 \times 4}{4 \times 4} \vec{Y}_3 = \left[ \frac{3}{8}, \frac{1}{7}, \frac{2}{4} \right] \end{aligned}$$

According to this, equation 4 can also be written as:

$$\vec{w} = \frac{W_1}{Y_1} \vec{Y}_1 + \frac{W_2}{Y_2} \vec{Y}_2 + \dots + \frac{W_n}{Y_n} \vec{Y}_n = \left[ \frac{W_1}{Y_1}, \frac{W_2}{Y_2}, \dots, \frac{W_n}{Y_n} \right],$$

where each component  $W_i/Y_i$  of the vector is referred to an axis  $\vec{Y}_i$  from the universal basis.

It is possible to give a probabilistic interpretation when a certain event/vector  $\vec{W}_1$  is composed of finite separate categories,  $\vec{Y}_i$ 's. For example,  $\vec{W}_1$  can be interpreted as the “statistical event” whose probability of belonging to class  $\vec{Y}_1$  is  $3/8$ , to class  $\vec{Y}_2$  is  $1/7$ , and to class  $\vec{Y}_3$  is  $2/4$ . Therefore, vector  $\vec{W}_1$  is treated as a probabilistic event, and so are the classes,  $\vec{Y}_i$ .

To obtain the different types of conditional probabilities the components relative to the basis elements are calculated:

$$C_i = \frac{\vec{W}^1 \cdot \vec{Y}_i}{\vec{Y}_i \cdot \vec{Y}_i} = \frac{(W_i^1 Y_i)/Y_i}{(Y_i Y_i)/Y_i} = \frac{W_i^1}{Y_i} = P(\vec{W}^1/\vec{Y}_i) \quad (6)$$

In the case of the example:

$$\begin{aligned} P(\vec{W}^1/\vec{Y}_1) &= C_1 = \frac{W_1}{Y_1} = \frac{3}{8}; \quad P(\vec{W}^1/\vec{Y}_2) = C_2 = \frac{W_2}{Y_2} = \frac{1}{7}; \\ P(\vec{W}^1/\vec{Y}_3) &= C_3 = \frac{W_3}{Y_3} = \frac{2}{4} \end{aligned}$$

According to this probabilistic interpretation each generic  $\vec{W}$  is a combination of its orthogonal axes where its corresponding components  $C_i$  can be interpreted as conditional probabilities

$$\vec{W} = \sum_{i=1}^N C_i \vec{Y}_i = \sum_{i=1}^n P(\vec{W}/\vec{Y}_i) \vec{Y}_i$$

For calculating the standard probability of  $W$ , the component relative to the universe,  $U$ , is calculated as if the universe were the only axis  $\vec{W}$ , where

$$C_U = \frac{\vec{W} \cdot \vec{U}}{\vec{U} \cdot \vec{U}} = \frac{(WU)/U}{(UU)/U} = \frac{W}{U} = P(\vec{W}/\vec{U}) = P(\vec{W}) \quad (7)$$

So that vector  $\vec{W}$  is defined as a fraction of the universe  $\vec{U}$ . In the case of the example:

$$P(\vec{W}^1) = P(\vec{W}^1/\vec{U}) = C_U = \frac{W^1}{U} = \frac{6}{19}$$

Performing the same operation with a generic  $\vec{W}$  but, in this case, having the  $\vec{U}$  in terms of the bases vectors  $\vec{Y}_i$  we

obtain:

$$\begin{aligned}
 P(\vec{W}) = C_U &= \frac{\vec{W} \cdot \vec{U}}{\vec{U} \cdot \vec{U}} = \frac{[W_1, W_2, \dots, W_n] \cdot [Y_1, Y_2, \dots, Y_n]}{[Y_1, Y_2, \dots, Y_n] \cdot [Y_1, Y_2, \dots, Y_n]} = \\
 &= \frac{\frac{W_1 Y_1}{Y_1} + \frac{W_2 Y_2}{Y_2} + \dots + \frac{W_n Y_n}{Y_n}}{\frac{Y_1 Y_1}{Y_1} + \frac{Y_2 Y_2}{Y_2} + \dots + \frac{Y_n Y_n}{Y_n}} = \frac{W_1 + W_2 + \dots + W_n}{Y_1 + Y_2 + \dots + Y_n} = \\
 &= \frac{W_1}{Y_1 + Y_2 + \dots + Y_n} + \frac{W_2}{Y_1 + Y_2 + \dots + Y_n} + \dots \\
 &\quad + \frac{W_n}{Y_1 + Y_2 + \dots + Y_n} = \\
 &= \frac{W_1}{Y_1} \frac{Y_1}{Y_1 + Y_2 + \dots + Y_n} + \frac{W_2}{Y_2} \frac{Y_2}{Y_1 + Y_2 + \dots + Y_n} + \dots \\
 &\quad + \frac{W_n}{Y_n} \frac{Y_n}{Y_1 + Y_2 + \dots + Y_n} = \\
 &= P(\vec{W}/\vec{Y}_1)P(\vec{Y}_1/\vec{U}) + \dots + P(\vec{W}/\vec{Y}_i)P(\vec{Y}_i/\vec{U}) + \dots \\
 &\quad + P(\vec{W}/\vec{Y}_n)P(\vec{Y}_n/\vec{U}) = \\
 &= P(\vec{W}/\vec{Y}_1)P(\vec{Y}_1) + \dots + P(\vec{W}/\vec{Y}_i)P(\vec{Y}_i) + \dots \\
 &\quad + P(\vec{W}/\vec{Y}_n)P(\vec{Y}_n)
 \end{aligned} \tag{8}$$

That corresponds to the, so called, Law of Total Probability. Another way of reaching to the same result is by calculating the projection of  $\vec{W}$  over  $\vec{U}$ . As an example, let us calculate  $P(\vec{W}^1)$ :

$$\begin{aligned}
 P(\vec{W}^1) = C_U &= \frac{\vec{W}^1 \vec{U}_i}{\vec{U} \vec{U}_i} = \frac{[3, 1, 2][8, 7, 4]}{[8, 7, 4][8, 7, 4]} = \\
 &= \frac{3}{8} \frac{8}{19} + \frac{1}{7} \frac{7}{19} + \frac{2}{4} \frac{4}{19}
 \end{aligned}$$

Another specific case of Eq. 7 is obtaining the probability of the Universe,  $U$ .

$$P(\vec{U}) = P(U/U) = \frac{U}{U} = 1 \tag{9}$$

So that we have:

$$\begin{aligned}
 C_U = P(\vec{U}) &= 1 \text{ and} \\
 C_U = \frac{\vec{U} \cdot \vec{U}}{\vec{U} \cdot \vec{U}} &= \frac{Y_1}{Y_1} \frac{Y_1}{U} + \dots + \frac{Y_i}{Y_i} \frac{Y_i}{U} + \dots + \frac{Y_n}{Y_n} \frac{Y_n}{U} \\
 P(Y_1/U) + \dots + P(Y_i/U) + \dots + P(Y_n/U)
 \end{aligned}$$

and, therefore the sum of the probabilities of the axes in the universal basis is equal to one.

$$P(\vec{Y}_1/U) + \dots + P(\vec{Y}_i/U) + \dots + P(\vec{Y}_n/U) = 1;$$

$$P(\vec{Y}_1) + \dots + P(\vec{Y}_i) + \dots + P(\vec{Y}_n) = 1$$

Let us have a generic  $\vec{W}$ ;  $\vec{W} = k_1 \vec{Y}_1 + k_2 \vec{Y}_2 + \dots + k_n \vec{Y}_n$ . Let us see where the probability operator can be used in both terms of the equation as if were a linear transformation. Calculating

$P(\vec{W})$ , as  $C_U$ :

$$\begin{aligned}
 P(\vec{W}) = C_U &= \frac{(k_1 \vec{Y}_1 + k_2 \vec{Y}_2 + \dots + k_n \vec{Y}_n) \cdot \vec{U}}{\vec{U} \cdot \vec{U}} = \\
 &= \frac{(k_1 \vec{Y}_1 + k_2 \vec{Y}_2 + \dots + k_n \vec{Y}_n) \cdot (\vec{Y}_1 + \vec{Y}_2 + \dots + \vec{Y}_n)}{(\vec{Y}_1 + \vec{Y}_2 + \dots + \vec{Y}_n) \cdot (\vec{Y}_1 + \vec{Y}_2 + \dots + \vec{Y}_n)} = \\
 &= \frac{\frac{k_1 Y_1 Y_1}{Y_1} + \frac{k_2 Y_2 Y_2}{Y_2} + \dots + \frac{k_n Y_n Y_n}{Y_n}}{\frac{Y_1 Y_1}{Y_1} + \frac{Y_2 Y_2}{Y_2} + \dots + \frac{Y_n Y_n}{Y_n}} = \\
 &= \frac{k_1 Y_1 + k_2 Y_2 + \dots + k_n Y_n}{Y_1 + Y_2 + \dots + Y_n} = k_1 \frac{Y_1}{U} + k_2 \frac{Y_2}{U} + \dots + k_n \frac{Y_n}{U} = \\
 &= k_1 P(Y_1) + k_2 P(Y_2) + \dots + k_n P(Y_n)
 \end{aligned}$$

So that

$$P(\vec{W}) = k_1 P(\vec{Y}_1) + k_2 P(\vec{Y}_2) + \dots + k_n P(\vec{Y}_n) \tag{10}$$

this last equation might not be valid for higher-than-one values of  $k_i$  as for example a case in which  $P(\vec{Y}_i) = 1$  and  $k_i > 1$  yielding a higher than one  $P(\vec{W})$ . However, in the case each factor is a probability (a less than one value) this operation is valid.

#### A. Calculating the net input of an artificial neuron

An example of a previous concepts is calculating the net input, net, to an artificial neuron with individual inputs  $I_i$ .

In this case, the  $C_I$ , the components of a generic  $\vec{W}$  relative to  $\vec{I}$  is

$$\begin{aligned}
 C_i = \frac{\vec{W} \cdot \vec{I}}{\vec{I} \cdot \vec{I}} &= \frac{[W_1, W_2, \dots, W_n][I_1, I_2, \dots, I_n]}{[I_1, I_2, \dots, I_n][I_1, I_2, \dots, I_n]} = \\
 &= \frac{\frac{W_1 I_1}{I_1} + \frac{W_2 I_2}{I_2} + \dots + \frac{W_n I_n}{I_n}}{\frac{I_1 I_1}{I_1} + \frac{I_2 I_2}{I_2} + \dots + \frac{I_n I_n}{I_n}} = \\
 &= \frac{W_1}{I_1} \frac{I_1}{I_1 + I_2 + \dots + I_n} + \frac{W_2}{I_2} \frac{I_2}{I_1 + I_2 + \dots + I_n} + \dots \\
 &\quad + \frac{W_n}{I_n} \frac{I_n}{I_1 + I_2 + \dots + I_n} = \\
 &= P(W/I_1) \frac{I_1}{\|I\|} + P(W/I_2) \frac{I_2}{\|I\|} + \dots + P(W/I_n) \frac{I_n}{\|I\|}
 \end{aligned}$$

This result can also be interpreted as the net input, net, of a neuron whose weights are  $P(W/I_i)$ .

$$\text{net} = \sum_{i=1}^n P(W/I_i) \frac{I_i}{\|I\|} = \sum_{i=1}^n P(W/I_i) P(I_i) \tag{11}$$

This equation is biologically plausible [3] and can be interpreted, as the projection of  $\vec{W}$  over input pattern  $\vec{I}$ . Let us recall that in competitive neural networks, each neuron's weight vector is projected over the current input pattern. The neuron with the higher projection is the one that "wins" in the so called, "winner take all" process.

### III. NEURON'S WEIGHT ADJUSTMENT THROUGH REDEFINITION.

In our neurons, synaptic weights are realistically modeled as conditional probabilities. Consequently,  $\vec{W}^1$ ,  $\vec{W}^2$  and  $\vec{W}^3$ , when expressed in terms of their universal axis, they can

represent the weights of three neurons in the second layer of a competitive neural network, with the first layer being where input patterns are positioned.

When a new input pattern is presented to the network, and one of the three competitive neurons fires, it means that the input pattern should be added to the category of the activated neuron. For instance, consider an input pattern  $\vec{I} = [5, 1, 3]$  being input to the network, and neuron 1 with the "raw" weight  $\vec{W}^1 = [3, 1, 2]$  fires. The process of modifying the weights of neuron 1 unfolds as follows. Initially, we update  $\vec{W}^1 = [3, 1, 2]$  by adding the n-tuple  $\vec{I} = [5, 1, 3]$ . This way, the new  $\vec{W}^1$  is obtained as follows:

$$\vec{W}_{new}^1 = \vec{W}^1 + \vec{I} = [3, 1, 2] + [5, 1, 3] = [8, 2, 5]$$

Subsequently, we express this  $\vec{W}_{new}^1$  in terms of the universal basis. In this scenario, the universal basis is updated in accordance with its definition by incorporating the contribution of each component of  $\vec{I} = [5, 1, 3]$  to each axis. Therefore, the new universal basis becomes:

$$\vec{Y}_1 = [Y_1, 0, 0] = [8 + 5, 0, 0] = [13, 0, 0];$$

$$\vec{Y}_2 = [0, Y_2, 0] = [0, 7 + 1, 0] = [0, 8, 0];$$

$$\vec{Y}_3 = [0, 0, Y_3] = [0, 0, 4 + 3] = [0, 0, 7]$$

Being the updated Universe

$$U_{new} = U + I = [8, 7, 4] + [5, 1, 3] = [13, 8, 7]$$

Therefore, when represented in terms of the Universal basis becomes:

$$\vec{W}_{new}^1 = \frac{8}{13}\vec{Y}_1 + \frac{2}{8}\vec{Y}_2 + \frac{5}{7}\vec{Y}_3 = \left[ \frac{8}{13}, \frac{2}{8}, \frac{5}{7} \right]$$

While the n-tuple  $\vec{W}^2 = [2, 1, 1]$  remains unchanged, the redefinition of  $\vec{W}^1 = [3, 1, 2]$  leads to a modification in the representation of  $\vec{W}^2 = [2, 1, 1]$  when expressed in terms of the universal basis:

$$\vec{W}_{new}^2 = \frac{2}{13}\vec{Y}_1 + \frac{1}{8}\vec{Y}_2 + \frac{1}{7}\vec{Y}_3 = \left[ \frac{2}{13}, \frac{1}{8}, \frac{1}{7} \right]$$

Following the redefinition of  $\vec{W}^1, \vec{W}^2$  transforms into  $\vec{W}_{new}^1$ , solely due to the modification of the universal basis during the redefinition of  $\vec{W}^1$ . Consequently, the synapses of  $O_2$ , activated by the input pattern  $\vec{I}$ , decrease their weights, diminishing future firing under similar conditions. We can see that once the sum of inputs is represented in the universal basis, its components become conditional probabilities like in the pre-synaptic rule that is the most biologically plausible rule among Hebbian rules [3]. Considering this fact, it is straightforward to comprehend the following criterion: "The training process of a neuron gradually aligns synaptic weights with the set of input patterns that activated that neuron." This occurs because the set of weights for a neuron is essentially the summation of all input patterns that triggered that neuron, referenced to the universal basis. Vector  $\vec{I}^1$  can also be viewed as the prototype, akin to an average vector, of the input vectors associated with the activation of neuron  $O_1$ .

We can broaden the "redefinition" concept for including not only step-functions (yielding binary outputs) but the output,  $O$ , of any other activation function  $f(x)$ :

$$\vec{W}_{new} = \vec{W} + O\vec{I} = \vec{W} + f(I_{net})\vec{I}$$

where  $O$  is usually between 0 and 1. In this scenario, these equations can be utilized by non-active neurons as well. For instance, let's reconsider the previous example, but this time with an output of  $O = 0.8$ . Starting with the same initial values as in the previous examples,  $\vec{W}^1$  is redefined as follows:

$$\vec{W}_{new}^1 = \vec{W}^1 + O\vec{I} = [3, 1, 2] + 0.8[5, 1, 3] = [7, 1.8, 4.4]$$

When represented in terms of the updated universal basis (which is not influenced by the factor  $O$ ), it produces:

$$\vec{W}_{new}^1 = \frac{7}{13}\vec{Y}_1 + \frac{1.8}{8}\vec{Y}_2 + \frac{4.4}{7}\vec{Y}_3 = \left[ \frac{7}{13}, \frac{1.8}{8}, \frac{4.4}{7} \right]$$

Considering the effect of the activation function, we can rewrite the "golden rule" for weight modification stated at previous section as follows: "*The training process of a neuron makes synaptic weights gradually follow the set of input patterns in a proportion indicated by the output of the activation function*". This simple rule for weight updating can boost neural networks training under both the conventional and quantum paradigms.

#### IV. NEURON'S WEIGHT CONVERGENCE TO PRINCIPAL COMPONENTS

Consider a scenario of a single-layer neural network where all neurons share nearly identical activation functions characterized by the following shape: starting from zero at the origin, they exhibit a moderate increase for average net inputs and experience a substantial, almost exponential increment for higher net inputs. This specific activation pattern aligns with the characteristics observed in thalamic reticular neurons, as depicted in Figure 8 of Mulie et al.'s seminal paper [5].

Let us also suppose that, regarding the inputs, we have a collection of input patterns  $\vec{I}^1, \vec{I}^2, \dots, \vec{I}^p$ . These patterns have been adjusted by subtracting their mean, resulting in inputs presented to the network as  $\vec{I}^1 - \vec{\theta}, \vec{I}^2 - \vec{\theta}, \dots, \vec{I}^p - \vec{\theta}$ . This mean subtraction process aligns with the behavior observed in thalamocortical neurons, as explained in the comments to Figure 4 in Aguiar & Peláez paper [6]. Thus, the output of thalamocortical neurons (neurons in the first layer of the thalamus) that feed into reticular neurons (neurons in the second layer of the thalamus) is stripped of its mean.

What would happen to the weights of reticular-like neurons when patterns  $\vec{I}^i$  similar to  $\vec{\theta}$  are presented? These patterns would result in an almost zero output for each of the reticular neurons. According to our "golden rule," their weights would tend towards zero. This reduction occurs because these patterns, similar to  $\vec{\theta}$  are, due to redefinition, summed in the denominator of our weight expression rather than in the numerators. Therefore, as mentioned earlier, the weights will diminish the contribution of input patterns that resemble  $\vec{\theta}$ , leading to reduced net inputs for these types of patterns.

Now that we know that only de-meant patterns are fed into our reticular-like neurons, what will be the effect of these patterns in reticular weights?

Only patterns that significantly deviate from their mean can activate reticular neurons, considering the shape of the activation function. These patterns will contribute to the weight increment. This cumulative weight sum is expected to indicate the direction of the first Principal Component since it represents the direction in which patterns exhibit the highest variability concerning their mean. In the thalamus, where only the highest activated neuron fires, weights of subsequently firing reticular neurons evolve to represent subsequent orthogonal principal components.

## V. QUANTUM ALTERNATIVE “BRA-KET” NOTATION

Our previous formulation could be used in quantum computing as an alternative notation to the usual “bra-ket” notation [7]. For programmers that do not want to delve into the complexities of the quantum physics notation, our vector formulation in which components are probabilities could be easier to understand. Let us explicit this idea with the classical example of two atoms whose magnetic field,  $M$ , is in a state of “quantum superposition”. We could, for example, obtain a probability of 0.25 of both being in North orientation,  $P(NN) = 0.25$ . The other orientations could be as follows:  $P(NS)=0.125$ ;  $P(SN)=0.125$ ;  $P(SS)=0.5$ . Our notation would show this situation in a very simple way:

$$\vec{M} = 0.25\overrightarrow{NN} + 0.125\overrightarrow{NS} + 0.125\overrightarrow{SN} + 0.5\overrightarrow{SS} \quad (12)$$

However, if we were to use the bra-ket notation the same phenomenon would be represented like this.

$$\vec{M} = \sqrt{0.25} |NN\rangle + \sqrt{0.125} |NS\rangle + \sqrt{0.125} |SN\rangle + \sqrt{0.5} |SS\rangle$$

Our notation would also facilitate the application of quantum logic gates since it is not necessary to square the result to obtain the probabilities at the end, like in this application of the CNOT gate. (In specific cases, little alterations of the matrix would be necessary.)

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0.25 \\ 0.125 \\ 0.5 \\ 0.125 \end{bmatrix} = \begin{bmatrix} 0.25 \\ 0.125 \\ 0.125 \\ 0.5 \end{bmatrix}$$

## VI. CONCLUSIONS

This paper introduces a rigorous mathematical approach integrating quantum computing with neural network methodologies through a Euclidean algebra framework. By adopting vectorial summations for synaptic weight calculations, this method not only aligns closely with the operational principles of quantum mechanics but also enhances the computational efficiency and transparency of neural networks. This foundational work leverages principal component analysis, an analytical tool prevalent in quantum mechanics, to streamline complex computations traditionally executed by artificial neural networks (ANNs).

Our approach extends beyond theoretical development by demonstrating practical implications for neural architecture

design, potentially leading to advancements in cognitive capabilities and processing speeds. By elucidating the relationship between biological neural processes and quantum mechanics, we pave the way for innovative brain-inspired computing architectures. These architectures promise to leverage the intrinsic efficiencies of quantum processes, possibly surpassing existing ANNs in both performance and cognitive depth.

## REFERENCES

- [1] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, 25, 2012.
- [2] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. *Advances in neural information processing systems*, 30, 2017.
- [3] Javier Ropero Peláez and Diego Andina. Do biological synapses perform probabilistic computations? *Neurocomputing*, 114:24–31, 2013.
- [4] Tom M Apostol et al. *Calculus ii: multi variable calculus and linear algebra, with applications to differential equations and probability*. 1969.
- [5] Ch Mulle, Anamaria Madariaga, and M Deschênes. Morphology and electrophysiological properties of reticularis thalami neurons in cat: in vivo study of a thalamic pacemaker. *Journal of Neuroscience*, 6(8):2134–2145, 1986.
- [6] Mariana Antonia Aguiar-Furucho, Francisco Javier Ropero Peláez, et al. Alzheimer’s disease as a result of stimulus reduction in a gaba-a-deficient brain: A neurocomputational model. *Neural Plasticity*, 2020, 2020.
- [7] Michael A. Nielsen and Isaac Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.

## APPENDIX

Here we demonstrate that our inner product accomplishes the axioms that defines any inner product for each pair of elements  $A$  and  $B$  of the linear space of  $n$ -tuples,  $T$ , and for all choices of  $A, B, C$  in  $T$  and all real scalars  $k$ : 1. Commutativity:  $AB = BA$ ; 2. Distributivity:  $A(B + C) = AB + AC$ ; 3. Associativity:  $k(AB) = (kA)B$ ; and, 4. Positivity: If  $A \neq 0 \Rightarrow A.A > 0$ .

$$\text{Proof. Commutativity: } AB = \frac{A_1B_1}{Y_1} + \frac{A_2B_2}{Y_2} + \dots + \frac{A_nB_n}{Y_n} = \frac{B_1A_1}{Y_1} + \frac{B_2A_2}{Y_2} + \dots + \frac{B_nA_n}{Y_n} = BA$$

$$\text{Distributivity: } A.(B + C) = \frac{A_1(B_1+C_1)}{Y_1} + \frac{A_2(B_2+C_2)}{Y_2} + \dots + \frac{A_n(B_n+C_n)}{Y_n} =$$

$$\left( \frac{A_1B_1}{Y_1} + \frac{A_2B_2}{Y_2} + \dots + \frac{A_nB_n}{Y_n} \right) + \left( \frac{A_1C_1}{Y_1} + \frac{A_2C_2}{Y_2} + \dots + \frac{A_nC_n}{Y_n} \right) = A.B + A.C.$$

$$\text{Associativity: } k(A.B) = k \frac{A_1B_1}{Y_1} + k \frac{A_2B_2}{Y_2} + \dots + k \frac{A_nB_n}{Y_n} = \frac{kA_1B_1}{Y_1} + \frac{kA_2B_2}{Y_2} + \dots + \frac{kA_nB_n}{Y_n} = (kA).B.$$

Now we demonstrate that the norm  $\|\vec{A}\| = \sum_{i=1}^n \|A_i \vec{Y}_i\| = \sum |A_i| |Y_i|$  accomplishes the following axioms that defines any norm for each pair of elements  $A$  and  $B$  of the linear space of  $n$ -tuples,  $T$ , and for all choices of  $A, B, C$  in  $T$  and all real scalars  $k$ : 1.  $\|\vec{A}\| = 0$  if  $\vec{A} = 0$ ; 2. Positivity:  $\|\vec{A}\| > 0$  if  $\vec{A} \neq 0$ ; 3. Homogeneity:  $\|k\vec{A}\| = |k| \|\vec{A}\|$ ; 4. Triangle inequality:  $\|\vec{A} + \vec{B}\| \leq \|\vec{A}\| + \|\vec{B}\|$

**Proof.** Properties 1, 2 and 3 directly follow from the norm definition. To demonstrate 4, notice that  $\|\vec{A} + \vec{B}\| = \sum_{i=1}^n |A_i + B_i| |Y_i|$  due to the possibility of  $A_i$  and  $B_i$  being of different sign, is always less or equal than  $\sum_{i=1}^n (|A_i| + |B_i|) |Y_i|$  which is equal to  $\|\vec{A}\| + \|\vec{B}\|$  as required.



# Simulação do Impacto do Espalhamento Raman Espontâneo na Taxa de Transmissão em Sistemas de QKD em Redes Ópticas Passivas

J. S. de Andrade e R. V. Ramos

**Resumo** — Neste trabalho utilizamos a função  $W_q$  de Lambert-Tsallis e simulações numéricas para analisar a taxa de transmissão de bits seguros de um protocolo de QKD em uma rede óptica passiva, com dados clássicos e quânticos coexistindo, quando a potência óptica dos sinais clássicos e o número de usuários variam. Observamos que um aumento da potência óptica dos sinais clássicos tem que ser compensada com o aumento do número de usuários para que a distribuição quântica de chaves possa ser realizada.

**Palavras-Chave** — Distribuição quântica de chaves, redes ópticas, espalhamento Raman espontâneo.

**Abstract** — In this work we use the Lambert-Tsallis  $W_q$  function and numerical simulations to analyze the secure bit rate of a QKD protocol in a passive optical network, with coexistence of classical and quantum data, when the optical power of classical data and the number of users change. We observe that an increase of the classical optical power must be compensated by an increase of the number of users to permit the realization of QKD.

**Keywords**— Quantum key distribution, optical networks, spontaneous Raman scattering.

## I. INTRODUÇÃO

A tecnologia quântica, já comercialmente disponível, conhecida como Distribuição Quântica de Chaves (*quantum key distribution* - QKD), possibilita o estabelecimento seguro de uma chave, uma sequência aleatória de bits, entre usuários espacialmente distantes conhecidos como Alice e Bob [1-12]. A chave distribuída é utilizada em protocolos de criptografia, permitindo a transmissão segura de informações entre Alice e Bob através do protocolo de chave simétrica *one-time pad*, no qual a chave é utilizada uma única vez e a codificação (decodificação) consiste na operação lógica XOR (ou-exclusivo) entre chave e mensagem (texto cifrado). Entretanto, a implementação de QKD em redes ópticas reais enfrenta desafios consideráveis. Um desses desafios é a coexistência de dados clássicos e quânticos na mesma rede óptica [13-18]. Neste caso em que dados clássicos (pulsos ópticos intensos) e quânticos (pulsos ópticos fracos) percorrem a mesma fibra óptica, o espalhamento Raman espontâneo surge como o principal ruído, limitando o comprimento máximo do canal. Note-se que, para ser amplamente adotada, uma configuração óptica de QKD precisa ser flexível, reconfigurável e escalável. Essas

características podem ser alcançadas ao se realizar QKD em redes ópticas já instaladas, integrando dados quânticos e clássicos na mesma fibra óptica. No entanto, devido à substancial diferença de potência óptica utilizada pelos protocolos de comunicação quântica e clássica, a coexistência de sinais de dados quânticos e clássicos na mesma fibra óptica pode prejudicar o protocolo quântico.

A presença de amplificadores ópticos na rede óptica impede a realização de QKD na janela de 1550 nm devido ao intenso ruído de emissão espontânea amplificada nessa parte do espectro. Em tal situação, o protocolo de QKD poderia ser implementado em 1310 nm. Entretanto, devido à elevada perda óptica na fibra nesse comprimento de onda, a distância entre o transmissor e o receptor é severamente limitada. Para alcançar distâncias maiores, é necessário executar o protocolo de QKD em 1550 nm e os dados clássicos em outro comprimento de onda, como 1310 nm. A colocação de dados quânticos e clássicos na janela de 1550 nm é possível se uma fibra multinúcleos for utilizada, embora essas fibras ainda sejam caras e apresentem diafonia entre diferentes núcleos, o que deve ser considerado. Outra opção é o uso de redes ópticas passivas (*passive optical network* - PON), onde amplificadores ópticos não são empregados. Em todos esses casos, o *crosstalk* linear proveniente de (de)multiplexadores e filtros ópticos imperfeitos, juntamente com vários efeitos não lineares, como mistura de quatro ondas (*four-wave mixing* - FWM) e os espalhamentos de Brillouin, Rayleigh e Raman, dificultam a integração eficiente de dados quânticos e clássicos [13-15].

Embora seja possível evitar a FWM e os espalhamentos Brillouin e Rayleigh alocando o canal quântico de forma espectralmente distante dos canais de dados clássicos, o espalhamento Raman espontâneo (*Spontaneous Raman Scattering* - SRS) apresenta uma grande largura espectral e, portanto, pode não ser completamente evitado. Assim, o desafio mais significativo na coexistência de dados quânticos e clássicos na mesma fibra óptica é a geração de falsas contagens causadas pelo espalhamento Raman espontâneo [13,16-18]. O SRS aumenta a taxa de erro quântico (*quantum bit error rate* - QBER), reduzindo a taxa de transmissão de bits seguros da chave. Desta forma, um projeto cuidadoso de redes ópticas que suportem serviços quânticos e clássicos deve considerar a geração do SRS e o impacto do mesmo em protocolos de QKD.

Neste contexto, o presente trabalho utiliza a função de Lambert-Tsallis e simulações numéricas na análise da taxa de transmissão de bits seguros do protocolo de QKD BB84 com dois estados iscas, em uma topologia de rede óptica passiva chamada configuração *downstream* [13,17,18] com coexistência

Joacir Soares de Andrade, Departamento de Telemática, IFCE, Fortaleza-Ce, e-mail: joacirandrade@ppget.ifce.edu.br; Rubens Viana Ramos, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce, e-mail: rubens.ramos@ufc.br.

de dados quânticos e clássicos, quando a potência óptica do sinal clássico e o número de usuários variam.

Este trabalho está dividido da seguinte forma: na Seção 2 é feita uma revisão da função de *Lambert-Tsallis*; Na Seção 3 o efeito do SRS no protocolo de QKD é descrito e as simulações numéricas são realizadas. Por fim as conclusões são descritas na Seção 4.

## II. A FUNÇÃO DE LAMBERT-TSALLIS

A função  $W_q$  de *Lambert-Tsallis* pode ser usada para resolver algumas equações não lineares nas quais as variáveis independente e dependente estão relacionadas por uma lei de potência. Ela é definida como a solução da equação [19]

$$W_q(z) e_q^{W_q(z)} = z \quad (1)$$

Em (1), a  $q$ -exponencial de *Tsallis* é dada por [20-21]

$$e_q^z = [1 + (1-q)z]^{1/(1-q)} \text{ for } q \neq 1 \text{ \& } 1 + (1-q)z \geq 0 \quad (2)$$

Além disso,  $e_q^z = 0$  quando  $1 + (1-q)z < 0$ . Obviamente,  $\lim_{q \rightarrow 1} e_q^z = e^z$ , portanto,  $\lim_{q \rightarrow 1} W_q(z) = W(z)$ , sendo  $W(z)$  a função de Lambert [22-23]. É possível encontrar a forma analítica de  $W_q$  para alguns poucos casos [19], sendo a mais simples delas obtida quando  $q=2$ ,  $W_2(z) = z/(1+z)$  definida para  $z > -1$ . No caso geral,  $W_q(z)$  tem que ser calculada numericamente. Por exemplo, usando o método de *Halley* para calcular  $W_q(z)$  tem-se:

$$w_q(j+1) = w_q(j) - \frac{A}{B - \frac{AC}{2B}} \quad (3)$$

$$A = w_q(j) e_q^{w_q(j)} - z \quad (4)$$

$$B = e_q^{w_q(j)} + w_q(j) e_q^{q w_q(j)} \quad (5)$$

$$C = 2e_q^{q w_q(j)} + \frac{w_q(j)}{q} e_q^{(2q-1)w_q(j)} \quad (6)$$

Na Fig. 1 podem-se ver as curvas de  $W_{3/4}(z)$  ( $q < 1$ ),  $W_{5/4}(z)$  ( $q > 1$ ) e  $W(z)$  ( $q = 1$ ) versus  $z$ . Pode-se mostrar que o ponto de ramificação de  $W_q(z)$  (ponto onde  $dW_q(z)/dz = \infty$ ) é dado pelos pontos  $z_b = \exp_q(q-2)/(q-2)$ ,  $W_q(z_b) = 1/(q-2)$ . Mais detalhes sobre a função  $W_q$  podem ser encontrados em [24-27].

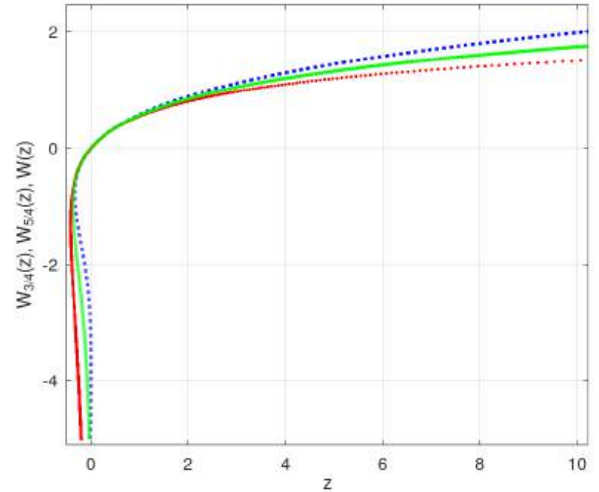


Fig. 1.  $W_{3/4}(z)$  (linha pontilhada azul),  $W_{5/4}(z)$  (linha pontilhada vermelha) e  $W(z)$  (linha contínua verde) versus  $z$ .

## III. IMPACTO DO SRS EM QKD EM REDES PON

Na comunicação clássica, o sinal *downstream* do terminal de linha óptica (*optical line terminal* - OLT) no escritório central é enviado a todos os usuários por um divisor de feixes, e o sinal *upstream* de apenas uma unidade de rede óptica (*Optical network unit* - ONU) colocada no nó do usuário é transmitido para OLT em cada intervalo de tempo [28]. No caso de uma rede de acesso quântico (*quantum access network* - QAN) usando a estrutura PON, pode-se ter duas configurações: 1) *Downstream*, em que o receptor QKD é colocado nos nós dos usuários [29] e 2) *upstream*, em que o transmissor QKD é colocado nos nós dos usuários [17]. Como a configuração *downstream* tem menos ruído SRS do que a configuração *upstream* e a taxa de geração segura não depende do número de usuários, neste trabalho consideraremos apenas a configuração *downstream*  $1 \times N$ : uma OLT com transmissor QKD e  $N$  ONU's, cada uma com seu receptor QKD. Entre a OLT e a ONU estão a fibra alimentadora, com comprimento  $L_F$ , um divisor de potência passivo  $1 \times N$  (alimentador único) e as fibras de descida com comprimento  $L_D \ll L_F$ . Assim como em [13], consideramos que os fótons de ruído SRS são gerados principalmente pelo sinal OLT. Além disso, consideramos que os dados clássicos são transmitidos em 1310 nm enquanto que os dados quânticos são transmitidos em 1550 nm. O sinal OLT gera fótons de ruído SRS tanto na fibra alimentadora (*feed* -  $S_F$ ) quanto na fibra de descida (*drop* -  $S_D$ ). Os valores de  $S_F$  e  $S_D$  são dados pelas equações [16]

$$S_F = \left\{ P\beta / \left[ N(\alpha_q - \alpha_c) \right] \right\} \left( e^{-\alpha_c L_F} - e^{-\alpha_q L_F} \right) e^{-\alpha_q L_D} \quad (7)$$

$$S_D = \left\{ P\beta / \left[ N(\alpha_q - \alpha_c) \right] \right\} \left( e^{-\alpha_c L_D} - e^{-\alpha_q L_D} \right) e^{-\alpha_c L_F} \quad (8)$$

nas quais  $P$  é a potência de lançamento do sinal OLT,  $N$  é a taxa de divisão do divisor de potência,  $\beta$  é o coeficiente SRS,  $\alpha_c$  ( $\alpha_q$ ) é a perda de fibra no comprimento de onda dos dados clássicos (quânticos). Consideramos o protocolo BB84 em QKD com dois

estados isca [30]. A taxa de chave segura do protocolo é limitada inferiormente por

$$R = q \left\{ Q_1 \left[ 1 - H_2(e_1) \right] - f_{ec} Q_\mu H_2(e_\mu) \right\} \quad (9)$$

sendo  $q = 1/2$  para o caso do protocolo BB84,  $f_{ec}$  é a eficiência da correção de erros,  $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ ,  $Q_\mu$  e  $e_\mu$  são o ganho geral e taxa de erro de bits quânticos (*qubit error rate* – QBER) do estado do sinal, enquanto  $Q_1$  e  $e_1$  são o ganho e QBER dos estados de um fóton do sinal. Assumindo o estado do sinal QKD com número médio de fótons  $\mu$  e dois estados iscas com números médios de fótons  $\nu$  ( $< \mu$ ) e 0, a eq. (9) é calculada usando [15, 16]

$$Q_{\mu(\nu)} = 1 - (1 - Y_0) \exp\left(-\mu(\nu) \eta_B e^{-\alpha_q L - 10 \log_{10}(N)}\right) \quad (10)$$

$$e_{\mu(\nu)} = e_d + \left[ (1/2 - e_d) Y_0 \right] / Q_{\mu(\nu)}, \quad (11)$$

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left( Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right), \quad (12)$$

$$e_1 = (e_\nu Q_\nu e^\nu - 0.5 Y_0) / (Y_1 \nu), \quad (13)$$

$$Y_1 = \frac{\mu}{\mu\nu - \nu^2} \left( Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right), \quad (14)$$

$$Y_0 = 2p_{dark} + p_R(L). \quad (15)$$

Em (10)-(11) o comprimento do canal é igual a  $L$  e  $\eta_b$  é a eficiência quântica do detector de fótons únicos do receptor. O parâmetro  $e_d$  representa os erros de desalinhamento, visibilidade não unitária do interferômetro e modulação imperfeita,  $p_{dark}$  é a taxa de contagem de escuro dos detectores de fótons únicos e  $p_R(L)$  é probabilidade de haver uma detecção causada por fótons gerados pelo SRS na fibra óptica sendo dada por [18]

$$p_R(L) = \left\{ [S_F(L) + S_D(L)] \Delta f \Delta t \eta_B \right\} / (hf). \quad (16)$$

Em (16)  $h$  é a constante de Planck,  $f$  é a frequência óptica do sinal quântico,  $\Delta f$  é a largura de banda de recepção do canal quântico e  $\Delta t$  é o intervalo de tempo efetivo em que o detector está apto a ter uma detecção (largura dos pulsos de gatilho do detector de fótons).

A partir de um valor para  $p_R$ , utiliza-se (16) para obter o valor de  $S_F + S_D$ . O valor de  $S_F + S_D$ , por sua vez, é utilizado em (7) + (8). Por fim, o comprimento do canal,  $L = L_D + L_F$ , é obtido usando a função  $W_q$  de Lambert-Tsallis para inverter (7) + (8). O resultado é  $(\alpha_q < \alpha_c)$  [27]

$$L = \frac{1}{\alpha_q - \alpha_c} \ln \left( \frac{\alpha_q}{\alpha_q - \alpha_c} W_{1 - \frac{\alpha_q}{\alpha_c - \alpha_q}} \left[ \frac{\alpha_q - \alpha_c}{\alpha_q} (-z)^{\frac{\alpha_c - \alpha_q}{\alpha_q}} \right] \right) \quad (17)$$

$$z = \frac{N(S_F + S_D)(\alpha_q - \alpha_c)}{P\beta} = \frac{Nhf p_R(\alpha_q - \alpha_c)}{\Delta f \Delta t \eta_B P \beta}. \quad (18)$$

Usando o ponto de ramificação de  $W_q$  na eq. (17) pode-se encontrar a seguinte relação entre  $P$ ,  $N$  e  $p_R$ :

$$\frac{N p_R}{P} \geq \frac{\Delta f \Delta t \eta_B \beta \left[ 1 - (\alpha_q / \alpha_c) \right]}{hf (\alpha_c - \alpha_q)} \left( \frac{\alpha_q}{\alpha_c} \right)^{\frac{\alpha_q}{\alpha_c - \alpha_q}}. \quad (19)$$

Em outras palavras, se a eq. (19) não for satisfeita, não será possível encontrar um valor para  $L$ . De acordo com (9)-(15),  $R$  é máximo quando  $Y_0$  é mínimo (quanto menor o ruído, maior a taxa de transmissão). O valor mínimo de  $Y_0$  é alcançado quando  $p_R$  é mínimo e, conforme (19), o valor mínimo de  $p_R$  é [27]

$$p_R^{\min} = \frac{P \Delta f \Delta t \eta_B \beta \left[ 1 - (\alpha_q / \alpha_c) \right]}{N hf (\alpha_c - \alpha_q)} \left( \frac{\alpha_q}{\alpha_c} \right)^{\frac{\alpha_q}{\alpha_c - \alpha_q}}. \quad (20)$$

Portanto, substituindo (20) em (17)-(18), o valor ótimo de  $L$  é dado por

$$L^{opt} = \frac{1}{\alpha_q - \alpha_c} \ln \left( \frac{\alpha_q}{\alpha_q - \alpha_c} W_{1 - \frac{\alpha_q}{\alpha_c - \alpha_q}} \left[ \frac{\alpha_q - \alpha_c}{\alpha_c} \left[ \frac{\alpha_c - \alpha_q}{\alpha_c} \right]^{\frac{\alpha_c - \alpha_q}{\alpha_q}} \right] \right). \quad (21)$$

Como se pode notar, quanto menor o valor de  $\alpha_c$  maior é o valor de  $L^{opt}$ . Isso acontece porque será necessário mais comprimento de fibra para atenuar o sinal clássico (o que diminui o SRS) ao nível aceitável.

Para analisar a variação da taxa de transmissão de bits seguros da chave quando a potência óptica clássica e o número de usuários variam, simulamos numericamente a eq. (9). Em nossa simulação usamos  $\alpha_c = 0.48$  dB/km (1310 nm),  $\alpha_q = 0.27$  dB/km (1550nm),  $\eta_B = 0.15$ ,  $P = \{0.25, 0.5, 0.6\}$  mW,  $N = \{4, 8, 16\}$ ,  $hf$  é a energia do fóton em 1550 nm,  $p_{dark} = 2 \times 10^{-7}$ ,  $\Delta t = 1$  ns,  $\Delta f = 100$  GHz,  $f_{ec} = 1.2$ ,  $\mu = 0.4$ ,  $\nu = 0.1$ ,  $e_d = 0.02$  e  $\beta = 7 \times 10^{-9} \text{nm}^{-1}$ . As perdas de inserção dos divisores de potência são 6.2 dB, 9.2 dB e 12.7 dB para  $1 \times 4$ ,  $1 \times 8$ ,  $1 \times 16$ , respectivamente. Não estamos considerando o efeito de *afterpulsing* nos detectores. Os resultados das simulações podem ser vistos nas Figs. 2 ( $P = 0.25$  mW), 3 ( $P = 0.5$  mW) e 4 ( $P = 0.6$  mW).

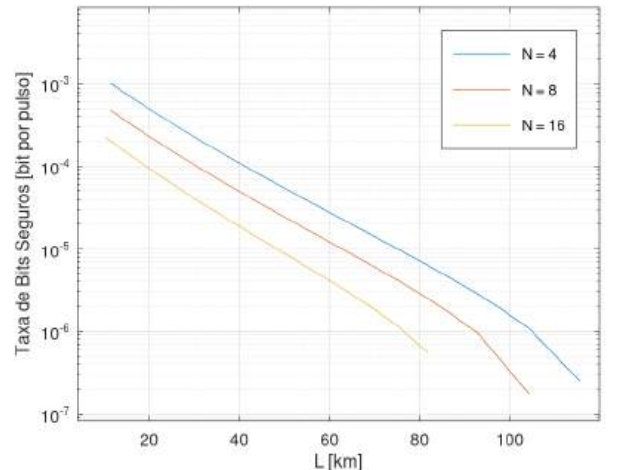


Fig. 2. Taxa de bits seguros versus  $L$  (comprimento do canal).  $\alpha_c = 0.48$  dB/km (1310 nm),  $\alpha_q = 0.27$  dB/km (1550nm),  $P = 0.25$  mW.

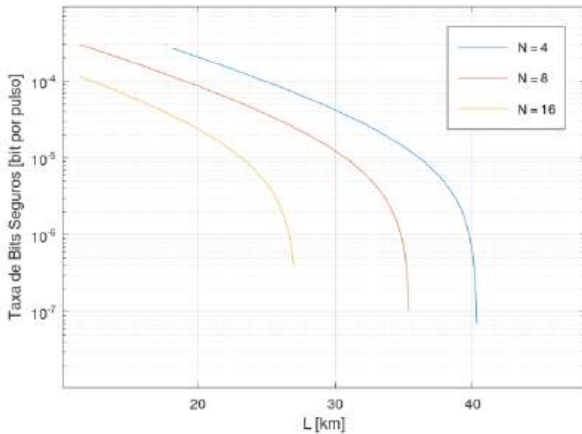


Fig. 3. Taxa de bits seguros versus  $L$  (comprimento do canal).  $\alpha_c = 0.48$  dB/km (1310 nm),  $\alpha_q = 0.27$  dB/km (1550nm),  $P = 0.5$  mW.

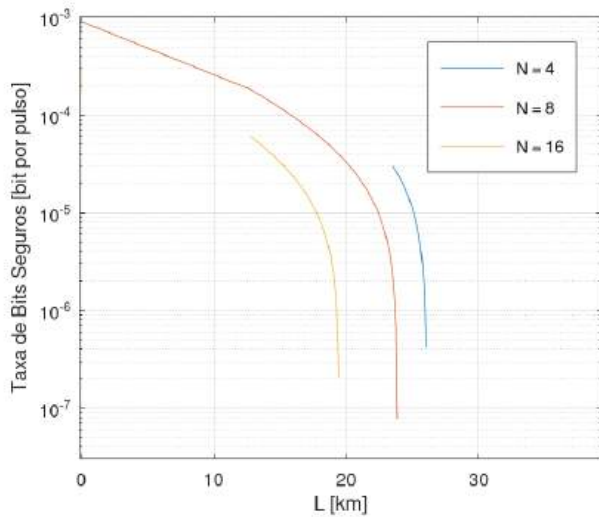


Fig. 4. Taxa de bits seguros versus  $L$  (comprimento do canal).  $\alpha_c = 0.48$  dB/km (1310 nm),  $\alpha_q = 0.27$  dB/km (1550nm),  $P = 0.6$  mW.

Como pode ser observado nas Figs. 2, 3 e 4, quanto maior o valor de  $P$ , maior o valor de  $p_R$  e menores serão a taxa  $R$  e o comprimento  $L$  do canal. Nota-se que, comprimentos menores de fibra (menor atenuação do sinal clássico) devem ser compensados com aumento do número de usuários para que o valor de  $p_R$  atinja um valor que permita a realização do protocolo. O mesmo ocorre se ao invés da diminuição do comprimento do canal, tivermos o aumento da potência  $P$ . De fato, a taxa  $R$  é maior para o valor de  $N$  que minimiza  $[\alpha_q L(N) + 10 \log_{10}(N)]$ . Para ter alta taxa de chave segura são necessários enlaces curtos (mais fótons do sinal quântico chegarão ao detector), porém, neste caso o SRS aumenta (os sinais clássicos são menos atenuados) o que aumenta o QBER diminuindo a taxa de chave segura. Por exemplo, para uma potência  $P$  de 0.7 mW não é possível realizar QKD com  $N = 4$  pois o sinal clássico não sofrerá a atenuação necessária para que o  $p_R$  atinja o valor que permita a realização de QKD.

#### IV. CONCLUSÕES

A realização de QKD em redes ópticas passivas com multiusuários e com coexistência de dados clássicos e quânticos, requer um projeto que faça o correto balanceamento entre o número de usuários e a potência óptica clássica utilizada, de forma a permitir a realização do protocolo de QKD. A eq. (19) mostra a relação entre número de usuários e potência óptica que deve ser obedecida. Perceba-se que são cruciais na eq. (19) os valores de atenuação dos sinais quântico ( $\alpha_q$ ) e clássico ( $\alpha_c$ ). Portanto, uma escolha apropriada dos comprimentos de onda utilizados também é fundamental. Por exemplo, utilizar o comprimento de onda de 1480 nm para o sinal clássico resulta em um valor menor de  $\alpha_c$ , que deve ser compensado com um aumento do comprimento do canal, o que por sua vez causará um aumento da perda em 1550 nm diminuindo a taxa de transmissão.

#### AGRADECIMENTOS

Este trabalho foi parcialmente financiado pelas agências CNPq (309374/2021-9) e CAPES (001).

#### REFERÊNCIAS

- [1] H.-K. Lo, M. Curty, K. Tamaki, “Secure quantum key distribution”, *Nature Photonics*, v. 18, pp. 595-604, 2014.
- [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, “The security of practical quantum key distribution”, *Rev. Mod. Phys.*, v. 81, pp. 1301–1350, 2009.
- [3] K. Inoue, “Differential phase-shift quantum key distribution systems”, *IEEE Sel. Top. in Quant. Elec.*, v. 21, no. 3, pp. 6600207, 2015.
- [4] Y.-P. Li, W. Chen, F.-X. Wang, Z.-Q. Yin, L. Zhang, H. Liu, S. Wang, D.-Y. He, Z. Zhou, G.-C. Guo, Z.-F. Han, “Experimental realization of a reference-frame independent decoy BB84 quantum key distribution based on Sagnac interferometer”, *Optics Letters*, v. 44, no. 18, pp. 4523-4526, 2019.
- [5] C. H. Bennett, G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing” in Proc. IEEE International Conference on Computers, Systems and Signal Processing. pp. 175–179 (IEEE Press, New York, 1984).
- [6] C. H. Bennet, “Quantum cryptography using any two non-orthogonal states”, *Phys. Rev. Lett.*, v. 68, pp. 3121, 1992.
- [7] K. Inoue, E. Waks, Y. Yamamoto, “Differential-phase-shift quantum key distribution using coherent light”, *Phys. Rev. A*, v. 68, no. 2, pp. 022317, 2003.
- [8] D. Stucki, N. Brunner, N. Gisin, V. Scarani, H. Zbinden, “Fast and simple one-way quantum key distribution”, *Appl. Phys. Lett.*, v. 87, no. 19, pp. 194108, 2005.
- [9] B.-H. Li, Y.-M. Xie, Z. Li, C.-X. Weng, C.-L. Li, H.-L. Yin, and Z.-B. Chen, “Long-distance twin-field quantum key distribution with entangled sources”, *Opt. Lett.*, v. 46, no. 22, pp. 5529, 2021.
- [10] H.-K. Lo, M. Curty, B. Qi, “Measurement-device-independent quantum key distribution”, *Phys. Rev. Lett.*, v. 108, pp. 130503, 2012.
- [11] P. V. P. Pinheiro, R. V. Ramos, “Two-layer quantum key distribution”, *Quantum Inf Process*, v. 14, pp. 2111, 2015.
- [12] G. L. de Oliveira, R. V. Ramos, “Quantum-chaotic cryptography”, *Quantum Inf Process*, v. 17, pp. 40, 2018.
- [13] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, G. Franzl, “Perspectives and limitations of QKD integration in metropolitan area networks”, *Opt. Express*, v. 23, no. 8, pp. 10359-10373, 2015.
- [14] A. Bahrami, A. Lord, T. Spiller, “Quantum key distribution integration with optical dense wavelength division multiplexing: a review”, *IET Quantum Commun.*, v. 1, no. 1, pp. 9-15, 2020.

- [15] I. Vorontsova, R. Goncharov, A. Tarabrina, F. Kiselev, V. Egorov, “Theoretical analysis of quantum key distribution systems when integrated with a DWDM optical transport network”, arXiv:2209.15507, 2022.
- [16] K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, A. J. Shields, “Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber”, *Phys. Rev. X*, v. 2, pp. 041010, 2012.
- [17] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. Yuan, A. J. Shields, “Quantum secured gigabit optical access networks”, *Scientific Reports*, v. 5, pp. 18121, 2015.
- [18] C. Cai, Y. Sun, Y. Ji, “Intercore spontaneous Raman scattering impact on quantum key distribution in multicore fiber”, *New J. Phys.*, v. 22, pp. 083020, 2020.
- [19] G. B. da Silva, R. V. Ramos, “The Lambert–Tsallis Wq function”, *Physica A*, v. 525, pp. 164, 2019.
- [20] E. M. F. Curado, C. Tsallis, “Generalized statistical mechanics: connection with thermodynamics”, *J. Phys. A*, v. 24, pp. L69, 1991. [Corrigenda: v. 24, pp. 3187, 1991 and v. 25, pp. 1019, 1992].
- [21] C. Tsallis, “Possible generalization of Boltzmann-Gibbs statistics”, *J. Stat. Phys.*, v. 52, pp. 479, 1988.
- [22] I. R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey and D. E. Knuth, “On the Lambert W function”, *Advances in Comput. Math.*, v. 5, pp. 329 – 359, 1996.
- [23] S. R. Valluri, D. J. Jeffrey, R. M. Corless, “Some applications of the Lambert W function to Physics”, *Canadian J. of Phys.*, v. 78, no. 9, pp. 823-831, 2000.
- [24] F.V. Mendes, C. Lima, R. V. Ramos, “Applications of the Lambert–Tsallis Wq function in quantum photonic Gaussian boson sampling”. *Quant. Inf Process.*, v. 21, pp. 215, 2022.
- [25] J. S. de Andrade, K. Z. Nobrega, R. V. Ramos, “Analytical solution of the current-voltage characteristics of circuits with power-law dependence of the current on the applied voltage using the Wq de Lambert-Tsallis function”, *IEEE Trans. Circuits Syst. II Express Briefs*, 2021.
- [26] J. R. da Silva, R. V. Ramos, “Applications of the Lambert–Tsallis Function in X-Ray Free Electron Laser”, *IEEE Trans. on Plasma Sci.*, v. 50, no. 10, pp. 3578-3582, 2022. doi: 10.1109/TPS.2022.3205545.
- [27] R. L. C. Damasceno, J. S. Andrade, R.V. Ramos, “Applications of the Lambert–Tsallis Wq function in QKD”, *J. Opt. Soc. Am. B*, v. 40, no. 9, pp. 2280-2286, 2023.
- [28] B.-X. Wang, S.-B. Tang, Y. Mao, W. Xu, M. Cheng, J. Zhang, T.-Y. Chen, J.-W. Pan, “Practical quantum access network over a 10 Gbit/s Ethernet passive optical network”, *Opt. Express*, v. 29, no. 23, pp. 38582/1-9, 2021.
- [29] P. D. Townsend, “Quantum cryptography on multiuser optical fibre networks” *Nature*, v. 385, pp. 47–49, 1997.
- [30] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution”, *Phys. Rev. A*, v. 72, pp. 012326/1-15, 2005.

# Análise do Desempenho de Geradores Quânticos de Números Aleatórios usando a Disentropia

S. T. de Oliveira, G. L. de Oliveira e R. V. Ramos

**Resumo** — Neste trabalho utilizamos a disentropia da autocorrelação, uma medida de aleatoriedade baseada na função  $W_q$  de Lambert-Tsallis, para medir a aleatoriedade de sequências binárias geradas por geradores quânticos de números aleatórios. É mostrado, desta forma, que a disentropia da autocorrelação pode ser utilizada para analisar o desempenho de geradores quânticos de números aleatórios, sendo sua principal vantagem a facilidade de cálculo quando comparada com testes de aleatoriedade do NIST.

**Palavras-Chave** — Gerador quântico de números aleatórios, aleatoriedade, disentropia, função  $W_q$  de Lambert-Tsallis.

**Abstract** — In this work we use the disentropy of the autocorrelation, a randomness measure based on the Lambert-Tsallis  $W_q$  function, to measure the randomness of the binary sequences generated by quantum random number generators. Thus, it is shown the disentropy of the autocorrelation can be used to analyze the performance of quantum random number generators, being the easiness of calculation its main advantage when compared to NIST's randomness tests.

**Keywords** — Quantum random number generator, randomness, disentropy, Lambert-Tsallis  $W_q$  function.

## I. INTRODUÇÃO

No mundo moderno a análise de dados é uma tarefa crucial que dá suporte à diversas atividades humanas. Por exemplo, dados médicos, sismológicos, econômicos, astronômicos, dentre outros. Em todos esses casos, de forma intencional ou não, os dados estão sempre contaminados com algum tipo de ruído, o que confere alguma aleatoriedade aos dados. A análise desses dados cada vez mais tem sido feita através do uso de algoritmos de aprendizagem profunda de máquina, como redes neurais multicamadas. Desta forma, quando dados reais não são utilizados, o treinamento de algoritmos de aprendizagem de máquina deve contar com uma fonte de ruído que simule os ruídos presentes em dados reais. Isso aumenta a robustez do algoritmo em questão. Portanto, uma fonte de aleatoriedade se faz importante para o treinamento de algoritmos de aprendizagem de máquina. Outra aplicação importante da aleatoriedade surge em protocolos de criptografia. Um grande número deles exige a geração de dados, no caso em questão bits, aleatórios, para garantir a segurança dos protocolos. Pode-se ainda citar a importância da aleatoriedade em loterias e jogos, dentre outros. Portanto, geradores de aleatoriedade, ou fontes de entropia como também são chamados, são importantes e precisam ser corretamente projetados. Basicamente, há dois

tipos de geradores de aleatoriedade: geradores pseudoaleatórios, baseados em software e geradores verdadeiramente aleatórios, baseados em propriedades físicas. O primeiro tipo apresenta memória e, portanto, não são completamente confiáveis. Por outro lado, geradores verdadeiramente aleatórios não possuem nenhuma memória e são preferidos em atividades como segurança de dados [1,2]. Nesta classe se destacam os geradores quânticos de números aleatório (QRNG – *quantum random number generators*), cuja aleatoriedade é baseada em alguma propriedade quântica de um sistema físico, como polarização de fótons, ruído de fase em fontes ópticas não coerentes, flutuações do vácuo, dentre outros [3-13].

Em QRNGs reais, os dispositivos utilizados em sua construção podem apresentar imperfeições que podem afetar a qualidade da aleatoriedade gerada. Por exemplo, detectores de fótons com valores diferentes de eficiência quântica e de contagem de escuro ou divisores de feixes que não são perfeitamente balanceados. Por isso, a aleatoriedade produzida deve ser testada para garantir o bom desempenho do QRNG construído. Comumente, testes de aleatoriedade do NIST são utilizados para certificar a aleatoriedade de um QRNG.

Por outro lado, uma importante ferramenta matemática utilizada na análise de aleatoriedade de sinais é a função de autocorrelação (FAC). Para um sinal contínuo  $s(t)$  a FAC é definida como sendo

$$R(\tau) = \int_{-\infty}^{\infty} s(t) s^*(t - \tau) dt, \quad (1)$$

enquanto que para um sinal discreto  $s_t$  a FAC no atraso  $k$  é definida como sendo

$$r_k = \frac{E[(s_t - \bar{s})(s_{t+k} - \bar{s})]}{\sigma_s^2} = \frac{1}{N} \frac{\sum_{t=1}^{N-k} (s_t - \bar{s})(s_{t+k} - \bar{s})}{\frac{1}{N} \sum_{t=1}^N (s_t - \bar{s})^2}. \quad (2)$$

Em (2)  $\bar{s}$  e  $\sigma_s^2$  são, respectivamente, o valor médio e a variância de  $s_t$ . Como é usual, o símbolo  $E$  indica o valor esperado. Basicamente, a FAC mostra a similaridade de uma função (sinal) com uma versão atrasada(o) da(o) mesma(o). Quanto maior a aleatoriedade de um sinal, mais a FAC deste sinal se aproxima de uma função delta. Uma medida de aleatoriedade baseada na FAC foi recentemente proposta, chamada de disentropia da autocorrelação [14] e utilizada para aumentar a segurança de distribuição quântica de chaves [15], analisar o desempenho de computador quântico baseado em amostragem

Sergio Tahim de Oliveira, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce e-mail: sergiotahim@gmail.com; Glaucionor Lima de Oliveira, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce email: [glau@ifce.edu.br](mailto:glau@ifce.edu.br); Rubens Viana Ramos, Departamento de Engenharia de Teleinformática, UFC, Fortaleza-Ce, e-mail: rubens.ramos@ufc.br.

de Gaussiana de bósons [16], e na análise de sinais astronômicos [17]. Nesta direção, o presente trabalho apresenta o uso da disentropia da autocorrelação na análise da aleatoriedade gerada por QRNGs.

Este trabalho está dividido da seguinte forma: na Seção II é feita uma revisão da função de Lambert-Tsallis e da disentropia; Na Seção III, usando a disentropia da autocorrelação, é feita a análise da aleatoriedade de sequências binárias geradas por geradores pseudoaleatórios e por QRNGs. Por fim as conclusões são descritas na Seção IV.

## II. A FUNÇÃO $W_q$ DE LAMBERT-TSALLIS E A DISENTROPIA

A função  $W(z)$  de Lambert é uma função matemática elementar que tem sido utilizada em diferentes áreas da matemática, física e ciência da computação [18-21]. A função  $W$  de Lambert é definida como sendo a solução de

$$W(z)e^{W(z)} = z. \quad (3)$$

Tomando o logaritmo em ambos os lados de (3) obtem-se

$$\log(z) = W(z) + \log[W(z)]. \quad (4)$$

Portanto, a entropia pode ser escrita como

$$S = -\sum_i p_i \log(p_i) = -\sum_i p_i W(p_i) - \sum_i p_i \log[W(p_i)]. \quad (5)$$

na qual  $\{p_1, p_2, \dots, p_n\}$  é uma distribuição discreta de probabilidade. O termo

$$D = \sum_i p_i W(p_i) \quad (6)$$

é chamado de disentropia. Quando a disentropia é mínima a entropia é máxima e vice-versa. A eq. (6) é a disentropia relacionada à entropia de Boltzmann-Gibbs. A eq. (3) pode ser modificada para a forma

$$R_2(z) 2^{R_2(z)} = z, \quad (7)$$

cujas soluções são

$$R_2(z) = \log_2(e) W\left(\frac{z}{\log_2(e)}\right) \quad (8)$$

e, neste caso, a disentropia relacionada à entropia de Shannon é

$$D = \sum_i p_i R_2(p_i). \quad (9)$$

A eq. (3) pode ainda ser modificada fazendo a troca da função exponencial pela função  $q$ -exponencial de Tsallis [22]:

$$W_q(z) e_q^{W_q(z)} = z, \quad (10)$$

sendo a função  $q$ -exponencial de Tsallis dada por

$$e_q^z = \begin{cases} e^z & q = 1 \\ [1 + (1-q)z]^{1/(1-q)} & q \neq 1 \text{ \& } 1 + (1-q)z \geq 0 \\ 0 & q \neq 1 \text{ \& } 1 + (1-q)z < 0 \end{cases} \quad (11)$$

A função  $W_q(z)$  é chamada de função de Lambert-Tsallis [23]. É possível encontrar a forma analítica de  $W_q$  para alguns poucos casos sendo a mais simples delas obtida quando  $q = 2$ :  $W_2(z) = z/(1+z)$  definida for  $z > -1$ . Por outro lado, para  $q = 3/2$  tem-se:

$$W_{3/2}^\pm(z) = \frac{2(z+1) \pm 2\sqrt{2z+1}}{z}, \quad z > -1/2 \quad (12)$$

Em geral,  $W_q(z)$  tem que ser calculada numericamente. Por exemplo, pode-se usar o método de Halley para calcular  $W_q(z)$ :

$$w_q(j+1) = w_q(j) - \frac{A}{B - \frac{AC}{2B}} \quad (13)$$

$$A = w_q(j) e_q^{w_q(j)} - z \quad (14)$$

$$B = e_q^{w_q(j)} + w_q(j) e_q^{q w_q(j)} \quad (15)$$

$$C = 2e_q^{q w_q(j)} + \frac{w_q(j)}{q} e_q^{(2q-1)w_q(j)}. \quad (16)$$

Por exemplo, na Fig. 1 pode-se ver a curva de  $W_{3/2}(z)$  versus  $z$ . Pode-se mostrar que o ponto de ramificação de  $W_q(z)$  ( $dW_q(z)/dz = \infty$ ) é dado pelo ponto  $\{z_b = \exp_q(q-2)/(q-2), W_q(z_b) = 1/(q-2)\}$ . Mais detalhes sobre a função  $W_q$  podem ser encontrados em [24-28].

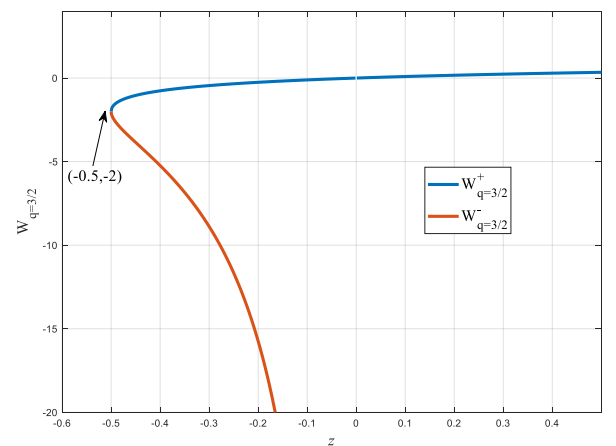


Fig. 1.  $W_{q=3/2}(z)$  versus  $z$ .

Tomando a função  $q$ -logaritmo em ambos os lados da eq. (10), obtém-se

$$\log_q(z) = W_q(z) + \log_q[W_q(z)] + (1-q)W_q(z)\log_q[W_q(z)]. \quad (17)$$

na qual

$$\log_q(z) = \begin{cases} \log(z) & x > 0 \text{ \& } q = 1 \\ \frac{x^{(1-q)} - 1}{1-q} & x > 0 \text{ \& } q \neq 1 \\ \text{indefinida} & x \leq 0 \end{cases}. \quad (18)$$

Portanto, a  $q$ -entropia de Tsallis [22] pode ser escrita como

$$\begin{aligned} S_T &= -\sum_i p_i^q \log_q(p_i) = \\ &= -\sum_i p_i^q W_q(p_i) - \sum_i p_i^q \log_q[W_q(p_i)] - \\ &= (1-q) \sum_i p_i^q W_q(p_i) \log_q[W_q(p_i)]. \end{aligned} \quad (19)$$

O termo

$$D_q = \sum_i p_i^q W_q(p_i) \quad (20)$$

é a disentropia relacionada à entropia de Tsallis.

### III. A DISENTROPIA DA FUNÇÃO DE AUTOCORRELAÇÃO E A ALEATORIEDADE DE SEQUÊNCIAS BINÁRIAS

Aproveitando as propriedades da FAC e da disentropia, a medida de aleatoriedade chamada disentropia da autocorrelação foi recentemente proposta em [14]. Para um sinal discreto  $s_t$  ela é dada simplesmente por  $D_{q=2}(R(s_t))$ , ou seja,

$$D_2 = \sum_{n=1}^N \frac{r_n^3}{r_n + 1}, \quad (21)$$

na qual  $r_n$  é o  $n$ -ésimo valor da FAC de  $s_t$ . Para um sinal com máxima aleatoriedade, como um ruído branco, a FAC é uma função delta e o valor de  $D_2$  em (21) é igual a 0.5. Portanto, quanto mais próximo de 0.5, mais aleatório é o sinal considerado. A Tabela 1 e a Fig. 2 a seguir mostram cinco exemplos, nos quais um sinal quadrado é contaminado com ruído Gaussiano cada vez mais intenso.

Tabela I – Sinal quadrado com diferentes níveis de ruído e seus respectivos valores de aleatoriedade calculados com uso da disentropia da autocorrelação:  $N(x,y)$  – ruído Gaussiano com média igual a  $x$  e variância igual a  $y$ .

	$s(t) = \text{onda quadrada}$	Aleatoriedade - $D_2(R(s(t)))$
I	$s(t)$	-29054.1802
II	$4 + s(t) + N(0,0.25)$	-7521.519
III	$8 + s(t) + N(0,0.5)$	-830.401
IV	$15 + s(t) + N(0,1)$	-15.482
V	$25 + N(0,1)$	0.49995

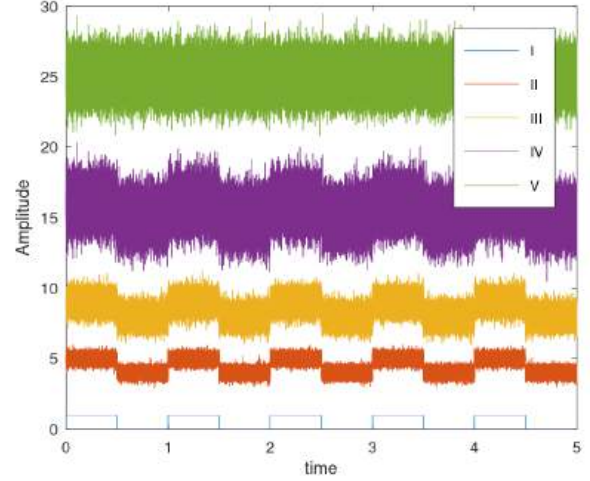


Fig. 2. Onda quadrada contaminada com ruído Gaussiano de diferentes valores de variância (V – ruído Gaussiano puro).

Como pode ser observado na Fig. 2 e na Tabela I, quanto maior o nível de ruído (valor da variância) mais próximo do valor 0.5 estará a disentropia da autocorrelação.

Para calcular a aleatoriedade de sequências binárias, deve-se lembrar que a FAC capta a presença de memória no sinal. Portanto, sequências de bits obtidas por um processo físico sem memória serão consideradas pela FAC como sendo maximamente aleatório, mesmo que o número total de ‘0’s e ‘1’s sejam muito diferentes. Em outras palavras, uma sequência binária obtida com uso de uma moeda honesta e outra sequência binária obtida com uso de uma moeda viciada, vão possuir a mesma FAC, uma função delta e, portanto, o mesmo valor de  $D_2 = 0.5$ . Para evitar este problema, somamos uma função determinística  $f$  (neste trabalho uma função seno) à sequência binária  $b$  a ser testada. Neste caso, quanto maior a aleatoriedade da sequência  $b$  maior o apagamento da memória da função  $f$  e, portanto, menor o valor da disentropia da autocorrelação do conjunto  $b + f$ .

Usando o gerador pseudoaleatório do software OCTAVE, 5.000 sequências de 1.000.000 de bits foram geradas, e classificadas como  $b_1$ ,  $b_2$  e  $b_3$ . Para a sequências  $b_1$  os bits ‘0’ e ‘1’ foram escolhidos com a mesma probabilidade  $p_0 = p_1 = 0.5$ . Para sequências  $b_2$  os bits ‘0’ e ‘1’ foram escolhidos com probabilidades  $p_0 = 0.7$  e  $p_1 = 0.3$ . Por fim, para sequências  $b_3$  os bits ‘0’ e ‘1’ foram escolhidos com probabilidades  $p_0 = 0.9$  e  $p_1 = 0.1$ . Os histogramas dos valores do cálculo da aleatoriedade usando a disentropia para estas sequências, podem ser vistos na Fig. 3.



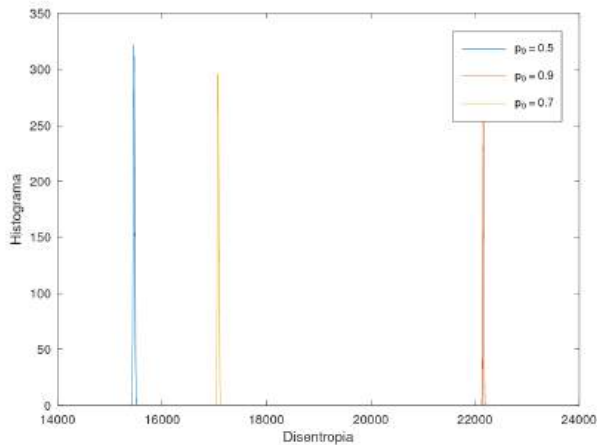


Fig. 3. Histogramas das aleatoriedades calculadas pela disentropia da autocorrelação das sequências  $b_1$ ,  $b_2$  e  $b_3$  (5.000 sequências de 1000.000 de bits) obtidas com um gerador pseudoaleatório.

Como pode ser observado na Fig. 3, as sequências  $b_1$  (maximamente aleatória),  $b_2$  (com viés) e  $b_3$  (com forte viés) são completamente distinguidas pela disentropia da autocorrelação. Os valores médios da disentropia para as sequências  $b_1$ ,  $b_2$  e  $b_3$  são, respectivamente: 15462.1837 ( $p_0 = 0.5$ ), 17074.1018 ( $p_0 = 0.7$ ) e 22160.5959 ( $p_0 = 0.9$ ). A disentropia da função  $f$  é 22842.7428.

A Fig. 4 mostra o mesmo para 1.000 sequências binárias de 150.000 bits.

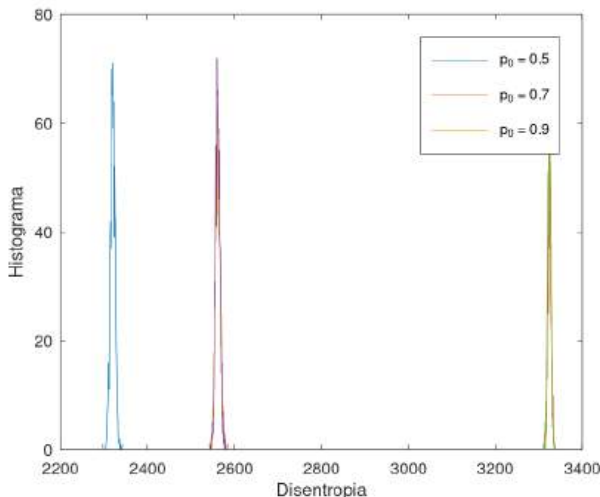


Fig. 4. Histogramas das aleatoriedades calculadas pela disentropia da autocorrelação das sequências  $b_1$ ,  $b_2$  e  $b_3$  (1.000 sequências de 150.000 bits) obtidas com um gerador pseudoaleatório.

Os valores médios da disentropia para as sequências  $b_1$ ,  $b_2$  e  $b_3$  são, respectivamente: 2319.3898 ( $p_0 = 0.5$ ), 2561.2481 ( $p_0 = 0.7$ ) e 3324.32 ( $p_0 = 0.9$ ). A disentropia da função  $f$  neste caso é 3426.4097.

Usando dez sequências de 150.000 bits, geradas por um QRNG real obtidos no sítio <http://qrng.ethz.ch/live/>, os valores da disentropia obtidos são mostrados na Tabela II.

Tabela II. Disentropia da autocorrelação de dez sequências binárias de 150.000 bits cada. Sequências obtidas no site <http://qrng.ethz.ch/live/>.

QRNG				
2322.8445	2309.9544	2318.5914	2320.5676	2315.9882
2318.5725	2320.5387	2325.5954	2312.7469	2306.9587

#### IV. CONCLUSÕES

A disentropia da autocorrelação é uma medida confiável de aleatoriedade e pode ser utilizada na análise de desempenho de geradores quânticos de números aleatórios. Sua grande vantagem é o fácil e rápido cálculo, além de permitir fazer uma gradação de diferentes níveis de aleatoriedade. As sequências binárias reais obtidas a partir do sítio disponível na internet apresentaram valores de disentropia compatíveis com os valores esperados para uma sequência binária maximamente aleatória ( $p_0 = p_1 = 0.5$ ). Portanto, a disentropia da autocorrelação é uma ferramenta que pode ser utilizada para detectar, de forma não invasiva, o mau comportamento de dispositivos utilizados no QRNG que, com o envelhecimento, podem mudar suas características e introduzir um viés na sequência binária gerada.

#### AGRADECIMENTOS

Este trabalho foi parcialmente financiado pelas agências CNPq (309374/2021-9) e CAPES (001).

#### REFERÊNCIAS

- [1] J. Bouda, M. Pivoluska, M. Plesch, C. Wilmott, “Weak randomness seriously limits the security of quantum key distribution”, *Phys. Rev. A*, v. 86, pp. 062308/1-5, 2012.
- [2] H. W. Li, Z. Q. Yin, S. Wang, Y. J. Qian, W. Chen, G. C. Guo, Z. F. Han, “Randomness determines practical security of BB84 quantum key distribution”, *Sci. Rep.*, v. 5, pp. 16200/1-8, 2015.
- [3] R. Serrano, C. Duran, T.-T. Hoang, M. Sarmiento, K.-D. Nguyen, A. Tsukamoto, K. Suzuki, “A fully digital true random number generator with entropy source based in frequency collapse”, *IEEE Access*, v. 9, pp. 105748-105755, 2021.
- [4] F. Monet, J.-S. Boisvert, R. Kashyap, “A simple high-speed random number generator with minimal post-processing using a random Raman fiber laser”, *Sci. Rep.*, v. 11, pp. 13182/1-8, 2021.
- [5] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator”, *Rev. Sci. Instrum.* V. 71, no. 4, pp. 1675-1680, 2000.
- [6] T. Gehring, C. Lupo, A. Kordts, D. S. Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, U. L. Andersen, “Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information”, *Nature Comm.*, v. 12, pp. 605/1-11, 2021.
- [7] Y. Zhang, H.-P. Lo, A. Mink, T. Ikuta, T. Honjo, H. Takesue, W. J. Munro, “A simple low-latency real-time certifiable quantum random number generator”, *Nature Comm.*, v. 12, pp. 1056/1-8, 2021.
- [8] B. Qi, “True randomness from an incoherent source”, *Rev. Sci. Instrum.*, v. 88, pp. 113101/1-6, 2017.
- [9] J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, B. Xu, H. Guo, “117 Gbits/s quantum random number generation with simple structure”, *IEEE Photon. Tech. Lett.*, v. 29, no. 3, pp. 283-286, 2017.
- [10] B. Bai, J. Huang, G.-R. Qiao, Y.-Q. Nie, W. Tang, T. Chu, J. Zhang, J.-W. Pan, “18.8 Gbps real-time quantum random number generator with a photonic integrated chip”, *Appl. Phys. Lett.*, v. 118, pp. 264001, 2021.
- [11] C. Bruynsteijn, T. Gehring, C. Lupo, J. Bauwelinck, X. Yin, “100-Gbit/s Integrated quantum random number generator based on vacuum fluctuations”, *PRX Quantum*, v. 4, pp. 010330/1-11, 2023.

- [12] Y.-X. Liu, K.-X. Huang, Y.-M. Bai, Z. Yang, J.-L. Li, “A High-Randomness and High-Stability Electronic Quantum Random Number Generator without Post Processing”, *Chinese Phys. Lett.*, v. 40, pp. 070303/1-5, 2023.
- [13] E. de J. L. Soares, F. A. Mendonca and R. V. Ramos, “Quantum Random Number Generator Using Only One Single-Photon Detector”, *IEEE Phot. Tech. Lett.*, v. 26, no. 9, pp. 851-853, 2014.
- [14] R. V. Ramos, “Estimation of the Randomness of Continuous and Discrete Signals Using the Disentropy of the Autocorrelation”, *SN Compt. Sci.*, v. 2, pp. 254/1-9, 2021.
- [15] G. S. Castro, R. V. Ramos, “Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness” *Quant. Inf. Process.*, v. 21, pp. 79/1-10, 2022.
- [16] F.V. Mendes, C. Lima, R. V. Ramos, “Applications of the Lambert–Tsallis Wq function in quantum photonic Gaussian boson sampling”. *Quant. Inf. Process.*, v. 21, pp. 215, 2022.
- [17] F. J. L. de Almeida, R. V. Ramos, Disentropy in astronomy, *Eur. Phys. J. Plus*, v. 138, pp. 20/1-10, 2023.
- [18] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey and D. E. Knuth, “On the Lambert W function”, *Adv. in Comp. Math.*, v. 5, pp. 329 – 359, 1996.
- [19] S. R. Valluri, D. J. Jeffrey, R. M. Corless, “Some applications of the Lambert W function to Physics”, *Can. J. of Phys.*, v. 78, no. 9, pp. 823-831, 2000.
- [20] F. C.-Blondeau and A. Monir, “Numerical evaluation of the Lambert W function and application to generation of generalized Gaussian noise with exponent  $\frac{1}{2}$ ”, *IEEE Trans. on Signal Processing*, v. 50, no. 9, pp. 2160-2165, 2002.
- [21] K. Roberts, S. R. Valluri, Tutorial: “The quantum finite square well and the Lambert W function”, *Can. J. of Phys.*, v. 95, no. 2, pp. 105-110, 2017.
- [22] C. Tsallis, “Possible generalization of Boltzmann-Gibbs statistics”, *J. Stat. Phys.*, v. 52, pp. 479, 1988.
- [23] G. B. da Silva, R. V. Ramos, “The Lambert–Tsallis Wq function”, *Physica A*, v. 525, pp. 164, 2019.
- [24] J. S. de Andrade, K. Z. Nobrega, R. V. Ramos, “Analytical solution of the current-voltage characteristics of circuits with power-law dependence of the current on the applied voltage using the Wq de Lambert-Tsallis function”, *IEEE Trans. Circuits Syst. II Express Briefs*, v. 69, n2022.
- [25] J. R. da Silva, R. V. Ramos, “Applications of the Lambert–Tsallis Function in X-Ray Free Electron Laser”, *IEEE Trans. on Plasma Sci.*, v. 50, no. 10, pp. 3578-3582, 2022.
- [26] R. L. C. Damasceno, J. S. Andrade, R.V. Ramos, “Applications of the Lambert–Tsallis Wq function in QKD”, *J. Opt. Soc. Am. B*, v. 40, no. 9, pp. 2280-2286, 2023.
- [27] R. V. Ramos, “The Rq,Q function and the q-diode”, *Physica A*, no. 556, p. 12485/1-9, 2020.
- [28] R. V. Ramos, “Disentropy of the Wigner function”, *J. of Opt. Soc. of Am. B*, 36, 8 2244, 2019.

# CVQKD Reconciliation with Slepian-Wolf LDPC Coding and Bit-Flipping Decoding

Rávilla R. S. Leite and Francisco M. de Assis

**Abstract**—In this paper we present an information reconciliation protocol designed for CVQKD based on Distributional Transform associated with well known results of coding theory. A simple algorithm is utilized to recover the Hamming difference  $E$  between two correlated vectors  $X$  and  $Y$  in  $GF(2^n)$ . This is done using their respective syndromes and assuming that the Hamming weight of difference vector  $E$  is less than or equal to the error-correction capability of chosen block error-correcting code. Numerical examples were performed with a LDPC code with rate  $1/2$  and a modification on the Bit-Flipping algorithm. The results encourage to apply this technique with LDPC codes for CVQKD applications.

**Keywords**—CVQKD, LDPC Codes, Bit-Flipping, Distributional Transform.

## I. INTRODUCTION

Quantum Key Distribution protocols (QKD) aims to provide a random secret key to two distant parties, Alice and Bob, which will be used in one-time-pad applications, so that an eavesdropper, Eve, has as little information as possible about the key [1]. Only in quantum communications is it possible to generate two correlated random variables without revealing information to Eve, as the security and reliability of the protocol are based on the principles of uncertainty and the non-cloning theorem of quantum states. Any attempt at eavesdropping will induce disturbances in the system [2].

The QKD protocol can be implemented in two main ways: DVQKD (*Discrete-Variable Quantum Key Distribution*), where the key information is encoded through the phase or polarization of single-photons [3], [4], [5] and at the receiver occurs the detection of single-photons; and CVQKD (*Continuous-Variable Quantum Key Distribution*), where the key information is encoded in continuous variables, such as the quadrature of the electromagnetic field of non-orthogonal coherent states [6], performing homodyne or heterodyne detection at reception [7], [8], [9]. From a practical point of view, CVQKD present the major advantage that they only require standard telecommunication technology, in addition to providing higher secret key rates than DVQKD [6], [8], [10].

Gaussian Modulation allows to CVQKD protocols to achieve the better theoretical secret key rates (SKR) [7], [9], but they already exists some works based on discrete modulations, in general M-PSK, which can achieve SKR very close to that obtained with Gaussian Modulation [11], [12]. CVQKD protocols with Gaussian Modulation occurs in four

main steps [6], [8]: (1) state distribution and measurement; (2) parameter estimation; (3) information reconciliation; and (4) privacy amplification.

The Gaussian random variables obtained at the end of the quantum step will be subjected to the sifting step, in which Bob informs Alice which of the quadratures he randomly selected for each of his element measurements, such that Alice may respectively discard her values measured with the wrong bases [13]. In addition, the subsequences used to estimate the channel parameters will also be discarded [14]. The remaining values are called *raw key* and they need to be quantized and further corrected, trough the use of error correction codes, in general LDPC (Low-Density Parity-Check) Codes, in a procedure named Information Reconciliation (IR) Protocol [1], [15], [16], [14]. IR has a direct impact on the performance of the protocol, as it limits both the secret key rate (due to decoding complexity) and the range (due to the effects that the channel applies on the signal in the low SNR (signal-to-noise ratio) regime) [17], [16]. Thus, proposals to reduce the complexity of reconciliation can improve the performance of the protocol as a whole.

In this paper will be presented an IR protocol for CVQKD based on Distributional Transform for the quantization of raw key's continuous values and presenting a little modification on the Bit-Flipping algorithm, proposed initially by Gallager [18], to obtain the error vector between the binary sequences of Alice and Bob, from the difference of their syndromes and the zero-vector, and then, make their sequences match, in a reverse reconciliation scheme. It is important to highlight that in reconciliation, unlike traditional channel coding, the goal is not necessarily to obtain codewords but to match the sequences of Alice and Bob. The technique is based on fundamentals of coding theory, and aims to offer a simple alternative for error correction in CVQKD protocols.

This paper is structured as follows: Section II presents the main concepts about IR for understanding this work, with focus in the Distributional Transform, used in the quantization of continuous variables [19], [14], and in the error correction using LDPC Codes and Slepian-Wolf coding; in III will be presented the decoding technique from zero-vector and the fundamentals that allow it; Section IV describes the simulations carried out and presents the main results obtained; and finally, Section V presents the conclusion and future works.

## II. INFORMATION RECONCILIATION

Reconciliation step can happen in two ways: direct reconciliation (DR), when Bob will correct his sequence so that it matches with Alice's sequence, and reverse reconciliation

Rávilla R. S. Leite and Francisco M. de Assis, Department of Electrical Engineering, Federal University of Campina Grande (UFCG), Campina Grande-PB, Brazil. E-mails: ravilla.leite@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br. This work was partially financed by CNPq. (311680/2022-4 and 140827/2022-6)

(RR), when it is Alice who will correct her sequence to match Bob's [20]. Reverse reconciliation is preferable because it allows the QKD protocol to be carried out even on channels whose losses are greater than 3 dB, unlike direct reconciliation [20].

After quantum step, the sifting step occurs, where Alice and Bob must discard the variables that were measured with the incorrect bases, resulting in two correlated Gaussian sequences:  $\mathbf{A} = A_1, \dots, A_n$  and  $\mathbf{B} = B_1, \dots, B_n$ , respectively, transmitted through a Gaussian additive channel, with mutual information greater than 0, i. e.,  $I(A; B) > 0$  [7]. For ease of notation, we assume:  $B = A + \sqrt{N}Z$  where  $A, Z \sim \mathcal{N}(0, 1)$ , independent, and  $N = \frac{1}{S^2NR}$  stands for the noise power.

Usually are used SEC (Slice Error Correction) [15], [16] or MD (Multidimensional) Reconciliation [21], [12], [13] to extract bit sequences from continuous valued data so that an error correcting code could be applied, typically LDPC codes [14]. Here, will be applied the quantization technique proposed by Araújo and Assis [19] which exploits the following well known Lemma from arithmetic coding [22]:

*Lemma 1:* Let  $V$  be a random variable with a continuous distribution function  $F_V$ , then  $U = F_V(V)$  is uniformly distributed at  $[0, 1]$ .

This Lemma is known in Copula Theory as Distributional Transform and ensures that transforming a continuous random variable by its cumulative distribution function always leads to a uniform distribution on the unit interval [14]. Combined with the fact that the bits in the binary expansion of a random variable with uniform distribution on  $[0, 1]$  are independent and Bernoulli ( $\frac{1}{2}$ ), Alice and Bob can calculate the Distributional Transform to map the raw key elements on the unit interval, that is, for each Gaussian input  $A$ , Alice calculate  $X = \Phi(A) \sim \text{unif}[0, 1]$  and similar for Bob,  $Y = \Phi(B) \sim \text{unif}[0, 1]$ , where  $\Phi(\cdot)$  stands for the cumulative distribution function.

After they apply a  $l$  bits of resolution binary expansion on each resulting value of  $X$ , respec.  $Y$ , they have the binary vectors:  $\mathcal{D}(X) = (\mathcal{D}_1(X), \dots, \mathcal{D}_l(X))$  where  $\mathcal{D}_i(X) \in \{0, 1\}$  represents the  $i$ -th digit in the base-2 expansion of  $X$  in Alice's side, and similar  $\mathcal{D}(Y) = (\mathcal{D}_1(Y), \dots, \mathcal{D}_l(Y))$  in Bob's side.

The overall picture of the procedure is summarized below for the Alice's side:

$$A_1, \dots, A_n \mapsto \begin{bmatrix} \mathcal{D}_1(X_1) & \cdots & \mathcal{D}_1(X_n) \\ \mathcal{D}_2(X_1) & \cdots & \mathcal{D}_2(X_n) \\ \vdots & & \vdots \\ \mathcal{D}_l(X_1) & \cdots & \mathcal{D}_l(X_n) \end{bmatrix},$$

and similarly for the Bob's side.

Observe that the sequences  $\mathcal{D}_j(X_i), \dots, \mathcal{D}_j(X_n)$  and  $\mathcal{D}_j(Y_i), \dots, \mathcal{D}_j(Y_n)$ , for  $j = 1, \dots, l$  define, for each  $j$  a input sequence to a memoryless binary symmetric channel (BSC). The transition probability,  $\alpha_j = \Pr[\mathcal{D}_j(X_i) \neq \mathcal{D}_j(Y_i)]$  for each induced BSC subchannel was estimated by simulation.

In favor to ease notation, we shall replace  $\mathcal{D}_j(X_i)$  by  $X_i$ , and similar  $Y_i$ , for any of the channels, as long as,

there is no possibility of confusion in the context. So, from now on,  $\mathbf{X} = (X_1, \dots, X_n)$  and  $\mathbf{Y} = (Y_1, \dots, Y_n)$  are assumed vectors in  $\text{GF}(2^n)$  corresponding to input and output sequences, respectively, of a BSC induced by the reverse reconciliation protocol.

This approach enables the application of compression and coding techniques that minimize the amount of information about the key accessible to an eavesdropper, such as the Slepian-Wolf coding [23], [24], [25]. In this type of coding, admitting a RR protocol, Bob must perform compute  $S(\mathbf{Y}) = \mathbf{Y}\mathbf{H}^T$  and send this to Alice through a error-free classical authenticated channel. So that she can reconstruct Bob's sequence from her own sequence  $\mathbf{X}$  and  $S(\mathbf{Y})$ . It should be noted that in this case, neither  $\mathbf{X}$  nor  $\mathbf{Y}$  are defined as being codewords of any block error-correcting code. The Alice's goal can be find out the difference vector  $\mathbf{E} = \mathbf{Y} - \mathbf{X}$  defined as elements of  $\text{GF}(2^n)$ . We will require size  $n$  compatible with the length of the parity-check matrix  $\mathbf{H}$ , of a LDPC code used. Note that induced sub-channels have different capacities, namely  $C_j = 1 - \mathcal{H}(\alpha_j)$  where  $\mathcal{H}(x) = -x \log(x) - (1-x) \log(1-x)$  stands for the binary entropy parameter  $\alpha \in (0, 1)$ . Obviously the code rate utilized to  $j$ -th channel must be compatible, that is less than  $C_j$ .

### III. RECOVERING THE DIFFERENCE VECTOR FROM SYNDROMES

In this section we refer Lin and Costello [26] w.r.t. coding theory. Let  $\mathcal{C}$  be a  $(n, k, d)$  linear block code defined by its parity-check matrix  $\mathbf{H}$ . If a vector  $\mathbf{E} \in \text{GF}(2^n)$  has Hamming weight  $wt(\mathbf{E}) \leq \lfloor \frac{d-1}{2} \rfloor$  the nearest codeword of  $\mathbf{E}$  is the null codeword  $\mathbf{0}$ . We will use this result in what follows.

Assuming  $\mathbf{X}, \mathbf{Y}$  and  $\mathbf{E}$  have length  $n$  of the code  $\mathcal{C}$  we have

$$\mathbf{E} = \mathbf{Y} \oplus \mathbf{X} \quad (1)$$

$$S(\mathbf{X}) = \mathbf{X}\mathbf{H}^T \quad (2)$$

$$S(\mathbf{Y}) = \mathbf{Y}\mathbf{H}^T. \quad (3)$$

From this

$$S(\mathbf{E}) = (\mathbf{X} \oplus \mathbf{Y})\mathbf{H}^T \quad (4)$$

$$= S(\mathbf{X}) \oplus S(\mathbf{Y}). \quad (5)$$

It is clear that Alice can calculate  $S(\mathbf{E})$  from  $\mathbf{X}$  syndrome, her own data, and from the knowledge of  $\mathbf{Y}$  informed by Bob.

That said, if  $wt(\mathbf{E})$  is smaller than the random-error-correcting capability of the code  $\mathcal{C}$ , it is capable to recover the difference vector  $\mathbf{E}$  from  $S(\mathbf{E})$  and the null codeword, through the use of a decoding algorithm. In this work a modification of the Bit-Flipping algorithm was used, based on the flip of the bits of the null sequence that are connected to the maximum number of failures in  $S(\mathbf{E})$  (with value 1).

*Inicialization:* compute the difference between the syndromes of Alice and Bob:  $S(\mathbf{E})$ ;

- 1) Find the number of failures in  $S(\mathbf{E})$  (with value 1) for each bit, denoted by  $f_i$ ,  $i = 1, \dots, n$ ;

- 2) Invert the bits for which  $f_i$  is the largest;
- 3) Compute the syndrome of the obtained vector  $E' \mapsto S(E')$ , and compare with the original  $S(E)$ ;
- 4) Repeat steps 2 to 4 until all the bits in  $S(E')$  are equal to  $S(E)$  or a preset maximum number of iterations is reached.

**Example 1.** Let the linear block code defined by  $H$  as follows:

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

which can be represented by the Tanner Graph of the Figure 1, where the squares corresponds to the parity-check nodes and the circles to the variable nodes. Let  $X$  and  $Y$  the binary sequences of Alice and Bob, and  $S(X)$  and  $S(Y)$  the syndromes of their sequences, respectively.

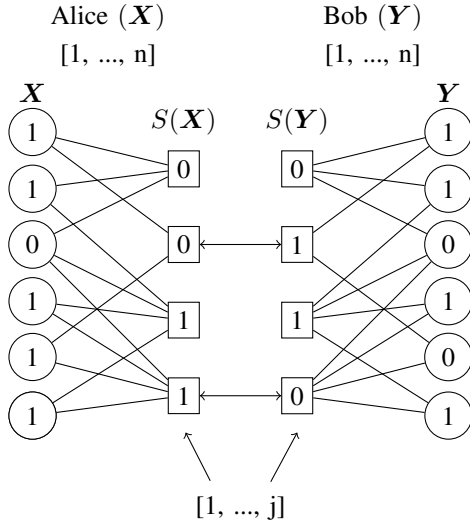


Fig. 1. Alice and Bob's sequences in the Tanner Graph.

First, as shown previously, we compute  $S(E)$ , that will be applied to the check nodes in the decoding algorithm, and the variable nodes are initialized with zeros, as can be seen in Figure 2. Counting the number of failures for each bit in the variable nodes ( $f_i$ ), the values presented in Table I are obtained.

TABLE I  
NUMBER OF FAILURES IN  $S(E)$  FOR EACH BIT.

Bit (1, ..., n)	$f_i$
1	1
2	0
3	1
4	1
5	2
6	1

Since the 5th bit has the largest number of parity failures, it will be flipped:  $E(5) = E(5) \oplus 1$ , as can be seen in Figure 2. Calculating the syndrome of this intermediate sequence, we

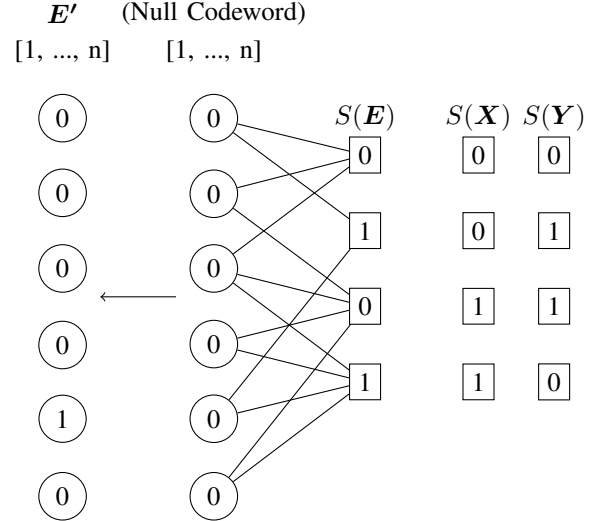


Fig. 2. Achieving the difference vector from the difference between the syndromes.

can obtain  $S(E') = [0 \ 1 \ 0 \ 1] = S(E)$ . Thus, decoding is completed.

In this example, just one iteration was enough to obtain the difference vector. In practical situations, this should not happen.

The difference vector obtained with this approach can be added to Alice's initial sequence  $X$ , so that it matches Bob's sequence (RR). This technique presents an alternative for correcting errors in the reconciliation step of CVQKD protocols, and aims to simplify the decoding process.

#### IV. RECONCILIATION USING LDPC CODES AND THE SLEPIAN-WOLF CODING

The simulations were conducted considering eleven SNR values, ranging from 0 to 40 dB. Correlated Gaussian samples were generated for Alice and Bob. The quantization technique described in section 2, based on DTE, was applied to these samples and only the bits of the first sub-channel were used, i.e. for  $j = 1$ , and it was assumed that  $X = (\mathcal{D}_1(X_1), \dots, \mathcal{D}_1(X_n))$  and  $Y = (\mathcal{D}_1(Y_1), \dots, \mathcal{D}_1(Y_n))$ .

Adopting a reverse reconciliation scheme and the Slepian-Wolf coding [24], [25], Bob must perform compute  $S(Y)$ , and send it to Alice through a error-free classical authenticated channel. This approach allows Bob to compress his sequence, respecting the noiseless compression limits presented in the Slepian-Wolf Theorem [23]. To do this, an LDPC Code was used, described by its parity-check matrix  $H$ , with  $n = 1920$ ,  $k = 960$  and rate  $r = 1/2$ , irregular and quasi-cyclic, available in standard G.hn ( $c = 12$ ,  $t = 24$ ,  $b = 80$ ) [27], where  $c$ ,  $t$  and  $b$  are the parameters of the mother matrix. The samples of  $X$  and  $Y$  (frames) were also of size  $n = 1920$ , compatible with the length of  $H$ . So that, Alice is able to recover the sequence  $Y$  from  $X$  and  $S(Y)$ , using a decoder. It is worth remembering that  $X$  and  $Y$  will not go through traditional LDPC encoding that turns them into codewords.

We then applied the modification to the Bit-Flipping decoding algorithm presented in Section III, trying to obtain the difference vector between Alice's and Bob's sequences, so

that by adding the vector obtained to her sequence  $\mathbf{X}$ , Alice can reconstruct Bob's sequence  $\mathbf{Y}$ . For each SNR value, the decoding algorithm was run 1000 times, with a maximum of 35 iterations. A decoding was considered successful when the vector obtained had a syndrome equal to  $S(\mathbf{E})$ , and successful decodings will not always lead to the reconstruction of Bob's sequence.

The average values of success rate and minimum distance were calculated from 1000 samples of  $\mathbf{X}$  and  $\mathbf{Y}$  generated for each SNR. The average Hamming distance between  $\mathbf{X}$  and  $\mathbf{Y}$  can be seen in Figure 3. The observed decrease is due to the fact that the increase in SNR leads to fewer errors imposed by the channel on the transmitted sequence.

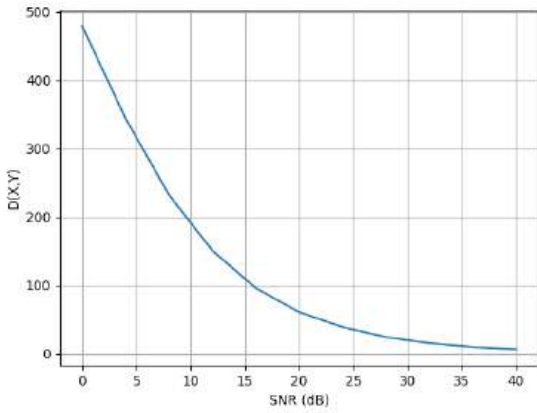


Fig. 3. Average Hamming distance between  $\mathbf{X}$  and  $\mathbf{Y}$ , before decoding, as a function of SNR, after 1000 executions of the algorithm.

Table II shows the capacity of the induced BSC sub-channel, according to each SNR considered, in bits per channel use, in addition to the percentage of successful decodings and the average Hamming Distance between  $\mathbf{X}$  and  $\mathbf{Y}$ . It is possible to observe that successful decodings begin to occur from 8 dB, but still in very low quantities. This happens because with this signal-to-noise ratio, the Channel Capacity is lower than the code rate ( $1/2$ ). According to Shannon's Coding Theorem, in this circumstance there is no coding scheme that allows error-free transmission. From 12 dB, however, the channel capacity already exceeds the code rate, and the number of successful decodings starts to grow quickly.

TABLE II  
NUMBER OF ERRORS BASED ON SNR.

SNR (dB)	Capacity	Success (%)	D(X,Y)
0	0,192	0	480,615
4	0,341	0	343,799
8	0,480	0,4	231,695
12	0,615	5,6	150,387
16	0,707	25,1	95,945
20	0,836	44,7	60,507
24	0,865	63,2	38,515
28	0,883	75,4	24,135
32	0,934	86,3	15,239
36	0,941	87,8	9,652
40	0,988	82,8	6,139

Given the construction of the LDPC code used (irregular

and quasi-cyclic), obtaining parameters such as the minimum distance becomes a NP-hard problem, then it is not easy to calculate the error-correcting capability of the code. From Table II it was possible to observe that the code is capable of correcting approximately 150 errors, although with a very small number of successes, around 5.6%. Figure 4 shows the increase in the number of successful decodings with increasing SNR.

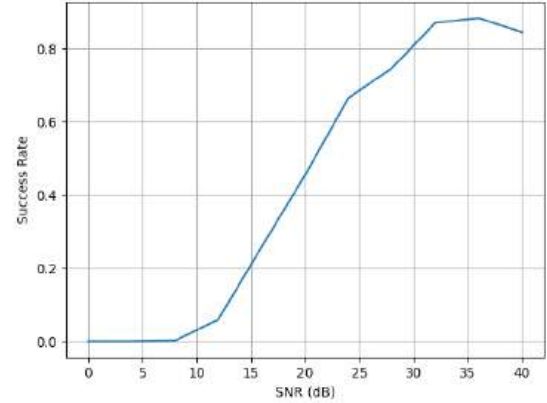


Fig. 4. Average number of successful decodes as a function of SNR, after 1000 executions of the algorithm.

Histograms were also generated based on six values of signal-to-noise ratio to better characterize the distribution of the Hamming weight of the difference vector  $\mathbf{E}$ . For each SNR, 1000 samples were generated, grouped into 20 intervals.

The results presented were achieved for SNR values above those cited in the CVQKD literature - below 5 dB. In addition, the parameters of the LDPC matrix used differ from those recommended for CVQKD application. The literature cites codes with lengths on the order of  $10^6$  and rates of 0.02 or lower, as well as more than 100 iterations of the decoding algorithm, usually employing soft-decision decoding [28], [13], [12], [16]. Here, the aim was to evaluate the functionality of the proposed abrupt decoding algorithm. The results encourage to apply this technique with LDPC codes specific for low SNR regimes, analyzing their viability and performance compared to the decoding algorithms most used in CVQKD protocols in order to reduce the computational cost of the decoding process.

## V. CONCLUSIONS

In this paper it was presented an information reconciliation protocol designed for CVQKD protocols, based on Distributional Transform for quantization of continuous values of the raw key, and on well-known results of coding theory to recover the difference vector between two correlated sequences  $\mathbf{E} = \mathbf{X} - \mathbf{Y}$  in  $GF(2)^n$  using their respective syndromes  $S(\mathbf{X})$  and  $S(\mathbf{Y})$ . Coding theory shows that this is possible if the Hamming weight of the difference vector  $\mathbf{E}$  is less than or equal to the error-correction capability of the code, even if  $\mathbf{X}$  and  $\mathbf{Y}$  are not codewords.

Numerical results were obtained using a LDPC code with rate  $1/2$  and a modification on Bit-Flipping algorithm. The

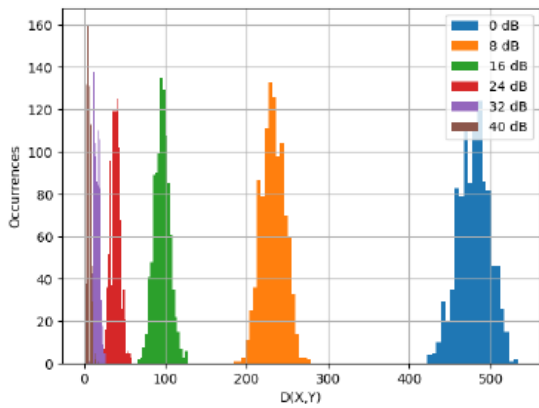


Fig. 5. Histograms with the Hamming distances between  $X$  and  $Y$  grouped into 20 intervals, based on SNR, after 1000 executions of the algorithm.

focus of this paper, therefore, was to analyze the viability of the idea in an initial application, using a simple and small LDPC code compared to those recommended for CVQKD protocols.

In future works, we will seek to apply this technique to LDPC codes specific for CVQKD applications, that is, with lower rates, compatible with capacity of the channels in low SNR regimes, and larger dimensions, investigating its viability in the face of to conventional reconciliation techniques.

#### ACKNOWLEDGEMENTS

The authors would like to thank CNPq and COPELE - UFCG for their financial support and IQuanta for the opportunity to carry out this research and for the availability of structure and material support.

#### REFERENCES

- [1] A. Leverrier and P. Grangier, “Continuous-variable quantum key distribution protocols with a discrete modulation,” jan 2011.
- [2] M. A. Nielsen and I. L. CHUANG, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *International Conference on Computers, Systems, and Signals Processing*, pp. 175–179, 1984.
- [4] C. H. Bennet, “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, pp. 3121–3124, may 1992.
- [5] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Physical Review Letters*, vol. 67, pp. 661–663, august 1991.
- [6] E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: Principle, security and implementations,” *Entropy*, august 2015.
- [7] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002.
- [8] P. D. E. Ghorai, Shouvik; Grangier and A. Leverrier, “Asymptotic security of continuous-variable quantum key distribution with a discrete modulation,” *Physical Review X*, vol. 9, june 2019.
- [9] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, “Quantum cryptography without switching,” *Phys. Rev. Lett.*, vol. 93, p. 170504, Oct 2004.
- [10] C. Weedbrook and K. Brádler, “Security proof of continuous-variable quantum key distribution using three coherent states,” *Physical Review A*, february 2018.
- [11] M. A. Dias and F. M. d. Assis, “Amplitude-phase modulated cvqkd protocol,” in *Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - SBrT 2021*, vol. 39, september 2021.
- [12] Y. L. Z. W. X. Wang, Pu; Zhang and Y. Li, “Discrete-modulation continuous-variable quantum key distribution with a high key rate,” *New Journal of Physics*, feb 2023.
- [13] C. Z. L. M. Milicevic, Mario; Feng and P. G. Gulak, “Key reconciliation with low-density parity-check codes for long-distance quantum cryptography,” *ArXiv*, 2017.
- [14] M. A. Dias and F. M. d. Assis, “Distributional transform based information reconciliation,” april 2022.
- [15] J. Assche, Gilles Van; Cardinal and N. J. Cerf, “Reconciliation of a quantum-distributed gaussian key,” *IEEE Transactions on Information Theory*, vol. 50, Feb 2004.
- [16] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, “High-bit-rate continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 90, p. 042329, Oct 2014.
- [17] A. Leverrier and P. Grangier, “Unconditional security proof long-distance continuous-variable quantum key distribution with discrete modulation,” *Physical Review Letters*, pp. 180504–1–180504–4, May 2009.
- [18] R. Gallager, “Low-density parity-check codes,” *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.
- [19] L. M. C. d. Araújo, “Novo método de quantização para protocolos de reconciliação de chaves secretas geradas quanticamente utilizando códigos ldpc no sentido slepian-wolf,” 2017.
- [20] N. J. W. J. T.-B. R. Grosshans, Frédéric; Cerf and P. Grangier, “Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables,” *Quantum Information and Computation*, vol. 0, no. 0, 2003.
- [21] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, “Multidimensional reconciliation for a continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 77, p. 042325, Apr 2008.
- [22] T. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.
- [23] D. Slepian and J. K. Wolf, “Noiseless coding of correlated information sources,” *IEEE Transactions on Information Theory*, vol. 19, jul 1973.
- [24] Z. Liveris, Angelos D.; Xiong and C. N. Georghiadis, “Compression of binary sources with side information at the decoder using ldpc codes,” *IEEE Communications Letters*, vol. 6, oct 2002.
- [25] K. Kasai, R. Matsumoto, and K. Sakaniwa, “Information reconciliation for qkd with rate-compatible non-binary ldpc codes,” in *2010 International Symposium On Information Theory Its Applications*, pp. 922–927, 2010.
- [26] S. Lin and D. J. Costello Jr., *Error Control Coding*. Pearson, second ed., may 2004.
- [27] *Unified high-speed wire-line based home networking transceivers - System architecture and physical layer specification*, jun 2010.
- [28] S. Bai, Zengliang; Yang and Y. Li, “High-efficiency reconciliation for continuous variable quantum key distribution,” *Japanese Journal of Applied Physics*, Apr 2017.

# Exploring Non-Gaussianity Reduction in Quantum Channels

Micael Andrade Dias and Francisco Marcos de Assis

**Abstract**—The quantum relative entropy between a quantum state and its Gaussian equivalent is a quantifying function of the system non-Gaussianity, which is useful in several applications, such as quantum communication and computation. One of its most fundamental properties is to be monotonic decreasing under Gaussian evolutions. In this paper we develop the conditions for a non-Gaussian quantum channel to preserve the monotonic decreasing property. We propose a necessary condition to classify between Gaussian and non-Gaussian channels and use it to construct a class of quantum channels that decreases the system non-Gaussianity. We also discuss how this property, combined with a restriction on the states at the channel’s input, can be applied to the security analysis of continuous-variable quantum key distribution protocols.

**Keywords**—Quantum Resource Theory, Gaussian Channels, non-Gaussianity.

## I. INTRODUCTION

Quantum resource theory (QRT) stands as a cornerstone in the field of quantum information science, providing a formal framework for understanding and manipulating various quantum resources [2]. From entanglement to coherence, quantum resource theories offer a systematic approach to quantifying and harnessing the unique properties of quantum systems, paving the way for advancements in quantum communication, computation, and beyond [20], [23].

Non-Gaussian resource theory, for instance, inquires how much resource there is in non-Gaussian states and operations, once the Gaussian sector of quantum states and operations is more simple to be operated in a laboratory. Central to the study of non-Gaussian quantum resource theory (nG-QRT) is quantum relative entropy (QRE), a powerful tool for quantifying the non-Gaussianity of quantum states [15]. In particular, the quantum relative entropy plays a pivotal role as a resource quantifying function, offering insights into the distinguishability between a quantum state and its Gaussian equivalent [8], [9]. A key property of the quantum relative entropy is its monotonic decrease under Gaussian operations, providing a robust foundation for characterizing non-Gaussian transformations and their effects on system non-Gaussianity.

Although quantum resource theory has found widespread applications across various domains of quantum information science [5], [10], [18], [19], its integration into continuous-variable quantum key distribution (CV-QKD) protocols has been relatively limited. In some foundational studies, its

developments have been utilized merely to corroborate well-known results from existing literature, such as the optimality of Gaussian states with respect to entropic quantities, rather than being actively exploited to improve the capabilities and security of CV-QKD schemes [7]. However, one promising avenue for application lies in the security analysis of CV-QKD protocols that utilize non-Gaussian modulation of coherent states.

In such a scenario, Alice and Bob (the trusted parties) must estimate how much information Eve (the eavesdropper) has had access during the protocol execution. When estimating this crucial quantity, Alice and Bob must decide which model they will use to describe the quantum channel linking them, either a Gaussian or a non-Gaussian. When assuming a Gaussian model, they in fact can upper bound Eve’s information by reconstructing a covariance matrix using solely the channel transmittance and excess noise. Despite its practical relevance, the Gaussian channel model does not cover the worst case scenario of Eve’s attacks given that Alice did not prepare her states according to a Gaussian distribution [3].

State-of-the-art security analyses of CV-QKD with non-Gaussian modulation often involve sophisticated optimization techniques [3], [13]. These analyses aim to determine the maximal eavesdropper information by exploring the space of non-Gaussian quantum channels compatible with the estimated parameters during quantum communication. When non-Gaussian modulation is used to quantum state transmission, non-Gaussianity has to be taken into account in the security analysis.

In this paper we investigate the gap between the Gaussian and non-Gaussian security model of CV-QKD by using non-Gaussian QRT. More precisely, we take as starting point one basic property of the QRE measure of non-Gaussianity, its monotone decrease under Gaussian operations, and investigate how it can be extended to non-Gaussian quantum channels. By presenting the conditions under which a nG quantum channel reduces the system nG, we discuss how it can be used in security proofs of CV-QKD protocols with non-Gaussian modulation. We also give examples of such quantum channels showing that, for specific mixtures of quantum states at the channel input, the covariance matrix does not change while the system nG is reduced.

The remainder of the paper is structured as follows. Section II states the formal definitions and the problem we aim to cover. In Section III we develop the main results with respect to nG quantum channels and in Section IV we explore how it can be used in the security analysis of CV-QKD protocols. In Section V we give our concluding remarks and in the Appendix we show how three types of quantum states behave

Micael Andrade Dias, QuIN - Quantum Industrial Innovation, Centro de Competência Embrapii Cimatec. SENAI CIMATEC, Av. Orlando Gomes, 1845, Salvador, BA-Brazil, e-mail: micael.dias@fieb.org.br; Francisco Marcos de Assis, Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande, PB-Brazil, e-mail: fmarcos@dee.ufcg.edu.br.



under the phase diffusion process.

### A. Notation

In what follows, we use the standard Dirac notation for quantum mechanics. If  $A$  and  $B$  are quantum systems with associated Hilbert spaces  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , respectively,  $\mathcal{B}(\mathcal{H}_A)$  and  $\mathcal{D}(\mathcal{H}_A)$  denote the space of bounded linear operators and the set of density operators in  $\mathcal{H}_A$ , respectively, with elements represented as  $\hat{A} \in \mathcal{B}(\mathcal{H}_A)$  and  $\hat{\rho} \in \mathcal{D}(\mathcal{H}_A)$ .

The subspace of completely positive trace preserving (CPTP) linear operators from  $\mathcal{H}_A$  to  $\mathcal{H}_B$  is denoted as  $\mathcal{Q}(\mathcal{H}_A \rightarrow \mathcal{H}_B)$ . All indexes will be dropped when implicit. If  $\mathcal{N}$  is a quantum channel, the evolution of a state, as well as the transformations of any of its quantities, are represented by  $\mathcal{N}(\cdot)$  or  $\xrightarrow{\mathcal{N}}$ . In special, we denote by  $\mathcal{G} \subset \mathcal{Q}$  the subset of all Gaussian quantum channels.

The weak convergence of a sequence  $\{P_n\}$  of probability measures is indicated as  $P_n \Rightarrow P$  and the convergence in distribution of a sequence  $\{X_n\}$  of random variables is indicated by  $X_n \xrightarrow{D} X$ . It is worth emphasizing that we will use the abbreviation ‘‘nG’’ to both ‘‘non-Gaussian’’ and ‘‘non-Gaussianity’’, with the distinction being clear from the context.

## II. PRELIMINARIES AND PROBLEM STATEMENT

The question we are proposing is: can a quantum state have its non-Gaussianity reduced after undergoing a non-Gaussian evolution? Alternatively, is there exists any non-Gaussian channel that makes quantum states ‘‘more Gaussian’’? By *non-Gaussianity* (nG) of an arbitrary quantum state, the literature often refers to a quantity informing ‘‘how much’’ that a non-Gaussian state fails to pass as a Gaussian state. More operationally, it may be defined as the distance from a Gaussian reference state [15]. Here we use the quantum relative entropy as a quantifying function of non-Gaussianity: even though it is not a metric, it satisfies all axioms for a resource quantifying function, which are all operationally oriented.

In the following definition, the Gaussian equivalent state means the Gaussian quantum state with the same mean vector and covariance matrix.

*Definition 1* ([9]): Let  $\hat{\sigma}$  be an arbitrary quantum state and  $\hat{\sigma}^G$  its Gaussian equivalent. The quantum relative entropy based non-Gaussianity  $\hat{\sigma}$  is defined as,

$$\delta_{vN}(\hat{\sigma}) = S(\hat{\sigma} || \hat{\sigma}^G). \quad (1)$$

Among the many properties of  $\delta_{vN}(\hat{\sigma})$ , we highlight its non-negativity and contractivity under Gaussian quantum channels, that is,  $\delta_{vN}(\hat{\sigma}) \geq 0$  and  $\delta_{vN}(\hat{\sigma}) \geq \delta_{vN}(\mathcal{N}(\hat{\sigma}))$  for any  $\hat{\sigma} \in \mathcal{D}(\mathcal{H})$  and  $\mathcal{N} \in \mathcal{G}$ .

Now, consider the following setup. Let  $\{X_n\}$  be a sequence of random variables (with corresponding alphabet  $\mathcal{X}_n$  and probability mass function  $p_{X_n}(x)$ ) such that  $X_n \xrightarrow{D} X_G \sim \mathcal{CN}(0, \bar{m})$  and define  $\hat{\rho}_{X_n} = \sum_{x \in \mathcal{X}_n} p_{X_n}(x) |x\rangle\langle x|$  where  $|x\rangle$  is a coherent state with parameter  $x$ . Such mixed state represent what a transmitter (Alice) can send to the receiver (Bob) though a quantum channel  $\mathcal{N}_{A \rightarrow B}$  in a CV-QKD protocol applying discrete modulation of coherent states.

In [4] it was proved that

$$\lim_{n \rightarrow \infty} \inf_{\mathcal{N}_{A \rightarrow B}} \{\delta_{vN}(\mathcal{N}_{A \rightarrow B}(\hat{\rho}_{X_n}))\} = 0, \quad (2)$$

where the infimum must be computed with respect to all quantum channels  $\mathcal{N}_{A \rightarrow B}$  compatible with the statistics observed at the output up to the second moment<sup>1</sup>. The demonstration of Equation (2) uses the following reasoning. Let  $\mathcal{N} \in \mathcal{G}$  and  $\mathcal{N}^* \in \mathcal{Q}$  the quantum channel achieving the infimum in Equation (2). Then, the following inequality holds,

$$\delta_{vN}(\hat{\rho}_{X_N}) \geq \delta_{vN}(\mathcal{N}(\hat{\rho}_{X_N})) \geq \delta_{vN}(\mathcal{N}^*(\hat{\rho}_{X_N})), \quad (3)$$

which, by the convergence  $X_n \xrightarrow{D} X_G \sim \mathcal{CN}(0, \bar{m})$ , one has that

$$\lim_{n \rightarrow \infty} \delta_{vN}(\mathcal{N}^*(\hat{\rho}_{X_N})) \leq \lim_{n \rightarrow \infty} \delta_{vN}(\hat{\rho}_{X_n}) = 0. \quad (4)$$

The intriguing fact we notice in Equation (3) is that the mixed state  $\hat{\rho}_{X_N}$  before the quantum channel is ‘‘more non-Gaussian’’ than the state after the quantum channel  $\mathcal{N}^*$  achieving the infimum, which were not imposed to be Gaussian. One reasonable question coming up is whether a non-Gaussian channel can reduce the non-Gaussianity of a quantum channel. In other words, we are interested in investigating if monotone property of the QRE-nG may be extended to some set of quantum channels further than the Gaussian sector, even if it is required to restrict the set of quantum states. We intend to answer these questions in the next section.

## III. QUANTUM RELATIVE ENTROPY MONOTONICITY UNDER NON-GAUSSIAN QUANTUM CHANNELS

We are now able to develop the conditions for which an nG quantum channel maintains the monotonic property of QRE-nG and how such channels can be useful in the description of the relevant quantum channels in a DM-CVQKD protocol. We begin by proving the following lemma.

*Lemma 1:* Let  $\mathcal{N}$  be a quantum channel,  $\hat{\rho}$  an arbitrary quantum state and define

$$\Delta(\mathcal{N}, \hat{\rho}) = \text{tr}[\mathcal{N}(\hat{\rho})(\log \mathcal{N}(\hat{\rho})^G - \log \mathcal{N}(\hat{\rho}^G))]. \quad (5)$$

If  $\mathcal{N} \in \mathcal{G}$  then  $\Delta(\mathcal{N}, \hat{\rho}) = 0$  for any quantum state  $\hat{\rho}$ .

*Proof:* If  $\mathcal{N}$  is a Gaussian channel and  $\mathbf{\Gamma}$  is the covariance matrix of an arbitrary quantum state  $\hat{\rho}$ , then  $\mathbf{\Gamma}(\hat{\rho}) = \mathbf{\Gamma}(\hat{\rho}^G)$  and  $\mathbf{\Gamma} \xrightarrow{\mathcal{N}} \mathbf{\Gamma}'$ . This means that  $\mathbf{\Gamma}(\mathcal{N}(\hat{\rho})^G) = \mathbf{\Gamma}(\mathcal{N}(\hat{\rho}^G)) = \mathbf{\Gamma}'$ . Since the first moment will follow as same,  $\mathcal{N}(\hat{\rho}^G) = \mathcal{N}(\hat{\rho})^G$  for any  $\hat{\rho} \in \mathcal{D}(\mathcal{H})$  and then  $\Delta(\mathcal{N}, \hat{\rho}) = 0$  for arbitrary  $\hat{\rho}$ . ■

This result gives a sufficient condition to classify a quantum channel with respect to its non-Gaussianity: if it is verified that  $\Delta(\mathcal{N}, \hat{\rho}) \neq 0$  for some quantum state  $\hat{\rho}$ , then  $\mathcal{N}$  is nG.

Now, define the set of quantum channels for which  $\Delta \geq 0$ ,  $\mathcal{F} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N}, \hat{\rho}) \geq 0 \forall \hat{\rho} \in \mathcal{D}(\mathcal{H})\}$ . Then,  $\mathcal{G} \subset \mathcal{F}$  and this allows us to propose the following statement:

<sup>1</sup>We point out that in [4] the main problem was the analysis of the role of non-Gaussianity in security proofs of continuous-variable quantum key distribution protocols using discrete modulation of coherent states. That is why it is relevant to restrict the quantum channels to the ones matching the first and second statistical moments at the reception when defining the infimum in Equation (2).

*Theorem 1:* If  $\mathcal{N} \in \mathcal{F}$  then  $\delta_{vN}(\mathcal{N}(\hat{\rho})) \leq \delta_{vN}(\hat{\rho})$  for any  $\hat{\rho} \in \mathcal{D}(\mathcal{H})$ .

*Proof:* Let  $\hat{\rho}$  and  $\mathcal{N}$  be as in the setup. From quantum relative entropy contractivity under quantum channels, one gets

$$\delta_{vN}(\hat{\rho}) \stackrel{(a)}{=} S(\hat{\rho}||\hat{\rho}^G) \quad (6)$$

$$\stackrel{(b)}{\geq} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G)) \quad (7)$$

$$\stackrel{(c)}{=} \text{tr}[\mathcal{N}(\hat{\rho})(\log \mathcal{N}(\hat{\rho}) - \log \mathcal{N}(\hat{\rho}^G))] + \text{tr}[(\mathcal{N}(\hat{\rho}) - \mathcal{N}(\hat{\rho}^G) \log \mathcal{N}(\hat{\rho}^G)] \quad (8)$$

$$\stackrel{(d)}{=} S(\mathcal{N}(\hat{\rho})^G) - S(\mathcal{N}(\hat{\rho})) + \Delta(\mathcal{N}, \hat{\rho}) \quad (9)$$

$$\stackrel{(e)}{=} S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho})^G) + \Delta(\mathcal{N}, \hat{\rho}) \quad (10)$$

$$\stackrel{(f)}{\geq} \delta_{vN}(\mathcal{N}(\hat{\rho})), \quad (11)$$

where (a) comes from the definition of  $\delta_{vN}$ , (b) from the monotonicity of quantum relative entropy [21], (c) one has that  $\text{tr}[(\hat{\sigma} - \hat{\sigma}^G) \log(\hat{\sigma}^G)] = 0$  for arbitrary  $\hat{\sigma}$  [11], (d) we used the definition in Lemma 1, (e) from Definition 1 and (f) because  $\mathcal{N}$  and  $\hat{\rho}$  where chosen such that  $\Delta(\mathcal{N}, \hat{\rho}) \geq 0$ . ■

The above result extends the monotone property of  $\delta_{vN}$  under Gaussian quantum channels to nG channels and also provides an interpretation of the quantity given by  $\Delta(\mathcal{N}, \hat{\rho})$ : if it is non-negative for every  $\hat{\rho}$ ,  $\mathcal{N}$  does not increase QRT-nG.

However, the specification of  $\mathcal{F}$  may have been too broad by demanding  $\Delta(\mathcal{N}, \hat{\rho})$  to be non-negative for all quantum states in the system and we cannot affirm whether  $\mathcal{F} \setminus \mathcal{G} = \{\emptyset\}$  or not. A relaxation in this condition can be done by considering only a specific set of quantum states, which we chose to be the states relevant to DM-CVQKD protocols, and can be helpful in describing a set of QRE-nG non-increasing quantum channels.

Let  $\mathcal{S}_{\bar{n}} = \{\hat{\sigma} \in \mathcal{D}(\mathcal{H}) : \hat{\sigma} = \sum_{x \in \mathcal{X}_n} p(x) \hat{\rho}^{th}(x, \bar{n})\}$  with  $X_n$  being a discrete symmetric random variable and  $\hat{\rho}^{th}(x, \bar{n})$  be the displaced thermal state with  $\bar{n}$  average photons and the first moment  $\bar{x} = 2 \cdot (\text{Re}\{x\}, \text{Im}\{x\})^T$ . Constellations of coherent states are represented by the set  $\mathcal{S}_0$  and any state in  $\mathcal{S}_{\bar{n}}$  has a diagonal covariance matrix for any value of  $\bar{n}$ , which means that its equivalent Gaussian quantum state is a thermal state with the appropriate mean photon number. Then, we can define a relaxed set  $\mathcal{F}_{\bar{n}} = \{\mathcal{N} \in \mathcal{Q} : \Delta(\mathcal{N}, \hat{\rho}) \geq 0 \forall \hat{\rho} \in \mathcal{S}_{\bar{n}}\}$  such that the QRE-nG of any quantum state in  $\mathcal{S}_{\bar{n}}$  is non-increasing under the action of any channel in  $\mathcal{F}_{\bar{n}}$ . Also, we have  $\mathcal{G} \subset \mathcal{F} \subset \mathcal{F}_{\bar{n}}$  for any  $\bar{n}$ . The states in  $\mathcal{S}_{\bar{n}}$  are relevant for the QKD setup because they represent the mixed states output by a thermal loss channel with thermal noise  $\bar{n}$ . We can affirm the following proposition.

*Proposition 1:*  $\mathcal{F}_0 \setminus \mathcal{G} \neq \{\emptyset\}$ .

*Proof:* Take the phase diffusion process described in Appendix and represented by  $\mathcal{N}_{\Delta}$ , which is the model of a non-Gaussian evolution of a quantum system. It is known that the QRE-nG of coherent states under phase diffusion increases with time and in Appendix we show that for any  $\hat{\rho} \in \mathcal{S}_0$ ,  $\bar{x}(\hat{\rho}) = \bar{x}(\mathcal{N}_{\Delta}(\hat{\rho}))$  and  $\Gamma(\hat{\rho}) = \Gamma(\mathcal{N}_{\Delta}(\hat{\rho}))$ , which implies that  $\hat{\rho}^G = \mathcal{N}_{\Delta}(\hat{\rho})^G$ . That is, the phase diffusion process does not modify the first and second statistical moments of appropriated mixtures of coherent states. In addition, it does

not have an effect on thermal states, meaning that  $\mathcal{N}_{\Delta}(\hat{\rho}^G) = \hat{\rho}^G$ . We conclude that  $\mathcal{N}_{\Delta}(\hat{\rho}^G) = \mathcal{N}_{\Delta}(\hat{\rho})^G$  which results in  $\Delta(\mathcal{N}_{\Delta}, \hat{\rho}) = 0$  for any state in  $\mathcal{S}_0$  and then in  $\mathcal{F}_0 \setminus \mathcal{G} \neq \{\emptyset\}$ . ■

We conjecture that Proposition 1 can be extended to other values of  $\bar{n}$  different from zero, although we have not yet worked out the proof.

#### IV. APPLICATION TO QKD PROTOCOLS

Finding the best eavesdropping strategy is a crucial step towards proving security of a QKD protocol. For protocols with continuous variables, the optimality of Gaussian attacks was a pivotal result simplifying the security analysis: if the protocol is based on a Gaussian modulation of coherent states<sup>2</sup>, the best Eve can do is to perform the “entangling cloner attack”, which is equivalent to a Gaussian quantum channel with transmittance  $\tau$  and excess noise  $\xi$  [1], [6], [17], [22]. The consequence is that Alice and Bob can safely assume the Gaussian channel model in the security analysis.

The problem completely changes when Alice does not use a Gaussian modulation. By using a set of coherent states according to some discrete random variable  $X_n$ , for example (as previously), it is not guaranteed that Gaussian attacks are optimal and security must include non-Gaussian quantum channels for computing the eavesdropper information [3]. Although, such nG channels must be compatible with the parameters observed in the classical data resulting from Bob’s measurements. It means that Alice and Bob must estimate the channel parameters  $\tau$  and  $\xi$  using its classical data and compute the *worst case scenario* eavesdropper information considering any kind of quantum channel yielding the estimated parameters.

It was shown that the phase diffusion process preserves the monotone property of the QRE-nG when restricted to an appropriate set of quantum states. Additionally, it does not modifies the covariance matrix of the input state. both statements can be used in the analysis of discrete modulation CVQKD protocols and we can propose the following arrangement to decompose the quantum channel between Alice and Bob. Define by  $\mathcal{T}$  the set of quantum channels that preserve the first and second moments of any quantum state in  $\mathcal{S}_{\bar{n}}$  for any value of  $\bar{n}$ . Now, take a quantum thermal loss channel (which is Gaussian)  $\mathcal{N}_1 \in \mathcal{G}$  with transmittance  $\tau$  and excess noise  $\xi$  and an arbitrary quantum channel  $\mathcal{N}_2 \in \mathcal{T}$ . We can, w.l.g., assume that Alice and Bob are linked by  $\mathcal{N} = \mathcal{N}_2 \circ \mathcal{N}_1$ , as depicted in Figure 1.

The idea here is that the quantum channels considered in a DM-CVQKD security analysis can be broken down into two channels, the Gaussian  $\mathcal{N}_1$  yielding physical parameters in a practical deployment of a QKD protocol, raising the observed parameters  $\tau$  and  $\xi$ , and  $\mathcal{N}_2$ , which does not modify the covariance matrix (and then does not affect the parameter estimation), but is responsible for non-Gaussian interactions

<sup>2</sup>This means that Alice will transmit coherent states whose amplitudes are drawn from a circular Gaussian distribution (equivalently, the amplitude on each quadrature is drawn from independent and equally distributed Gaussian random variables.

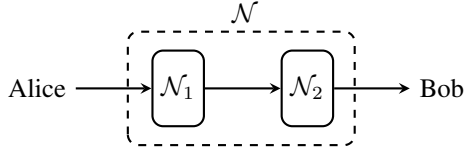


Fig. 1

REPRESENTATION OF THE PROPOSED QUANTUM CHANNEL DECOMPOSITION. THE CHANNEL  $\mathcal{N}$  CONNECTING ALICE AND BOB IS SPLIT IN A THERMAL-LOSS PART  $\mathcal{N}_1$  AND A NON-GAUSSIAN EVOLUTION  $\mathcal{N}_2$ . ALICE AND BOB RECONSTRUCT THE COVARIANCE MATRIX BY ESTIMATING THE PARAMETERS YIELD BY  $\mathcal{N}_1$ . ANY SECURITY ANALYSIS THAT GOES BEYOND CONSIDERING GAUSSIAN CHANNELS SHOULD THEN QUANTIFY THE EFFECT OF  $\mathcal{N}_2$  DURING QUANTUM COMMUNICATION.

giving more information to the eavesdropper. With such decomposition, we expect that security analysis can be made more accurately e efficient by restricting the set of quantum channels taken into account when computing the eavesdropper information.

## V. CONCLUSION

We explored the conditions under which a non-Gaussian quantum channel reduces the amount of non-Gaussianity of a quantum channel using the quantum relative entropy as a quantifying function. We proposed the functional  $\Delta(\mathcal{N}, \hat{\rho})$  that can be used to classify the channel  $\mathcal{N}$  as Gaussian or non-Gaussian. Based on  $\Delta(\mathcal{N}, \hat{\rho})$ , we developed a condition under which a non-Gaussian channel reduces the non-Gaussianity of its input states. This result extends the monotone decreasing property of the quantum relative entropy-based non-Gaussianity measure to outside the Gaussian sector of quantum operation.

The characterization of non-Gaussian channels reducing the non-Gaussianity of input states was used to establish a link between security analysis of CVQKD protocols and the class of non-Gaussianity reducing quantum channels. A decomposition of the general channels considered in the security analysis of CVQKD was proposed, with operational implications. It is still an open problem how this decomposition can improve the secret key rate bounds computed with today's security analysis framework. In addition, it may be possible that this decomposition can be used to improve parameter estimation procedures.

Future work can also be concentrated in generalizing the Proposition 1 and developing the properties of  $\Delta(\mathcal{N}, \hat{\rho})$ . Besides, it should be noticed that the difference  $S(\hat{\rho}||\hat{\rho}^G) - S(\mathcal{N}(\hat{\rho})||\mathcal{N}(\hat{\rho}^G))$  (see the proof of Theorem 1) is related to state recovery maps (Petz recovery maps), which are maps that can recover the state that suffered some physical evolution. Such recovery maps can be extended to quantum systems in infinite dimensions [12] and then may have connections with the “production of non-Gaussianity” and with CVQKD security analysis.

## ACKNOWLEDGMENTS

This work was supported in part by the National Council for Scientific and Technological Development (CNPq) under research Grant No. 305918/2019-2, CAPES, EMBRAP II and the Brazilian Ministry for Science, Technology and Innovation - MCTI.

## APPENDIX

One of the most harmful noisy processes in quantum information is the one that provokes decoherence, where the quantum states lose their “quantumness” — the full decohered states reduce to mixtures of orthogonal states which can be perfectly distinguished. Some open system processes result in random changes in the relative phase of the states that are in superposition in the main quantum system. Such a relative phase fluctuation results in a loss of coherence and is called phase damping or phase diffusion [14].

The single mode evolution of the system under such process can be described by the master equation [7], [16]

$$\frac{d}{dt}\hat{\rho} = \Gamma \mathcal{L}[\hat{a}^\dagger \hat{a}]\hat{\rho}, \quad (12)$$

where  $\mathcal{L}[\hat{O}]\hat{\rho} = 2\hat{O}^\dagger \hat{\rho} \hat{O} - \hat{O}^\dagger \hat{O} \hat{\rho} - \hat{\rho} \hat{O}^\dagger \hat{O}$ , or as the Hamiltonian of a harmonic oscillator open to an  $N$  mode environment [14]

$$H = \hbar\omega \hat{a}^\dagger \hat{a} + \hbar \sum_{i=1}^N \omega_i \hat{a}_i^\dagger \hat{a}_i + \hbar \sum_{i=1}^N \chi_i \hat{a}^\dagger \hat{a} (\hat{a}_i + \hat{a}_i^\dagger), \quad (13)$$

where  $\hat{a}$  and  $\hat{a}^\dagger$  are the annihilation and creation operators of the main system with frequency  $\omega$  and  $\hat{a}_i$  and  $\hat{a}_i^\dagger$  refer to the  $i$ th environment system with frequency  $\omega_i$ . The quantity  $\chi_i$  represents a coupling parameter between the main system and the  $i$ th environment mode.

This non-Gaussian evolution of a quantum state is an important source of noise in optical communication links. Its Krauss operator set  $\{P_k(t)\}$ ,  $0 \leq k \leq \infty$  has elements

$$P_k(t) = \sum_{n=0}^{\infty} e^{-\frac{1}{2}n^2\lambda^2} \sqrt{\frac{(n^2\lambda^2)^k}{k!}} |n\rangle\langle n| \quad (14)$$

where  $\lambda = t\sqrt{\Lambda}$  and  $\Lambda = \sum_i \chi_i^2 \sqrt{1 - e^{-n^2\lambda^2}}$ .

Lets see the effect of the phase diffusion process one three types of quantum states. First, the thermal state with average photon number  $\bar{n}$ ,  $\hat{\rho}^{th}(\bar{n})$ , is invariant under the phase diffusion process state as both  $\bar{n}$  and  $P_k(t)$  are diagonal in the same basis.

Our second case, the coherent state, is sensible to relative phase fluctuations. Define the complex amplitude  $|\alpha\rangle$  with  $\alpha = (q + ip)/2$ , one has that

$$\begin{aligned} \mathcal{N}_\Delta(|\alpha\rangle\langle\alpha|) &= e^{-|\alpha|^2} \sum_{m,n=0}^{\infty} \exp\{-\Delta^2(n-m)^2\}, \\ &\times \frac{\alpha^n \alpha^{*m}}{\sqrt{n!m!}} |n\rangle\langle m|, \end{aligned} \quad (15)$$

which is a non-Gaussian mixed state with  $\Delta = \lambda^2/2$ . Its first and second statistical moments evolve as

$$\bar{x} \xrightarrow{\mathcal{N}_\Delta} \begin{pmatrix} q \cdot e^{-\Delta^2} \\ p \cdot e^{-\Delta^2} \end{pmatrix}, \quad (16)$$

and the covariance matrix elements are

$$[\mathbf{\Gamma}]_{1,1} = 1 + 2|\alpha|e^{-\Delta^2} + e^{-4\Delta^2}(\alpha^2 + \alpha^{*2}) - q^2e^{-2\Delta^2} \quad (17)$$

$$[\mathbf{\Gamma}]_{2,2} = 1 + 2|\alpha|e^{-\Delta^2} - e^{-4\Delta^2}(\alpha^2 + \alpha^{*2}) - p^2e^{-2\Delta^2} \quad (18)$$

$$[\mathbf{\Gamma}]_{1,2} = [\mathbf{\Gamma}]_{2,1} = qp(e^{-4\Delta^2} - e^{-2\Delta^2}) \quad (19)$$

In contrast to thermal states, coherent states suffer from decoherence in a phase-diffusion evolution, with the off-diagonal elements of the density operator being more affected as the noise parameter  $\Delta$  becomes larger. In addition, the mean vector and the covariance matrix also change with  $\Delta$ . It contributes to the increasing non-Gaussianity of the state observed in [ref].

For our third and last example, let us consider mixtures of coherent states, specifically those representing proper digital modulation constellations, such as  $\hat{\rho} = \sum_i p_i |\alpha_i\rangle\langle\alpha_i|$ , and denote  $\hat{\rho}_\Delta = \mathcal{N}_\Delta(\hat{\rho})$ . Due to the linearity of the channel, we use (15) directly and have

$$\hat{\rho}_\Delta = \sum_{m,n=0}^{\infty} e^{-\Delta^2(n-m)^2} \sum_{i=0}^N p_i e^{-|\alpha_i|^2} \frac{\alpha_i^n \alpha_i^{*m}}{\sqrt{n!m!}} |n\rangle\langle m| \quad (20)$$

Clearly, as each coherent state is transformed into an nG mixed state, the resultant mixture will also be nG. Although, in contrast to a single coherent state, a symmetric convex mixture has the first and second moments invariant under phase diffusion, that is,

$$\text{tr}(\hat{q}\hat{\rho}_\Delta) = \text{tr}(\hat{p}\hat{\rho}_\Delta) = 0, \quad (21)$$

and

$$[\mathbf{\Gamma}]_{1,1} = [\mathbf{\Gamma}]_{2,2} = 1 + 2 \sum_{i=1}^N p_i |\alpha_i|^2, \quad (22)$$

$$[\mathbf{\Gamma}]_{1,2} = [\mathbf{\Gamma}]_{2,1} = 0, \quad (23)$$

so that  $\mathbf{\Gamma}(\hat{\rho}_\Delta) = \mathbf{\Gamma}(\hat{\rho})$ . In what was exposed, the phase diffusion channel, not being Gaussian, does not necessarily map Gaussian states into Gaussian states, but there are cases in which this happens: thermal states are invariant under such physical process, in opposition to coherent states. Interestingly, if one prepares “symmetric” mixtures (with respect to the origin in the phase space) of coherent states, which already is not Gaussian so that the process would not “map it back” do Gaussianity, its first and second moments are preserved under phase diffusion evolution. We can then assume that there is a set of quantum states (convex mixtures of coherent states) whose first and second statistical moments are invariant under some non-Gaussian evolutions of the system.

## REFERENCES

- [1] N. J. Cerf, G. Leuchs, and E. S. Polzik. *Quantum Information with Continuous Variables of Atoms and Light*. Icp, 2007.
- [2] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2):025001, April 2019.
- [3] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, September 2021.
- [4] Micael Andrade Dias and Francisco Marcos de Assis. Converging State Distributions for Discrete Modulated CVQKD Protocols, May 2023.
- [5] Jaromír Fiurášek. Gaussian Transformations and Distillation of Entangled Gaussian States. *Physical Review Letters*, 89(13):137904, September 2002.
- [6] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):1–4, 2006.
- [7] Marco G. Genoni and Matteo G. A. Paris. Quantifying non-Gaussianity for quantum information. *Physical Review A*, 82(5):052341, November 2010.
- [8] Marco G. Genoni, Matteo G. A. Paris, and Konrad Banaszek. Measure of the non-Gaussian character of a quantum state. *Physical Review A*, 76(4):042327, October 2007.
- [9] Marco G. Genoni, Matteo G. A. Paris, and Konrad Banaszek. Quantifying the non-Gaussian character of a quantum state by quantum relative entropy. *Physical Review A*, 78(6):060303, December 2008.
- [10] Géza Giedke and J. Ignacio Cirac. Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66(3):032316, September 2002.
- [11] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum Gaussian channels. *Physical Review A*, 59(3):1820–1828, March 1999.
- [12] Marius Junge, Renato Renner, David Sutter, Mark M. Wilde, and Andreas Winter. Universal Recovery Maps and Approximate Sufficiency of Quantum Relative Entropy. *Annales Henri Poincaré*, 19(10):2955–2978, October 2018.
- [13] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Physical Review X*, 9(4):041064, December 2019.
- [14] Yu-xi Liu, Şahin K. Özdemir, Adam Miranowicz, and Nobuyuki Imoto. Kraus representation of a damped harmonic oscillator and its application. *Physical Review A*, 70(4):042308, October 2004.
- [15] Paulina Marian and Tudor A. Marian. Relative entropy is an exact measure of non-Gaussianity. *Physical Review A*, 88(1):012322, July 2013.
- [16] Laleh Memarzadeh and Stefano Mancini. Minimum output entropy of a non-Gaussian quantum channel. *Physical Review A*, 94(2):022341, August 2016.
- [17] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97(19):2–5, 2006.
- [18] Julien Niset, Jaromír Fiurášek, and Nicolas J. Cerf. No-Go Theorem for Gaussian Quantum Error Correction. *Physical Review Letters*, 102(12):120501, March 2009.
- [19] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy. Quantum computation with optical coherent states. *Physical Review A*, 68(4):042319, October 2003.
- [20] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-Gaussianity. *Physical Review A*, 97(6):062337, June 2018.
- [21] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2 edition, 2017.
- [22] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.*, 96(8):080502, March 2006.
- [23] Quntao Zhuang, Peter W. Shor, and Jeffrey H. Shapiro. Resource theory of non-Gaussian operations. *Physical Review A*, 97(5):052317, May 2018.

# Enhanced Channel Estimation and Data Detection in OFDM Systems without Cyclic Prefix using Quantum Machine Learning Algorithms

Demerson N. Gonçalves and João T. Dias

**Abstract**—Channel estimation in OFDM systems requires minimal complexity with one-tap equalizers. However, this depends on cyclic prefixes, which must be sufficiently large to cover the channel impulse response. Conversely, the use of cyclic prefix (CP) decreases the useful information that can be conveyed in an OFDM frame, thereby degrading the spectral efficiency of the system. In this context, we propose the use of quantum kernel in support vector machine (SVM) algorithm for channel estimation and symbol detection in OFDM systems without CP and compare its performance with the LS and the classic support vector regressor (SVR) for channel estimation and coherent demodulation for symbol detection. The viability of our approach is substantiated by computational simulation results obtained in frequency selective channel models with the presence of Gaussian noise.

**Keywords**—Channel estimation, symbol detection OFDM, SVR, QSVR.

## I. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) has emerged as a prominent scheme for high-bit-rate wireless networking standards [1]-[6]. Its primary advantage lies in its ability to eliminate intersymbol interference (ISI) and intercarrier interference (ICI) without necessitating complex equalization filters at the receiver. While ISI is mitigated through the use of a cyclic prefix, ICI poses challenges in dynamic channels or when there are local oscillator mismatches with high carrier frequency offsets (CFOs). Common strategies to enhance the useful data rate in OFDM systems include reducing the pilot rate, expanding the number of subcarriers, or increasing the modulation order. However, each approach introduces its own set of complications. Decreasing the pilot rate compromises channel estimation accuracy and renders the system more vulnerable to rapid channel variations observed in dynamic channels. Expanding the number of subcarriers, while maintaining the same bandwidth to avoid interference in adjacent channels, escalates both computational complexity and the required clock speed for signal processing. Lastly, increasing the modulation order exacerbates the bit error rate (BER) at the receiver.

In the context of advancing digital communications systems, Support Vector Regression (SVR) has proven effective, particularly in addressing challenges like channel estimation

in scenarios with non-linearities [7]. To optimize SVR performance, selecting an appropriate kernel based on Mercer's conditions is essential, alongside parameter adjustments for achieving optimal regression outcomes [8]-[9]. In OFDM systems, SVR emerges as a powerful tool for efficient and robust channel estimation and data detection. By formulating channel estimation as an SVR problem, we aim to find the best-fitting hyperplane that minimizes error between predicted and actual channel coefficients. SVR achieves this by mapping received signals to true channel coefficients, optimizing a loss function, and considering a regularization parameter to manage model complexity. This approach enables efficient channel response estimation, even amidst noise and interference.

In recent years, there has been a growing interest in quantum computing as a potential solution to the computational challenges faced by modern Machine Learning (ML) systems. Quantum computing has made significant progress, promising faster computations across various scientific and industrial applications. Some studies assert time advantage [10]-[17], while others showcase enhancements in accuracy and convergence [18]-[21]. In this study, we propose using a quantum support vector regressor (QSVR) to address channel estimation and quantum support vector classifier (QSVC) to address data detection in an OFDM system without CP, especially in scenarios characterized by frequency-selective channels and Gaussian noise presence.

This article is divided as follows: in section II, the OFDM system are described. The channel estimations and data detection models are presented in section III. In section IV, the QSVR and QSVC are presented. The results are shown in section V, and conclusions are made in section VI.

## II. OFDM SYSTEM MODELING FRAMEWORK

The block diagram of the implemented OFDM system is shown in Fig. 1. In this system,  $b$  are the bits to be transmitted,  $s$  are the frequency domain data symbols,  $x$  are the time domain data samples,  $y$  is the received signal in the time domain,  $\tilde{s}$  is the received signal in the frequency domain and  $\hat{b}$  are the estimated bits.

The OFDM signal can be expressed in the time domain by [1]

$$x[n] = \sum_{k=0}^{K-1} s_k e^{j2\pi \frac{k}{K} n}, \quad (1)$$

where  $s_k$  is the data symbol on the  $k$ -th subcarrier and  $K$  is the number of subcarriers in the OFDM symbol.

Demerson N. Gonçalves is professor at Collegiate of Mathematics, CEFET/RJ, Petrópolis, RJ, E-mail: demerson.goncalves@cefet-rj.br. João T. Dias is professor at the Department of Telecommunications, CEFET/RJ, Maracanã, RJ, E-mail: joao.dias@cefet-rj.br. This work was partially financed by the program "GPESq-CEFET/RJ"

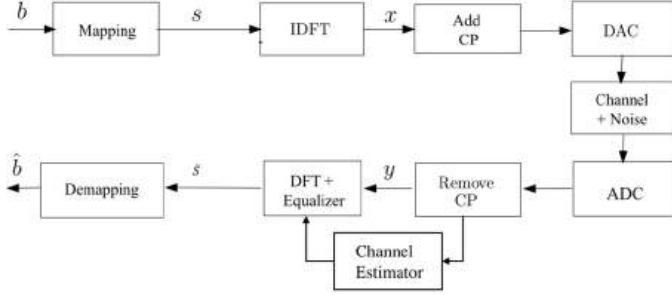


Fig. 1. Block diagram of the implemented OFDM system.

The signal at the receiver can be written by

$$y[n] = \sum_{k=0}^{K-1} s_k H_k e^{j2\pi \frac{k}{K} n} + \omega_n, \quad (2)$$

where  $y[n]$  are time-domain sample before DFT transformation,  $H_k$  is the channel's frequency response at the  $k$ th frequency and  $\omega_n$  is additive white Gaussian noise (AWGN).

### III. CHANNEL ESTIMATION AND DATA DETECTION

#### A. Channel Estimators

Channel estimation can be performed either in the time domain or in the frequency domain. In OFDM systems, pilot symbols  $s_p$  are typically inserted between data symbols for the purpose of channel estimation. These pilot symbols allow for the initial estimation of the channel's frequency response across a subset  $\kappa_p$  of subcarriers, known as pilot positions, with a cardinality  $|\kappa_p|$ . Then, the channel's frequency response is interpolated across the remaining  $K - |\kappa_p|$  subcarriers. Hence, the OFDM system can be expressed as

$$y[n] = \sum_{k \in \kappa_p} s_p(k) H_p(k) e^{j2\pi \frac{k}{K} n} + e_n, \quad (3)$$

where,  $y[n]$  represents the received signal in the time domain;  $s_p(k)$  denotes the pilot symbol transmitted on the  $k$ -th subcarrier;  $H_p(k)$  represents the frequency response of the channel at the  $k$ -th subcarrier and  $e_n = \sum_{k \notin \kappa_p} s(k) H(k) e^{j2\pi \frac{k}{K} n} + z_n$  encompasses the residual noise and the interference from data symbols on non-pilot subcarrier. Here, these unknown symbols carrying information will be considered as noise during the training phases. It is well known that for a channel impulse response with a maximum of  $L$  resolvable paths (and, consequently, degrees of freedom), then  $|\kappa_p| \geq L$  [22].

In this study, we will evaluate the performance of various channel estimation techniques. The estimators selected for comparison have been carefully chosen based on their relevance and effectiveness in the context of our investigation:

##### 1) LS:

The least squares (LS) channel estimator yields the estimation of the channel's frequency response at the pilot tone positions as referenced in [23]

$$\hat{H}(k) = \frac{\hat{s}_p(k)}{s_p(k)}, \quad (4)$$

where  $\hat{s}_p(k)$  represents the received signal on the  $k$ -th subcarrier in the frequency domain, while  $s_p(k)$  denotes the pilot

signal transmitted on the  $k$ -th subcarrier. Following the estimation process, a linear interpolation technique is employed to derive the channel's frequency response across all subcarriers within the OFDM symbol.

##### 2) SVR:

SVR is an extension of the widely-known Support Vector Machine (SVM) technique, initially proposed by Drucker et al. [24]. While SVM aims to find an optimal hyperplane for classification tasks, SVR seeks an optimal hyperplane with an  $\epsilon$ -tube around it to accommodate a continuous output variable. This  $\epsilon$ -tube ensures that most data points fall within its boundaries. Like SVM, SVR employs the kernel trick to map the input data into a higher-dimensional feature space, facilitating linear regression analysis.

Considering that SVR was originally designed to operate on real-valued samples [25], we adapt our methodology to handle OFDM symbols, which are typically complex-valued. Our proposed SVR estimator is divided into two parallel estimators, each focusing on either the real part  $\Re(y[n])$  or the imaginary part  $\Im(y[n])$  of the OFDM symbol. For simplicity and clarity, we detail only the estimation process for the real part below, as the development for the imaginary part is analogous.

The dual optimization problem for  $\epsilon$ -kernel-SVR is given by (Refs. [26], [27]):

$$\begin{aligned} \max_{\alpha, \alpha^*} & -\epsilon \sum_{i=1}^{l_{sv}} (\alpha_i + \alpha_i^*) + \sum_{i=1}^{l_{sv}} (\alpha_i^* - \alpha_i) \Re(y[i]) \\ & - \frac{1}{2} \sum_{j=1}^{l_{sv}} \sum_{i=1}^{l_{sv}} (\alpha_i^* - \alpha_i) (\alpha_j^* - \alpha_j) K(s_p(i), s_p(j)) \end{aligned} \quad (5)$$

subject to the constraints:

$$0 \leq \alpha_i, \alpha_i^* \leq C, \quad \sum_{i=1}^{l_{sv}} \alpha_i^* \alpha_i = 0, \quad (6)$$

where the kernel function is defined as:

$$K(s_p(i), s_p(j)) = \langle \phi(s_p(i)), \phi(s_p(j)) \rangle. \quad (7)$$

Here,  $C$  serves as a regularization parameter, while  $\alpha$  and  $\alpha^*$  represent Lagrange multipliers. The parameter  $l_{sv}$  is the number of support vectors,  $s_p$  represents an individual datum, and  $\phi$  denotes the transformation from the feature space to the kernel space.

SVR allows for the use of different kernel functions such as linear, polynomial, or radial basis function (RBF) kernels. The choice of kernel depends on the nature of the problem and the characteristics of the dataset. In this study, we employ a variety of kernels, including traditional ones such as the linear and RBF, alongside the innovative quantum kernel.

#### B. Data Detection

##### 1) coherent demodulation:

The data detection with coherent demodulation, normally, is made assuming symbol-by-symbol minimum distance detection. In this case, the detector can be expressed as

$$\hat{S}_k = \arg \min_{\tilde{S}_i} J(\tilde{S}_i), \forall i \in \{0, 1, \dots, M-1\}, \quad (8)$$

where,

$$J(\tilde{S}_i) = |\tilde{S}_k - \tilde{S}_i|^2. \quad (9)$$

$\tilde{S}_k$  is the complex symbol at the output of the equalizer on the  $k$ -th subcarrier,  $\tilde{S}_i$  is the  $i$ -th complex symbol of the demodulator constellation of order  $M$ , that is, for 16-QAM modulation,  $M = 16$ , and for QPSK modulation,  $M = 4$ . Due to the need to know the reference signal  $\tilde{S}_i$ , this demodulation is called coherent demodulation [28].

2) SVC:

Support Vector Classifier (SVC) is a useful technique for data classification and is considered to be the state-of-the-art tool for linear and nonlinear classification. It realizes classification tasks for two-class problem by using the separating hyperplane [29]. The hyperplane is found by estimating the maximum distance to the closest data points of the training set. These closest data points are named support vectors (SVs). Data points can be transformed into a high dimensional space (HDS) by using a nonlinear transformation if they are not linearly separable in the input space. HDS is called feature space. These nonlinear transformations are represented by using kernel functions. The data points in the feature space are divided by the optimal separating hyperplane estimated by using the maximum distance to the closest data points of the training set mentioned as above. Although SVM is used to solve two-class learning problems, there are many ways to solve multi-class classification problems with SVM, such as: One Against One (OAO) and One Against All (OAA).

In this work we apply two multiclass SVCs to detect the 16-QAM symbols, one in the real part and the other in the imaginary part, respectively, and an analogous procedure with the binary version to detect the QPSK symbols.

#### IV. QUANTUM-BASED APPROACHES FOR CHANNEL ESTIMATION AND DATA DETECTION

##### A. Quantum Kernels

Quantum kernels represent a fundamental concept in quantum machine learning (QML), leveraging the principles of quantum computing to process and analyze data. It encapsulates the essence of classical kernels within a quantum framework, enabling the exploration of complex data structures and relationships in higher-dimensional quantum feature spaces [30].

Quantum kernels utilize quantum feature maps to implement the kernel trick. This transformation is carried out by a quantum feature map  $\phi : \mathcal{X} \rightarrow \mathcal{H}$  that maps a data point  $\mathbf{x}$  to a corresponding quantum state in a Hilbert space. The entries of the quantum kernel  $K(\mathbf{x}_i, \mathbf{x}_j)$  represent the fidelities or transition amplitudes between the states  $|\phi(\mathbf{x}_i)\rangle$  and  $|\phi(\mathbf{x}_j)\rangle$ , which correspond to the transformed feature vectors  $\mathbf{x}_i$  and  $\mathbf{x}_j$ , respectively [31]. For two quantum states  $|\phi(\mathbf{x}_i)\rangle$  and  $|\phi(\mathbf{x}_j)\rangle$ , the kernel is defined as  $K(\mathbf{x}_i, \mathbf{x}_j) = |\langle\phi(\mathbf{x}_i)|\phi(\mathbf{x}_j)\rangle|^2$ , where  $|\phi(\mathbf{x}_i)\rangle = \mathcal{U}_{\phi(\mathbf{x}_i)}|0\rangle$  and the circuit  $\mathcal{U}_{\phi(\mathbf{x}_i)}$  encodes the classical data  $\mathbf{x}_i$  into the quantum state  $|\phi(\mathbf{x}_i)\rangle$  using a unitary operator  $\mathcal{U}$ .

On a quantum computer, the kernel circuit is set up for every conceivable pair of training samples, and the probability of measuring an all-zero string in the  $Z$ -basis serves as an

estimate of the fidelity of their respective encoded quantum states. For predicting a new data point  $\mathbf{x}$ , it suffices to estimate the kernel using all the  $l_{sv}$  support vectors.

##### B. Pauli Feature Maps

In traditional ML, feature maps are essential for converting raw input data into a higher-dimensional feature space, aiding in uncovering meaningful patterns and relationships. Similarly, quantum feature maps play a key role in QML, transforming classical data into quantum states suitable for quantum computers.

Quantum feature maps operate by leveraging quantum gate operations to transform input data into a new quantum state vector [30]-[31]. Notably, the Pauli Feature Map, first introduced by V. Havlíček et al. [18], employs Pauli gate operations to efficiently encode classical data into quantum states. This map enables complex transformations by converting input data with  $n$  features  $\mathbf{x} \in \mathbb{R}^n$  into quantum information in  $n$  qubits  $|\psi(\mathbf{x})\rangle$  using a unitary operator:

$$\mathcal{U}_{\Phi(\mathbf{x})} = \prod_d \mathcal{U}_{\Phi(\mathbf{x})} H^{\otimes n}, \quad (10)$$

where

$$\mathcal{U}_{\Phi(\mathbf{x})} = \exp\left(i \sum_{S \in \mathcal{I}} \phi_S(\mathbf{x}) \prod_{k \in S} P_k\right), \quad (11)$$

$S$  is a set of qubit indices that describes the connections in the feature map,  $\mathcal{I}$  is a set containing all these index sets and  $P_k \in \{\mathbb{I}, X, Y, Z\}$  represents the Pauli matrices. The encoding function is given by

$$\phi_S : \mathbf{x} \mapsto \begin{cases} x_i & \text{if } S = \{i\} \\ (\pi - x_i)(\pi - x_j) & \text{if } S = \{i, j\}. \end{cases} \quad (12)$$

The Pauli Feature Map enables the representation of higher-order correlations between original data points, allowing for the capture of complex relationships that may not be easily discernible classically. This capability is particularly valuable in tasks such as classification, regression, and clustering, where capturing intricate data dependencies is crucial for achieving high predictive performance.

In our study, we introduce a 5-qubit QSVR algorithm applied to channel estimation in OFDM systems. This QSVR model is designed to handle the intricacies of channel estimation within OFDM systems, where the number of pilot tones, crucial for accurate estimation, corresponds to number of qubits utilized in our proposed model. In the second part of our work we use a two-qubit QSVC to detect the data replacing the coherent demodulator.

To configure our QSVR and QSVC model effectively, we carefully selected values for essential parameters, including the Pauli sequence, the number of repetitions, and the type of entanglement. These parameters serve as arguments within the PauliFeatureMap class, which is implemented in the Qiskit Python package [32]. For our specific implementation, we opted for a Pauli sequence comprising the  $Z$  and  $ZZ$  operators, with no repetition ( $d = 1$ ) and linear entanglement. This

configuration was chosen based on its compatibility with the characteristics of OFDM systems and its potential to yield accurate channel estimation and data detection results. For 2 features (2 qubits), the Pauli expansion matrix of  $ZZ$  feature map can be written as:

$$U_{\phi}(\mathbf{x}) = \exp(i(x_1 Z_1 + x_2 Z_2 + (\pi - x_1)(\pi - x_2) Z_1 Z_2)). \quad (13)$$

The first two terms are equivalent with  $R_Z$  rotation gates on each individual qubit. Specifically,  $\exp(ix_1 Z_1) = R_Z(2x_1)$  and  $\exp(ix_2 Z_2) = R_Z(2x_2)$ . Furthermore, the tensor product  $\exp(i(\pi - x_1)(\pi - x_2) Z_1 Z_2)$  is equivalent to entangled gates:  $CX \cdot (I \otimes R_Z(2(\pi - x_1)(\pi - x_2))) \cdot CX$ .

## V. RESULTS

To validate the proposed quantum kernel for the SVR and SVC, and compare its performance with the classic SVR and the LS in channel estimation, and coherent demodulation and classic SVC for symbol detection in OFDM systems, bit error rate (BER) and mean square error (MSE), i.e.  $MSE = E[|H - \hat{H}|^2]$ , curves were created, considering the following simulation parameters:

TABELA I  
SIMULATION PARAMETERS

number of subcarriers [K]	16
subcarrier modulation	QPSK 16-QAM
cyclic prefix length in number of subcarriers	4 and zero
number of pilot subcarriers [ $S_p$ ]	5

The tests were performed on a frequency selective channel with a delay profile given by  $h = [1 \ 0 \ 0.3 + 0.3j]$ .

We consider a packet-based transmission, where each packet consists of a header at the beginning of the packet with a known training sequence or preamble to carry out channel estimation, followed by the OFDM data symbols. At the preamble, there are two OFDM symbol with pilot subcarriers. After the estimation (with either QSVR, SVR or LS) of channel coefficients at pilot positions  $\hat{H}_p(k)$ , we use them to compute the interpolation of the channel. Next, we perform zero forcing (ZF) equalization [33] using the interpolated channel. Detection is carried out with a hard-decision slicer over the equalized data in the first teste and, SVM and quantum kernel SVM classifier (QSVM) in the second test. For each estimator, 100 packets were transmitted to calculate the average and raising the BER.

We studied the performance variation in the system due to changes in the kernel and free parameters of the SVR and SVC. We tested the linear, radial and polynomial kernels and varied the  $C$  parameter from 1 to 1000. The optimal parameter found for  $C$  was  $C = 100$ , and RBF kernel. We also utilized the Qiskit Python package [32] for the quantum tasks with a local quantum simulator. The classical kernel-based method for SVR and SVC was run on a classical computer with a regular CPU. Figs. 2 and 3 show, respectively, the MSE and BER performance as a function of the signal-to-noise ratio ( $E_b/N_0$ ) for the first test with 16-QAM.

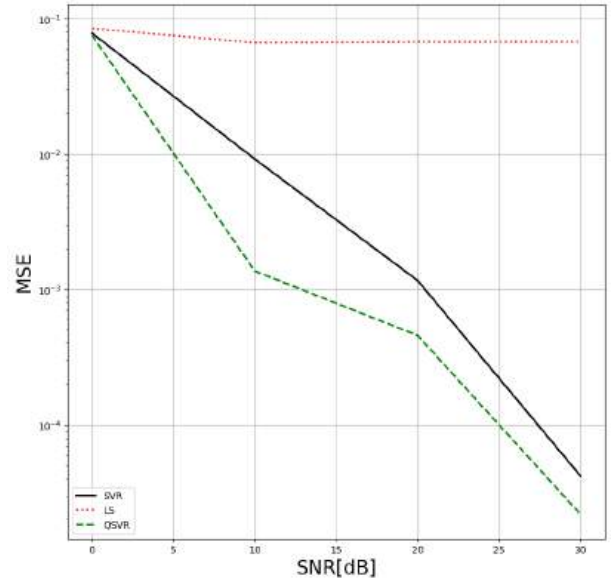


Fig. 2. MSE performance comparison.

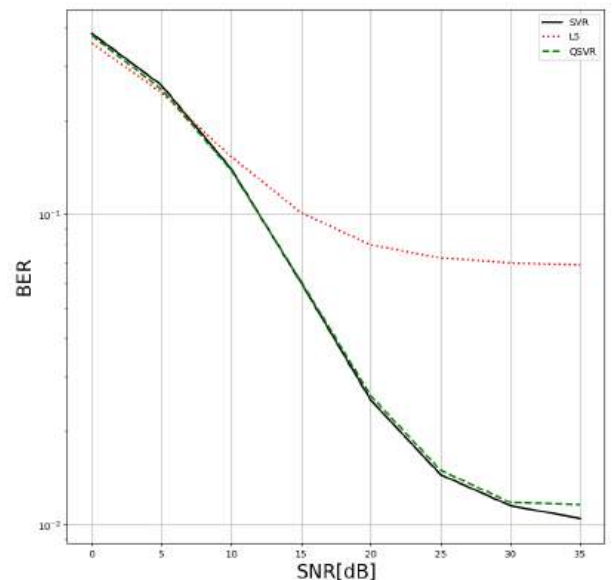


Fig. 3. BER performance comparison.

Analyzing the MSE and BER performance obtained from the three tested estimators, we observe in Fig. 2 that the MSE curve obtained with the LS estimator does not decay due to ISI caused by the lack of the cyclic prefix. The BER curve, 3, also decays very slowly up to 20 dB of SNR and presents a plateau from this value onwards, indicating its sensitivity to ISI. In contrast, the curves obtained with the SVR and QSVR estimators demonstrate robustness to ISI, with slightly better performance for QSVR in terms of MSE. This can be attributed to the better suitability of the quantum kernel for linearizing the input space data.

The plateau trend observed in the BER curves for the SVR and QSVR from 30 dB of SNR can be explained by the ISI generated by the lack of CP, impacting coherent detection



while leaving channel estimation unaffected. To mitigate ISI and enhance robustness, we explored replacing the coherent detector with an SVM and QSVM classifier. Despite observing a reduction in BER with tests using a multiclass SVM classifier the plateau trend persisted. The inability to implement a multiclass QSVM classifier led us to transition to QPSK modulation, enabling testing with a binary QSVM classifier. Figs. 4 and 5 illustrate the BER performance versus signal-to-noise ratio ( $E_b/N_0$ ) for the first QPSK test and the second test solely with the classic SVC classifier, respectively. We can see in Fig. 4 that the switch to QPSK, maintaining coherent detection, was not enough to eliminate the plateau after 30 dB of SNR. However, in Fig. 5, it is possible to observe that the SVC is robust to ISI caused by the absence of the CP, independent of the regressor type used in channel estimation (LS, SVR or QSVR).

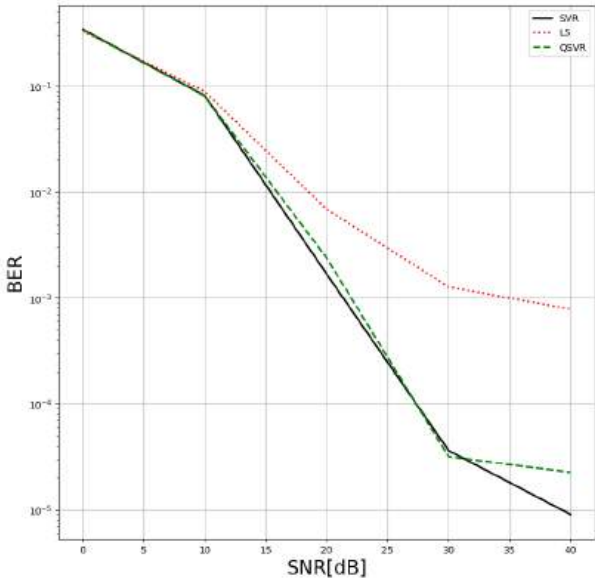


Fig. 4. BER performance comparison for the first test with QPSK modulation.

Several experiments are being carried out with the aim of adjusting the QSVC parameters, including increasing the number of steps performed during the training process ( $\tau$ ), varying the number of samples for training and testing, and varying the parameter  $C$ . The best performance obtained so far was with 10000 samples, 6000 for training and 4000 for testing,  $\tau=1000$  and  $C = 1000$ , using "ZfeatureMap" coding. However, the performance of QSVC is still slightly worse than that of classic SVC, as can be seen in Fig. 6, requiring further investigation. Additionally, the development of effective multiclass quantum classifiers is needed, as current results indicate inferior performance compared to classical multiclass SVMs.

## VI. CONCLUSIONS

In this work, an SVR and an SVC algorithms with a quantum kernel for channel estimation and data detection in OFDM systems were proposed. Therefore, the structure of the adopted OFDM system, the channel estimation process in the time domain, by the SVR, the frequency domain, by

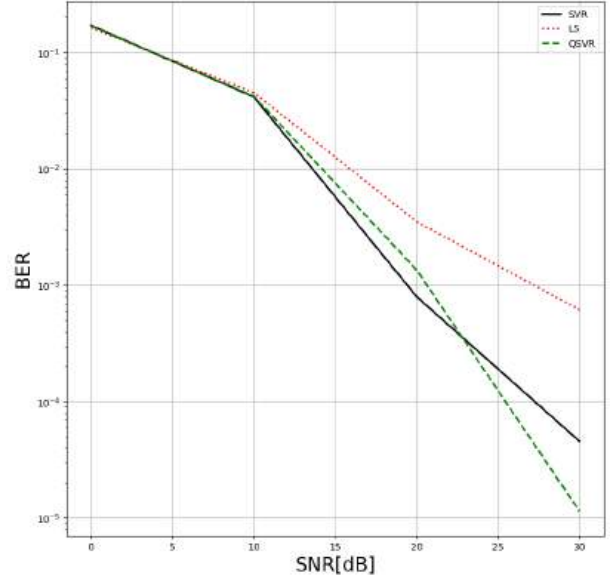


Fig. 5. BER performance comparison for the second test with QPSK modulation and SVC classifier.

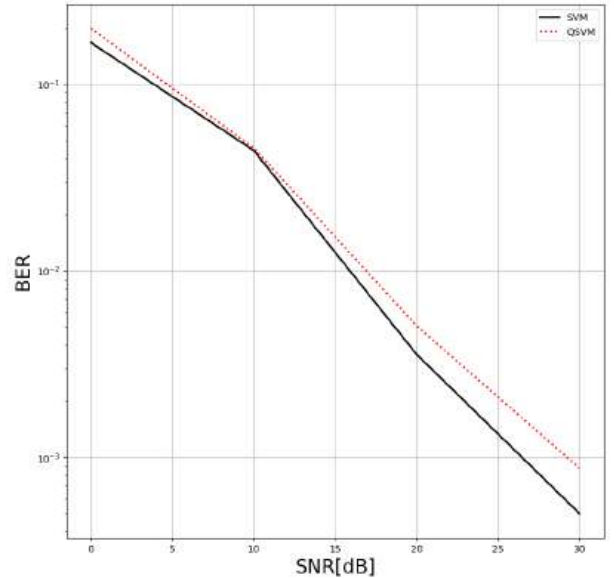


Fig. 6. BER performance comparison for the second test with QPSK modulation and QSVC classifier.

the LS, the data detection model and the SVC, in addition to the fundamentals of quantum computing for generating the quantum kernel were described. Several tests were carried out in search of the optimal parameters of the SVR, SVC and the OFDM system. The simulations confirmed the robustness of the QSVR in the presence of ISI and the results show that the proposal outperforms the classic SVR and the LS for channel estimation. Following this work, we intend to investigate the parameters and adjustments to improve the performance of multiclass QSVC in data detection in OFDM systems.

## REFERENCES

- [1] N. Marchetti, M. I. Rahman, S. Kumar, R. Prasad, *New Directions in Wireless Communications Research*. cap. 2, OFDM-Principles and Challenges, 2009.
- [2] A. F. Molisch. *Orthogonal Frequency Division Multiplexing (OFDM)*. in *Wireless Communications*, IEEE, 2011.
- [3] B. R. Ballal, A. Chadha, N. Satam. *Orthogonal Frequency Division Multiplexing and its Applications*. International Journal of Science and Research (IJSR), 2319-7064 Volume 2 Issue 1, 2013.
- [4] B. Wang, K. J. R. Liu. *Advances in cognitive radio networks: A survey*. in *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5-23, Feb. 2011.
- [5] Z. Du, X. Song, J. Cheng and N. C. Beaulieu. *A channel estimation technique for OFDM systems in dispersive time-varying channels*. 11th Canadian Workshop on Information Theory, Ottawa, ON, Canada, 2009.
- [6] D. Shrestha, X. Mestre and M. Payaró, *On channel estimation for power line communication systems in the presence of impulsive noise*, *Computers & Electrical Engineering*, Volume 72, Pages 406-419, 2018.
- [7] M. P. Sánchez-Fernández, M. de Prado-Cumplido, J. Arenas-García, and F. Pérez-Cruz, *SVM multiregression for nonlinear channel estimation in multiple-input multiple-output systems*. *IEEE Trans. Signal Process.*, vol. 52, no. 8, pp. 2298–2307, 2004.
- [8] D. Sebald and A. Buclaw, *Support vector machine techniques for nonlinear equalization*. *IEEE Trans. Signal Process.*, vol. 48, no. 11, pp.3217–3226, Nov. 2000.
- [9] L. V. Nguyen, D. H. N. Nguyen, and A. L. Swindlehurst, *SVM-based channel estimation and data detection for massive MIMO systems with one-bit ADCs*. to appear at *IEEE Int. Conf. Commun.*, 2020.
- [10] A. W. Harrow, A. Hassidim, and S. Lloyd. *Quantum algorithm for linear systems of equations*. *Physical Review Letters*, vol. 103, no. 15, oct 2009.
- [11] Schuld, M.; Petruccione, F. *Supervised learning with quantum computers*. Cham: Springer, 2018.
- [12] I. Kerenidis, J. Landman, A. Luongo, and A. Prakash. *q-means: A quantum algorithm for unsupervised machine learning*. arXiv:1812.03584, 2018.
- [13] S. Lloyd, M. Mohseni, and P. Rebentrost. *Quantum algorithms for supervised and unsupervised machine learning* arXiv:1307.0411, 2013.
- [14] J. Preskill. *Quantum computing in the NISQ era and beyond*. *Quantum*, vol. 2, p. 79, aug 2018.
- [15] P. Botsinis, S. X. Ng and L. Hanzo. *Quantum Search Algorithms, Quantum Wireless, and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design* in *IEEE Access*, vol. 1, pp. 94-122, 2013, doi: 10.1109/ACCESS.2013.2259536.
- [16] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng and L. Hanzo. *Joint Quantum-Assisted Channel Estimation and Data Detection* in *IEEE Access*, vol. 4, pp. 7658-7681, 2016, doi: 10.1109/ACCESS.2016.2591903.
- [17] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary and M. Asadzaman. *Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future* in *IEEE Access*, vol. 7, pp. 46317-46350, 2019.
- [18] V. Havlíček, A. D. Córcoles, K. Temme, Et al. *Supervised learning with quantum-enhanced feature spaces*. *Nature* 567, 209–212 (2019).
- [19] J. E. Park, B. Quanz, S. Wood, H. Higgins, and R. Harishankar. *Practical application improvement to quantum svm: theory to practice*. 2020. [Online]. Available: <https://arxiv.org/abs/2012.07725>
- [20] A. Viladomat Jasso, A. Modi, R. Ferrara, C. Deppe, J. Nötzel, F. Fung, M. Schädler. *Quantum and quantum-inspired stereographic k nearest-neighbour clustering*. *Entropy*, vol. 25, no. 9, 2023.
- [21] M. Schuld and N. Killoran. *Is quantum advantage the right goal for quantum machine learning?* *PRX Quantum*, vol. 3, p. 030101, Jul 2022.
- [22] M. J. Fernández-Getino García, J. M. Páez-Borrillo, and S. Zazo, *DFT-based channel estimation in 2D-pilot-symbol-aided OFDM wireless systems*. In: *Proc IEEE Vehicular Technology Conf.*, 2001, vol. 2, pp. 815–819.
- [23] A. Papoulis. *Probability Random Variables and Stochastic Processes*. McGraw-Hill, NY, 3 edition, 1991.
- [24] H. Drucker, C. J. C. Burges, L. Kaufman, A. Smola, and V. Vapnik. *Support vector regression machines*. In: *Advances in Neural Information Processing Systems*, M. Mozer, M. Jordan, and T. Petsche, Eds., vol. 9. MIT Press, 1996.
- [25] Smola, A.J., Schölkopf, B. *A tutorial on support vector regression*. *Statistics and Computing* 14, 199–222 (2004).
- [26] V. Vapnik. *The Support Vector Method of Function Estimation*. Boston, MA: Springer US, 1998, pp. 55–85.
- [27] R. Khanna and M. Awad. *Efficient Learning Machines: Theories, Concepts, and Applications for Engineers and System Designers*. Apress, 04 2015.
- [28] Ali Grami. *Introduction to Digital Communications* Academic Press, Elsevier, 2016.
- [29] Yao, Y., Frasconi, P., Pontil, M. *Fingerprint classification with combinations of support vector machines*. In *AVBPA 2001, LNCS 2091* (pp. 253-258).
- [30] M. Schuld. *Supervised quantum machine learning models are kernel methods* in arXiv preprint arXiv:2101.11020, 2021.
- [31] M. Schuld, N. Killoran. *Quantum machine learning in feature hilbert spaces* in *Physical review letters*, vol. 122, 2019.
- [32] A. Asfaw, L. Bello, Y. Ben-Haim, Et al. *Qiskit: An Open-Source Framework for Quantum Computing*. ArXiv, 2020.
- [33] U. Katare, P. Patidar e A.C. Tiwari, *Comparative Analysis of ZF and MMSE Receiver for Multicode MC-CDMA Downlink Channels*. *International Journal of Engineering Science and Innovative Technology (IJESIT)* Volume 3, Issue 4, Julho 2014.

# Recorrência de Cadeias de Markov Quânticas

Newton Loebens

**Resumo**— Este trabalho aborda os passeios aleatórios induzidos por cadeias de Markov quânticas. Estudamos sua recorrência, mostrando que um vértice recorrente em relação a alguma densidade qual-quer garante a recorrência para certas densidades. Como consequência, verificamos que a transiência de um vértice em relação a alguma densidade fiel garante a transiência completa do vértice. Nos casos mais gerais, a obtenção de critérios de recorrência associados às transições iniciais são muito difíceis, assim, com o intuito de nos aproximarmos de algum critério de recorrência, tratamos do caso homogêneo e obtemos uma tricotomia associada aos subespaços invariantes do conjunto de densidades.

**Palavras-Chave**— Cadeias de Markov quânticas; passeios aleatórios; recorrência; densidade fiel.

**Abstract**— This work addresses random walks induced by quantum Markov chains. We study their recurrence, showing that a recurrent vertex with respect to some density guarantees recurrence for certain densities. As a consequence, we verify that the transience of a vertex with respect to some faithful density guarantees the complete transience of the vertex. In more general cases, obtaining recurrence criteria associated with initial transitions is very difficult, so, in order to get closer to some recurrence criterion, we deal with the homogeneous case and obtain a trichotomy associated with the invariant subspaces of the set of densities.

**Keywords**— Quantum Markov Chains; random walks; recurrence; faithful density.

## I. INTRODUÇÃO

Os passeios aleatórios (PAs) induzidos por cadeias de Markov desempenham uma importante área de estudo nos processos estocásticos [10], fornecendo distintas dinâmicas para compreender uma ampla gama de fenômenos naturais [13] e artificiais [1].

Newton Loebens, Universidade Federal do Pampa (Unipampa), Itaquí - RS, email: newtonloebens@gmail.com. Este trabalho foi parcialmente financiado pela Unipampa.

Os PAs clássicos abrem caminho para uma exploração ainda mais profunda através de sistemas quânticos, como os PAs quânticos unitários [12] e os abertos em suas versões a tempo discreto (OQWs) [2] e tempo contínuo [11]. Entre estas variantes, os PAs induzidos por cadeias de Markov quânticas (CMQs) permitem uma abordagem mais profunda que os OQWs, sendo uma generalização (veja [3, Seção 8]). Isto permite mais variações na definição inicial de transição e, conseqüentemente, aplicações mais abrangentes.

A recorrência é um conceito fundamental na análise de PAs, indicando o número médio de vezes que um sistema retorna a seu estado inicial após um número finito de passos. Esta propriedade é objeto de estudo nas diversas formas de PAs daqueles citados acima [4, 7, 8, 10]. A compreensão da recorrência não apenas fornece ideias sobre a dinâmica do sistema, mas também tem implicações profundas na teoria da informação quântica, onde a preservação da informação desempenha um papel central.

Os PAs induzidos por CMQs representam uma generalização significativa dos seus homólogos clássicos. Enquanto as cadeias clássicas evoluem de acordo com probabilidades fixas de transição, as quânticas incorporam elementos de memória através da densidade, refletindo a natureza probabilística inerente à mecânica quântica, conferindo uma maior riqueza exploratória desses PAs.

Sendo assim, discutimos a recorrência desses PAs através das propriedades da densidade inicial e dos espaços vetoriais onde elas estão contidas.

## II. BASE TEÓRICA

Consideramos um conjunto finito ou infinito enumerável de vértices  $V$  e um espaço de Hilbert separável da forma

$$\mathcal{H} = \bigoplus_{i \in V} \mathfrak{h}_i. \quad (1)$$

Um PA quântico aberto induzido por uma CMQ é definido por um mapa  $\Phi : \mathcal{I}_1(\mathcal{H}) \rightarrow \mathcal{I}_1(\mathcal{H})$  tal que se um operador  $\rho = \sum_{i,j \in V} \rho(i,j) \otimes |i\rangle\langle j|$  pertence a  $\mathcal{I}_1(\mathcal{H})$ , então

$$\Phi(\rho) = \sum_{i \in V} \left( \sum_{j \in V} \Phi_{ij}(\rho(j,j)) \right) \otimes |i\rangle\langle i|, \quad (2)$$

onde cada  $\Phi_{ij} : \mathcal{I}_1(\mathfrak{h}_j) \rightarrow \mathcal{I}_1(\mathfrak{h}_i)$  é um operador completamente positivo satisfazendo

$$\sum_{i \in V} \Phi_{i,j}^*(I_{\mathfrak{h}_i}) = I_{\mathfrak{h}_j} \quad \forall j \in V. \quad (3)$$

Chamaremos tal PA de QMC<sup>1</sup>, também denotado por  $\Phi$  em referência ao mapa original, gerando a matriz de operação de transição [5].

Iniciando o QMC em um estado  $\rho = \sum_{i \in V} \rho(i) \otimes |i\rangle\langle i|$ , podemos definir os processos estocásticos “sem medição”

$$\left( \tilde{Q}_n, \frac{\Phi^n(\rho, \tilde{Q}_n)}{\text{Tr} \Phi^n(\rho, \tilde{Q}_n)} \right)_{n \in \mathbb{N}}, \quad (4)$$

onde reescrevemos

$$\Phi^n(\rho) = \sum_{i \in V} \Phi^n(\rho, i) \otimes |i\rangle\langle i|. \quad (5)$$

Assim, o processo “sem medição” é determinado pela variável  $\tilde{Q}_n$ , cuja lei de probabilidade é

$$\mathbb{P}(\tilde{Q}_n = i) = \text{Tr} \Phi^n(\rho, i), \quad (6)$$

e o processo “com medição”  $(\tilde{X}_n, \tilde{\rho}_n)_{n \in \mathbb{N}}$  por

$$(\tilde{X}_0, \tilde{\rho}_0) = (j, \rho(j)) \text{ com probabilidade } \text{Tr} \rho(j). \quad (7)$$

Em suma, temos  $Z_n := \{(\tilde{X}_{n+1}, \tilde{\rho}_{n+1})\}$  e  $\text{Tr} \Phi_{i,j}$  tem valor

$$\mathbb{P}\left(Z_{n+1} = \left(i, \frac{\Phi_{i,j}(\tilde{\rho}_n)}{\text{Tr} \Phi_{i,j}(\tilde{\rho}_n)}\right) \mid Z_n = (j, \tilde{\rho}_n)\right) \quad (8)$$

para todo  $i \in V$ . Se  $\dim(\mathfrak{h}_i) < \infty \quad \forall i \in V$ , então o QMC é dito semifinito.

O conjunto de densidades agindo em um espaço de Hilbert  $\mathcal{K}$  será denotado por

$$\mathcal{S}(\mathcal{K}) := \{\rho \in \mathcal{I}_1(\mathcal{K}), \rho \geq 0, \text{Tr}(\rho) = 1\}, \quad (9)$$

<sup>1</sup>QMC é a sigla para Quantum Markov Chain, logo, é a mais empregada no meio científico. Ainda, note que QMC está sendo chamado de PA induzido por uma CMQ.

enquanto que o conjunto de densidades diagonais em blocos de  $\mathcal{H}$  por

$$\mathcal{D} := \left\{ \rho \in \mathcal{S}(\mathcal{H}) : \rho = \sum_{i \in V} \rho(i) \otimes |i\rangle\langle i| \right\}. \quad (10)$$

Desta forma, se  $\rho \in \mathcal{D}$ , então  $\rho(i) \in \mathcal{D}$ ,  $\rho(i) \geq 0$  (positivo semidefinido) e  $\sum_{i \in V} \text{Tr}(\rho(i)) = 1$ . Um operador densidade positivo definido também é chamado de densidade **fiel**.

Suponha que  $\rho \otimes |i\rangle\langle i|$  seja uma densidade inicial concentrada em  $|i\rangle$ . Podemos descrever  $n$  iterações do QMC assim: definindo  $\rho^{(0)} = \rho \otimes |i\rangle\langle i|$ , com  $\text{Tr}(\rho) = 1$ , escrevemos

$$\Phi^n(\rho \otimes |i\rangle\langle i|) = \sum_{k \geq 0} \rho_k^{(n)} \otimes |k\rangle\langle k|. \quad (11)$$

A probabilidade da partícula estar no vértice  $|j\rangle$  no  $n$ -ésimo salto, dado que começamos no vértice  $|i\rangle$  com a densidade inicial  $\rho$  concentrada em  $|i\rangle$ , é dada por:

$$p_{ji;\rho}(n) = p_n(\rho \otimes |i\rangle \rightarrow |j\rangle) := \text{Tr} \left( \rho_j^{(n)} \right). \quad (12)$$

Assim, considere um QMC semifinito em algum conjunto de vértices  $V$ , seja  $i \in V$  e  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ . Dizemos que um vértice  $|i\rangle$  é **recorrente** em relação a  $\rho$  (ou  $\rho$ -recorrente) se

$$\sum_{n=0}^{\infty} p_{ii;\rho}(n) = \infty. \quad (13)$$

Caso contrário,  $|i\rangle$  é dito **transiente** em relação a  $\rho$  (ou  $\rho$ -transiente). Se  $|i\rangle$  é  $\rho$ -recorrente para todo  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ , então  $|i\rangle$  é dito simplesmente recorrente. Por fim, se  $|i\rangle$  é  $\rho$ -transiente para todo  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ , então  $|i\rangle$  é dito transiente.

Um QMC é dito: **recorrente** se todo vértice for recorrente; **transiente** se todo vértice for transiente.

Continuando as definições, um QMC com conjunto de vértices  $V = \mathbb{Z}$  é chamado de **homogêneo** se  $\Phi_{ij}(\cdot) = \Phi_{i+k,j+k}(\cdot)$  para todo  $i, j, k \in \mathbb{Z}$ . Em particular, se o QMC é homogêneo e existem operadores  $\Phi_L, \Phi_R$  tais que

$$\begin{aligned} \Phi_{i+1,i}(\cdot) &= \Phi_L(\cdot), & \Phi_{i-1,i}(\cdot) &= \Phi_R(\cdot) \quad \forall i \in V, \\ \Phi_{i,j}(\cdot) &= 0 \quad \text{para } |j-i| \neq 1, \end{aligned} \quad (14)$$

dizemos que o QMC é **induzido por uma moeda**  $(\Phi_L, \Phi_R)$ . Neste caso, podemos simplificar  $\mathfrak{h}_i = \mathfrak{h}$  para todo  $i \in \mathbb{Z}$ . Se  $\dim(\mathfrak{h}) = d$ , então  $\Phi_L$  e  $\Phi_R$  podem ser representados por matrizes quadradas de ordem  $d$  e dizemos que  $(\Phi_L, \Phi_R)$  é uma moeda de dimensão  $d$ .

### III. QUANTUM MARKOV CHAINS

Começaremos esta seção exibindo uma propriedade que fornece uma descrição da  $\rho$ -recorrência em um vértice  $|i\rangle \in V$  quando assumimos que  $|i\rangle$  é recorrente para alguma densidade fiel e  $\mathfrak{h}_i$  tem um grau de liberdade interno finito. Com isto, obtemos também uma consequência imediata que será dada para o caso em que  $|i\rangle$  é  $\sigma$ -transiente para alguma densidade não fiel.

**Proposição III.1.** *Considere um QMC  $\Phi$  semifinito em algum conjunto de vértices  $V$  e seja  $|i\rangle \in V$ . Se  $|i\rangle$  é  $\tau$ -recorrente para algum  $\tau \in \mathcal{S}(\mathfrak{h}_i)$ , então*

- 1) *o vértice  $|i\rangle$  é  $\rho$ -recorrente para todas as densidades fiéis  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ ;*
- 2) *existe alguma densidade não-fiel  $\tilde{\rho}$  tal que  $|i\rangle$  é  $\tilde{\rho}$ -recorrente;*
- 3) *existe alguma densidade pura  $|w\rangle\langle w|$  tal que  $\Phi$  é  $|w\rangle\langle w|$ -recorrente, onde  $|w\rangle$  é um vetor unitário de  $\mathfrak{h}_i$ .*

*Demonstração:* 1) *Seja  $\rho$  fiel. Pela compatibilidade de  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ , existe  $c > 0$  tal que  $\rho > c\tau$ , assim*

$$\begin{aligned} \sum_{n=0}^{\infty} p_{ii;\rho}(n) &= \sum_{n=0}^{\infty} \text{Tr}(\Phi_{ii}^{(n)}(\rho)) > \sum_{n=0}^{\infty} \text{Tr}(\Phi_{ii}^{(n)}(c\tau)) \\ &= c \sum_{n=0}^{\infty} \text{Tr}(\Phi_{ii}^{(n)}(\tau)) = c \sum_{n=0}^{\infty} p_{ii;\tau}(n) \\ &= \infty. \end{aligned} \quad (15)$$

2) *Seja  $\rho \in \mathcal{S}(\mathfrak{h}_i)$  não-fiel. Pelo Teorema Espectral [9, Teorema 2.1],  $\rho$  pode ser escrito como*

$$\rho = \sum_{x=1}^n \lambda_x |x\rangle\langle x|, \quad (16)$$

onde os vetores  $|x\rangle$  são os autovetores de  $\rho$  com autovalores  $\lambda_x$ . Como  $\rho$  é não-fiel, possui pelo menos um autovalor nulo e os demais autovalores

são não-negativos somando 1. Assim, (16) pode ser reescrito como

$$\rho = \sum_{x \in S} \lambda_x |x\rangle\langle x|, \quad S \subsetneq \{1, \dots, n\}. \quad (17)$$

Tome uma sequência de números positivos  $(\alpha_r)_{r \in T}$ , onde  $T := \{1, \dots, n\} \setminus S \neq \emptyset$ , cuja soma em  $r \in T$  é 1.

Definindo

$$\begin{aligned} \rho_X &= \sum_{x \in S} \frac{\lambda_x}{2} |x\rangle\langle x| + \sum_{x \in R} \frac{\alpha_x}{2} |x\rangle\langle x| \\ &= \sum_{x=1}^n \frac{\tilde{\alpha}_x}{2} |x\rangle\langle x|, \end{aligned} \quad (18)$$

onde

$$\tilde{\alpha}_x = \begin{cases} \lambda_x, & \text{se } x \in S \\ \alpha_x, & \text{se } x \in T \end{cases}, \quad (19)$$

obtemos pelo primeiro item que  $|i\rangle$  é  $\rho_X$ -recorrente, já que  $\rho_X$  é fiel.

Agora, defina

$$\rho_Y = \sum_{x \in R} \alpha_x |x\rangle\langle x|, \quad (20)$$

que é uma densidade não-fiel, assim temos que  $2\rho_X = \rho + \rho_Y$ . Logo, se  $\omega_n^{(\tau)} = p_{ii;\tau}(n)$ ,

$$\begin{aligned} \sum_{n=0}^{\infty} \omega_n^{(\rho)} + \sum_{n=0}^{\infty} \omega_n^{(\rho_Y)} &= \sum_{n=0}^{\infty} (\omega_n^{(\rho)} + \omega_n^{(\rho_Y)}) \\ &= 2 \sum_{n=0}^{\infty} \omega_n^{(\rho_X)}. \end{aligned} \quad (21)$$

A série do lado direito diverge, pois  $|i\rangle$  é  $\rho_X$ -recorrente, o que implica que pelo menos uma das séries do lado esquerdo diverge. Portanto,  $|i\rangle$  é  $\rho$ -recorrente ou  $\rho_Y$ -recorrente, ambas sendo não-fiéis.

3) *Seja  $\tilde{\rho}$  uma densidade não-fiel obtida pelo item 2). Pelo Teorema Espectral,  $\tilde{\rho} = \sum_j \lambda_j |e_j\rangle\langle e_j|$ , onde cada  $\lambda_j$  é um autovalor de  $\tilde{\rho}$  com autovetor correspondente  $|e_j\rangle$ .*

Temos  $\lambda_j \geq 0$ . Se  $\tilde{\rho}$  tem apenas um autovetor, então a demonstração está finalizada. Se  $\tilde{\rho}$  tem

pelos menos dois autovetores, então

$$\begin{aligned} \infty &= \sum_{n=0}^{\infty} \text{Tr} \left( \Phi_{ii}^{(n)}(\rho) \right) \\ &= \sum_j \left( \lambda_j \sum_{n=0}^{\infty} \text{Tr} \left( \Phi_{ii}^{(n)}(|e_j\rangle \langle e_j|) \right) \right), \end{aligned} \quad (22)$$

onde pelo menos um dos termos da soma deve ser infinito. Isto completa a prova.

**Corolário III.2.** *Seja  $\Phi$  um QMC semifinito e  $|i\rangle \in V$ . Se  $|i\rangle$  é  $\tau$ -transiente para algum  $\tau \in \mathcal{S}(\mathfrak{h}_i)$  fiel, então  $|i\rangle$  é transiente.*

Outra consequência direta da Proposição III.1 está relacionada ao caso homogêneo:

**Corolário III.3.** *Seja  $\Phi$  um QMC homogêneo em  $\mathbb{Z}$  com  $\dim(\mathfrak{h}) = d < \infty$ . Se  $\Phi$  é  $\tau$ -recorrente para algum  $\tau \in \mathcal{S}(\mathfrak{h})$ , então*

- 1)  $\Phi$  é  $\rho$ -recorrente para todas as densidades fiéis;
- 2) existe uma densidade não-fiel  $\tilde{\rho}$  tal que  $\Phi$  é  $\tilde{\rho}$ -recorrente;
- 3) existe uma densidade pura  $|w\rangle \langle w|$  tal que  $\Phi$  é  $|w\rangle \langle w|$ -recorrente, onde  $|w\rangle$  é um vetor unitário de  $\mathfrak{h}$ .

**Exemplo III.4.** *Vamos considerar um QMC cujos operadores de transição são  $\Phi_{11}(\cdot) = A_1(\cdot)A_1^*$ ,  $\Phi_{12}(\cdot) = A_2(\cdot)A_2^* + A_3(\cdot)A_3^*$ ,  $\Phi_{21}(\cdot) = B_1(\cdot)B_1^*$  e  $\Phi_{22}(\cdot) = B_2(\cdot)B_2^*$ , onde*

$$\begin{aligned} A_1 &= \frac{1}{\sqrt{8}} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad A_2 = B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \\ A_3 &= \frac{1}{\sqrt{8}} \begin{bmatrix} 0 & 1 \\ 0 & \sqrt{6} \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned} \quad (23)$$

O grafo correspondente está representado na Figura 1.

Dada a densidade

$$\rho = \frac{1}{5} \begin{bmatrix} 1 & i \\ -i & 4 \end{bmatrix}, \quad (24)$$

obtemos<sup>2</sup>

$$p_{11;\rho}(n) = \frac{1}{5} + \frac{(-1)^n}{10}, \quad n = 1, 2, 3, \dots \quad (25)$$

<sup>2</sup>Os cálculos foram realizados através do Software Maple 15. Primeiramente tomamos a representação matricial do QMC  $\Phi$  como construído em [6] e os valores de  $\Phi^n$  foram obtidos através da forma canônica de Jordan.

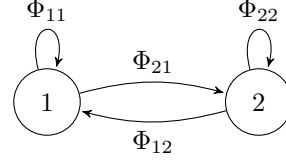


Fig. 1

GRAFO DE UM PA QUÂNTICO DE DOIS VÉRTICES INDUZIDO POR UM QMC.

Note que a densidade em (24) é fiel e que o QMC é  $\rho$ -recorrente, já que

$$\sum_{n=0}^{\infty} p_{11;\rho}(n) = \infty. \quad (26)$$

Pelos itens 1) e 2) da Proposição III.1, o QMC é  $\sigma$ -recorrente para todas densidades fiéis de  $\mathbb{C}^2$  e  $\tau$ -recorrente para alguma densidade não-fiel de  $\mathbb{C}^2$ , respectivamente.

A homogeneidade dos QMCs em  $\mathbb{Z}$  induzida por uma moeda permite a divisão de  $\mathcal{S}(\mathfrak{h})$  em dois subconjuntos  $\mathcal{S}(\mathcal{Y})$  e  $\mathcal{S}(\mathcal{X})$  de tal forma que o PA seja transiente para  $\mathcal{S}(\mathcal{Y})$  e recorrente para  $\mathcal{S}(\mathcal{X})$ , onde  $\mathcal{Y}$  é um subespaço invariante comum dos componentes da moeda. Este fato será explicitado pela tricotomia a seguir.

**Teorema III.5.** *Considere um QMC induzido por uma moeda  $(\Phi_L, \Phi_R)$  de dimensão  $d$ . Então uma (e apenas uma) das seguintes situações ocorre:*

- $(\Phi_L, \Phi_R)$  é recorrente;
- $(\Phi_L, \Phi_R)$  é transiente;
- $(\Phi_L, \Phi_R)$  é recorrente em relação a todas as densidades, exceto por um conjunto convexo  $\mathcal{S}(\mathcal{Y})$ . Neste caso,  $\mathcal{Y}$  é um subespaço invariante para ambos  $\Phi_L, \Phi_R$  e

$$\mathfrak{h} = \mathcal{Y} \oplus \mathcal{X}, \quad \mathcal{Y}, \mathcal{X} \neq \{0\} \quad (27)$$

para algum subespaço  $\mathcal{X}$  de  $\mathfrak{h}$ .

*Demonstração:* Vamos supor que  $(\Phi_L, \Phi_R)$  não é nem recorrente nem transiente. Pela Proposição III.1, existem vetores unitários  $|u\rangle, |v\rangle \in \mathfrak{h}$  tais que o PA é  $|u\rangle \langle u|$ -recorrente e  $|v\rangle \langle v|$ -transiente. Seja  $\mathcal{Y}$  o subconjunto de  $\mathfrak{h}$  tal que  $\mathcal{S}(\mathcal{Y})$  é o conjunto de densidades de  $\mathcal{B}(\mathfrak{h})$  em que

$(\Phi_L, \Phi_R)$  é transiente. Escolhendo  $\rho \in \mathcal{S}(\mathcal{Y})$ , podemos afirmar pela Equação (8) que  $\rho_n \in \mathcal{S}(\mathcal{Y})$ , onde  $(X_n, \rho_n)_n$  são as trajetórias quânticas do QMC. De fato, se tivéssemos  $\rho_n \in \mathcal{S}(\mathfrak{h}) \setminus \mathcal{S}(\mathcal{Y})$  para algum  $n$ , então poderíamos recomeçar o PA e o vértice  $|X_n\rangle$  seria  $\rho_n$ -recorrente, contradizendo a hipótese de homogeneidade, assim devemos ter que  $\mathcal{Y}$  é um subespaço invariante comum de  $\Phi_L$  e  $\Phi_R$ .

#### IV. CONCLUSÕES

Estabelecendo a  $\rho$ -recorrência para uma densidade arbitrária num QMC, inferimos a  $\sigma$ -recorrência para qualquer densidade fiel  $\sigma$  e a  $\tau$ -recorrência para certa densidade não-fiel, incluindo densidades puras. Esta caracterização foi alcançada por meio de uma decomposição adequada da densidade, onde empregamos a notação de Dirac para facilitar a análise e tratamos da positividade do operador. Além disso, ampliamos nossos resultados para QMCs infinitos homogêneos, fortalecendo a aplicabilidade desses resultados, avançando também na obtenção de um teorema de tricotomia para recorrência, baseado nas propriedades de subespaços invariantes, fortalecendo nosso entendimento teórico e oferecendo um ponto de partida sólido para investigações futuras em diversos contextos da física quântica e da teoria da informação.

#### AGRADECIMENTOS

O autor agradece seu antigo orientador Carlos F. Lardizabal. Este trabalho foi financiado pela Universidade Federal do Pampa (Unipampa).

#### REFERÊNCIAS

- [1] L. Alkema, A. E. Raftery, P. Gerland, S. J. Clark, F. Pelletier, T. Buettner e G. Heilig. “Probabilistic projections of the total fertility rate for all countries”. Em: **Demography** 48.3 (2011), pp. 815–839.
- [2] S. Attal, F. Petruccione, C. Sabot e I. Sinayskiy. “Open quantum random walks”. Em: **Journal of Statistical Physics** 147.4 (2012), pp. 832–852.
- [3] R. Carbone e Y. Pautrat. “Open quantum random walks: reducibility, period, ergodic properties”. Em: **Annales Henri Poincaré**. Vol. 17. Springer. 2016, pp. 99–135.
- [4] F. A. Grünbaum, L. Velázquez, A. H. Werner e R. F. Werner. “Recurrence for discrete time unitary evolutions”. Em: **Communications in Mathematical Physics** 320.2 (2013), pp. 543–569.
- [5] S. Gudder. “Quantum Markov chains”. Em: **Journal of Mathematical Physics** 49.7 (jul. de 2008), p. 072105. ISSN: 0022-2488. DOI: 10.1063/1.2953952.
- [6] M. D. de la Iglesia, C. F. Lardizabal e N. Loebens. “Quantum Markov chains on the line: matrix orthogonal polynomials, spectral measures and their statistics”. Em: **Quantum Information Processing** 22.1 (2023), p. 60.
- [7] T. S. Jacq e C. F. Lardizabal. “Homogeneous open quantum walks on the line: criteria for site recurrence and absorption”. Em: **Quantum information and computation** 21.1&2 (2021), pp. 37–58.
- [8] N. Loebens. “Site Recurrence for continuous-time open quantum walks on the line”. Em: **Quantum information and computation** 23.7&8 (2023), pp. 577–602.
- [9] M. A. Nielsen e I. L. Chuang. **Quantum computation and quantum information**. Cambridge university press, 2010.
- [10] J. R. Norris. **Markov chains**. 2. Cambridge university press, 1998.
- [11] C. Pellegrini. “Continuous time open quantum random walks and non-Markovian Lindblad master equations”. Em: **Journal of Statistical Physics** 154.3 (2014), pp. 838–865.
- [12] R. Portugal. **Quantum walks and search algorithms**. Vol. 19. Springer, 2013.
- [13] J. da Silva Jale, S. F. A. X. Júnior, É. F. M. Xavier, T. Stošić, B. Stošić e T. A. E. Ferreira. “Application of Markov chain on daily rainfall data in Paraíba-Brazil from 1995-2015”. Em: **Acta Scientiarum. Technology** 41 (2019), e37186.

# Exponential Decay for Continuous-time Open Quantum Walks

Newton Loebens

*Abstract*—We study the exponential decay parameter for finite continuous-time open quantum walks. This statistic is defined by a therm obtained by a composed function that associates the natural logarithmic to the transition probability of the walk. Since we are dealing with a statistic value, it is expected to be a real number, which we show that happens and is intimate connected to the spectrum of the Lindblad generator describing the dynamics. Some properties regarding these values are shown and interesting examples are presented to describe distinct graphs.

**Keywords.** Exponential decay; continuous-time open quantum walk; probability.

## I. INTRODUCTION

A key area of research in quantum information theory is the study of quantum variations of classical random walks [8, 10]. The so-called quantum walks ([13]) can be defined in a variety of ways. They show natural examples of both a) closed quantum dynamics [12], which is described by unitary operators, and b) open (dissipative) quantum dynamics [7], which are, for example, given by positive or completely positive operators acting on a trace-class vector space [2, 5]. In both scenarios, we start with a fundamental structure that includes a graph with a finite number of vertices on which a particle is positioned and transition operators that specify how a particle might jump from one vertex to another. The classical settings of "Markov chains" are a natural source of inspiration for the probabilistic and statistical notions connected with quantum walks, even though the corresponding quantum formulations are not always obtained immediately (if they exist at all), and quite frequently the search for useful notions leads us to several possibilities. Regarding the

Newton Loebens, Universidade Federal do Pampa (Unipampa), Itaquí - RS, email: newtonloebens@gmail.com. Este trabalho foi parcialmente financiado pela Unipampa.

dynamics of continuous-time open quantum walks (CTOQWs), we show how the probabilities generate a decay when we associate the logarithmic function to it in order to obtain an exponential decay. The classical version is well understood even for the infinite case [1], however we bring the first results in this direction for finite CTOQWs.

## II. BASIC SETTINGS

To define a CTOQW, we take an operator semigroup  $\mathcal{T}$  on a Hilbert space  $\mathcal{H}$ , which is a family of bounded linear operators  $T_t$ ,  $t \geq 0$ , acting on  $\mathcal{H}$  such that

$$T_t T_s = T_{t+s}, \forall s, t \in \mathbb{R}^+ \text{ and } T_0 = I_{\mathcal{H}}. \quad (1)$$

If  $t \mapsto T_t$  is continuous for the operator norm of  $\mathcal{H}$ , we call  $\mathcal{T}$  an **uniformly continuous semigroup**, which is equivalent to have (see [6], page 161) a bounded linear operator  $L$  on  $\mathcal{H}$  such that  $T_t = e^{tL}$ ,  $\forall t \geq 0$ . When this is the case,

$$L = \lim_{t \rightarrow \infty} \frac{1}{t} (T_t - I_{\mathcal{H}}), \quad (2)$$

and the operator  $L$  is called the **generator** of  $\mathcal{T}$ .

A semigroup  $\mathcal{T} := (\mathcal{T}_t)_{t \geq 0}$  of completely positive (CP) trace-preserving (TP) maps acting on the set of trace-class operators on  $\mathcal{H}$ , denoted  $\mathcal{I}_1(\mathcal{H})$ , is called a **Quantum Markov Semigroup** (QMS) on  $\mathcal{I}_1(\mathcal{H})$ . When  $\lim_{t \rightarrow 0} \|\mathcal{T}_t - I\| = 0$ , then  $\mathcal{T}$  has a special generator  $\mathcal{L} = \lim_{t \rightarrow \infty} (\mathcal{T}_t - I)/t$  (see [9]), also known as **Lindblad operator**.

We consider a finite set of vertices  $V$  and then take the composite system

$$\mathcal{H} = \bigoplus_{i \in V} \mathfrak{h}_i, \quad (3)$$

where each  $\mathfrak{h}_i$  represents a separable Hilbert space. The label  $i \in V$  is interpreted as being the position of the walker and, when the walker is located at the vertex  $|i\rangle$ , its internal state is



encoded in the space  $\mathfrak{h}_i$  describing the internal degrees of freedom of the particle when it is sitting at site  $i \in V$ .

**Definition II.1** ([3, 11]). *Let  $V$  be a finite or countable infinite set and  $\mathcal{H}$  be a Hilbert space of the form (3). A **Continuous-Time Open Quantum Walk (CTOQW)** in  $V$  is an uniformly continuous QMS on  $\mathcal{L}_1(\mathcal{H})$  whose Lindblad operator is of the form*

$$\rho \mapsto -i[H, \rho] + \sum_{i,j \in V} \left( S_i^j \rho S_i^{j*} - \frac{1}{2} \{S_i^{j*} S_i^j, \rho\} \right). \quad (4)$$

We can put  $S_i^j = R_i^j \otimes |j\rangle \langle i|$ ,  $H = \sum_{i \in V} H_i \otimes |i\rangle \langle i|$ , where  $R_i^j \in \mathcal{B}(\mathfrak{h}_i, \mathfrak{h}_j)$  and  $H_i$  denote bounded operators,  $H_i$  is self-adjoint on  $\mathfrak{h}_i$ , and  $\sum_{i,j \in V} S_i^{j*} S_i^j$  converges in the strong sense.

Starting a CTOQW on vertex  $|i\rangle$  with initial density operator  $\rho \in \mathcal{S}(\mathfrak{h}_i) = \sum_{i \in V} \rho(i) \otimes |i\rangle \langle i|$ , the quantum measurement of the “position” gives rise to a probability distribution  $p_0$  on  $V$ , such that  $p_0(i) = \text{Tr}(\rho(i))$  is the probability of the quantum particle being located in site  $|i\rangle$ , and for evolution on time  $t \geq 0$ ,  $p_t(i) = \text{Tr}(\rho_t(i))$  is the probability for the quantum particle, at time  $t$  be located in site  $|i\rangle$ , where

$$e^{t\mathcal{L}}(\rho) = \sum_{i \in V} \rho_t(i) \otimes |i\rangle \langle i|. \quad (5)$$

Unlike the classical random walks, a CTOQW describes the behavior of a walk that retains some amount of memory, and this memory is encoded by a quantum state, which is a density operator acting on the associated Hilbert space.

Fixed a CTOQW on  $V$ ,  $i, j \in V$ ,  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ , the probability of being at site  $j$  at time  $t$ , given that the CTOQW started at vertex  $i$ , with initial density  $\rho$  concentrated at  $i$ , is denoted by

$$\begin{aligned} p_{ji;\rho}(t) &= \text{Tr}(\rho_t(j) \otimes |j\rangle \langle j|) \\ &= \text{Tr}(e^{t\mathcal{L}}(\rho \otimes |i\rangle \langle i|)(I \otimes |j\rangle \langle j|)). \end{aligned} \quad (6)$$

Therefore, the quantum random walk starts with a density operator  $\rho$  concentrated at some vertex  $i$ , takes the evolution up to time  $(t)$  through the exponential of the Lindblad operator  $\mathcal{L}$ , producing a new density operator

$$\rho_t = \sum_k \rho_t(k) \otimes |k\rangle \langle k| = e^{t\mathcal{L}}(\rho \otimes |i\rangle \langle i|), \quad (7)$$

where  $\text{Tr}(\sum_k \rho_t(k)) = 1$ , and then we project  $\rho_t$  onto the subspace generated by vertex  $j$ . The value

$$e^{t\mathcal{L}}(\rho \otimes |i\rangle \langle i|)(I \otimes |j\rangle \langle j|) = \rho_t(j) \otimes |j\rangle \langle j| \quad (8)$$

represents the data concentrated at vertex  $|j\rangle$  at time  $t$ .

### III. TECHNICAL RESULTS

We will employ the canonical Jordan form to show the significance of the spectrum (the set of eigenvalues) of the generator in the context of finite CTOQWs. The following lemma is obtained with basic results of linear algebra and we use the Dirac notation to give a nicely proof.

**Lemma III.1.** *Let  $J_\lambda$  be a  $n \times n$  Jordan block, that is,*

$$J_\lambda = \begin{bmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{bmatrix} \in \mathbb{M}_n(\mathbb{C}). \quad (9)$$

Then  $e^{tJ_\lambda} = e^{\lambda t} X(t)$ , where

$$X(t) = \begin{bmatrix} 1 & t & \frac{t^2}{2} & \cdots & \frac{t^{n-1}}{(n-1)!} \\ & 1 & t & \frac{t^2}{2} & \cdots & \frac{t^{n-2}}{(n-2)!} \\ & & \ddots & \ddots & & \\ & & & \ddots & \ddots & \vdots \\ & & & & 1 & t \\ 0 & & & & & 1 \end{bmatrix}. \quad (10)$$

*Proof:* By taking  $\{|k\rangle, k = 1, \dots, n\}$  the canonical basis of  $\mathbb{C}^n$ , the block  $J_\lambda$  may be rewritten as  $J_\lambda = \lambda I_n + N$ , where  $N$  is a nilpotent matrix which commutes with  $\lambda I_n$  and is of the form

$$N = \sum_{k=1}^{n-1} |k\rangle \langle k+1|. \quad (11)$$

We claim that

$$N^m = \sum_{k=1}^{n-m} |k\rangle \langle k+m|, \quad m = 1, \dots, n-1. \quad (12)$$

Indeed, for  $m = 1$  the claim is true by Equation (11). Suppose now that  $N^m =$

$\sum_{k=1}^{n-m} |k\rangle \langle k+m|$ , then

$$\begin{aligned} N^{m+1} &= \sum_{k=1}^{n-m} \sum_{k'=1}^{n-1} |k\rangle \langle k+m|k'\rangle \langle k'+1| \\ &= \sum_{k=1}^{n-m-1} |k\rangle \langle k+m+1|, \end{aligned} \quad (13)$$

hence the claim holds.

The definition of exponential matrix and the claim above give

$$\begin{aligned} e^{tN} &= \sum_{m=0}^{\infty} \frac{t^m}{m!} N^m = \sum_{m=0}^{n-1} \sum_{k=1}^{n-m} \frac{t^m}{m!} |k\rangle \langle k+m| \\ &= \sum_{k=1}^n |k\rangle \langle k| + \sum_{k=1}^{n-1} t |k\rangle \langle k+1| + \dots + \\ &\quad + \sum_{k=1}^2 \frac{t^{n-2}}{(n-2)!} |k\rangle \langle n| + \frac{t^{n-1}}{(n-1)!} |1\rangle \langle n|. \\ &= X(t). \end{aligned} \quad (14)$$

Finally,  $e^{tJ\lambda} = e^{t(\lambda I + N)} = e^{t\lambda} e^{tN} = e^{t\lambda} X(t)$ .

Now we are able to describe the main result of this article, which will allow us to define the exponential decay parameter for CTOQWs.

**Theorem III.2.** *Let  $\Lambda$  be a finite CTOQW,  $i, j \in V, \rho \in \mathcal{S}(\mathfrak{h}_i)$ . If  $p_{ji;\rho}(t) > 0$  for some  $t > 0$ , then the limit*

$$\lim_{t \rightarrow \infty} \frac{\log p_{ji;\rho}(t)}{t} \quad (15)$$

exists and

$$\lambda_{ji;\rho} := \lim_{t \rightarrow \infty} -\frac{\log p_{ji;\rho}(t)}{t} = -\text{Re}(\lambda) \quad (16)$$

for some eigenvalue  $\lambda$  of  $\mathcal{L}$ , where  $\mathcal{L}$  is the generator of  $\Lambda$ .

*Proof:* Suppose  $|V| = d < \infty$ , denote  $\dim(\mathfrak{h}_z) = d_z, z = 1, \dots, d$ . Then  $[\mathcal{L}]$  is a matrix of order

$$m = \sum_{z=1}^d d_z^2, \quad (17)$$

which can be brought into the Jordan normal form by an appropriate invertible matrix  $V \in \mathbb{M}_m$ , that is,

$$[\mathcal{L}] = VJV^{-1}, \quad (18)$$

where  $J = \text{diag}(J_1, \dots, J_p)$ ,

$$J_q = \begin{bmatrix} \lambda_q & 1 & & & \\ & \lambda_q & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_q \end{bmatrix}, \quad (19)$$

and  $\lambda_1, \dots, \lambda_p$  are the eigenvalues of  $\mathcal{L}$ , which have non-positive real part (see [4]).

Consider the block decomposition into  $p$  blocks of  $J$  as above, then denote for the  $k$ -th block the matrices

$$\mathbb{P}_k = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & I & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix} \quad (20)$$

and

$$[e^{tJ_k}]_k = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & e^{tJ_k} & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix}, \quad (21)$$

$k = 1, \dots, p$ , thus we get

$$\begin{aligned} p_{ji;\rho}(t) &= \text{Tr}(\mathbb{P}_j e^{t[\mathcal{L}]} \mathbb{P}_i \rho) \\ &= \text{Tr}(\mathbb{P}_j V e^{tJ} V^{-1} \mathbb{P}_i \rho) \\ &= \sum_{k=1}^p \text{Tr}(\mathbb{P}_j V [e^{tJ_k}]_k V^{-1} \mathbb{P}_i \rho) \\ &= \sum_{k=1}^p e^{\lambda_k t} f_k(t), \end{aligned} \quad (22)$$

where  $f_k(t) := \text{Tr}(\mathbb{P}_j V [X_k(t)]_k V^{-1} \mathbb{P}_i \rho)$  and  $X_k(t)$  is of the form (10).

For simplicity, assume

$$p_{ji;\rho}(t) = \sum_{k=1}^{p_0} e^{\lambda_k t} f_k(t), \quad f_k \neq 0, \quad (23)$$

$k = 1, \dots, p_0 \leq p$ ,  $0 \geq \text{Re}(\lambda_1) \geq \dots \geq \text{Re}(\lambda_{p_0})$ .

The linearity of the trace guarantees that each  $f_k$  is a non-null polynomial with complex coefficients

$$f_k(t) = \sum_{l=0}^{n_k} \alpha_l t^l, \quad (24)$$

thus, there exists  $t_0 > 0$  such that  $f_k(t) \neq 0$ , for all  $t > t_0$ , for all  $k \in \{1, \dots, p_0\}$ .

Let  $A = \{k; \text{Re}(\lambda_k) = \text{Re}(\lambda_1)\}$ ,  $\omega_k = \lambda_k - \text{Re}(\lambda_1)$  and  $\phi_k^t = \log f_k(t)$  then logarithmic properties give

$$\begin{aligned} & \frac{\log p_{ji;\rho}(t) - (-\text{Re}(\lambda_1))}{t} \\ &= \frac{\log \left( \sum_{k=1}^{p_0} e^{\lambda_k t} e^{\phi_k^t} \right) - \text{Re}(\lambda_1)t}{t} \\ &= \frac{\log \left( \sum_{k=1}^{p_0} e^{\lambda_k t + \phi_k^t} \right) - \log e^{\text{Re}(\lambda_1)t}}{t} \\ &= \frac{\log \left( \sum_{k \in A} e^{it\text{Im}(\lambda_k) + \phi_k^t} + \sum_{k \notin A} e^{\omega_k t + \phi_k^t} \right)}{t} \\ &= \frac{\log \left( \sum_{k \in A} e^{it\text{Im}(\lambda_k)} f_k(t) + \sum_{k \notin A} e^{\omega_k t} f_k(t) \right)}{t}. \end{aligned} \quad (25)$$

Since  $\lim_{t \rightarrow \infty} t^{x/t} = 1$  for any natural  $x$ ,

$$\begin{aligned} \lim_{t \rightarrow \infty} \frac{\log f_k(t)}{t} &= \lim_{t \rightarrow \infty} \frac{\log \alpha_{n_k} t^{n_k}}{t} \\ &= \lim_{t \rightarrow \infty} \frac{\log \alpha_{n_k} + \log t^{n_k}}{t} \\ &= \lim_{t \rightarrow \infty} \frac{\log t^{n_k}}{t} \\ &= \lim_{t \rightarrow \infty} \log t^{n_k/t} \\ &= \log \lim_{t \rightarrow \infty} t^{n_k/t} \\ &= 0. \end{aligned} \quad (26)$$

Now, note that

$$\lim_{t \rightarrow \infty} e^{(\lambda_k - \text{Re}(\lambda_1))t} f_k(t) = 0, \text{ if } k \notin A, \quad (27)$$

and  $|e^{it\text{Im}(\lambda_k)}| \leq 1$  for any  $k$ , thus the Theorem follows.

Given a finite CTOQW,  $i \in V$ ,  $\rho \in \mathcal{S}(\mathfrak{h}_i)$ , we will call  $\lambda_{ji;\rho}$  the **decay parameter** of  $j, i$  with respect to  $\rho$ . Although the decay parameter on the classical model is associated to a communicating class, in the quantum model the limits  $\lambda_{ii;\rho}$  and  $\lambda_{ii;\rho'}$  may exist for distinct densities  $\rho$  and  $\rho'$  with  $\lambda_{i;\rho} \neq \lambda_{i;\rho'}$ , once the nullity of  $f_k$  on equation 23 depends on  $\rho$ .

**Example 1.** Let  $\Lambda$  be a CTOQW with generator  $\mathcal{L} = \Phi - I$ , where the Kraus operators are

$$\begin{aligned} B_{32} &= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 \\ -1 & 1 \end{bmatrix}, B_{11} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \\ B_{21} &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B_{12} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \\ B_{33} &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \end{aligned} \quad (28)$$

$B_{kl} = 0$  otherwise. The walk is represented on the figure 1.

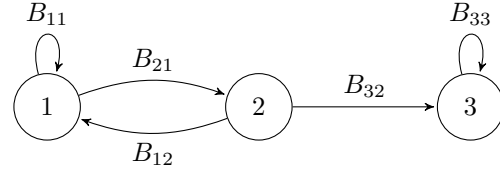


Fig. 1  
A CTOQW WITH 3 VERTICES.

Denote a generic density operator on  $\mathbb{C}^2$  by

$$\rho = \begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix}. \quad (29)$$

The eigenvalues of  $\mathcal{L}$  are  $0, -1, -1 + \frac{\sqrt{2}}{2}, -1 - \frac{\sqrt{2}}{2}$  and  $-2$ , while the decay parameters are

$$\begin{aligned} \lambda_{11;\rho} &= \lambda_{21;\rho} = 1 - \frac{\sqrt{2}}{2} \\ \lambda_{31;\rho} &= \lambda_{32;\rho} = \lambda_{33;\rho} = 0; \\ \lambda_{21;\rho} &= 1 - \frac{\sqrt{2}}{2} \text{ if } b \neq -\frac{1}{2}; \\ \lambda_{22;\rho} &= \begin{cases} 1 - \frac{\sqrt{2}}{2}, & \text{if } b \neq -\frac{1}{2} \\ 1, & \text{if } b = -\frac{1}{2} \end{cases}. \end{aligned} \quad (30)$$

If  $b = -1/2$ , then  $\lambda_{21;\rho}$  is not defined, since  $i = 2$  is not accessible from  $j = 1$  with such density.

As we can see in the following example, perturbing the operators that define the generator of a CTOQW may give other decay parameters for some vertices of the chain.

**Example 2.** Let  $p \in [0, 1]$ ,  $U$  any unitary operator on  $\mathbb{C}^2$ ,  $\Lambda$  be a CTOQW with generator  $\mathcal{L} = \Phi - I$ , with Kraus operators  $B_{22} = U$ ,

$$B_{11} = \begin{bmatrix} \sqrt{p} & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}, B_{21} = \begin{bmatrix} \sqrt{1-p} & 0 \\ 0 & \sqrt{p} \end{bmatrix}. \quad (31)$$

The walk is represented on Figure 2.

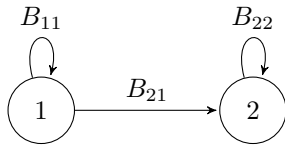


Fig. 2  
A CTOQW WITH 2 VERTICES.

Take a density  $\rho$  as in Equation (29). After some calculus, we get  $p_{11;\rho}(t) = (1 - a)e^{-tp} + ae^{-t(1-p)}$ ,  $t \geq 0$ , and

$$\lambda_{11;\rho} = \begin{cases} p, & \text{if } a = 0 \\ 1 - p, & \text{if } a = 1 \\ \min\{p, 1 - p\}, & \text{otherwise.} \end{cases} \quad (32)$$

It is trivial that a necessary condition to  $\lambda_{ji;\rho}$  be greater than 0 is  $p_{ji;\rho}(t) \xrightarrow{t \rightarrow \infty} 0$ , otherwise  $\log p_{ji;\rho}(t)$  would be bounded and  $\lambda_{ji;\rho}$  would be null.

#### IV. CONCLUSIONS

We show that we can define an exponential decay parameter for any finite CTOQW. This parameter is a real number, being the real part of some eigenvalue of the generator. The next steps in this direction involve infinite CTOQWs, and a nice case is the one where graphs are composed of transitions between nearest-neighbors.

#### ACKNOWLEDGEMENTS

The author wishes to thank his former Ph.D. advisor Carlos F. Lardizabal, and Thomas S. Jacq, for their invaluable guidance and insights. This work is financially supported by Universidade Federal do Pampa (Unipampa).

#### REFERENCES

- [1] W. J. Anderson. **Continuous-time Markov chains: An applications-oriented approach**. Springer Science & Business Media, 2012.
- [2] S. Attal, F. Petruccione, C. Sabot, and I. Sinayskiy. “Open quantum random walks”. In: **Journal of Statistical Physics** 147.4 (2012), pp. 832–852.
- [3] I. Bardet, H. Bringuier, Y. Pautrat, and C. Pellegrini. “Recurrence and transience of continuous-time open quantum walks”. In: **Séminaire de Probabilités L** (2019), pp. 493–518.
- [4] B. Baumgartner and H. Narnhofer. “Analysis of quantum semigroups with GKS–Lindblad generators: II. General”. In: **Journal of Physics A: Mathematical and Theoretical** 41.39 (2008), p. 395303.
- [5] F. Benatti. **Dynamics, information and complexity in quantum systems**. Springer Science & Business Media, 2009.
- [6] O. Bratelli and D. W. Robinson. “Operator algebras and quantum statistical mechanics”. In: **Bull. Amer. Math. Soc** 7 (1982), p. 425.
- [7] E. B. Davies. “Quantum theory of open systems”. In: (**No Title**) (1976).
- [8] R. Durrett. **Probability: theory and examples**. Vol. 49. Cambridge university press, 2019.
- [9] G. Lindblad. “On the generators of quantum dynamical semigroups”. In: **Communications in Mathematical Physics** 48 (1976), pp. 119–130.
- [10] J. R. Norris. **Markov chains**. 2. Cambridge university press, 1998.
- [11] C. Pellegrini. “Continuous time open quantum random walks and non-Markovian Lindblad master equations”. In: **Journal of Statistical Physics** 154.3 (2014), pp. 838–865.
- [12] R. Portugal. **Quantum walks and search algorithms**. Vol. 19. Springer, 2013.
- [13] S. E. Venegas-Andraca. “Quantum walks: a comprehensive review”. In: **Quantum Information Processing** 11.5 (2012), pp. 1015–1106.

# Connections between the Zero-Error Capacity and the Common Invariant Subspace of Quantum Channels

Marciel M. de Oliveira, Andressa da Silva, Micael A. Dias and Francisco M. de Assis

**Abstract**—This article investigates connections between the zero-error capacity of quantum channels and the common invariant subspace under Kraus operators that represent the channel. Initially, we show that a subspace generated by eigenstates common to the Kraus operators is a common invariant subspace under these operators. If the number of eigenstates common to these operators is at least two, we can conclude that the zero-error capacity of the channel is positive.

**Keywords**—Quantum Channel, Zero-error Capacity, Common Invariant Subspace.

## I. INTRODUCTION

Quantum information theory is a field that deals with problems related to the processing and transmission of information through quantum channels [1], [2]. The research areas of quantum information theory are multiple and multidisciplinary, including application perspectives in computing [3], as well as the study of quantum error-correcting codes [4], quantum entanglement [5] and the zero-error capacity of quantum channels [6], [7]. This last area of research is the focus of this paper.

Thus, classical information is coded into quantum states using quantum block coding and transmitted over a discrete memoryless channel (DMC). The quantum states are then measured in the channel output using a Positive Operator-valued Measure (POVM). The zero-error capacity of quantum channels is a generalization of the zero-error capacity of DMC originally defined by Shannon [8].

In studies involving the zero-error capacity of quantum channels, an important aspect is to define whether a quantum channel has a positive zero-error capacity. In this sense, there are at least four known studies in the literature to verify the zero-error capacity condition of quantum channels, which are the works by Medeiros and Rex [6], [9], Gupta *et al.* [10] and, a more recently, Oliveira *et al.* [11].

In addition to these studies involving the verification of the zero-error capacity of a quantum channel, some investigations into quantum channels represented by Kraus [1] operators have made it possible to learn about the relationships that

exist between the quantum channel and the subspace generated by the eigenstates common to the Kraus operators, if these operators have common eigenstates. The issue involving eigenstates common to Kraus operators that represent the quantum channel is connected to the concept of so-called invariant subspaces of Kraus operators.

The concept of an invariant subspace of a linear operator is a well-studied topic. In particular, there is substantial information known about operators that have a non-trivial common invariant subspace [12]. A fundamental question in this context concerns the existence conditions of this non-trivial invariant subspace common to two or more operators [13], [14]. In studies of quantum channels represented by Kraus operators, the concept of non-trivial common invariant subspace appears as a crucial tool, for example, in the discussion involving the irreducibility of quantum channels [15], [16].

In this article, we will investigate the relationship between common invariant subspaces and the zero-error capacity of quantum channels. We will examine how to use the subspace generated by the eigenstates common to the Kraus operators of the channel, which is also an common invariant subspace, to demonstrate that the zero-error capacity of a quantum channel is positive.

In order to achieve the aim of this article, we have organized this work as follows: In Section II, we present the fundamentals of the zero-error capacity of a quantum channel and the Kraus operators. In Section III, we discuss the concept of the common invariant subspace of a quantum channel. In Section IV, we examine the relationship between zero-error capacity and the common invariant subspace of a quantum channel and present the main result. Finally, in Section V, we present the conclusions.

## II. ZERO-ERROR CAPACITY OF QUANTUM CHANNELS

In this section, we will present the main definitions and results regarding the zero-error capacity of quantum channels, which are important to facilitate this paper reading and understanding [6], [7].

We will start this discussion with some notation. For the Hilbert space  $\mathcal{H}$  of dimension  $d$  and the space of operators of  $\mathcal{H}$  of dimension  $d^2$ , we will assume that  $\mathcal{H} \cong \mathbb{C}^d$  and  $\mathcal{B}(\mathcal{H}) \cong M_d(\mathbb{C})$ . Thus, a quantum channel  $\mathcal{E}$  defined on  $\mathbb{C}^d$ , can be modeled by a completely positive and trace-preserving linear map of the density matrices,  $\mathcal{E} \equiv \{A_i\}$ , where  $A_i \in M_d(\mathbb{C})$  are Kraus operators or matrices that satisfy the condition  $\sum_i^\kappa A_i^\dagger A_i = \mathbb{I}$ , with  $\kappa \leq d^2$ .

Marciel M. de Oliveira, Department of Electrical Engineering, Federal University of Campina Grande, Campina Grande-PB, e-mail: marciel.oliveira@ee.ufcg.edu.br; Andressa da Silva, DEE, UFCG, Campina Grande-PB, e-mail: andressa.silva@ee.ufcg.edu.br; Micael A. Dias, DEE, UFCG, Campina Grande-PB, e-mail: micael.souza@ee.ufcg.edu.br; Francisco M. de Assis, DEE,UFCG, Campina Grande-PB, e-mail: fmarcos@ee.ufcg.edu.br. This work was partially support by CNPq (311680/2022-4 and 140327/2023-1).

Let  $\mathcal{X} \subset \mathbb{C}^d$  be the set of possible input states for the quantum channel  $\mathcal{E}$ . If  $\rho \in \mathcal{X}$ , we denote it by  $\sigma = \mathcal{E}(\rho)$ , the quantum state received when  $\rho$  is transmitted through the quantum channel  $\mathcal{E}$  and this can be written as  $\mathcal{E} : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$  such that

$$\mathcal{E}(\rho) = \sum_{i=1}^{\kappa} A_i \rho A_i^\dagger. \quad (1)$$

Let  $\mathcal{E}$  be a quantum channel. The communication protocol associated with the zero-error capacity is summarized as follows. Initially, define  $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\} \subset \mathcal{X}$  to be a finite subset. The states  $\rho_i \in \mathcal{S}$  constitute the alphabet of a zero-error quantum code. The set of codewords of length  $n$  is a superset of the sequences of  $n$  tensor product of states  $\mathcal{S}$ , denoted by  $\mathcal{S}^{\otimes n}$ . For  $\rho_{i_j}$  the  $i$ -th code word is given by  $\bar{\rho}_i = \rho_{i_1} \otimes \dots \otimes \rho_{i_n}$ . If Bob makes measurements using a POVM  $\{M_j\}$ , where  $\sum_j M_j = I$ , then  $p(j|i)$  is the probability that Bob measures  $j$  given that Alice sent the state  $\rho_i$ . Thus,

$$p(j|i) = \text{tr}[\sigma_i M_j] = \text{tr}[\mathcal{E}(\rho_i) M_j]. \quad (2)$$

A zero-error quantum code  $(m, n)$  for  $\mathcal{E}$  is composed of:

- 1) A set of indexes  $\{1, \dots, m\}$ , where each index is associated with a classic message;
- 2) A coding function

$$f_n : \{1, \dots, m\} \rightarrow \mathcal{S}^{\otimes n} \quad (3)$$

which takes each source codeword  $f_n(1) = \bar{\rho}_1, \dots, f_n(m) = \bar{\rho}_m$ .

- 3) A decoding function

$$g : \{1, \dots, k\} \rightarrow \{1, \dots, m\} \quad (4)$$

which deterministically associates a message with one of the possible measurements  $y \in \{1, \dots, k\}$  made by the POVM  $\{M_i\}_{i=1}^k$ . In addition, the decoding function has the following property:

$$\Pr[g(\mathcal{E}(f_n(i))) \neq i] = 0 \quad (5)$$

for all  $i \in \{1, \dots, m\}$ .

The rate of an  $(m, n)$  code is defined as

$$R = \frac{1}{n} \log m \text{ bits/use.} \quad (6)$$

On this basis, we can define the zero-error capacity of quantum channels.

*Definition 1 (Zero-error capacity of quantum channels [6]):* The quantum zero-error capacity of a quantum channel  $\mathcal{E}(\cdot)$ , denoted by  $C^{(0)}(\mathcal{E})$ , is the supremum of the rates achievable with decoding error probability equal to zero,

$$C^{(0)}(\mathcal{E}) = \sup_S \sup_n \frac{1}{n} \log m \quad (7)$$

where  $m$  is the maximum number of classical messages the system can transmit without error when a zero-error quantum block code  $(m, n)$  is used and the input alphabet is  $\mathcal{S}$ .

A fundamental property of quantum states is distinguishability. Two quantum states are distinguishable if, and only if, the Hilbert subspaces generated by the supports of these

quantum states are orthogonal. Thus, given two quantum states  $|\rho_i\rangle, |\rho_j\rangle \in \mathcal{S}$  with  $i \neq j$ , then we say that  $|\rho_i\rangle$  and  $|\rho_j\rangle$  are *non-adjacent* (or distinguishable) at the quantum channel output if  $\mathcal{E}(|\rho_i\rangle)$  and  $\mathcal{E}(|\rho_j\rangle)$  belong to orthogonal Hilbert subspaces. Otherwise, we say that  $|\rho_i\rangle$  and  $|\rho_j\rangle$  are *adjacent* (or indistinguishable) in the output of  $\mathcal{E}$ . The zero-error capacity of a quantum channel  $\mathcal{E}$  is, by definition, related to the concept of distinguishability of quantum states at the channel output.

It is known [6, Proposition 1],[9, Proposition 3] that a quantum channel  $\mathcal{E}$  has positive zero-error capacity if, and only if, there are at least two non-adjacent quantum states. In other words, let  $|\rho_1\rangle$  and  $|\rho_2\rangle$  be two states at the channel input. If  $\text{tr}[\mathcal{E}(\rho_1)\mathcal{E}(\rho_2)] = 0$ , then the channel  $\mathcal{E}$  has positive zero-error capacity.

There is also a relationship between the zero-error capacity and the fixed point of the  $\mathcal{E}$  quantum channel, which is stated in the following proposition. It is important to note that Schauder's fixed point theorem guarantees that a quantum channel has at least one quantum state  $\rho$ , which is a fixed point for the quantum channel  $\mathcal{E}$ , i.e.,  $\mathcal{E}(\rho) = \rho$ .

*Proposition 2:* Let  $\mathcal{E}$  be a quantum channel with  $N_f$  fixed points. Then the zero-error capacity of  $\mathcal{E}$  is at least  $\log N_f$ .

*Proof:* The proof of this proposition can be found in [6, Proposition 2]. ■

Regarding the concept of the fixed point of a quantum channel, for a given quantum channel  $\mathcal{E}$ , represented by Kraus operators  $A_i \in M_d(\mathbb{C})$ , it is proved [11], that if the operators  $A_i$  have eigenstates in common, then these eigenstates are fixed points of the quantum channel  $\mathcal{E}$ . This result made it possible to propose a new result involving the zero-error capacity of a quantum channel, which is stated below.

*Theorem 3:* Let  $N_f$  be the number of fixed points of a quantum channel  $\mathcal{E}$ . Then  $N_f \geq |N_{\mathcal{E}}|$  and  $C^{(0)}(\mathcal{E}) \geq \log |N_{\mathcal{E}}|$ , where  $|N_{\mathcal{E}}|$  is the number of eigenstates common to the Kraus operators  $A_i$  representing the channel.

*Proof:* The proof of this theorem can be found in [11, Theorem 3.2]. ■

### III. COMMON INVARIANT SUBSPACE OF A QUANTUM CHANNEL

Let  $W \subseteq \mathbb{C}^d$  be a vector subspace. We say that  $W$  is an invariant subspace for an operator  $A \in M_d(\mathbb{C})$ , or *A-invariant*, if  $A|\nu\rangle \in W$  for all  $|\nu\rangle \in W$  [12]. We also say that  $W$  is a common invariant subspace for a set  $A_1, \dots, A_s \in M_d(\mathbb{C})$ , if  $W$  is  $A_i$ -invariant for all  $i = 1, \dots, s$ , i.e.,  $A_i|\nu\rangle \in W$  for all  $|\nu\rangle \in W$ .

In the context of studies involving invariant subspaces for matrices or linear operators, we will always have that the null and  $\mathbb{C}^d$  subspaces are always invariant, and these are called trivial invariant subspaces. So, in what follows, when we refer to common invariant subspaces, we refer to non-trivial subspaces.

We can translate the concept of subspace common to linear operators to quantum channels. For this purpose, we use the following definition.

*Definition 4 (Invariant subspace of a quantum channel [17]):* Let  $\mathcal{E} : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$  a quantum channel represented by

Kraus operators  $A_1, \dots, A_\kappa$ . A subspace  $W \subseteq \mathbb{C}^d$  is invariant for a quantum channel  $\mathcal{E}$ , when  $W$  is a common invariant subspace for operators  $A_i$  with  $i = 1, \dots, \kappa$ , i.e.  $A_i |\nu\rangle \in W$  for all  $|\nu\rangle \in W$ .

In the definition of invariant subspace of a quantum channel with representation in terms of Kraus operators  $A_i$ , note the invariance of the subspace  $W \subseteq \mathbb{C}^d$  through the quantum channel  $\mathcal{E}$ , depends on the subspace  $W$  being common invariant to the operators  $A_i$  with  $i = 1, \dots, \kappa$ .

In this context, it is worth highlighting the generalized Shemesh theorem, which proves a condition for operators  $A_i$  to have a common eigenstate.

*Theorem 5 (Generalized Shemesh Theorem [18]):* The matrices  $A_1, \dots, A_t \in M_d(\mathbb{C})$  have common eigenstate if, and only if, the subspace

$$\mathcal{M} = \bigcap_{\alpha_i, l_i=1}^{d-1} \ker [A_1^{\alpha_1} \dots A_t^{\alpha_t}, A_1^{l_1} \dots A_t^{l_t}] \quad (8)$$

is a non-trivial subspace of  $\mathbb{C}^d$ , i.e., there is some  $|x\rangle \in \mathcal{M}$  with  $0 \neq |x\rangle \in \mathbb{C}^d$  and  $\sum_i \alpha_i \neq 0$ ,  $\sum_i l_i \neq 0$ .

The fact that the Kraus operators  $A_i$ , which represent a quantum channel  $\mathcal{E}$ , have a common eigenstate, whose condition is present in the generalized Shemeshe theorem, implies that the quantum channel  $\mathcal{E}$  has an invariant common subspace  $W \subseteq \mathbb{C}^d$  with  $\dim W = 1$ , generated by the common eigenstate of the Kraus operators  $A_i$ . This result is proved in the following proposition.

*Proposition 6:* Let  $\mathcal{E} : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$  be a quantum channel with a Kraus representation  $A_i$ , where  $i = 1, \dots, \kappa$ . If operators the  $A_i$  have a common eigenstate  $|\psi\rangle$ , then the subspace  $W = \text{span}\{|\psi\rangle\}$  is common invariant to the quantum channel  $\mathcal{E}$ .

*Proof:* Since  $|\psi\rangle$  is a common eigenstate of the operators  $A_i$ , then  $A_i |\psi\rangle = \lambda_i |\psi\rangle$  for  $i = 1, \dots, \kappa$ . So, assuming that  $|\nu\rangle \in W = \text{span}\{|\psi\rangle\}$ , we have that  $|\nu\rangle = \lambda |\psi\rangle$ . Thus,

$$A_i |\nu\rangle = \lambda A_i |\psi\rangle = \lambda \lambda_i |\psi\rangle, \quad (9)$$

i.e.,  $A_i |\nu\rangle \in W = \text{span}\{|\psi\rangle\}$ , implying that  $W = \text{span}\{|\psi\rangle\}$  is an invariant subspace for  $A_i$  with  $i = 1, \dots, \kappa$ . In conclusion,  $W = \text{span}\{|\psi\rangle\}$  is an invariant subspace of  $\mathcal{E}$ . ■

In the following section, we will relate the invariant subspace concept of a quantum channel  $\mathcal{E}$  and the zero-error capacity of the channel.

#### IV. ZERO-ERROR CAPACITY AND THE INVARIANT SUBSPACE OF A QUANTUM CHANNEL

This section will be dedicated to presenting the main results of this article regarding the relationship between the invariant subspace and the zero-error capacity of a quantum channel.

To initiate the discussion involving the relationships between the invariant subspace and the zero-error capacity of a quantum channel, we can analyze a channel having an invariant common subspace of dimension one and check its zero-error capacity. Consider the quantum channel  $\mathcal{E}$  called *Amplitude Damping* [19], defined in a Hilbert space of dimension 2, and represented by the Kraus operators:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \text{ e } A_2 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \quad (10)$$

where  $\gamma = \sin^2(\theta)$  is the probability of a photon being lost in a cavity subject to damping. The *Amplitude Damping* channel has a zero-error capacity equal to zero but has an invariant common subspace with dimension one

$$W = \text{span}\{|\psi\rangle\} \quad (11)$$

generated by the eigenstate  $|\psi\rangle = (1, 0)$  common to the Kraus operators  $A_1$  and  $A_2$ .

On the other hand, when it comes to the common invariant subspace of the quantum channel  $\mathcal{E}$ , generated by at least two eigenstates common to the Kraus operators  $A_i$  representing the channel  $\mathcal{E}$ , there is a direct relationship with the zero-error capacity of the quantum channel. This relationship is the main result of this article and is stated in the following theorem.

*Theorem 7:* Let  $\mathcal{E} : M_d(\mathbb{C}) \rightarrow M_d(\mathbb{C})$  be a quantum channel with Kraus operators  $A_1, \dots, A_\kappa$ . If  $W \subset \mathbb{C}^d$  is a subspace with  $\dim W = s$ ,  $2 \leq s < d$ , generated by  $s$  eigenstates  $\{|\psi_j\rangle : j = 1, \dots, s\}$  common to the operators  $A_i$ , then  $W$  an invariant subspace of  $\mathcal{E}$  and  $C^{(0)}(\mathcal{E}) \geq \log(s)$ .

*Proof:* By hypothesis the  $|\psi_j\rangle$  with  $j = 1, \dots, s$  are eigenstates common to the Kraus operators  $A_i$ , with  $i = 1, \dots, \kappa$ , so by definition, we have that

$$A_i |\psi_j\rangle = \lambda_j |\psi_j\rangle, \quad i = 1, \dots, \kappa \text{ e } j = 1, \dots, s. \quad (12)$$

Also, by hypothesis, the subspace  $W$  is generated by these  $s$  eigenstates common to the Kraus operators  $A_i$ , or written in generated subspace notation,

$$W = \text{span}\{|\psi_j\rangle : j = 1, \dots, s\}. \quad (13)$$

To show that  $W$  is invariant to every Kraus operator  $A_i$ , suppose that  $|\nu\rangle \in W$ , then we can write  $|\nu\rangle$  as a linear combination of the eigenstates  $|\psi_j\rangle$  with  $j = 1, \dots, s$ , i.e.  $|\nu\rangle = \alpha_1 |\psi_1\rangle + \dots + \alpha_s |\psi_s\rangle$  or,

$$|\nu\rangle = \sum_{j=1}^s \alpha_j |\psi_j\rangle. \quad (14)$$

Applying the Kraus operators  $A_i$  to the equation (14) and using the linearity properties of these operators, we get

$$A_i |\nu\rangle = \sum_{j=1}^s \alpha_j A_i |\psi_j\rangle = \sum_{j=1}^s \alpha_j \lambda_j |\psi_j\rangle. \quad (15)$$

Since  $\sum_{j=1}^s \alpha_j \lambda_j |\psi_j\rangle \in W$ , then  $A_i |\nu\rangle \in W$ , for all  $i = 1, \dots, \kappa$ . Therefore,  $W$  is  $A_i$ -invariant, so  $W$  is an invariant subspace of  $\mathcal{E}$ . Moreover, the  $\{|\psi_j\rangle : j = 1, \dots, s\}$  generators of the subspace  $W$  are eigenstates common to the Kraus operators  $A_i$ , which are fixed points for the quantum channel  $\mathcal{E}$ , ([11, Lemma 3.1]). Thus, as the number of common eigenstates  $s \geq 2$ , then by Theorem 3, we can conclude that  $C^{(0)}(\mathcal{E}) \geq \log 2$ . ■

Next, we will illustrate the ideas presented in this article with an example of a quantum channel  $\mathcal{E}$  that has an invariant common subspace generated by two eigenstates common to the Kraus operators.

*Example 8:* Given  $p \in (0, 1)$ , consider the quantum channel  $\mathcal{E}$  represented by the Kraus operators  $A_1$  and  $A_2$  given by

$$A_1 = \sqrt{p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_2 = \sqrt{1-p} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For the particular case  $p = 0.5$ , we have that  $|\phi\rangle = (1, 0, 0, 0)$  and  $|\varphi\rangle = (0, 0, 0, 1)$  are eigenstates in common with the Kraus operators  $A_1$  and  $A_2$ , thus by the ideas developed in Theorem 7, the subspace  $W = \text{span}\{|\phi\rangle, |\varphi\rangle\}$  is a common invariant subspace for the Kraus operators  $A_1$  and  $A_2$  and consequently is invariant for the quantum channel  $\mathcal{E}$ . Furthermore, we can also conclude from the ideas developed that the zero-error capacity of the channel  $C^{(0)}(\mathcal{E}) \geq \log 2$ .

## V. CONCLUSIONS

In this article, we presented some preliminary results involving the zero-error capacity of a quantum channel and a common invariant subspace. This common invariant subspace is generated by eigenstates common to the Kraus operators that represent the channel and is an invariant subspace to the quantum channel.

We have shown that if there are at least two eigenstates in common Kraus operators of a channel, then the zero-error capacity of the channel is positive, and these eigenstates define an invariant common subspace. In other words, it is possible to construct a trivial quantum block code with positive zero-error capacity by encoding the classical information of the states of the invariant subspace of the quantum channel.

As future work, we will further explore the connections between quantum zero error capacity and common invariant subspaces.

## ACKNOWLEDGMENTS

The authors would like to thank CNPq and COPELE for their financial support.

## REFERENCES

- [1] M.A Nielsen; I. L.Chuang *Quantum Computation and Quantum Information: 10th Anniversary Edition*. [S.l.]: Cambridge University Press, 2010.
- [2] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. Cambridge, New York: Cambridge University Press, 2019.
- [3] Hiu Y. Wong. *Introduction to Quantum Computing*. Springer, 2022.
- [4] Daniel A. Lidar and T. A. Brun. *Quantum Error Correction*. Cambridge University Press, 2013.
- [5] Mayank Gupta and Manisha J Nene. Quantum Computing: An Entanglement Measurement. *IEEE Xplore*, 12 April 2021, doi: 10.1109/ICATMRI51801.2020.9398441.
- [6] Rex A. C. Medeiros and F. M. de Assis. Quantum Zero-Error Capacity. *International Journal of Quantum Information*, vol. 3, n. 1, pp. 135-139, 2005, doi: 10.1142/S0219749905000682.
- [7] Eloá. B. Guedes; F. M. de Assis; Rex A. C. Medeiros. *Quantum Zero-Error Information Theory*. Springer, 2016.
- [8] C. E. Shannon. The zero error capacity of a noisy channel. *IRE Trans. Inform. Theory*, IT-2(3):8-19, September 1956, doi: 10.1109/TIT.1956.1056798.
- [9] R. A. C. Medeiros, R. Alleaume, G. Cohen and F. M. de Assis. Zero-error capacity of quantum channels and noiseless subsystems. *International Telecommunications Symposium*, Fortaleza, Brazil, pp. 900-905, 2006, doi: 10.1109/ITS.2006.4433399.
- [10] Ved P. Gupta, Prabha Mandayam e V.S Sunder, *The Functional Analysis of Quantum Information Theory*. Springer, 2015.
- [11] Marciel M. Oliveira, Francisco M. de Assis, Micael A. Dias. A condition for the zero-error capacity of quantum channels. *XLL Brazilian Symposium On Telecommunications And Signal Processing - Sbrt 2023*, São José dos Campos, São Paulo, 2023, <https://doi.org/10.48550/arXiv.2312.13406>.
- [12] I. Gohberg, P. Lancaster, L. Rodman. *Invariant Subspaces of Matrices with Applications*. Wiley-Interscience, New York, 1986.
- [13] M. Tsatsomeros. *A criterion for the existence of common invariant subspaces of matrices*. Linear Algebra and its Applications, Volume 322, Issues 1-3, 1 January 2001, Pages 51-59.
- [14] A. Jamiolkowski and G. Pastuszak. Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive super-operators. *arXiv:1306.0083*, v.1, [math.QA], p. 1-17, 2013.
- [15] A. Jamiolkowski. On applications of pi-algebras in the analysis of quantum channels. *International Journal of Quantum Information*. Vol. 10, No. 8, 1241007, 2012, doi: 10.1142/S0219749912410079.
- [16] D. R. Farenick. Irreducible positive linear maps on operator algebras. *Proc. AMS* 124, 3381, 1996.
- [17] D. Burgarth, G. Chiribella, V. Giovannetti, P. Perinotti and K. Yuasa. Ergodic and mixing quantum channels in finite dimensions. *New Journal of Physics*, vol. 15 073045, 2013, doi: 10.1088/1367-2630/15/7/073045.
- [18] A. Jamiolkowski and G. Pastuszak. Generalized Shemesh criterion, common invariant subspaces and irreducible completely positive super-operators. *arXiv:1306.0083*, v.1, [math.QA], p. 1-17, 2013.
- [19] Rex A. C. Medeiros e F. M. de Assis. Capacidade erro-zero de canais quânticos e estados puros. *XXXI Simpósio Brasileiro de Telecomunicações - SBrT 2013*, Fortaleza, Ceará, Brasil, 2013.



# Feature Map Selection for Quantum Classifiers using Pauli Decomposition

Andrias M. M. Cordeiro, Caio N. Silva, Tharso D. Fernandes, Demerson N. Gonçalves and João T. Dias

**Abstract**—Quantum machine learning holds the potential to address classification problems effectively. In our study, we investigate the Pauli Decomposition method, an important technique for visualizing feature spaces and selecting appropriate feature maps. By applying this method to diverse unitary operators, we improve dataset classification accuracy compared to traditional approaches. Our research aims to contribute to advancing quantum machine learning by highlighting the critical role of selecting the optimal feature map.

**Keywords**—Support Vector Machine, Quantum Classification Algorithms, Pauli Decomposition, Minimum Accuracy.

## I. INTRODUCTION

In recent years, machine learning (ML) has become widespread across diverse domains like education, healthcare, finance, and more, due to notable advancements in computational efficiency [1]. The support vector machine (SVM) stands out as a prominent technique in data analysis, valued for its capacity to handle nonlinear datasets by employing a feature map and delineating them with a hyperplane in feature space, often leveraging the Gaussian kernel for this purpose [2].

Quantum computing holds the promise of accelerating ML by harnessing quantum mechanical properties such as superposition, interference, and entanglement [3]. In the last years, there has been a surge in quantum classifier development, including methods like quantum SVMs (QSVMs) and quantum variational classifiers (QVCs). These initiatives, supported by several research teams, demonstrate the potential of quantum computing in enhancing ML problems [4], [5].

The kernel method plays a crucial role in QSVMs, similar to its classical counterpart [6]. Experimental demonstrations have validated the concept of kernel-based quantum classifiers using real quantum devices. These advancements indicate that quantum computing could significantly impact machine learning in the near future [7]. QSVM relies on the selection of an appropriate kernel function, which maps the input data into a larger-dimensional feature space, allowing for linear separation of classes. However, its effectiveness depends heavily on choosing a suitable feature map, as different feature maps can greatly affect classification accuracy.

Andrias M. Cordeiro is student of Computation Engineering, CEFET/RJ, Petrópolis, RJ, E-mail: andrias.cordeiro@aluno.cefet-rj.br. Caio N. Silva is student of Computation Engineering, CEFET/RJ, Petrópolis, RJ, E-mail: caio.silva.1@aluno.cefet-rj.br. Tharso D. Fernandes is professor at Department of Mathematics, UFES, Alegre, ES, E-mail: tharso.fernandes@ufes.br. Demerson N. Gonçalves is professor at Collegiate of Mathematics, CEFET/RJ, Petrópolis, RJ, E-mail: demerson.goncalves@cefet-rj.br. João T. Dias is professor at the Department of Telecommunications, CEFET/RJ, Maracanã, RJ, E-mail: joao.dias@cefet-rj.br.

In this study we present a method to estimate the accuracy of a set of feature map candidates. We expand upon the investigation of Suzuki et al. [5], exploring a range of unitary operators for enhanced analysis. As the kernel can be expressed in terms of the density operator, we focus on the real representation of the feature map candidates by expressing the density operator in terms of Pauli basis. Similar to prior work [5], we employ the concept of *minimum accuracy* to evaluate the accuracy of the training dataset without requiring the design of an actual classifier, thus bypassing the need for calculating the kernel function. Furthermore, we explore whether the minimum accuracy attains a significant value, ensuring that any optimized classifier in the feature space achieves equal or superior accuracy.

## II. PAULI DECOMPOSITION

The Pauli matrices commonly used in quantum physics and quantum computing are defined as follows:

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

They form a basis of  $\mathbb{C}^2 \times \mathbb{C}^2$ , and when combined using  $n$  tensor products, they give rise to  $4^n$  matrices referred to as Pauli operators.

A density operator  $\rho$  of a 2-qubit quantum state can be expressed as [8]:

$$\rho = \sum_{i,j=1}^{\mathbf{X}} t_{ij} \sigma_i \otimes \sigma_j, \quad (1)$$

where  $t_{ij} \in \mathbb{R}$  are the coefficients of the decomposition. These coefficients can be computed using the trace method

$$t_{ij} = \frac{1}{4} \text{Tr}(\rho \cdot (\sigma_i \otimes \sigma_j)). \quad (2)$$

This decomposition allows us to express the density operator  $\rho$  in terms of linear combinations of Pauli matrices, providing insight into its structure and properties.

## III. FEATURE MAP REPRESENTATION USING PAULI DECOMPOSITION

In QSVM approach, the feature map transforms an input dataset into a set of multi-qubit states, constituting the feature space (Hilbert space). The kernel matrix is then constructed by computing inner products of these quantum states and then employed in the SVM for dataset classification. Analyzing the feature space is essential, yet its complex structure makes this task challenging. Here, we present the Pauli-decomposition method in order to visualize the feature space, offering guidance in selecting an appropriate feature map.

The Ref. [4] presents a kernel-based quantum SVM where classical data  $x \in \mathbb{R}^n$  is encoded into the unitary operator  $U_{\Phi}(x)$  through the encoding function  $\Phi(x)$ . This operator is applied to the initial state  $|0\rangle^{\otimes n}$ , with  $|0\rangle$  representing the qubit ground state. Then, the feature

map transforms classical data  $x$  into the quantum state  $|\Phi(x)\rangle = U_{\Phi}(x)|0\rangle^{\otimes n}$ , where

$$U_{\Phi(x)} = \exp \left( i \begin{matrix} \mathbf{X} & \mathbf{Y} \\ \Phi_S(\mathbf{x}) & \sigma_k \end{matrix} \right), \quad (3)$$

$S$  is a set of qubit indices that describes the connections in the feature map,  $\mathcal{I}$  is a set containing all these index sets and  $\sigma_k$  represents the Pauli matrices. Then, the quantum kernel is naturally defined as  $K(x, x') = |\langle \Phi(x) | \Phi(x') \rangle|^2$ , which can be estimated using the SWAP test.

Now, note that the kernel can be represented in terms of the density operator  $\rho(x) = |\Phi(x)\rangle\langle\Phi(x)|$ , that is,  $K(x, x') = |\langle \Phi(x) | \Phi(x') \rangle|^2 = \text{tr}[\rho(x)\rho(x')]$ . In contrast, following Eq. (1), the decomposition of a  $n$ -qubit density operator is  $\rho(x) = \frac{1}{2^n} \sum_{i=1}^{4^n} t_i(x) \sigma^i$ , where  $t_i(x) \in \mathbb{R}$  and  $\sigma^i \in \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}^{\otimes n}$ . Substituting this expression into the kernel and utilizing the trace relation  $\text{tr}(\sigma_i \sigma_j) = 2^n \delta_{ij}$ , the kernel can be written as

$$K(x, x') = \prod_{i=1}^n t_i(x) t_i(x'). \quad (4)$$

Hence, a data point  $x$  is encoded in a real feature space  $\mathbb{R}^{4^n}$  by the vector  $\mathbf{t}(x) = [t_1(x), t_2(x), \dots, t_{4^n}(x)]$ .

#### IV. MINIMUM ACCURACY ALGORITHM

The concept of minimum accuracy, as defined in Ref. [5], refers to the highest classification accuracy achievable when the hyperplane used for classification is constrained to be orthogonal to any basis axis in the feature space  $\mathbb{R}^{4^n}$ . This measure does not depend on specific classifiers, allowing for the evaluation of feature maps and kernels without the need to design a classifier directly.

The Algorithm 1 iterates over each of the  $4^n$  axes of the feature space, computing the accuracy for each threshold. Here, a threshold represents a cut along a specific axis by a hyperplane, thereby dividing the axis into two parts. After computing the accuracy for each threshold, the algorithm identifies the maximum accuracy achieved for each axis. Then, it determines the minimum accuracy by selecting the highest among these maximum accuracies.

---

#### Algorithm 1 Minimum Accuracy

---

**Input:** Dataset  $\{(\mathbf{t}(x_k), y_k)_{k=1}^N\}$ , with  $y_k \in \{-1, +1\}$

**Output:** Minimum accuracy  $R$

max\_accuracy = [ ]

**for**  $i = 1$  **to**  $4^n$  **do**

Initialize best\_accuracy = 0

**for**  $j = 1$  **to**  $N + 1$  **do**

$L_+ \leftarrow$  number of +1 on left side of  $j$ -th threshold

$L_- \leftarrow j - L_+$

accuracy  $\leftarrow \frac{1}{N} (\max\{L_+, L_-\} + \frac{N}{2} - \min\{L_+, L_-\})$

best\_accuracy  $\leftarrow \max(\text{best\_accuracy}, \text{accuracy})$

**end**

max\_accuracy.append(best\_accuracy)

**end**

return  $R = \max(\text{max\_accuracy})$

---

#### V. RESULTS

We implement Algorithm 1 using the feature map defined by unitary operator (3), with the number of qubits set to 2, and sequences of Pauli matrices  $[Z, ZZ]$  and  $[X, YZ]$ , along with the following set

of encoding functions:

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = (\pi - x_1)(\pi - x_2) \quad (5)$$

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = \pi x_1 x_2 \quad (6)$$

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = \frac{\pi}{2}(1 - x_1)(1 - x_2) \quad (7)$$

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = \exp\left(\frac{|x_1 - x_2|^2}{8/\ln(\pi)}\right) \quad (8)$$

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = \frac{\pi}{3 \cos(x_1) \cos(x_2)} \quad (9)$$

$$\Phi_1(\mathbf{x}) = x_1, \quad \Phi_2(\mathbf{x}) = x_2, \quad \Phi_{1,2}(\mathbf{x}) = \pi \cos(x_1) \cos(x_2). \quad (10)$$

We consider the nonlinear 2-dimensional dataset named XOR, comprising 1000 data points  $(x_k, y_k)$ , where  $k = 1, \dots, 1000$ . These points are generated and classified into two groups based on  $y_k = +1$  or  $y_k = -1$ . The results of the simulation are depicted in Table I:

TABELA I

MINIMUM ACCURACY FOR DIFFERENT ENCODING FUNCTIONS AND PAULI SEQUENCES

Encoding function	[X, YZ]	[Z, ZZ]
(5)	0.814	0.734
(6)	0.805	0.773
(7)	0.734	0.719
(8)	0.901	0.955
(9)	0.766	0.888
(10)	0.773	0.730

#### VI. CONCLUSIONS

The obtained results are preliminary, and Table 1 illustrates that the best minimum accuracy is achieved with encoding function (8) and Pauli sequence  $[Z, ZZ]$ . However, further validation is required by running a quantum classifier, for which the minimum accuracy has already been established.

We are currently investigating whether Algorithm 1 provides a lower bound on accuracy, that is, whether any classifier would produce an equal or better result given a certain established minimum accuracy. Initially, experiments are being conducted by varying the set of Pauli matrices as well as encoding functions. However, a more rigorous mathematical analysis is necessary to confirm these findings. Although calculating the minimum accuracy becomes intractable for increasing values of  $n$ , it remains particularly interesting for applications involving few qubits, as such strategies do not require computing the quantum kernel for each feature map, thus simplifying the computational process.

#### REFERENCES

- [1] M. Cerezo, G. Verdon, H.Y. et al. *Challenges and opportunities in quantum machine learning*. Nat Comput Sci 2, 567–576 (2022). <https://doi.org/10.1038/s43588-022-00311-3>
- [2] V. Vapnik. *The Support Vector Method of Function Estimation*. Boston, MA: Springer US, 1998, pp. 55–85. [Online]. Available: [https://doi.org/10.1007/978-1-4615-5703-6\\_3](https://doi.org/10.1007/978-1-4615-5703-6_3)
- [3] M. Schuld, F. Petruccione. *Machine Learning with Quantum Computers*. Springer International Publishing, January 2021.
- [4] Havlíček, V., Córcoles, A.D., Temme, K. et al. *Supervised learning with quantum-enhanced feature spaces*. Nature 567, 209–212 (2019).
- [5] Y. Suzuki, H. Yano, Q. Gao, et al. *Analysis and synthesis of feature map for kernel-based quantum classifier*. Quantum Mach. Intell. 2, 9 (2020). <https://doi.org/10.1007/s42484-020-00020-y>
- [6] M. Schuld. *Supervised quantum machine learning models are kernel methods* in arXiv preprint arXiv:2101.11020, 2021.
- [7] T. Hubregtsen, D. Wierichs, E. Gil-Fuster, H. S. Peter-Jan, P. K. Faehrmann, J. J. Meyer. *Training quantum embedding kernels on near-term quantum computers*. Phys. Rev. A, v. 106, Oct, 2022.
- [8] A. De Vos and S. De Baerdemacker. *The decomposition of an arbitrary  $2w \times 2w$  unitary matrix into signed permutation matrices*. Linear Algebra and its Applications, V. 606, 2020, Pages 23–40.

# Pilotless Channel Estimation Scheme in OFDM Systems using K-Means and Quantum K-Means

Caio N. Silva, Andrias M. M. Cordeiro, Tharso D. Fernandes, Demerson N. Gonçalves and João T. Dias

**Abstract**—In a mobile wireless communication systems, channel estimation is generally performed based on pilot symbols, but it consumes radio resources to transmit data. If the channel can be estimated without transmitting the pilot signal, efficiency of radio resource utilization for data transmission can be maximized. In this work we propose the use of a quantum version of the Kmeans clustering algorithm for channel estimation. The viability of our approach is substantiated by computational simulation results obtained in frequency selective channel models with the presence of Gaussian noise. The mean square error (MSE) performance of the proposal outperform those of the least square (LS) channel estimator.

**Keywords**— Channel estimation, OFDM, K-Means, QK-Means.

## I. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) has become a popular scheme for wireless networking standards that operate at a high bit rate [1]. The main advantage of OFDM over single-carrier schemes is its ability to eliminate intersymbol interference (ISI) without the need for complex equalization filters at the receiver [1]. Channel estimation in OFDM systems is usually performed based on pilot symbols using least squares (LS) [2]. However, since the pilot signal transmission also consumes radio resources, the transmission of the pilot signal is also a cause of reducing an effective data throughput. Therefore, as long as the performance of the wireless communication system is maintained, minimizing the transmission of the pilot signal maximizes the throughput [3].

Machine unsupervised learning, like K-Means, have been proposed to solve a variety of problems in digital communications systems [4], including channel estimation [5].

Quantum algorithms have been proposed to solve problems with prohibitive complexity in classical algorithms [6]. In this work, we propose the use of a quantum K-means for channel estimation in an OFDM system with frequency selective channel and Gaussian noise presence.

This article is divided as follows: in section II, the OFDM system are described. The estimator models are presented in section III. In section IV, the simulation results are presented, and conclusions are made in section V.

Caio N. Silva and Andrias M. M. Cordeiro are students of Computation Engineering, CEFET/RJ, Petrópolis, RJ, E-mails: {caio.silva.1 and andrias.cordeiro}@aluno.cefet-rj.br. Tharso D. Fernandes is professor at Department of Mathematics, UFES, Alegre, ES, E-mail: tharso.fernandes@ufes.br. Demerson N. Gonçalves is professor at Collegiate of Mathematics, CEFET/RJ, Petrópolis, RJ, E-mail: demerson.goncalves@cefet-rj.br. João T. Dias is professor at the Department of Telecommunications, CEFET/RJ, Maracanã, RJ, E-mail: joao.dias@cefet-rj.br. This work was partially financed by the program “INOVA-CEFET/RJ – PIBITI/CNPq”.

## II. SIGNAL MODEL

The OFDM signal can be expressed in the time domain by [1]

$$x[n] = \sum_{k=0}^{K-1} s_k e^{j2\pi \frac{k}{K} n}, \quad (1)$$

where  $s_k$  is the data symbol on the  $k$ -th subcarrier and  $K$  is the number of subcarriers in the OFDM symbol.

The signal at the receiver input can be written by

$$\mathbf{y} = \mathbf{x} * \mathbf{h} + \omega, \quad (2)$$

where  $\mathbf{y} \in C^{(K+CP+N_p-1) \times 1}$ ,  $CP$  is the length of the cyclic prefix,  $N_p$  is the number of paths considered in the channel,  $\mathbf{x} \in C^{(K+CP) \times 1}$ ,  $\mathbf{h} \in C^{(N_p) \times (1)}$  is the channel impulse response,  $*$  is the convolution operation,  $\omega \in C^{(K+CP+N_p-1) \times 1}$  is additive white Gaussian noise (AWGN).

## III. CHANNEL ESTIMATORS

The estimators that will be used in the performance comparison in this work are:

### A. LS

The least squares (LS) channel estimator is [2]

$$\hat{H}(k) = \frac{Y(k)}{S_p(k)}, \quad (3)$$

where  $Y(k)$  is the received signal on the  $k$ -th subcarrier in frequency domain and  $S_p(k)$  is the pilot signal transmitted on the  $k$ -th subcarrier.

### B. K-Means

The unsupervised machine learning method K-Means for channel estimation [5] clusters each of the  $k$  subcarriers from the  $N$  received signals  $Y$ . This process provides  $c_m$  centroids corresponding to the number of constellations in the modulation method. With  $c_m$  centroids on each subcarrier, we can compute  $A_k$  and  $\theta_k$ , that are the amplitude and phase of the channel response in the subcarrier  $k$ , respectively, by:

$$A_k = \exp\left(\operatorname{Re}\left(\frac{\sum \log(c_m)}{4}\right)\right), \theta_k = \operatorname{Im}\left(\frac{\sum \log(c_m)}{4} - \pi\right). \quad (4)$$

After that, to determine the channel response of each  $k$  subcarrier, as follows:

$$\hat{H}(k) = A_k e^{j\theta_k}. \quad (5)$$

### C. QK-Means

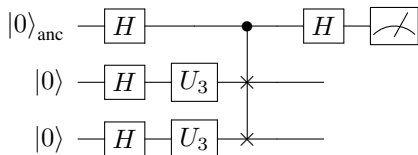
The version of Lloyd’s algorithm for K-Means clustering used in this paper alters the way distances are calculated, using quantum computing to enhance computational complexity [7]. We map the coordinates of a point as follows:

$$\theta = \arctan\left(\frac{y}{x}\right) \quad (6)$$

where  $\theta$  is the phase of the complex number composed of the coordinates  $(x, y)$ . For using this expression in quantum computing, the phase above is used in a  $U_3$  gate:

$$U_3(\theta, \pi, \pi) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\pi} \sin\left(\frac{\theta}{2}\right) \\ e^{i\pi} \sin\left(\frac{\theta}{2}\right) & e^{i2\pi} \cos\left(\frac{\theta}{2}\right) \end{bmatrix}. \quad (7)$$

Since we have the coordinates of the points in a way that is possible to use quantum computing, the distance calculation method is based on the SWAP test operator. Introducing the  $U_3$  gate with the coordinates of the points that we want to calculate, the distance in the method leads to the following quantum circuit:



The rest of the algorithm performs as the classical part, and the channel estimations are as mentioned earlier.

## IV. RESULTS

To validate the proposed quantum K-Means and compare its performance with the classical K-Means algorithm and LS in OFDM systems channel estimation, we measured the mean square error (MSE), i.e.  $MSE = E[|H - \hat{H}|^2]$ , of the estimated channel in the range of 0 to 25dB signal-to-noise ratio (SNR), considering the following simulation parameters:

TABELA I  
SIMULATION PARAMETERS

Number of subcarriers [K]	256
Subcarrier modulation	QPSK
Cyclic prefix length in number of subcarriers	8
Number of pilot subcarriers [ $S_p$ ]	32

The tests were performed on a frequency-selective channel with a delay profile given by  $\mathbf{h} = [1 \ 0 \ 0.3 + 0.3j]$ , and Gaussian noise. For each estimator,  $N = 100$  OFDM symbols were transmitted to calculate  $\hat{H}$  or the average of  $\hat{H}$ . We also utilized the Qiskit library (an open-source quantum computing framework created by IBM®) [8] for the quantum machine learning task and a local quantum simulator. Figure 1 shows the MSE as a function of signal-to-noise ratio SNR.

Analyzing the performance of the MSE obtained from the three tested estimators, we can observe in the Fig. 1 that the MSE curve obtained with the K-Means estimator is significantly lower than that obtained with the LS estimator, which shows its robustness to noise, while the curve obtained with the QK-Means estimator shows similar behavior

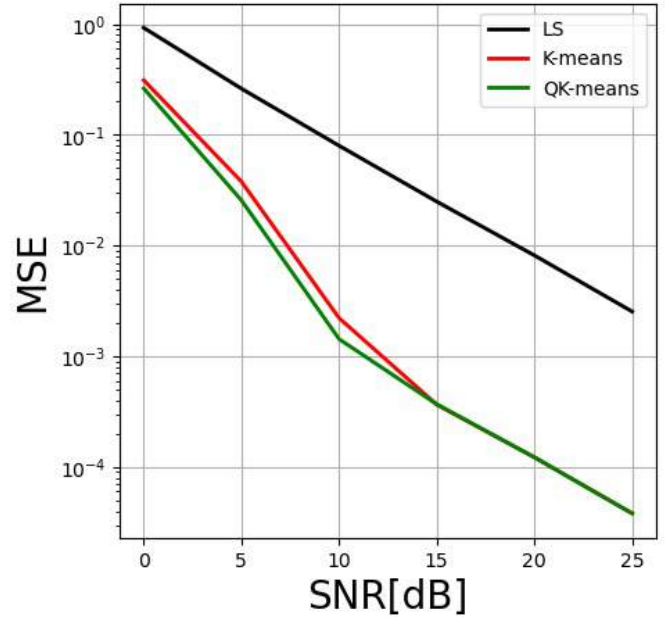


Fig. 1. MSE of estimation.

and robustness to noise that K-Means, with a slightly better performance in the range of 0 to 14 dB, which shows greater robustness to noise.

## V. CONCLUSION

In this work, a QK-Means algorithm was proposed for channel estimation in OFDM systems. The structure of the adopted OFDM system and the channel estimation process for each of the estimators were described. Several tests were carried out in search of the ideal number of samples in the OFDM system. The simulations confirmed the robustness of QK-Means in the presence of noise and the results show that the proposal outperforms the classic K-Means and LS.

## REFERENCES

- [1] N. Marchetti, et al., *New Directions in Wireless Communications Research*, cap. 2, OFDM-Principles and Challenges, 2009.
- [2] O. Edfors, et al., *Analysis of DFT-based channel estimators for OFDM* Div. Signal Process., Luleå Univ. Technol., Sweden, Res. Rep. TULEA, 1996, vol. 17.
- [3] O. Elijah, et al., *A Comprehensive Survey of Pilot Contamination in Massive MIMO-5G System* IEEE Commun. Surveys and Tutorials, Vol. 18, Issue 2, pp. 905-923, Feb. 2016.
- [4] O. Simeone, *A Very Brief Introduction to Machine Learning With Applications to Communication Systems*, IEEE Transactions on Cognitive Communications and Networking, vol. 4, no. 4, pp. 648-664, Dec. 2018
- [5] K. Jung, H. Wang, *Pilotless Channel Estimation Scheme using Clustering-based Unsupervised Learning*, 15th International Symposium on Wireless Communication Systems, pp. 1-5, 2018
- [6] D. Neves, J. Drago, E. Dalcumune, D. Gonçalves, J. Dias, *Q-SVM Applied to Multi-User Detection in DS-CDMA Systems*. In: VI Workshop Escola de Computação e Informação Quântica, 2022, Alfenas. VI WECIQ, 2022.
- [7] S. Lloyd1 , M. Mohseni, P. Rebentrost, *Quantum algorithms for supervised and unsupervised machine learning*, arXiv preprint arXiv:1307.0411, Nov. 2013.
- [8] Qiskit Community. *Qiskit Machine Learning overview*. <https://qiskit.org>. (Last accessed: 13.05.2024).

# Simulação do algoritmo de fatoração usando GPU

Raian Pierre e Luis Kowada

**Resumo**— Estudos sobre simulação de um computador quântico usando GPU. Algoritmo usado para poder fazer a simulação foi o de Peter Shor para fatoração de números compostos.

**Palavras-Chave**— Fatoração, GPU, Peter Shor, CUDA, Computação quântica.

## I. INTRODUÇÃO

O artigo de Peter Shor [3], publicado no ano de 1994, foi um grande salto para Computação Quântica [1]. O autor propôs algoritmo para dois problemas, um deles é a fatoração de um número  $N$ , ou seja, encontrar um fator (divisor) não trivial, caso possua. Se  $N$  é primo ou uma potência de primo, o problema da fatoração pode ser resolvido classicamente em tempo polinomial. Para o caso de  $N$  ser produto de primos distintos, o problema de fatoração pode ser reduzido ao problema de encontrar a ordem de um número módulo  $N$ . Shor, em seu algoritmo, usa a computação quântica apenas para calcular a ordem  $r$  módulo  $N$  de um valor  $x$  escolhido aleatoriamente. Ou seja, encontrar o menor inteiro positivo  $r$  que satisfaz a expressão  $x^r \bmod N \equiv 1$ . Não se conhece algoritmo polinomial clássico para isso.

Para calcular a ordem de  $x$ , cria-se um estado num computador quântico com potências de  $x$  módulo  $N$  em superposição. Em seguida é calculada a Transformada de Fourier Inversa, para então deduzir o valor de  $r$  a partir dos valores medidos.

A criptografia RSA [6], um dos sistemas criptográficos mais utilizados, foi significativamente impactada pelo advento do algoritmo de Shor [3]. Essa técnica criptográfica depende de uma chave pública, denotada por  $N = p \cdot q$ , onde  $N$  faz parte da chave pública. A segurança do RSA [6] baseia-se na dificuldade de fatorar  $N$  em seus componentes primos,  $p$  e  $q$ . Se estes fatores são descobertos, a partir da chave pública, pode-se encontrar a chave privada.

Embora a implementação do RSA [6] seja relativamente simples, a segurança do sistema é garantida quando  $p$  e  $q$  são suficientemente grandes, tipicamente na ordem de pelo menos 256 bits cada. Com a capacidade computacional atual, a tarefa de descriptografar uma mensagem protegida por chaves de tal magnitude levaria muitos anos, tornando o RSA [6] seguro sob condições convencionais.

No entanto, essa segurança é desafiada pelo algoritmo de Shor, que pode encontrar os fatores de  $N$  em tempo polinomial quando implementado em um computador quântico. Esse avanço representa uma mudança paradigmática, pois reduz o tempo necessário para quebrar a criptografia RSA [6], expondo suas vulnerabilidades e destacando a necessidade de

desenvolver novos métodos criptográficos resistentes a ataques quânticos.

O objetivo deste trabalho é tentar simular o algoritmo de Shor usando paralelismo clássico, obter resultados e poder tirar conclusões sobre o estudo e a tentativa de aumentar o número de bits para a simulação e fatorar um  $N$  maior.

## II. METODOLOGIA

A ideia geral de simular o algoritmo de fatoração do Shor [3] é poder mostrar como um valor acima dos 100 bits pode ser fatorado usando o algoritmo de Shor.

### A. Objetivo

Para poder fazer um simulador com essas características, tivemos que analisar quais ferramentas iríamos usar. Para ter mais margem de resultados usamos duas linguagens de programação: Python [2] e C [4]. Além delas, usei muitas bibliotecas, mas a principal delas foi o CUDA [5].

Neste caso vamos tratar a biblioteca para paralelizar como uma linguagem, mesmo que ele seja apenas uma biblioteca usada em C [4]. Ele usa outro compilador e a arquitetura do arquivo executável é híbrido, sendo usando para arquitetura do proprio computador como o da placa de video. Lembrando que CUDA [5] é uma biblioteca da empresa Nvidia e que só as placas do modelo RTX pode fazer algoritmos paralelos. Paralelizar algumas funções para que a eficiência fosse maior foi o maior objetivo dessa pesquisa, contudo mesmo que tenhamos todo o algoritmo paralelizado, poderíamos não ter a eficiência esperada.

### B. Algoritmo

Iniciamos o estudo desenvolvendo um simulador na linguagem Python [2], empregando matrizes e vetores de grandes dimensões. Diante do desejo de paralelizar o código para otimizar o desempenho, enfrentamos desafios iniciais que impediram o sucesso dessa abordagem. Em busca de uma solução, migramos para a linguagem C [4], mantendo a correteude do código equivalente ao do Python [2]. Após essa migração, conseguimos finalmente paralelizar o código. Subsequentemente, procedemos à comparação dos três algoritmos desenvolvidos para determinar qual seria o mais eficaz e se a utilização de GPU seria vantajosa. A decisão de aumentar o número de bits dependia desses resultados.

No entanto, enfrentamos dificuldades com o uso de CUDA [5] em C [4] devido a problemas de *overflow*, onde, por vezes, o resultado era nulo ou retornava o próprio  $N$ . Determinados a identificar e corrigir o erro, descobrimos que uma função em C [4] que calculava o mínimo múltiplo comum (MMC) de forma iterativa contribuía para o estouro

Raian Pierre, Instituto de Computação, Universidade Federal Fluminense, Niterói-RJ, e-mail: raianpierre@id.uff.br; Luis Kowada, Instituto de Computação, Universidade Federal Fluminense, Niterói-RJ, e-mail: luis@ic.uff.br. Este trabalho foi parcialmente financiado por PIBIC - UFF, CNPq e projeto FAPERJ APQ1.

da variável, dada a ausência de mecanismos de tratamento de *overflow*.

A solução encontrada foi a implementação da biblioteca GMP [7] para precisão arbitrária, permitindo o manejo adequado do *overflow*. Com essa alteração, retomamos a fase de testes, visando consolidar uma base de dados robusta que suportasse uma análise criteriosa sobre as linguagens utilizadas e sobre o desempenho do simulador que desenvolvemos.

### C. Resultados

Foram dez rodadas de testes usando 5  $N$  diferentes para poder fatorar e usamos 20 a 24 bits nesse teste. Não aumentamos a quantidade de bits por alguns motivos, como *overflow*.

Após coletar os dados e identificar as inconsistências, ficou claro que a existência dos insucessos não era inesperada. Além disso, após uma investigação sobre as causas de todos os erros, também foi encontrado o motivo, que era o *overflow*. Esse fenômeno ocorre porque a linguagem C [4] tem variáveis de tamanho estático. Ou seja, se o valor obtido for mais do que um tamanho da variável aceitável, não fornece nenhuma mensagem para tratar disso.

A Tabela I contém os resultados obtidos de 10 rodadas para o valor de  $N$  e o tamanho de bits.

TABELA I  
TABELA DE TESTES.

	Rodada	$N$	Bits
	Primeira	899	20
	Segunda	899	24
	Terceira	7.387	20
	Quarta	7.387	24
	Quinta	1.451	20
	Sexta	1.451	24
	Sétima	2.419	20
	Oitava	2.419	24
	Nona	943	20
	Décima	943	24

Por outro lado, Python [2], ao empregar variáveis de tamanho dinâmico, automaticamente ajusta o tamanho das variáveis quando ocorre um *overflow*. Essa capacidade intrínseca de Python [2] para gerenciar o *overflow* contrasta significativamente com a abordagem estática adotada por C [4], oferecendo uma robustez adicional no tratamento de dados em grande escala.

A Tabela II contém o tempo que foi executado o simulador em cada linguagem.

A Tabela III contém os acertos ou erros do simulador.

### III. CONCLUSÕES

Um ponto de interesse a destacar ocorreu durante a sétima rodada, na qual, apesar de o número de bits ser inferior, o tempo de execução do CUDA [5] superou o registrado na quarta rodada, que apresentava um número maior de bits. Tal observação sugere a necessidade de otimizações no algoritmo, a fim de aprimorar tanto o tempo de execução quanto a eficácia na obtenção de soluções. Nesse contexto, o Python [2] mostrou-se relativamente mais eficiente, concluindo todas

TABELA II  
TABELA DE TEMPO (SEGUNDOS).

	CUDA	Python	C
Primeira	0.16	0.39	0.04
Segunda	3.16	6.03	0.90
Terceira	0.15	0.39	0.04
Quarta	0.73	6.09	0.96
Quinta	3.74	0.39	0.96
Sexta	3.74	6.18	0.05
Sétima	0.16	0.39	0.06
Oitava	0.10	5.10	0.94
Nona	2.05	6.17	0.94
Décima	0.17	0.41	0.04

TABELA III  
TABELA DE ACERTOS.

	CUDA	Python	C
Primeira	Acerto	Acerto	Acerto
Segunda	Não acerto	Não acerto	Acerto
Terceira	Acerto	Acerto	Acerto
Quarta	Não acerto	Acerto	Acerto
Quinta	Não acerto	Acerto	Não acerto
Sexta	Não acerto	Acerto	Acerto
Sétima	Acerto	Acerto	Acerto
Oitava	Acerto	Acerto	Acerto
Nona	Não acerto	Acerto	Não acerto
Décima	Acerto	Acerto	Acerto

as rodadas com apenas uma ausência de solução, embora tenha demandado mais tempo para a execução. Este resultado sublinha a eficiência comparativa do algoritmo implementado em Python [2].

Quanto às ocasiões em que os programas falharam em encontrar soluções, tal questão permanece sob investigação. Embora o CUDA [5] possua capacidades para manipular vetores maiores e executar outros cálculos complexos, seu desempenho não alcançou a plena satisfação, evidenciando uma taxa de sucesso de apenas 50%. Além disso, apesar do bom desempenho do Python [2] com vetores de 20 bits, o aumento no tempo de execução com o mesmo valor de  $N$  é motivo de preocupação.

Esta análise evidencia a complexidade inerente à otimização e paralelização de algoritmos, indicando a necessidade de aprimoramentos contínuos para garantir uma eficiência consistente tanto em termos de tempo de execução quanto na capacidade de resolução de problemas.

### REFERÊNCIAS

- [1] GALVÃO, E. *O que é computação quântica?*, 2007. Editora Vieira e Lent. 1ª edição.
- [2] Site [www.python.org/doc/](http://www.python.org/doc/), consultado em junho de 2023.
- [3] SHOR, Peter W. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM review, v. 41, n. 2, p. 303-332, 1999.
- [4] FEOFILOFF, Paulo. *Algoritmos em linguagem C*, Elsevier Brasil, 2009.
- [5] GARLAND, Michael et al. *Parallel computing experiences with CUDA*, IEEE micro, v. 28, n. 4, p. 13-27, 2008.
- [6] BONFIM, Daniele Helena. *Criptografia RSA*, 2017. Tese de Doutorado. Universidade de São Paulo.
- [7] CLAUDINO, Rafael Ayres; ESTECA, Antonio Marcos Neves. ANÁLISE DE DESEMPENHO DA BIBLIOTECA GMP: UM ESTUDO DE CASO COM A FATORAÇÃO DE NÚMEROS.



**Organização**



**Apoio**



**Patrocínio Ouro**



**Patrocínio Prata**

