

CSRN 3502

(Eds.)

Sabre Kais

North Carolina State University, North Carolina, USA

Vaclav Skala

University of West Bohemia, Czech Republic

Computer Science Research Notes

Quantum Informatics, Computing & Technology 2025

QC-HORIZON 2025

Plzen, Czech Republic

August 26-27, 2025

Proceedings

QC-HORIZON 2025

Proceedings

ISSN 2464-4617 (print)

ISSN 2464-4625 (online)

CSRN 3502

(Eds.)

Sabre Kais

North Carolina State University, North Carolina, USA

Vaclav Skala

University of West Bohemia, Czech Republic

Quantum Informatics, Computing & Technology 2025

QC-HORIZON 2025

Plzen, Czech Republic

August 26-27, 2025

Proceedings

QC-HORIZON 2025

Proceedings

This work is copyrighted.

However all the material can be freely used for educational and research purposes if publication properly cited. The publisher, the authors and the editors believe that the content is correct and accurate at the publication date. The editor, the authors and the editors cannot take any responsibility for errors and mistakes that may have been taken.

Computer Science Research Notes CSRN 3502

Editor-in-Chief: Vaclav Skala
c/o University of West Bohemia
Univerzitni 8
CZ 306 14 Plzen
Czech Republic
skala@kiv.zcu.cz <http://www.VaclavSkala.eu>

Managing Editor: Vaclav Skala

Publisher & Author Service Department & Distribution:
Vaclav Skala - UNION Agency
Na Mazinach 9
CZ 322 00 Plzen
Czech Republic
Reg.No. (ICO) 416 82 459

Published in cooperation with the University of West Bohemia
Univerzitní 8, 306 14 Pilsen, Czech Republic

DOI: <http://www.doi.org/10.24132/CSRN.QC.2025-A0>

ISSN 2464-4617 (Print)

ISSN 2464-4625 (online)

CSRN 3502

International Program Committee

QC-Horizon 2025

Quantum Informatics, Computing & Technology 2025

Bharadwaj, Sachin,S.New York University, USA

Di Molfetta, Giuseppe - Aix-Marseille University, France

Kais, Sabre - North Carolina State University, USA

Mateus, Paulo - Universidade de Lisboa, Portugal

Mezzini, Mauro - Roma Tre University, Italy

Möller, Matthias - Delft University of Technology, The Netherlands

Pelayo, Fernando,L. - University of Castilla-La Mancha, Spain

Petrosyan, David - Foundation for Research and Technology-Hellas (FORTH), Greece

Phillipson, Frank - Maastricht University, Netherlands

Sagaut, Pierre - Aix-Marseille University, France

Skala, Vaclav - University of West Bohemia, Czech Republic

Sreenivasan, Katepalli,R. - New York University, USA

CSRN 3502

Board of Reviewers

QC-Horizon 2025

Quantum Informatics, Computing & Technology 2025

Ambika Sasikumar, Arun (USA)	Möller, Matthia (The Netherlads)
Bayro-Corrochano, Eduardo (Poland)	Nandy Pal, Mahua (India)
Bharadwaj, Sachin,S. (USA)	Park, Seongbin (Korea)
Di Molfetta, Giuseppe (France)	Pelayo, Fernando,L. (Spain)
Gayathri, S.S. (India)	Peng, Zedong (USA)
Gouri, Faiz (USA)	Petrosyan, David (Greece)
Grigoryan, Artyom (USA)	Phillipson, Frank (The Netherlands)
Gutti, Chandu (USA)	Polepalli, Shashidhar Reddy (USA)
Holla, Hariprasad (USA)	Puchhakayala, Raghavender (USA)
Challenger, Moharram (Belgium)	Sagaut, Pierre (France)
Chatterjee, Avimita (USA)	Skala, Vaclav (Czech Rep.)
Irujolla, Sridhar (USA)	Soni, Jayesh (USA)
Jansi, K.R. (India)	Soni, Jayesh (USA)
Kais, Sabre (USA)	Sriman, B. (India)
Konofaos, Nikos (Greece)	Srinivasan, Parthasarathy (USA)
Kotha, Sudarshan (USA)	Tuama, Hussein (Hungary)
Krishnama, Chatanya Reddy (USA)	Wang, Yan (USA)
Kushimo, Tunde (USA)	Wu, Cheng (USA)
Liu, Pengyu (USA)	Xenakis, Apostolos (Greece)
Mateus, Paolo (Portugal)	Yeleswarapu, Ganapathi (USA)
Mezzini, Mauro (Italy)	

CSRN 3502**Board of Reviewers****QC-Horizon 2025****Quantum Informatics, Computing & Technology 2025****Contents**

	Title	Page
Keynote Talks		
•	Xie,S., Kais,S.: Quantum Energy Teleportation without Classical Communication	1
•	Wu,Ch.-H.: Nonlocal quantum computing theory	9
•	Bayro-Corrochano,E.: Geometric Algebra in Quantum Computational Intelligence	13
Research Papers		
•	Bunk,N., Govaers, F.: Bayesian Update Step Using Adiabatic Quantum Computing	21
•	Polat,F., Tuncer,H., Gholipour,H., Neves,J., Challenger,M.: Model-driven development of heterogeneous quantum models for multi-vehicle route planning	27
•	Chouraqui,F.: Applications of the Tracy-Singh product of matrices in quantum computation	37
•	Raheman,A., Bhagat,T., RahemanF.: Quantum -Resilient User-Evasive Cryptographic Authenticatuon (QRUECA) for WEB 3.0 Sec in the Post-Quantum Era	45
•	Franco,C., De la Cruz,H., Pelayo,F., Pascual,V., Mezzini,M., Paulet,J., Cuartero,F.: Extending Bloch Sphere model to a 2-qubits system	53
•	Skarlatos,V., Kydros,A., Konofaos,N.: Adaptive Entanglement Purification for Real-Time Quantum Noise Mitigation in Fiber-Optic Qubit Channels	63
•	Leporini,R., Bertini,C.: Quantum-inspired classifiers	73
•	Choi,E., Kim,J.E., Wang,Y.: Variational Quantum Eigen-Decomposition Preconditioning Method for Solving Computational Mechanics Problems	79
•	Peng,Z., Roux,D., Bernal Neira,D.E.: Hybrid Quantum Branch-and-Bound Method for Quadratic Unconstrained Binary Optimization	87
•	Zhu,Z., Gaberle,C., Neuwirth,S., Lippert,T., Jattana,M.: Q-AIM: A Unified Portable Workflow for Seamless Integration of Quantum Resources	97
•	Tuoam,H., Imre,S.: Design and Evaluation of Quantum OFDMA under Depolarization Conditions	107
•	Grigoryan,A., Gomez,A., Espinoza,I., Agaian,S.: Quantum Signal-Induced Heap Transform Based Realization of Multi-Qubit Operations	117

- Desdentado,E., Polo,M., Calero,C., Moraga,M.A.: Studying how changes on the transpilation and the number of shots can be used to optimize quantum circuits 121
- Evangelides,P.: Theta Function Framework for Quantum Systems with Magnetic Flux 127

Poster

- Kim,S., Seo,J., Kim,M., Kim,Y., Baek,S., Park,S.: Introducing the hidden subgroup problem in discrete mathematics class 135

Quantum Informatics, Computing & Technology 2025

QC–HORIZON 2025

Preface

The QC–HORIZON 2025 Conference on *Quantum Informatics, Computing & Technology* was held online on August 26, 2025, under the auspices of the **www.QC-Horizon.eu** initiative. Originally intended as an in-person event, the conference was successfully conducted entirely online via Zoom due to the prevailing world security and political situation. This change of format allowed broader international participation while maintaining the high standards of scientific exchange and collaboration that the conference series represents.

The aim of QC–HORIZON 2025 was to bring together leading experts from academia, industry, and defense sectors to explore the rapidly advancing field of quantum computing. The conference served as a forum to present new findings, exchange ideas, and stimulate collaborations in areas spanning quantum informatics, algorithms, architectures, communication, and applications. The guiding motto of the event emphasized its mission:

“The QC–Horizon conference will bring together leading experts from academia, industry, and defense sectors to explore the rapidly advancing field of quantum computing. It aims to uncover emerging breakthroughs, share insights, and support collaborations to drive quantum innovation and impact across various topics and applications.”

The conference program included keynote talks, regular presentations, and discussions covering a wide spectrum of topics in quantum science and technology.

We were honored to welcome distinguished keynote speakers:

- **Sabre Kais**, North Carolina State University, North Carolina, USA
Modulator-Assisted Local Control of Quantum Battery via Zeno Effect
- **Cheng Wu**, Missouri University of Science and Technology, USA
Nonlocal quantum computing theory.
- **Eduardo Bayro-Corrochano**, Poznan University of Technology, Poland
Geometric Algebra in Quantum Computational Intelligence.

More than 65 participants joined the conference online, with the 21 research papers originating from institutions across the world, demonstrating the truly international scope and strong global support for the event.

The proceedings presented in this issue of the *Computer Science Research Notes (CSRN)* reflect the diversity and depth of the contributions. They include theoretical advances, algorithmic developments, implementation studies, and application-oriented research, all of which highlight the transformative potential of quantum computing for science, technology, and society.

We express our deep gratitude to all authors, reviewers, and participants for their valuable contributions and engagement. Special thanks are due to the organizing and technical teams who ensured that the transition to an online format was smooth and effective. Their dedication made QC-HORIZON 2025 a successful and memorable event.

We hope that this collection of research papers will inspire further advances and collaborations in the quantum computing community. We look forward to future editions of QC-HORIZON and to continuing the tradition of fostering innovation and dialogue in this rapidly evolving field.

Sabre Kais
North Carolina State University
Raleigh, North Carolina
USA
ORCID: 0000-0003-0574-5346

Vaclav Skala
University of West Bohemia
Pilsen
Czech Republic
ORCID: 0000-0001-8886-4281

Quantum Energy Teleportation without Classical Communication

Songbo Xie

Department of Electrical
and Computer
Engineering,
North Carolina State
University,
Raleigh, NC 27606, USA
sxie2@ncsu.edu

Sabre Kais

Department of Electrical
and Computer
Engineering,
Department of Chemistry,
North Carolina State
University,
Raleigh, NC 27606, USA
skais@ncsu.edu

ABSTRACT

Quantum energy teleportation (QET) is a protocol that unlocks the extraction of local energy and has been thought to fundamentally require classical communication (CC), since Bob must normally learn Alice's measurement outcome to perform the proper conditional operation (CO). In this work, we demonstrate that CC itself can be removed for the purpose of QET: When Bob's local operation is implemented through a weak coupling to an auxiliary qubit, the interaction naturally adapts to Alice's post-measurement state, thereby realizing the necessary CO without any classical message. This establishes a CC-free form of QET, which broadens its conceptual scope and suggests practical applications such as indirect external control for charging of quantum batteries.

Keywords

Quantum energy teleportation, classical communication, rotating wave approximation, conditional operation

1 INTRODUCTION

Quantum state teleportation (QST) is a well-recognized protocol in quantum information science, enabling the transfer of an arbitrary quantum state between spatially separated parties [BBC⁺93, BPM⁺97, FSB⁺98]. Its validity has been extensively demonstrated through numerous experimental implementations [UJA⁺04, JRY⁺10, MHS⁺12, RXY⁺17]. The protocol requires a shared pair of entangled qubits between the sender (Alice) and the receiver (Bob), as well as a classical communication channel for transmitting two classical bits. Thus, QST intrinsically relies on both quantum entanglement and classical communication. Importantly, it is well understood that the physical energy associated with the teleported state is not transmitted from Alice. Instead, it is supplied locally by Bob during the state reconstruction process.

In parallel, Hotta introduced quantum energy teleportation (QET), a protocol that enables local energy transfer [Hot09a, Hot11]. First proposed in spin-chain

systems [Hot08a], QET has since been generalized to various settings, ranging from relativistic quantum field theory and black-hole physics to trapped ions, harmonic oscillators, and topological phases [Hot08b, Hot10a, Hot09b, Hot10c, Ike23b]. Its relevance to condensed matter and quantum information science has also been explored, including connections to quantum Hall systems, squeezed states, and Gibbs spin models [YIH11, HMY14, FGH13, TH15, IL24]. On the experimental side, initial demonstrations have been reported in NMR platforms and superconducting circuits [RBKML23, Ike23a, XSK24]. Recent developments highlight long-range QET protocols enabled by combining QST with QET [Ike23c], trade-off relations between the two schemes [WY24], and links to quantum steering [FWW⁺24].

At first glance, one might be tempted to interpret QET as a protocol for transferring energy between distant locations, analogous to how QST transfers quantum states [Hot09a, Hot11]. Such an interpretation, however, could be misleading and potentially problematic, as it appears to conflict with relativistic causality. A more careful analysis reveals that QET does not directly teleport energy. Instead, what restricts local energy extraction is the principle of strong local passivity (SLP) [FFH14, ASRB⁺19]. QET acts as a protocol to overcome SLP: it does not transmit energy itself, but rather leverages classical communication to unlock local en-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ergy from systems that would otherwise remain energetically passive [RBKMML23].

In its original formulation, QET was argued to require four elements: (i) ground-state preparation, (ii) shared entanglement, (iii) Alice's measurement operators commuting with the interaction Hamiltonian, and (iv) classical communication. These conditions, once proposed, have since been widely adopted in subsequent studies. However, from the perspective of SLP, the first three conditions should be regarded as sufficient but not necessary for a system to exhibit SLP and thereby necessitate the use of QET. Recent work has shown that SLP can be present even in the absence of these conditions [XSK25]. This suggests that the traditional requirements can be relaxed, thereby enabling a broader conceptual framework for discussions and practical implementations of QET.

Despite these relaxations, the fourth requirement of classical communication (CC) still remains: Bob must receive information from Alice in order to perform the proper conditional operation (CO) that breaks his local SLP. At first glance, it seems unavoidable that CO necessarily implies CC.

However, relying on CC can introduce several drawbacks. From a security standpoint, the classical channel is vulnerable to interception, allowing an eavesdropper to obtain Alice's measurement outcomes. From a physical standpoint, CC is constrained by the speed of light, which limits the rate at which the protocol can be executed over long distances, thus restricting efficiency. At the microscopic scale, implementing CC can be challenging, since both Alice and Bob may themselves be microscopic quantum systems. Furthermore, transmitting classical signals carries an energy cost, which can render CC impractical in resource-limited environments.

These considerations motivate the question: Can the requirement of CC be eliminated while retaining CO? If so, all four traditional QET requirements would effectively be eliminated.

At first glance, eliminating CC may appear impractical, as it seems to risk violating relativistic constraints. However, our recent investigations indicate that a positive answer is possible, which we now explain.

2 REVIEW ON THE MINIMAL MODEL OF QET

To begin, we briefly review the original minimal model of QET introduced in [Hot10b], which involves two qubits, A and B , shared between two distant parties, Alice and Bob. The Hamiltonian is

$$H_{AB} = -hZ_A - hZ_B + 2\kappa X_A \otimes X_B, \quad (1)$$

where h and κ are positive constants, and X_i and Z_i (with $i \in \{A, B\}$) denote the Pauli operators for qubit

i . The two qubits are initially prepared in the ground state $|g\rangle$ of H_{AB} , given by

$$|g\rangle = \cos(\theta)|00\rangle_{AB} - \sin(\theta)|11\rangle_{AB}, \quad (2)$$

with $\tan(2\theta) \equiv \kappa/h$. Since the ground state has the lowest possible energy, neither Alice nor Bob can locally extract the energy from $|g\rangle$.

To enable energy extraction, the QET protocol requires Alice to perform a local measurement using the operators $\{|+\rangle\langle+|, |-\rangle\langle-|\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice's measurement disturbs the ground state $|g\rangle$, thus injecting energy into the system. Because her measurement operators commute with the interaction Hamiltonian, the injected energy remains localized at Alice's site, only raising the expectation value $\langle -hZ_A \rangle$. One can verify that Bob, by any local general operation (which can be characterized by a general set of Kraus operators) alone, cannot reduce the expectation value $\langle H_{AB} \rangle$, which means that his local energy extraction is forbidden.

For Bob to extract energy, Alice must send her measurement result (+ or -) via classical communication. Based on this information, Bob applies the CO:

$$G_{\pm} \equiv \exp[\pm i(\phi - \theta)Y], \quad (3)$$

where $\tan(2\phi) \equiv 2\kappa/h$ and Y is the Pauli- Y operator. One can show that, this CO reduces the expectation value $\langle H_{AB} \rangle$, indicating that Bob has successfully extracted energy locally with the help of CC.

At first glance, the sequence of steps suggests the following interpretation: the system begins in the ground state with no available energy, Alice injects energy on her side, and after transmitting classical information, Bob extracts energy on his side. Importantly, the entire process can be executed on a time scale limited only by the speed of classical communication, which is much faster than the intrinsic dynamics of H_{AB} . As a result, energy cannot naturally propagate from Alice to Bob during this interval. Consequently, the protocol appears to mimic the teleportation of energy between distant parties, with the classical channel enforcing causality by restricting the transfer speed to that of light. Such reasoning seems to justify the protocol's name: "quantum energy teleportation."

However, a closer inspection shows that this interpretation is misleading. Bob's local operations commute with Alice's local Hamiltonian term, $H_A = -hZ_A$, so Alice's injected energy, $\langle H_A \rangle$, remains unaffected by Bob's actions. This implies that the energy Bob extracts does not originate from Alice. Instead, consider the part of the Hamiltonian accessible to Bob,

$$H'_B \equiv -hZ_B + 2\kappa X_A \otimes X_B. \quad (4)$$

Although $|g\rangle$ is the ground state of the full Hamiltonian H_{AB} , it is an excited state of H'_B . From this perspective,

Alice's message enables that Bob extracts energy from an excited state, which is not surprising in itself. What is indeed surprising is the opposite fact: why energy extraction is forbidden from such excited states without Alice's message. The answer lies in the principle of *strong local passivity* (SLP).

Formally, a state ρ is SLP with respect to a Hamiltonian H if no local operation on Bob's side can reduce the system's energy, i.e.,

$$\text{Tr}[H(I_A \otimes G_B)\rho - H\rho] \geq 0 \quad (5)$$

for all completely positive trace-preserving (CPTP) maps G_B . In fact, after Alice's measurement, even though energy is injected into the system, the resulting state is still SLP, thereby preventing Bob's local energy extraction. The classical message from Alice provides Bob with just enough information to break the SLP restriction. In this sense, QET does not literally teleport energy. Instead, it serves as a key to unlock energy that would otherwise remain inaccessible due to SLP.

In constructing this minimal model, four specific requirements have been imposed: (i) ground-state preparation, (ii) shared entanglement, (iii) Alice's measurement commuting with the interaction Hamiltonian, and (iv) classical communication. As the above analysis shows, the first three conditions are sufficient to establish SLP and thus block Bob's energy extraction. However, they are not strictly necessary. In what follows, we demonstrate a related system where the first three conditions are relaxed, yet SLP still emerges. Consequently, Bob still requires Alice's message to perform local energy extraction, thereby broadening the applicability of QET.

3 A FAMILY OF SYSTEMS WITH THE FIRST THREE REQUIREMENTS RELAXED

Here, we provide a method to construct a family of systems that can exhibit SLP with the first three of the above requirements relaxed. We begin with the parameterized spectrum of a general two-qubit Hamiltonian, whose four eigenvalues and eigenvectors are given by

Eigenvalues	Eigenvectors
\mathcal{E}_4	$ v_4\rangle = \psi^\perp\rangle \otimes \phi^\perp\rangle$
\mathcal{E}_3	$ v_3\rangle = 1\rangle \otimes \phi\rangle$
\mathcal{E}_2	$ v_2\rangle = 0\rangle \otimes \phi\rangle$
\mathcal{E}_1	$ v_1\rangle = \psi\rangle \otimes \phi^\perp\rangle$

where the hierarchy $\mathcal{E}_1 < \mathcal{E}_2 < \mathcal{E}_3 < \mathcal{E}_4$ is assumed. The single-qubit states can be parameterized as (phases omitted for simplicity):

$$\begin{aligned} |\phi\rangle &= \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle, \\ |\phi^\perp\rangle &= \sin(\alpha)|0\rangle - \cos(\alpha)|1\rangle, \\ |\psi\rangle &= \cos(\beta)|+\rangle + \sin(\beta)|-\rangle, \\ |\psi^\perp\rangle &= \sin(\beta)|+\rangle - \cos(\beta)|-\rangle. \end{aligned} \quad (6)$$

The total Hamiltonian is then

$$H_{AB} = \sum_i \mathcal{E}_i |v_i\rangle\langle v_i|. \quad (7)$$

We set the initial state to $|v_2\rangle$, which is an excited state without entanglement, and let Alice measure her qubit in the Pauli-X basis. The joint post-measurement states are then

$$|+\rangle_A \otimes |\phi\rangle_B, \quad |-\rangle_A \otimes |\phi\rangle_B, \quad (8)$$

each occurring with probability 50%.

For simplicity, we choose the energy spectrum such that $\mathcal{E}_4 = -\mathcal{E}_1 = \mathcal{E} > 0$ and $\mathcal{E}_3 = -\mathcal{E}_2 = \mathcal{F} > 0$. Other choices are possible, but they lead to more general (and more complicated) analyses.

To proceed, we introduce the concept of Bob's *local effective Hamiltonian* (LEH). When Alice's qubit is in state $|i\rangle$, Bob's LEH is defined as

$$H_{\text{eff}}^i = \langle i|H_{AB}|i\rangle. \quad (9)$$

As explained in [XSK25], this LEH has two key roles. First, Bob's energy expectation under H_{eff}^i coincides with the total system energy: if Bob's state is $|j\rangle$, then $\langle j|H_{\text{eff}}^i|j\rangle = \langle H_{AB} \rangle$. Thus, after Alice's measurement, for Bob to extract energy locally, he rotates his state to the ground state of H_{eff}^i . Since this ground state depends on Alice's outcome, the required rotation necessarily depends on Alice's message. This explains the need for conditional operations. Second, when Alice's qubit is frozen to $|i\rangle$, LEH has dynamical effects: Bob's state evolves under H_{eff}^i .

In this model, Bob's LEHs are

$$\begin{aligned} H_{\text{eff}}^+ &= -\mathcal{E} \cos(2\beta) |\phi^\perp\rangle\langle\phi^\perp|, \\ H_{\text{eff}}^- &= +\mathcal{E} \cos(2\beta) |\phi^\perp\rangle\langle\phi^\perp| = -H_{\text{eff}}^+. \end{aligned} \quad (10)$$

Because $\langle\phi|\phi^\perp\rangle = 0$, Bob's post-measurement state $|\phi\rangle$ is an eigenstate of both H_{eff}^\pm . Depending on the sign of $\cos(2\beta)$, it is the ground state in one case and the excited state in the other. Consequently, any local operation by Bob cannot extract energy *on average*: energy extracted in one case is exactly offset by energy injected in the other. The equal mixture of Eq. (8) therefore satisfies the SLP condition, preventing Bob from extracting energy locally after Alice's measurement.

Nevertheless, classical communication restores the possibility of local energy extraction. Upon receiving Alice's message, Bob learns whether his state is the ground state or the excited state. If it is the ground state, he applies the identity operation. If it is the excited state, he applies a π rotation to map the state to $|\phi^\perp\rangle$, thereby extracting energy on average from the system.

In addition, the authors of [ASRB⁺19] provided a necessary and sufficient condition to determine whether a given state is SLP with respect to a Hamiltonian. Using this criterion, one can verify that for arbitrary values of α and β in Eq. (6), the initial state $|v_2\rangle\langle v_2|$ is SLP for H_{AB} on Bob's side. Furthermore, the post-measurement mixed state obtained from Eq. (8) also remains SLP on Bob's side. This construction thus yields a two-parameter family of Hamiltonians exhibiting SLP both for an excited initial state and for the corresponding post-measurement state. Entanglement is absent throughout the entire process. Moreover, Alice's measurement basis (Pauli- X) need not commute with the interaction term in Eq. (7). This demonstrates that the first three requirements mentioned above are relaxed in this construction. The result highlights the necessity of QET for enabling local energy extraction in broader scenarios and applications.

4 CAN CLASSICAL COMMUNICATIONS BE REMOVED FROM QET?

Up to this moment, classical communication (CC) has been regarded as a necessary component of QET. While conditional operations (CO) are indeed essential for breaking SLP, it has not been explicitly proven that CC itself is as essential. This naturally raises the question: can CO be achieved without CC? We show that the answer is affirmative.

Recall the second role of Bob's LEH: it governs dynamical evolution. When Alice's qubit is frozen in the post-measurement state, Bob's qubit evolves under the corresponding LEH. Consequently, the eigenstructure of Bob's qubit depends on Alice's measurement outcome. Suppose now that Bob couples his qubit B to a third qubit C , with the coupling assumed to be weak compared to both the natural frequencies of all qubits and the AB coupling. In this regime, the Rotating Wave Approximation (RWA) can be applied. Under the RWA, the BC interaction Hamiltonian is expressed in the eigenbasis of qubit B , with fast-oscillating terms omitted. As a result, the BC interaction itself becomes dependent on the H_B^{eff} , and thus on Alice's measurement outcome. When the BC interaction is viewed as a general operation on qubit B , this operation thus becomes conditional on Alice's measurement outcome, thereby eliminating the need for classical communication.

Specifically, we consider three qubits interacting via the Hamiltonian

$$H_{ABC} = H_A + V_{AB} + H_B + V_{BC} + H_C. \quad (11)$$

Without loss of generality, suppose Alice's measurement is in the basis $\{|0\rangle, |1\rangle\}$. Bob's two LEHs are then

$$\langle i|_A V_{AB} |i\rangle_A + H_B, \text{ with } i = \{0, 1\} \quad (12)$$

and the resulting energy offset achievable through this process is on the order of $|V_{AB}|$.

For the BC coupling, since we want that CC is removed, Bob does not know Alice's outcome and therefore cannot introduce outcome-dependent parameters. Instead, Bob simply switches on the BC interaction immediately after Alice's measurement and turns it off after a fixed time interval. This procedure requires no CC. The interaction with the auxiliary qubit C for a fixed duration constitutes a general local operation on qubit B . If SLP holds, such an operation cannot extract energy from the AB system governed by $H_{AB} \equiv H_A + V_{AB} + H_B$.

Also, since the BC coupling must remain sensitive to changes in the eigenstructure of qubit B , it enforces the condition

$$|V_{BC}| \ll |V_{AB}|, \quad (13)$$

namely, that the BC coupling is weaker than the AB coupling.

One important aspect still needs to be considered. The characteristic timescale for Bob's energy extraction is $T_{BC} \sim 1/|V_{BC}|$, while the intrinsic evolution timescale of the AB system is $T_{AB} \sim 1/|H_{AB}|$. Clearly, this leads to $T_{BC} \gg T_{AB}$, meaning that Bob's energy extraction is much slower than the natural evolution of the AB system. However, one of the main advantages of QET is precisely that energy extraction can occur *faster* than the system's intrinsic evolution. This ensures that QET is a useful protocol for accessing localized energy. Otherwise, once Alice injects energy locally, Bob could simply wait for the energy to propagate naturally to his side and extract it in a time on the order of T_1 . If $T_1 \ll T_2$, it would appear unnecessary to invoke QET to break SLP, since waiting would be faster.

This issue can be avoided by choosing the two post-measurement states to be eigenstates of H_{AB} . In this case, Alice's measurement injects energy into the system, but because the post-measurement states are stationary, the injected energy remains localized at Alice's site and does not propagate to Bob. To achieve this, we require a system satisfying three conditions: (i) the post-measurement mixed state is SLP with respect to H_{AB} , so that Bob cannot locally extract energy; (ii) the two post-measurement pure branch states are eigenstates of H_{AB} , so that their mixture remains SLP without further disturbance; (iii) not all of the post-measurement pure branch states are ground states of

their corresponding LEHs, which ensures that Bob can, in principle, use QET to break SLP and extract local energy.

As an explicit example, we construct a system where CC can be removed from QET. Defining $H_{AB} \equiv H_A + V_{AB} + H_B$, we consider the Hamiltonian

$$H_{AB} = -Z_A \otimes \mathbb{I}_B + X_A \otimes X_B. \quad (14)$$

Here, for simplicity, we have set $H_B = 0$. A nonzero H_B can also be included without altering the essential physics, as discussed in [XSAK25]. The eigenstructure of this Hamiltonian is given by Table 1.

Eigenvalues	Eigenvectors
$\lambda_4 = \sqrt{2}$	$ v_4\rangle = \tilde{-}\rangle \otimes - \rangle$
$\lambda_3 = \sqrt{2}$	$ v_3\rangle = \tilde{1}\rangle \otimes +\rangle$
$\lambda_2 = -\sqrt{2}$	$ v_2\rangle = \tilde{0}\rangle \otimes +\rangle$
$\lambda_1 = -\sqrt{2}$	$ v_1\rangle = \tilde{+}\rangle \otimes - \rangle$

Table 1: The eigenstructure of H_{AB} in Eq. (14).

Here, we define $|\tilde{\varphi}\rangle \equiv \exp(i\sigma_y\pi/8)|\varphi\rangle$. The tilde thus denotes a rotation of an arbitrary state $|\varphi\rangle$ around the y -axis.

We choose the initial state to be an equal superposition of $|v_2\rangle$ and $|v_3\rangle$:

$$|\tilde{+}_A\rangle \otimes |+\rangle_B \equiv \frac{1}{\sqrt{2}} \left(|\tilde{0}\rangle_A + |\tilde{1}\rangle_A \right) \otimes |+\rangle_B. \quad (15)$$

Alice measures her qubit A using the projectors $|\tilde{0}\rangle\langle\tilde{0}|$ and $|\tilde{1}\rangle\langle\tilde{1}|$, leading to the following two possible outcomes, each with probability 50%:

Outcome	Bob's local Hamiltonian
$ v_2\rangle = \tilde{0}\rangle \otimes +\rangle_B$	$H_B^{\text{eff}} = -X_B/\sqrt{2}$
$ v_3\rangle = \tilde{1}\rangle \otimes +\rangle_B$	$H_B^{\text{eff}} = +X_B/\sqrt{2}$

We now revisit the three conditions that we just outlined for removing CC in QET. First, the post-measurement mixed state $\mathbb{I}_A \otimes |+\rangle\langle+|_B$ is SLP for Eq. (14), as can be verified using the method in [ASRB⁺19]. This prevents Bob from locally extracting energy on average. Second, the two post-measurement states $|v_2\rangle$ and $|v_3\rangle$ are eigenstates of H_{AB} , so the system remains stationary after Alice's measurement and SLP persists. Third, in the

traditional QET protocol, Bob can still extract energy once Alice communicates her measurement outcome: if the outcome is $|\tilde{0}\rangle$, Bob's local Hamiltonian is $\sim -X_B$, where $|+\rangle$ is already the ground state, so he performs the identity operation. If the outcome is $|\tilde{1}\rangle$, Bob's local Hamiltonian is $\sim X_B$, where $|+\rangle$ is the excited state, so he applies the operation $|+\rangle\langle-| + |- \rangle\langle+|$. In this way, Bob locally extracts energy on average. However, this scheme of energy extraction still requires CC. The question remains: how can we remove CC while retaining CO, as demanded by QET?

As pointed out earlier, the key idea is to implement Bob's local general operation by coupling his qubit B to an auxiliary qubit C . We choose the Hamiltonian

$$V_{BC} = g(X_B \otimes X_C + Y_B \otimes Y_C), \quad H_C = -Z_C/\sqrt{2}, \quad (16)$$

where g is the BC coupling strength. Qubit C is initialized in its ground state $|0\rangle$ to serve as the recipient of energy from qubit B .

We let Alice's qubit A be frozen in its post-measurement state, either $|\tilde{0}\rangle$ or $|\tilde{1}\rangle$. This can be achieved, for instance, by repeated projective measurements in the $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ basis, or by repeatedly applying the operator $|\tilde{0}\rangle\langle\tilde{0}| - |\tilde{1}\rangle\langle\tilde{1}|$ as a form of bang-bang control, as introduced in [XSAK25]. Afterward, Bob's qubit B evolves under its local effective Hamiltonian $\mp X_B/\sqrt{2}$. In the conventional QET approach, Bob would apply a *fast* local operation (e.g., via classical pulses), which cannot extract energy on average. This corresponds to the regime $g \gg 1$ in Eq. (16). We now demonstrate that when $g \ll 1$, the BC interaction itself becomes dependent on Alice's measurement outcome and automatically implements the desired CO.

When $g \ll 1$ in Eq. (16), the Rotating Wave Approximation (RWA) can be applied, neglecting fast-oscillating terms. Here, the notion of "fast" and "slow" depends on the eigenstructures of H_B^{eff} and H_C .

Case 1: $H_B^{\text{eff}} = -X_B/\sqrt{2}$.

In this case, the BC interaction expands to

$$\begin{aligned} V_{BC} &= 2g|1\rangle\langle 0| \otimes |0\rangle\langle 1| + 2g|0\rangle\langle 1| \otimes |1\rangle\langle 0| \\ &= g(|+\rangle\langle+| + |+\rangle\langle-| - |- \rangle\langle+| - |- \rangle\langle-|) \otimes |0\rangle\langle 1| \\ &\quad + g(|+\rangle\langle+| - |+\rangle\langle-| + |- \rangle\langle+| - |- \rangle\langle-|) \otimes |1\rangle\langle 0|. \end{aligned} \quad (17)$$

Moving to the Heisenberg picture and assuming weak coupling $g \ll 1$, the Heisenberg equations of motion reduce to

$$\begin{aligned} \frac{d}{dt} \mathcal{O}_B(t) &\approx i[H_B^{\text{eff}}, \mathcal{O}_B(t)], \\ \frac{d}{dt} \mathcal{O}_C(t) &\approx i[H_C, \mathcal{O}_C(t)]. \end{aligned} \quad (18)$$

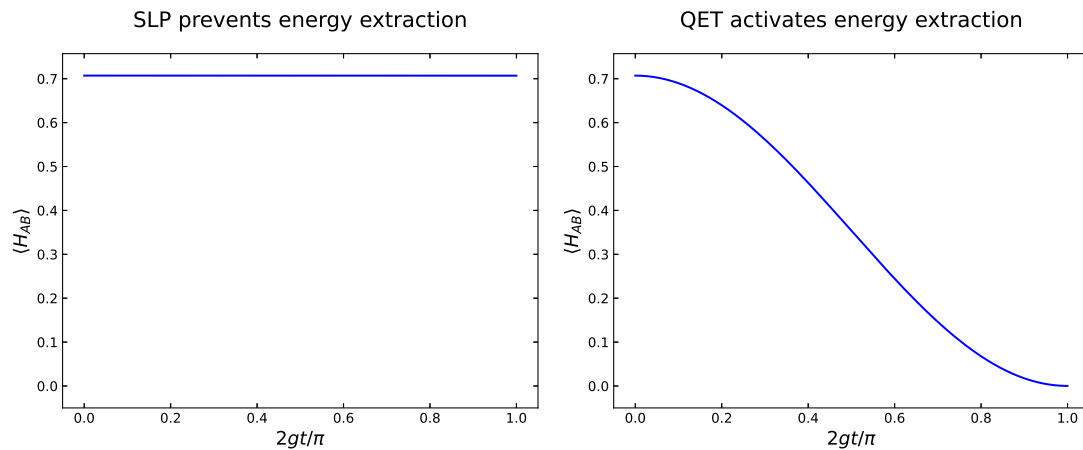


Figure 1: Numerical simulation for quantum energy teleportation without classical communication. Parameters: $g = 0.01$. Alice's operation interval for freezing qubit A: $gt/(5000\pi)$. Left panel: Following Alice's measurement, the AB system enters a stationary SLP state, preventing Bob from extracting local energy. Right panel: When Alice freezes qubit A in the post-measurement state, the BC coupling is activated, enabling Bob's local energy extraction.

This leads to the relations

$$\begin{aligned} |+\rangle\langle+|_B &\sim |-\rangle\langle-|_B \sim 1, \\ |-\rangle\langle+|_B &\sim |1\rangle\langle 0|_C \sim e^{i\sqrt{2}t}, \\ |+\rangle\langle-|_B &\sim |0\rangle\langle 1|_C \sim e^{-i\sqrt{2}t}. \end{aligned} \quad (19)$$

Thus, the slow terms reduce to

$$V_{BC} \approx g|-\rangle\langle+| \otimes |0\rangle\langle 1| + g|+\rangle\langle-| \otimes |1\rangle\langle 0|. \quad (20)$$

Given the initial state $|+\rangle_B|0\rangle_C$, both B and C are in their ground states. This interaction has no effect, corresponding to the identity operation on qubit B .

Case 2: $H_B^{\text{eff}} = +X_B/\sqrt{2}$.

A similar analysis yields

$$\begin{aligned} |+\rangle\langle+|_B &\sim |-\rangle\langle-|_B \sim 1, \\ |+\rangle\langle-|_B &\sim |1\rangle\langle 0|_C \sim e^{i\sqrt{2}t}, \\ |-\rangle\langle+|_B &\sim |0\rangle\langle 1|_C \sim e^{-i\sqrt{2}t}. \end{aligned} \quad (21)$$

leading to

$$V_{BC} \approx g|+\rangle\langle-| \otimes |0\rangle\langle 1| + g|-\rangle\langle+| \otimes |1\rangle\langle 0|. \quad (22)$$

With the initial state $|+\rangle_B|0\rangle_C$, qubit B is excited while C is in its ground state. Choosing the interaction time $t = \pi/(2g)$ results in complete energy transfer from B to C . This corresponds to a π rotation on qubit B .

Consequently, in the weak-coupling regime, the physical process naturally implements a CO on qubit B that precisely matches the operation required for local energy extraction. Specifically, when Alice's outcome is $|0\rangle$, Bob effectively performs the identity operation; when Alice's outcome is $|\hat{1}\rangle$, Bob effectively applies

$|+\rangle\langle-| + |-\rangle\langle+|$, exactly as in the conventional QET protocol. Crucially, this is achieved without any CC: the BC interaction automatically adapts to the appropriate form depending on Alice's outcome. In this way, CO is realized without CC, thereby completing the QET protocol while eliminating the need for classical communication.

For the numerical simulation, see Fig. 1. In the left panel, we show that after Alice's measurement, the system remains SLP for Bob, and coupling to a third qubit C does not allow any energy extraction. By contrast, if Alice repeatedly measures her qubit to freeze A in its post-measurement state, the BC coupling breaks SLP and effectively performs the conditional operation required for Bob to extract energy from the system.

5 DISCUSSIONS AND SUMMARY

In summary, we have reviewed the principle of quantum energy teleportation (QET), which was originally thought to rely on four requirements: (i) ground-state preparation, (ii) shared entanglement, (iii) Alice's measurement commuting with the interaction Hamiltonian, and (iv) classical communication (CC). Recent developments have shown that the first three requirements can be relaxed, yet CC appeared to remain indispensable. In this work, we have demonstrated that when Bob's local operation is implemented in the weak-coupling regime, CC itself can also be removed.

In quantum state teleportation (QST), CC is strictly necessary, as information transfer cannot exceed the speed of light. In QET, however, CC can indeed be eliminated without violating relativistic constraints. This is because in QET, energy is not physically transmitted between Alice and Bob; rather, Bob only extracts local energy.

As one potential application of this CC-free QET protocol, we may reinterpret Bob's two qubits as a charger (qubit B) and a battery (qubit C), while Alice's qubit A acts as an external control switch. When Alice performs a measurement, direct energy transfer from B to C remains forbidden due to SLP. However, once Alice freezes the state of her qubit through repeated operations, the BC coupling is effectively activated, enabling energy transfer between B and C . This provides a concrete realization of indirect external control for charging of quantum batteries, as discussed in [XSAK25].

6 ACKNOWLEDGMENTS

We would like to acknowledge funding from the Office of Basic Energy Sciences Energy Frontier Research Centers program under Award Number DE-SC0025620.

7 REFERENCES

- [ASRB⁺19] Álvaro M Alhambra, Georgios Styliaris, Nayeli A Rodríguez-Briones, Jamie Sikora, and Eduardo Martín-Martínez. Fundamental limitations to local energy extraction in quantum systems. *Phys. Rev. Lett.*, 123(19):190601, 2019.
- [BBC⁺93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993.
- [BPM⁺97] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.
- [FFH14] Michael Frey, Ken Funo, and Masahiro Hotta. Strong local passivity in finite quantum systems. *Phys. Rev. E*, 90(1):012127, 2014.
- [FGH13] Michael R Frey, Karl Gerlach, and Masahiro Hotta. Quantum energy teleportation between spin particles in a gibbs state. *J. Phys. A: Math. Theor.*, 46(45):455304, 2013.
- [FSB⁺98] Akira Furusawa, Jens Lykke Sørensen, Samuel L Braunstein, Christopher A Fuchs, H Jeff Kimble, and Eugene S Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.
- [FWW⁺24] Hao Fan, Feng-Lin Wu, Lu Wang, Shu-Qian Liu, and Si-Yuan Liu. Strong quantum energy teleportation. *Phys. Rev. A*, 110(5):052424, 2024.
- [HMY14] Masahiro Hotta, Jiro Matsumoto, and Go Yusa. Quantum energy teleportation without a limit of distance. *Phys. Rev. A*, 89(1):012311, 2014.
- [Hot08a] Masahiro Hotta. A protocol for quantum energy distribution. *Phys. Lett. A*, 372(35):5671–5676, 2008.
- [Hot08b] Masahiro Hotta. Quantum measurement information as a key to energy extraction from local vacuums. *Phys. Rev. D*, 78(4):045006, 2008.
- [Hot09a] Masahiro Hotta. Quantum energy teleportation in spin chain systems. *J. Phys. Soc. Jpn.*, 78(3):034001, 2009.
- [Hot09b] Masahiro Hotta. Quantum energy teleportation with trapped ions. *Phys. Rev. A*, 80(4):042323, 2009.
- [Hot10a] Masahiro Hotta. Controlled hawking process by quantum energy teleportation. *Phys. Rev. D*, 81(4):044025, 2010.
- [Hot10b] Masahiro Hotta. Energy entanglement relation for quantum energy teleportation. *Phys. Lett. A*, 374(34):3416–3421, 2010.
- [Hot10c] Masahiro Hotta. Quantum energy teleportation with an electromagnetic field: discrete versus continuous variables. *J. Phys. A: Math. Theor.*, 43(10):105305, 2010.
- [Hot11] Masahiro Hotta. Quantum energy teleportation: An introductory review. *arXiv:1101.3954*, 2011.
- [Ike23a] Kazuki Ikeda. Demonstration of quantum energy teleportation on superconducting quantum hardware. *Phys. Rev. Applied*, 20(2):024051, 2023.
- [Ike23b] Kazuki Ikeda. Investigating global and topological orders of states by local measurement and classical communication: Study on spt phase diagrams by quantum energy teleportation. *AVS Quantum Science*, 5(3), 2023.
- [Ike23c] Kazuki Ikeda. Long-range quantum energy teleportation and distribution on a hyperbolic quantum network. *IET Quantum Communication*, 2023.
- [IL24] Kazuki Ikeda and Adam Lowe. Quantum interactive proofs using quantum

- energy teleportation. *Quantum Information Processing*, 23(6):236, 2024.
- [JRY⁺10] Xian-Min Jin, Ji-Gang Ren, Bin Yang, Zhen-Huan Yi, Fei Zhou, Xiao-Fan Xu, Shao-Kai Wang, Dong Yang, Yuan-Feng Hu, Shuo Jiang, et al. Experimental free-space quantum teleportation. *Nature photonics*, 4(6):376–381, 2010.
- [MHS⁺12] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, et al. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, 2012.
- [RBKMML23] Nayeli A Rodríguez-Briones, Hemant Katiyar, Eduardo Martín-Martínez, and Raymond Laflamme. Experimental activation of strong local passive states with quantum information. *Phys. Rev. Lett.*, 130(11):110801, 2023.
- [RXY⁺17] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, 2017.
- [TH15] Jose Trevison and Masahiro Hotta. Quantum energy teleportation across a three-spin ising chain in a gibbs state. *J. Phys. A: Math. Theor.*, 48(17):175302, 2015.
- [UJA⁺04] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger. Quantum teleportation across the danube. *Nature*, 2004.
- [WY24] Jinzhao Wang and Shunyu Yao. Quantum energy teleportation versus information teleportation. *arXiv:2405.13886*, 2024.
- [XSAK25] Songbo Xie, Manas Sajjan, Ashok Ajoy, and Sabre Kais. Modulator-assisted local control of quantum battery via zeno effect. *arXiv preprint arXiv:2506.18276*, 2025.
- [XSK24] Songbo Xie, Manas Sajjan, and Sabre Kais. Extracting and storing energy from a quasi-vacuum on a quantum computer. *arXiv preprint arXiv:2409.03973*, 2024.
- [XSK25] Songbo Xie, Manas Sajjan, and Sabre Kais. Quantum energy teleportation: A novel protocol relaxing previous constraints. *arXiv preprint arXiv:2502.05288*, 2025.
- [YIH11] Go Yusa, Wataru Izumida, and Masahiro Hotta. Quantum energy teleportation in a quantum hall system. *Phys. Rev. A*, 84(3):032336, 2011.

Nonlocal Quantum Computing Theory

Cheng-Hsiao Wu

Missouri Univ. of Science &
Technology
301 W 16th St.
Rolla, Missouri, 65409
chw@mst.edu

Keywords

Non-local, operator-state relations, time crystals, cellular automata architecture

1. INTRODUCTION

As we are entering the centennial year of quantum mechanics theory, a new kind of science from non-local concept is emerging to supplement the existing local theory for science and engineering problems through the investigation of quantum parallel computing. It has been more than 340 years since Issaic Newton and Gottfried Leibniz developed the Calculus/Differential equation approach, from classical mechanics to quantum mechanics, to supplement the algebra approach before that. It is a local theory because an operator is to operate on a function (or a state) at the same location. In addition, the concept of time is introduced as an independent variable as dynamics. This local theory is based on Euclidean geometry imposed by the condition from the addition of two numbers, the starting point of computing. In essence, algebraic computation, matrix operation and differential equation are all local theory and based on Euclidean geometry.

The emerging new kind of science is a non-local theory in the sense that an operator can operate on a function (or an eigen-state) at a proper distance away from each other. Of course, the quantities at two different locations are linked. This non-local concept is to move away from Euclidean to a piece-wise-Euclidean geometry and thus the computation is no longer “addition-rule compatible” for most of the quantum computing, save one. Therefore “universal computer” is not a valid concept. This is realized when we investigate the quantum parallel computing. Computing deals with huge spatially distributed numbers, in a digital or analog numbering system. Thus, spatial relations among those numbers form the rules of computing. In algebraic operations, starting from the addition operation on two strings of numbers, the concept of “carry” was introduced to make the computing a “local” approach. That means with 8 computation states employed, a local (and man-made) processor can sequentially generate two outputs,

“carry” and “sum”, at each step to complete the 16 needed outcomes.

2. ARGUMENTS

Generally, 16 Boolean operations are achieved using transistors to build the 16 logic gates (or through the equivalent minimum-gate approach). Thus, the logic-gate concept is for sequential computing and a von-Neumann (or Charles Babbage) computing architecture is employed. For massive parallel computing, billions of processors are interconnected. The number of interconnections must be at a minimum. This requirement reduces the computer architecture to only one: cellular automata architecture.

Quantum computing is “parallel” computing. All spatially distributed numbers (or the states) are altered in every step through the 16 needed spatial rules to replace the 16 Boolean operations in sequential computing. So, what are those 16 rules? However, the first step is to realize that quantum computing is “rule-based”, not “quantum logic-gate-based”. In this new concept, we can view the entire universe as a giant parallel computer. Spatial relations change the contents of the universe as human beings start observing it.

Non-local operator-state rules can also be viewed as “symbolic substitution” or “pattern transformation/recognition” rules. The graphical transformation process in classical computing already moves us into a GPU concept from the original CPU concept. This is because computing was originally rule-based. But the pattern transformation operation is still performed sequentially. In quantum computing, pattern recognitions are performed simultaneously. Instead of using graphical description, we describe this concept in terms of “non-local operator-state relations” because this is from the terminologies used in quantum mechanics, operators and eigen-states. But it also means an operator is a state at the same time. Thus, the standard textbook notations of local quantum mechanics description cannot be used. With

the understanding that we need 16 nonlocal operator-state rules operated under a cellular automata architecture, we are now able to place the “superposition and entanglement” of electrons into actions for quantum parallel computing.

There are many different types of computing (because there is no such thing as “universal computer” as stated earlier), and they are all to be compared at the Fourier space, the momentum space of atoms. The non-local nature implies “time” is associate with the “space” under consideration and is not an independent variable. This is in sharp contrast with Schrodinger’s differential equation description.

Quantum computing is a parallel “phase” computing from the nature that is executed in the Fourier space. From a chain of atoms in superposition and in entanglement conditions, all eigen-vectors of the same energy across the atomic chain are phase-coupled through the external Fourier transform, the entanglement condition. All the eigen-vectors of different energies within the atom are internally Fourier transformed, in superposition condition. So indeed, superposition and entanglement together establish multi-channel superconducting chain in the atoms, because of the phase relations established across the chain. This can be achieved through photons, instead of phonons in BCS theory.

3. DETAILED DESCRIPTION

First, we provide an equivalent qubit description of quantum computing and then point out the incompleteness of the qubit theory. In a chain of two-level atoms of energies E_1 and E_2 and eigen states, $\bar{S}_1(\ell)$ and $\bar{S}_2(\ell)$, located at position ℓ on the chain, as in Fig. 1, the computation states, $S_1(\ell)$ and $S_2(\ell)$ are from the superpositions (or the Fourier transform) of the two eigen-states and can be written as:

$$\begin{array}{c} \ell \\ \leftarrow a \rightarrow \ell-1 \\ \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} E_2, \bar{S}_2(\ell) \\ E_1, \bar{S}_1(\ell) \end{array} \quad \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} E_2, \bar{S}_2(\ell-1) \\ E_1, \bar{S}_1(\ell-1) \end{array} \end{array} \quad \begin{pmatrix} S_2 \\ S_1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \bar{S}_2 \\ \bar{S}_1 \end{pmatrix}$$

Fig. 1: Hadamard transformation, internal Fourier transform in an atom of two energies.

This is also known as the Hadamard transformation. That simply means at the internal Fourier-transform space, the two eigen-vector form a π and 2π phase difference to generate two computation states. The entanglement between eigen-vector, $\bar{S}_1(\ell)$ and its neighboring one, $\bar{S}_1(\ell-1)$, is π phase difference and between the eigen-vectors, $\bar{S}_2(\ell)$ and $\bar{S}_2(\ell-1)$ has a 2π phase difference. This entanglement is achieved if there is a minimum separation distance, the focal distance, a , such that $\hbar a = \pi$, where \hbar is the wave vector of the lowest energy E_1 . That means entanglement is simply an external Fourier transformation. So, for a small chain

of atoms prepared in an initial configuration of computation states in $S_2 S_1 S_2 S_2$ can be illustrated as in Fig. 2.

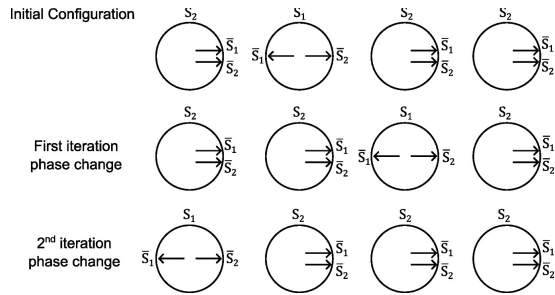


Fig. 2: Computation state phase-changing sequences.

That means in Fourier space, a plane wave is not prepared by a single electron of one energy. Rather they can be two plane waves, extended to infinities with two energies E_1 and E_2 and are prepared by a chain of N atoms under the Fourier transform. Thus, each atom contributes only part of the plane wave for that energy in Fourier space. Say, we have just a pair of electrons ($N=2$) in entanglement at the lowest energy level E_1 . If it is just one atom alone, then it occupies the entire infinite space with a well-defined momentum vector. That would be fine. But it is now occupied only half of the space on the left side and another half space on the right side is occupied by another electron of the same energy and between the left space and right space has a separation distance, a , the focal length, such that $\hbar a = \pi$ is achieved, that is called the entanglement condition. Now both sides of the electron waves can extend to the other side because an electron with well-defined momentum can extend to an infinite space. The net result is eigen-vector, $\bar{S}_1(\ell-1)$, will extend the wave over the distance, a , and gain an additional phase of π and interacts with the eigen vector $\bar{S}_1(\ell)$ such that a non-local operator-state relation, $\bar{S}_1(\ell-1)\bar{S}_1(\ell) = \pi\bar{S}_1(\ell)$, at time, τ , is achieved. In a coherent particle picture, an electron at energy E_1 at $\ell-1$ can travel over the focal distance, a , and gain an additional phase π before interacting with the state, $\bar{S}_1(\ell)$, the eigen vector of the same energy, after a time of τ is consumed. So, τ is just a parameter related to the focal distance, a . Similarly, electrons at energy E_2 can interact at half value of τ . So, a chain of atoms with a sequence of S_1 and S_2 computation states will change the phases according to the four following rules:

- 1) $S_1(\ell-1)S_1(\ell) = S_1(\ell)$
- 2) $S_1(\ell-1)S_2(\ell) = S_2(\ell)$
- 3) $S_2(\ell-1)S_1(\ell) = S_2(\ell)$
- 4) $S_2(\ell-1)S_2(\ell) = S_1(\ell)$

Similarly, for the four time-reversal relations.

Even though non-local operator-state relations can be established, there are only four relations that exist, and we need a complete 16 simultaneous relations to replace the 16 Boolean sequential operations. This points out the deficiencies or the incompleteness of qubit computing theory. A qubit forms a quantum processor at the smallest size and the bit-content of the processor is too small to provide the 16 needed instruction capabilities. Because with two computation states used in a processor, there requires eight instruction capabilities on the tiny processor. This is then not possible to construct.

But this non-local concept described here does show an extended non-local Schrodinger description. Namely, in Fourier space, a Hamiltonian operator (of the kinetic energy part) moves the electron energy located at position $\ell - 1$ over a focal distance, a , to location ℓ and operate on the eigenvector $\bar{S}_1(\ell)$. The net result is a phase of π is added to $\bar{S}_1(\ell)$ after time, τ . The relative phase difference of π value is maintained for \bar{S}_1 eigenvectors between two atoms. Similarly, for \bar{S}_2 eigenvectors, the phase value is maintained at 2π to complete the external Fourier transform.

Thus, an initial computation state configuration will keep changing the phase values over an entire atomic chain and perform perpetual computing. The result is a generation of a space-time Sierpinski triangle of fractals. Sierpinski triangle is where this new kind of science is anchored in. Time crystals, birth-and-death of space-time structures and the development from microscopic structure to mesoscopic and then to macroscopic structure can all be answered by examining the Sierpinski triangle.

But before that, we need to present a proper quantum parallel computing theory with the proper 16 non-local operator-state rules. First is to understand what the proper number of computation states is needed. This is not a trivial question. In local theory when eight computation states are used, there needs two instruction capabilities on the processor. With two computation states employed in qubit theory, there is a need for eight instructions that is too much for a two-state processor to provide. That is obvious problem appeared the Turing adder has already appeared. The correct method is four computation states with four instruction capabilities imposed on the processor. The four computation states are in two layers; computation result is at the lower level and a nutrition level at the top. They are shown in Fig. 3.

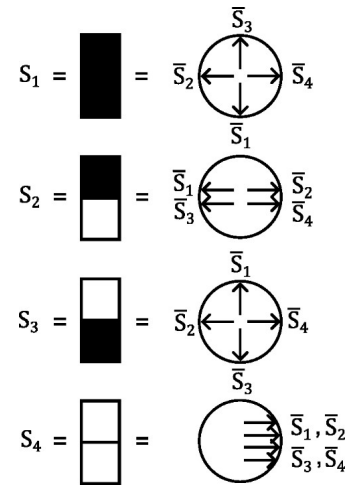


Fig. 3: Superposition of four eigen-states $\bar{S}_1, \bar{S}_2, \bar{S}_3$, and \bar{S}_4 to form four computation states S_1, S_2, S_3 , and S_4 in one atom.

4. RESULTS

The four computation states, S_1, S_2, S_3 , and S_4 , needed means they are generated from the superpositions of four energy levels, or four eigen states, $\bar{S}_1, \bar{S}_2, \bar{S}_3$, and \bar{S}_4 of an atom as shown. The entanglement conditions imposed additional four non-local operator-states relations, tensorial relations shown in Fig. 4(a) and labeled as Rules I, II, III and IV. Fig. 4(a) extends the local theory of quantum mechanics to non-local quantum mechanics in the sense that there exist two mixed-conjugate relations as indicated by Rule II and Rule III. The corresponding computation-state relations are shown in Fig. 4(b) in four possible cyclic distribution of the 16 outcomes.

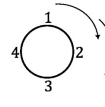
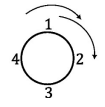
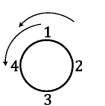
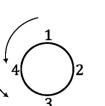
	A) Four Orthogonal Operations	B) Four Computation-State Transition Rules																																								
Rule I	<p>Operator</p> $\bar{S}(\ell-1)$ <table><tr><td>\bar{S}_1</td><td>\bar{S}_2</td><td>\bar{S}_3</td><td>\bar{S}_4</td></tr><tr><td>\bar{S}_1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>\bar{S}_2</td><td>0</td><td>$-\bar{S}_2$</td><td>0</td></tr><tr><td>\bar{S}_3</td><td>0</td><td>0</td><td>$-\bar{S}_3$</td></tr><tr><td>\bar{S}_4</td><td>0</td><td>0</td><td>0</td></tr></table> <p>State $\bar{S}(\ell)$</p>	\bar{S}_1	\bar{S}_2	\bar{S}_3	\bar{S}_4	\bar{S}_1	0	0	0	\bar{S}_2	0	$-\bar{S}_2$	0	\bar{S}_3	0	0	$-\bar{S}_3$	\bar{S}_4	0	0	0	<p>$S(\ell-1)$</p> <table><tr><td>S_1</td><td>S_2</td><td>S_3</td><td>S_4</td></tr><tr><td>S_1</td><td>S_1</td><td>S_2</td><td>S_3</td></tr><tr><td>S_2</td><td>S_2</td><td>S_3</td><td>S_4</td></tr><tr><td>S_3</td><td>S_3</td><td>S_4</td><td>S_1</td></tr><tr><td>S_4</td><td>S_4</td><td>S_1</td><td>S_2</td></tr></table> <p>$S(\ell)$</p> 	S_1	S_2	S_3	S_4	S_1	S_1	S_2	S_3	S_2	S_2	S_3	S_4	S_3	S_3	S_4	S_1	S_4	S_4	S_1	S_2
\bar{S}_1	\bar{S}_2	\bar{S}_3	\bar{S}_4																																							
\bar{S}_1	0	0	0																																							
\bar{S}_2	0	$-\bar{S}_2$	0																																							
\bar{S}_3	0	0	$-\bar{S}_3$																																							
\bar{S}_4	0	0	0																																							
S_1	S_2	S_3	S_4																																							
S_1	S_1	S_2	S_3																																							
S_2	S_2	S_3	S_4																																							
S_3	S_3	S_4	S_1																																							
S_4	S_4	S_1	S_2																																							
Rule II	<p>Operator</p> $\bar{S}^*(\ell-1)$ <table><tr><td>\bar{S}_1^*</td><td>\bar{S}_2^*</td><td>\bar{S}_3^*</td><td>\bar{S}_4^*</td></tr><tr><td>\bar{S}_1^*</td><td>0</td><td>0</td><td>0</td></tr><tr><td>\bar{S}_2^*</td><td>0</td><td>$-\bar{S}_2^*$</td><td>0</td></tr><tr><td>\bar{S}_3^*</td><td>0</td><td>0</td><td>$-\bar{S}_3^*$</td></tr><tr><td>\bar{S}_4^*</td><td>0</td><td>0</td><td>0</td></tr></table> <p>State $\bar{S}(\ell)$</p>	\bar{S}_1^*	\bar{S}_2^*	\bar{S}_3^*	\bar{S}_4^*	\bar{S}_1^*	0	0	0	\bar{S}_2^*	0	$-\bar{S}_2^*$	0	\bar{S}_3^*	0	0	$-\bar{S}_3^*$	\bar{S}_4^*	0	0	0	<p>$S(\ell-1)$</p> <table><tr><td>S_1</td><td>S_2</td><td>S_3</td><td>S_4</td></tr><tr><td>S_1</td><td>S_1</td><td>S_2</td><td>S_3</td></tr><tr><td>S_2</td><td>S_2</td><td>S_1</td><td>S_4</td></tr><tr><td>S_3</td><td>S_3</td><td>S_4</td><td>S_1</td></tr><tr><td>S_4</td><td>S_4</td><td>S_3</td><td>S_2</td></tr></table> <p>$S(\ell)$</p> 	S_1	S_2	S_3	S_4	S_1	S_1	S_2	S_3	S_2	S_2	S_1	S_4	S_3	S_3	S_4	S_1	S_4	S_4	S_3	S_2
\bar{S}_1^*	\bar{S}_2^*	\bar{S}_3^*	\bar{S}_4^*																																							
\bar{S}_1^*	0	0	0																																							
\bar{S}_2^*	0	$-\bar{S}_2^*$	0																																							
\bar{S}_3^*	0	0	$-\bar{S}_3^*$																																							
\bar{S}_4^*	0	0	0																																							
S_1	S_2	S_3	S_4																																							
S_1	S_1	S_2	S_3																																							
S_2	S_2	S_1	S_4																																							
S_3	S_3	S_4	S_1																																							
S_4	S_4	S_3	S_2																																							
Rule III	<p>Operator</p> $\bar{S}(\ell-1)$ <table><tr><td>\bar{S}_1</td><td>\bar{S}_2</td><td>\bar{S}_3</td><td>\bar{S}_4</td></tr><tr><td>\bar{S}_1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>\bar{S}_2</td><td>0</td><td>$-\bar{S}_2$</td><td>0</td></tr><tr><td>\bar{S}_3</td><td>0</td><td>0</td><td>$-\bar{S}_3$</td></tr><tr><td>\bar{S}_4</td><td>0</td><td>0</td><td>0</td></tr></table> <p>State $\bar{S}(\ell)$</p>	\bar{S}_1	\bar{S}_2	\bar{S}_3	\bar{S}_4	\bar{S}_1	0	0	0	\bar{S}_2	0	$-\bar{S}_2$	0	\bar{S}_3	0	0	$-\bar{S}_3$	\bar{S}_4	0	0	0	<p>$S(\ell-1)$</p> <table><tr><td>S_1</td><td>S_2</td><td>S_3</td><td>S_4</td></tr><tr><td>S_1</td><td>S_1</td><td>S_4</td><td>S_3</td></tr><tr><td>S_2</td><td>S_2</td><td>S_1</td><td>S_4</td></tr><tr><td>S_3</td><td>S_3</td><td>S_2</td><td>S_1</td></tr><tr><td>S_4</td><td>S_4</td><td>S_3</td><td>S_2</td></tr></table> <p>$S(\ell)$</p> 	S_1	S_2	S_3	S_4	S_1	S_1	S_4	S_3	S_2	S_2	S_1	S_4	S_3	S_3	S_2	S_1	S_4	S_4	S_3	S_2
\bar{S}_1	\bar{S}_2	\bar{S}_3	\bar{S}_4																																							
\bar{S}_1	0	0	0																																							
\bar{S}_2	0	$-\bar{S}_2$	0																																							
\bar{S}_3	0	0	$-\bar{S}_3$																																							
\bar{S}_4	0	0	0																																							
S_1	S_2	S_3	S_4																																							
S_1	S_1	S_4	S_3																																							
S_2	S_2	S_1	S_4																																							
S_3	S_3	S_2	S_1																																							
S_4	S_4	S_3	S_2																																							
Rule IV	<p>Operator</p> $\bar{S}^*(\ell-1)$ <table><tr><td>\bar{S}_1^*</td><td>\bar{S}_2^*</td><td>\bar{S}_3^*</td><td>\bar{S}_4^*</td></tr><tr><td>\bar{S}_1^*</td><td>0</td><td>0</td><td>0</td></tr><tr><td>\bar{S}_2^*</td><td>0</td><td>$-\bar{S}_2^*$</td><td>0</td></tr><tr><td>\bar{S}_3^*</td><td>0</td><td>0</td><td>$-\bar{S}_3^*$</td></tr><tr><td>\bar{S}_4^*</td><td>0</td><td>0</td><td>0</td></tr></table> <p>State $\bar{S}(\ell)$</p>	\bar{S}_1^*	\bar{S}_2^*	\bar{S}_3^*	\bar{S}_4^*	\bar{S}_1^*	0	0	0	\bar{S}_2^*	0	$-\bar{S}_2^*$	0	\bar{S}_3^*	0	0	$-\bar{S}_3^*$	\bar{S}_4^*	0	0	0	<p>$S(\ell-1)$</p> <table><tr><td>S_1</td><td>S_2</td><td>S_3</td><td>S_4</td></tr><tr><td>S_1</td><td>S_1</td><td>S_4</td><td>S_3</td></tr><tr><td>S_2</td><td>S_2</td><td>S_3</td><td>S_1</td></tr><tr><td>S_3</td><td>S_3</td><td>S_2</td><td>S_4</td></tr><tr><td>S_4</td><td>S_4</td><td>S_1</td><td>S_2</td></tr></table> <p>$S(\ell)$</p> 	S_1	S_2	S_3	S_4	S_1	S_1	S_4	S_3	S_2	S_2	S_3	S_1	S_3	S_3	S_2	S_4	S_4	S_4	S_1	S_2
\bar{S}_1^*	\bar{S}_2^*	\bar{S}_3^*	\bar{S}_4^*																																							
\bar{S}_1^*	0	0	0																																							
\bar{S}_2^*	0	$-\bar{S}_2^*$	0																																							
\bar{S}_3^*	0	0	$-\bar{S}_3^*$																																							
\bar{S}_4^*	0	0	0																																							
S_1	S_2	S_3	S_4																																							
S_1	S_1	S_4	S_3																																							
S_2	S_2	S_3	S_1																																							
S_3	S_3	S_2	S_4																																							
S_4	S_4	S_1	S_2																																							

Fig. 4: (a) Four fundamental diagonal non-local operator-state relations for and operator $\bar{S}_1(\ell-1)$ at location, $\ell-1$, to operate on the state $\bar{S}(\ell)$ at location, ℓ , on the chain. The diagonal results are the states located at ℓ . (b) The four corresponding computation-states are in four complete cyclic form as shown in the four sequences. The inner arrows first and then the outer arrows. The four 16-rule sets are shown as Rule I-IV.

In this new kind of science, the implications of left-right symmetry and time-reversal symmetry are important enough to change our thinking of time symmetry for past and future. Fig. 5 shows the difference between local and non-local concepts of the symmetries.

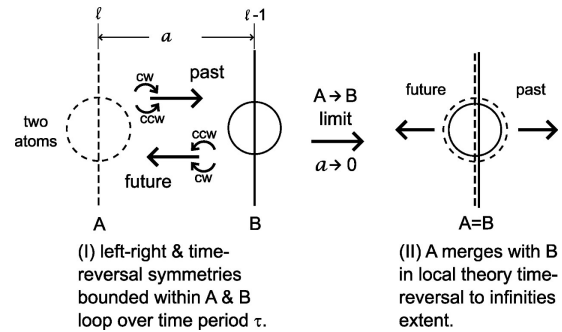


Fig. 5: Origin of time and the change of time symmetry concept from non-local theory to local.

In other words, in Fig. 5 (I), the time arrow from B to A (future) can be constructed clockwise (cw) or counterclockwise (ccw), to establish Rule I and Rule II of Fig. 4. Similarly, the time arrow from A to B (time reversal) can also be constructed through the cw and ccw distinctions to establish Rule III and Rule IV of Fig. 4. Those four symmetries are concurrently applied between two locals, A and B, and they exist at that space scale only. However, when this non-local theory is approaching to the local theory limit, $A \rightarrow B$ as one point as shown in Fig.5(II), the two-time arrows now move to two infinities as past and future. There is an important conceptual change when a non-local concept is reduced to a local concept.

5. CONCLUSION

A nonlocal quantum computing theory is presented here with four parallel 16-rule sets under cellular automata architecture. The deficiencies of the qubit theory are shown and several new physical concepts and consequences are presented to point out the arrival of a new kind of science.

6. REFERENCES

- C. H. Wu and A. Van Horn, *Res. Inventy: Int. J. Eng. Sci.* 10 (2020) 12.
- C. H. Wu, *Int. J. Eng. Sci.* 8 (2019) 1.

Geometric Algebra in Quantum Computational Intelligence

Eduardo
Bayro-Corrochano
Institute of Robotics and
Automation
Poznan University of
Technology
Poznan, Poland
eduardo.bayro@put.poznan.pl

ABSTRACT

Recent advancements in artificial intelligence (AI), machine learning, and quantum computing have positioned quantum machine learning as a transformative field. Quantum computers offer a significant advantage in solving complex problems that are difficult for classical systems, by leveraging quantum algorithms for more efficient computations. These developments open up vast possibilities across a wide range of disciplines. In traditional quantum mechanics, the tensor product is employed to construct multiparticle states and define operators acting on them, serving as a tool to distinguish the Hilbert spaces of individual particles. Alternatively, the geometric algebra framework offers an innovative approach to representing the tensor product through the geometric product, utilizing multivectors. In this paper, we introduce several advanced algorithms, including the Quantum Quaternion Fourier Transform, Quantum Key Distribution, Geometric Algebra Quantum Convolutional Neural Networks, and the Geometric Fuzzy Inference Engine, aimed at enhancing robotic decision-making processes.

Keywords

Quantum Computing, Machine Learning, Geometric Algebra, medical image processing, Quantum Key distribution and Robotics

1 INTRODUCTION

Unlike tensor products, which lack an intuitive geometric interpretation, the geometric product and k-vectors (such as points, lines, planes, and volumes) provide a more natural and visualizable framework. Within this context, entangled quantum states can be reinterpreted as k-vectors, representing structured assemblies of geometric entities, including vectors, planes, volumes, hyperplanes, and hypervolumes. For a comprehensive treatment of quantum theory through the lens of geometric algebra, readers are referred to *Geometric Algebra Applications Vol. III: Integral Transforms, Machine Learning, and Quantum Computing* by E. Bayro-Corrochano (Springer Verlag, 2024).

Quantum machine learning is an emerging interdisciplinary field that merges quantum computing with machine learning techniques. In this lecture, we investigate the foundational principles of quantum machine learning within the geometric algebra framework. Additionally, we present advanced algorithmic approaches, including the Quantum Quaternion Fourier Transform, Geometric Algebra Quantum Convolutional Neural Networks, and the Geometric Fuzzy Inference Engine, with applications in robotic decision-making.

2 GATES IN GEOMETRIC ALGEBRA

Our goal is to use neural networks with neurons that represent gates acting on n -qubits and working in the geometric algebra framework [2, 6]. Thus, we need first to formulate a convenient universal set of quantum gates and then implement them as processing units of neural networks. According to [10], a set of quantum gates $\{\hat{U}_i\}$ is seen as universal if any logical operator \hat{U}_L can be written as

$$\hat{U}_L = \prod_{\hat{U}_i \in \{\hat{U}_i\}} \hat{U}_i. \quad (1)$$

Next, according to the proposed formulations by [4, 6], we will represent simple circuit models of quantum computation with 1-qubit quantum gates in the geometric algebra framework. This subsection is based on the work of Cafaro and Mancini [4].

2.1 The 2-Qubit Space-Time Algebra

Cafaro and Mancini [4] described the 2-Qubit STA; for the sake of completeness, we describe it as well. In the 2-particle algebra there are two bivectors, Ie_3^1 and Ie_3^2 , playing the role of $i_{\mathbb{C}}$. The 2-particle spin states in $B_{[G_3^+ \otimes G_3^+]/E}$. As illustration, the entangled state between

a pair of 2-level systems, called a *spin singlet state*, is formulated as follows:

$$|\psi_{\text{singlet}}\rangle = \frac{1}{2} \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \in \mathbb{H}_2^2. \quad (2)$$

$$|\psi_{\text{singlet}}\rangle \in \mathbb{H}_2^2 \leftrightarrow \psi_{\text{singlet}}^{GA} \in [G_3^+ \otimes G_3^+], \quad (3)$$

where

$$\psi_{\text{singlet}}^{GA} = \frac{1}{2^{\frac{3}{2}}} (Ie_2^1 - Ie_2^2)(1 - Ie_3^1 Ie_3^2). \quad (4)$$

Following the work of Cafaro and Mancini [4], the multiplication by the quantum imaginary $i_{\mathbb{C}}$ for 2-particle states is taken by the multiplication with J from the right.

$$J = E Ie_3^1 = E Ie_3^2 = \frac{1}{2} (Ie_3^1 + Ie_3^2). \quad (5)$$

Henceforth $J^2 = -E$. The action of 2-particle Pauli operators reads

$$\hat{\Sigma}_k \otimes \hat{I} |\psi\rangle \leftrightarrow -Ie_k^1 \psi J, \quad \hat{\Sigma}_k \otimes \hat{\Sigma}_l |\psi\rangle \leftrightarrow -Ie_k^1 Ie_l^2 \psi E, \quad \hat{I} \otimes \hat{\Sigma}_k |\psi\rangle \leftrightarrow -Ie_k^2 \psi J.$$

2.2 Quantum NOT Gate (or Bit Flip Quantum Model)

A nontrivial reversible operation applied to a single qubit is done by means of the NOT operation gate denoted here by $\hat{\Sigma}_1$. Let us apply a 1-qubit quantum gate given by $\psi_q^{GA} = a_0 + a_2 Ie_2$. Then, the $\hat{\Sigma}_1$ is defined as

$$\hat{\Sigma}_1 |q\rangle \stackrel{\text{def}}{=} |q \oplus 1\rangle \leftrightarrow \psi_{|q \oplus 1\rangle}^{GA} \stackrel{\text{def}}{=} e_1(a_0 + a_2 Ie_2)e_3.$$

Since $Ie_i = e_i I$ and $e_i e_j = e_i \wedge e_j$, we obtain

$$\hat{\Sigma}_1 |q\rangle \stackrel{\text{def}}{=} |q \oplus 1\rangle \leftrightarrow \psi_{|q \oplus 1\rangle}^{GA} = -(a_2 + a_0 Ie_2).$$

The action of the unitary quantum gate $\hat{\Sigma}_1^{GA}$ on the basis $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$ is as follows:

$$\begin{aligned} \hat{\Sigma}_1^{GA} : 1 &\rightarrow -Ie_2, \quad \hat{\Sigma}_1^{GA} : Ie_1 \rightarrow Ie_3, \quad \hat{\Sigma}_1^{GA} : Ie_2 \rightarrow \\ &-1, \quad \hat{\Sigma}_1^{GA} : Ie_3 \rightarrow Ie_1. \end{aligned}$$

2.3 Quantum Phase Flip Gate

The reversible operation to a single qubit is the phase flip gate denoted by $\hat{\Sigma}_3$. In the GA framework, the action of the unitary quantum gate $\hat{\Sigma}_3^{GA}$ on the multivector $\psi_{|q\rangle}^{GA} = a_0 + a_2 Ie_2$ is given by

$$\begin{aligned} \hat{\Sigma}_3 |q\rangle &\stackrel{\text{def}}{=} (-1)^q |q\rangle \leftrightarrow \psi_{(-1)^q |q\rangle}^{GA} \stackrel{\text{def}}{=} \\ &= e_3(a_0 + a_2 Ie_2)e_3 \\ &= a_0 - a_2 Ie_2. \end{aligned}$$

The unitary quantum gate $\hat{\Sigma}_3^{GA}$ acts on the basis $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$ as follows

$$\begin{aligned} \hat{\Sigma}_3^{GA} : 1 &\rightarrow 1, \quad \hat{\Sigma}_3^{GA} : Ie_1 \rightarrow -Ie_1, \quad \hat{\Sigma}_3^{GA} : Ie_2 \rightarrow \\ &-Ie_2, \quad \hat{\Sigma}_3^{GA} : Ie_3 \rightarrow Ie_3. \end{aligned}$$

2.4 Quantum Bit and Phase Flip Gate

A combination of two reversible operations, $\hat{\Sigma}_1^{GA}$ and $\hat{\Sigma}_3^{GA}$ results in another reversible operation to be applied on a single qubit. This will be denoted by $\hat{\Sigma}_2 \stackrel{\text{def}}{=} i_{\mathbb{C}} \hat{\Sigma}_1 \circ \hat{\Sigma}_3$ and its action on $\psi_{|q\rangle}^{GA} = a_0 + a_2 Ie_2$ is given by

$$\begin{aligned} \hat{\Sigma}_2 |q\rangle &\stackrel{\text{def}}{=} i_{\mathbb{C}} (-1)^q |q \oplus 1\rangle \leftrightarrow \psi_{(-1)^q |q \oplus 1\rangle}^{GA} \stackrel{\text{def}}{=} \\ &= e_2(a_0 + a_2 Ie_2)e_3 = (a_2 - a_0 Ie_2)Ie_3. \end{aligned}$$

The unitary quantum gate $\hat{\Sigma}_2^{GA}$ acts on the basis $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$ as follows

$$\begin{aligned} \hat{\Sigma}_2^{GA} : 1 &\rightarrow Ie_1, \quad \hat{\Sigma}_2^{GA} : Ie_1 \rightarrow 1, \quad \hat{\Sigma}_2^{GA} : Ie_2 \rightarrow \\ &Ie_3, \quad \hat{\Sigma}_2^{GA} : Ie_3 \rightarrow Ie_2. \end{aligned}$$

2.5 Hadamar Quantum Gate

The GA formulation of the Walsh-Hadamard quantum gate $\hat{H} \stackrel{\text{def}}{=} \frac{\hat{\Sigma}_1 + \hat{\Sigma}_3}{\sqrt{2}}$ named \hat{H}^{GA} acts on $\psi_{|q\rangle}^{GA} = a_0 + a_2 Ie_2$ as follows

$$\begin{aligned} \hat{H} |q\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} [|q \oplus 1\rangle + (-1)^q |q\rangle] \\ &\leftrightarrow \psi_{\hat{H}|q\rangle}^{GA} \stackrel{\text{def}}{=} \left(\frac{e_1 + e_3}{\sqrt{2}} \right) (a_1 + a_2 Ie_2)e_3 \\ &= \frac{a_0}{\sqrt{2}} (1 - Ie_2) - \frac{a_2}{\sqrt{2}} (1 + Ie_2). \end{aligned}$$

The Hadamar transformations of the states, $|+\rangle$ and $|-\rangle$ are given as follows:

$$\begin{aligned} |+\rangle &\stackrel{\text{def}}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \leftrightarrow \psi_{|+\rangle}^{GA} = \frac{1 - Ie_2}{\sqrt{2}}, \\ |-\rangle &\stackrel{\text{def}}{=} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \leftrightarrow \psi_{|-\rangle}^{GA} = \frac{1 + Ie_2}{\sqrt{2}}. \end{aligned}$$

The unitary quantum gate \hat{H}^{GA} acts on the basis $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$ as follows

$$\begin{aligned}\hat{H}^{GA} : 1 &\rightarrow \frac{1 - Ie_2}{\sqrt{2}}, \hat{H}^{GA} : Ie_1 \rightarrow \frac{-Ie_1 + Ie_3}{\sqrt{2}}, \\ \hat{H}^{GA} : Ie_2 &\rightarrow -\frac{1 + Ie_2}{\sqrt{2}}, \hat{H}^{GA} : Ie_3 \rightarrow \frac{Ie_1 + Ie_3}{\sqrt{2}}.\end{aligned}$$

2.6 Rotation Quantum Gate

The action of rotation gates \hat{R}_θ^{GA} acts on $\psi_{|q\rangle}^{GA} = a_0 + a_2 Ie_2$ as follows

$$\begin{aligned}\hat{R}_\theta |q\rangle &\stackrel{\text{def}}{=} \left(\frac{1 + \exp(i\mathbb{C}\theta)}{2} + (-1)^q \frac{1 - \exp(i\mathbb{C}\theta)}{2} \right) |q\rangle \\ &\leftrightarrow \psi_{\hat{R}_\theta |q}^{GA} \stackrel{\text{def}}{=} a_0 + a_2 Ie_2 (\cos \theta + Ie_3 \sin \theta)\end{aligned}$$

The unitary quantum gate \hat{R}_θ^{GA} acts on the basis $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$ in the following manner:

$$\begin{aligned}\hat{R}_\theta^{GA} : 1 &\rightarrow 1, \hat{R}_\theta^{GA} : Ie_1 \rightarrow Ie_1 (\cos \theta + Ie_3 \sin \theta), \\ \hat{R}_\theta^{GA} : Ie_2 &\rightarrow Ie_2 (\cos \theta + Ie_3 \sin \theta), \hat{R}_\theta^{GA} : Ie_3 \rightarrow Ie_3.\end{aligned}$$

Table 2 presents a summary of the most relevant quantum gates in the geometric algebra framework to act on the basis states $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$.

1 - QubitState	N	PF	BPF
1	$-Ie_2$	1	Ie_1
Ie_1	Ie_3	$-Ie_1$	1
Ie_2	-1	$-Ie_2$	Ie_3
Ie_3	Ie_1	Ie_3	Ie_2

Table 1: Quantum gates act on the basis states $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$, NOT (N), Phase Flip (PF), Bit and Phase Flip (BPF).

1 - QubitState	Hadamard	Rotation
1	$\frac{1 - Ie_2}{\sqrt{2}}$	1
Ie_1	$\frac{-Ie_1 + Ie_3}{\sqrt{2}}$	$Ie_1 (\cos \theta + Ie_3 \sin \theta)$
Ie_2	$-\frac{1 + Ie_2}{\sqrt{2}}$	$Ie_2 (\cos \theta + Ie_3 \sin \theta)$
Ie_3	$\frac{Ie_1 + Ie_3}{\sqrt{2}}$	Ie_3

Table 2: Quantum gates to act on the basis states $\{1, Ie_1, Ie_2, Ie_3\} \in G_3^+$, Hadamar and Rotation.

3 TWO-QUBIT QUANTUM COMPUTING

In this subsection, we study simple circuit models with 2-qubit quantum gates using the geometric algebra framework. This subsection is based on the work of Cafaro and Mancini [4].

We will show that the set of maximally entangled 2-qubit Bell states can be represented in geometric algebra. The Bell states are an interesting example of maximally entangled quantum states, and they form an orthonormal basis \mathcal{B}_{Bell} in the product Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$. Given the 2-qubit computational basis $\mathcal{B}_c = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, according to [10] the four Bell states can be constructed in the following way:

$$\begin{aligned}|0\rangle \otimes |0\rangle &\rightarrow |\psi_{Bell_1}\rangle \stackrel{\text{def}}{=} [\hat{U}_{CNOT} \circ (\hat{U} \otimes \hat{I})] (|0\rangle \otimes |0\rangle) = \\ &\frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle), \\ |0\rangle \otimes |1\rangle &\rightarrow |\psi_{Bell_2}\rangle \stackrel{\text{def}}{=} [\hat{U}_{CNOT} \circ (\hat{U} \otimes \hat{I})] (|0\rangle \otimes |1\rangle) = \\ &\frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle), \\ |1\rangle \otimes |0\rangle &\rightarrow |\psi_{Bell_3}\rangle \stackrel{\text{def}}{=} [\hat{U}_{CNOT} \circ (\hat{U} \otimes \hat{I})] (|1\rangle \otimes |0\rangle) = \\ &\frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle), \\ |1\rangle \otimes |1\rangle &\rightarrow |\psi_{Bell_4}\rangle \stackrel{\text{def}}{=} [\hat{U}_{CNOT} \circ (\hat{U} \otimes \hat{I})] (|1\rangle \otimes |1\rangle) = \\ &\frac{1}{\sqrt{2}} (|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle),\end{aligned}\quad (7)$$

where \hat{H} and \hat{U}_{CNOT} stand for the Hadamard and the CNOT gates respectively. The Bell basis in $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ is given by

$$\mathcal{B}_{Bell} \stackrel{\text{def}}{=} \{|\psi_{Bell_1}\rangle, |\psi_{Bell_2}\rangle, |\psi_{Bell_3}\rangle, |\psi_{Bell_4}\rangle\}.$$

According to equation (7), we obtain

$$\begin{aligned}|\psi_{Bell_1}\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, |\psi_{Bell_2}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \\ |\psi_{Bell_3}\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, |\psi_{Bell_4}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}.\end{aligned}$$

Using equation (7), the formulation of the Bell states in geometric algebra is as follows:

$$\begin{aligned}|\psi_{Bell_1}\rangle &\leftrightarrow \psi_{Bell_1}^{GA} = \frac{1}{2^{\frac{3}{2}}} (1 + Ie_2^1 Ie_2^2) (1 - Ie_3^1 Ie_3^2), \\ |\psi_{Bell_2}\rangle &\leftrightarrow \psi_{Bell_2}^{GA} = -\frac{1}{2^{\frac{3}{2}}} (Ie_2^1 + Ie_2^2) (1 - Ie_3^1 Ie_3^2), \\ |\psi_{Bell_3}\rangle &\leftrightarrow \psi_{Bell_3}^{GA} = \frac{1}{2^{\frac{3}{2}}} (1 - Ie_2^1 Ie_2^2) (1 - Ie_3^1 Ie_3^2), \\ |\psi_{Bell_4}\rangle &\leftrightarrow \psi_{Bell_4}^{GA} = \frac{1}{2^{\frac{3}{2}}} (Ie_2^1 - Ie_2^2) (1 - Ie_3^1 Ie_3^2).\end{aligned}$$

3.1 2-Qubit CNOT Quantum Gate

According to [10] a CNOT quantum gate can be written as

$$\hat{U}_{CNOT}^{12} = \frac{1}{2} \left[(\hat{I}^1 + \hat{\Sigma}_3^1) \otimes \hat{I}^2 + (\hat{I}^1 - \hat{\Sigma}_3^1) \otimes \hat{\Sigma}_1^2 \right] \quad (8)$$

where \hat{U}_{CNOT}^{12} is the CNOT gate from qubit 1 to qubit 2, thus

$$\begin{aligned} \hat{U}_{CNOT}^{12} |\psi\rangle &= \\ \frac{1}{2} \left[\hat{I}^1 \otimes \hat{I}^2 + \hat{\Sigma}_3^1 \otimes \hat{I}^2 + \hat{I}^1 \otimes \hat{\Sigma}_1^2 - \hat{\Sigma}_3^1 \otimes \hat{\Sigma}_1^2 \right] |\psi\rangle. \end{aligned} \quad (9)$$

Using equations (10) and (6), it follows

$$\begin{aligned} \hat{I}^1 \otimes \hat{I}^2 |\psi\rangle &\leftrightarrow \psi, \hat{\Sigma}_3^1 \otimes \hat{I}^2 |\psi\rangle \leftrightarrow -Ie_3^1 \psi J, \\ \hat{I}^1 \otimes \hat{\Sigma}_1^2 |\psi\rangle &\leftrightarrow -Ie_1^2 \psi J, \\ -\hat{\Sigma}_3^1 \otimes \hat{\Sigma}_1^2 |\psi\rangle &\leftrightarrow Ie_3^1 Ie_1^2 \psi E \end{aligned} \quad (10)$$

Now using equation (6), the CNOT gate of equation (10) is formulated in GA as follows:

$$\hat{U}_{CNOT}^{12} |\psi\rangle \leftrightarrow \frac{1}{2} (\psi - Ie_3^1 \psi J - Ie_1^2 \psi J + Ie_3^1 Ie_1^2 \psi E). \quad (11)$$

3.2 2-Qubit Controlled-Phase Gate

According to [10], the action of the Controlled Phase gate \hat{U}_{CP}^{12} on $|\psi\rangle \in \mathbb{H}_2^2$ can be formulated as

$$\begin{aligned} \hat{U}_{CP}^{12} |\psi\rangle &= \\ \frac{1}{2} \left[\hat{I}^1 \otimes \hat{I}^2 + \hat{\Sigma}_3^1 \otimes \hat{I}^2 + \hat{I}^1 \otimes \hat{\Sigma}_3^2 - \hat{\Sigma}_3^1 \otimes \hat{\Sigma}_3^2 \right] |\psi\rangle. \end{aligned} \quad (12)$$

Using equations (13) and (6), it follows

$$\begin{aligned} \hat{I}^1 \otimes \hat{I}^2 |\psi\rangle &\leftrightarrow \psi, \hat{\Sigma}_3^1 \otimes \hat{I}^2 |\psi\rangle \leftrightarrow \\ -Ie_3^1 \psi J, \hat{I}^1 \otimes \hat{\Sigma}_3^2 |\psi\rangle &\leftrightarrow -Ie_3^2 \psi J, \\ -\hat{\Sigma}_3^1 \otimes \hat{\Sigma}_3^2 |\psi\rangle &\leftrightarrow Ie_3^1 Ie_3^2 \psi E \end{aligned} \quad (13)$$

Using equations (6) and (13), one can formulate in geometric algebra the controlled-phase quantum gate as follows:

$$\hat{U}_{CP}^{12} |\psi\rangle \leftrightarrow \frac{1}{2} (\psi - Ie_3^1 \psi J - Ie_3^2 \psi J + Ie_3^1 Ie_3^2 \psi E). \quad (14)$$

3.3 2-Qubit SWAP Gate

According to [10], the action of the Swap gate \hat{U}_{SWAP}^{12} on $|\psi\rangle \in \mathbb{H}_2^2$ can be formulated as

$$\begin{aligned} \hat{U}_{SWAP}^{12} |\psi\rangle &= \\ \frac{1}{2} \left[\hat{I}^1 \otimes \hat{I}^2 + \hat{\Sigma}_1^1 \otimes \hat{\Sigma}_1^2 + \hat{\Sigma}_2^1 \otimes \hat{\Sigma}_2^2 + \hat{\Sigma}_3^1 \otimes \hat{\Sigma}_3^2 \right] |\psi\rangle. \end{aligned} \quad (15)$$

Using equations (16), it follows

$$\begin{aligned} \hat{I}^1 \otimes \hat{I}^2 |\psi\rangle &\leftrightarrow \psi, \hat{\Sigma}_1^1 \otimes \hat{\Sigma}_1^2 |\psi\rangle \leftrightarrow -Ie_1^1 Ie_2^2 \psi E, \\ \hat{\Sigma}_2^1 \otimes \hat{\Sigma}_2^2 |\psi\rangle &\leftrightarrow -Ie_2^1 Ie_2^2 \psi E, \hat{\Sigma}_3^1 \otimes \hat{\Sigma}_3^2 |\psi\rangle \leftrightarrow -Ie_3^1 Ie_3^2 \psi E \end{aligned} \quad (16)$$

Using equation (17), the SWAP quantum gate in GA reads

$$\hat{U}_{SWAP}^{12} |\psi\rangle \leftrightarrow \frac{1}{2} (\psi - Ie_1^1 Ie_1^2 \psi E - Ie_2^1 Ie_2^2 \psi E - Ie_3^1 Ie_3^2 \psi E).$$

Table 3 summarizes the most important 2-qubit quantum gates formulated in the geometric algebra basis.

$\mathcal{B}_{[G_3^+ \otimes G_3^+]/E}$

2Q Gat	Gate Action on States
CNOT	$\frac{1}{2}(\psi - Ie_3^1 \psi J - Ie_1^2 \psi J + Ie_3^1 Ie_1^2 \psi E)$
CP	$\frac{1}{2}(\psi - Ie_3^1 \psi J - Ie_3^2 \psi J + Ie_3^1 Ie_3^2 \psi E)$
SWAP	$\frac{1}{2}(\psi - Ie_1^1 Ie_1^2 \psi E - Ie_2^1 Ie_2^2 \psi E - Ie_3^1 Ie_3^2 \psi E)$

Table 3: 2-Qubit Quantum gates: CNOT, Controlled Phase, and SWAP gates to act on the basis $\mathcal{B}_{[G_3^+ \otimes G_3^+]/E}$.

4 QUANTUM COMPUTING FOR COMMUNICATION

Distributing quantum information between remote locations requires the integration of emerging quantum technologies with existing communication infrastructure, [5, 7] Achieving this integration necessitates a thorough understanding of how communication channels degrade transmitted quantum signals, an essential step toward implementing practical solutions for theoretically unconditionally secure key generation. However, current experimental quantum key distribution (QKD) systems, which rely on photon transmission, face limitations due to various hardware imperfections. These non-idealities restrict the overall

performance and scalability of QKD technologies. To advance the engineering of future QKD systems, classical simulations of the optical components used in these systems may play a critical role, going beyond traditional characterization techniques employed in classical communication systems. The main obstacle in long-distance quantum communication remains transmission loss, primarily caused by absorption and scattering in optical fibers or atmospheric channels. While classical systems compensate for such losses with optical amplifiers acting as repeaters, this approach is not viable in quantum systems, as amplifying individual photons would irreversibly destroy the quantum information they carry. Although research into quantum repeaters is ongoing, these technologies are not yet mature enough to support intercontinental quantum communication [11].

In Quantum Communications we deal with teleportation; as an illustration, we present below the implementation for the Bob and Alice problem using Quaternion Algebra.

Bob and Alice Problem

Preparation

If Alice chooses bit $a \in \{0, 1\}$ and base $b \in \{comp, j\}$:

$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } b = comp, \\ |b_0\rangle & \text{if } b = j \end{cases}$$

depending upon if $a = 0$ or $a = 1$.

Intercept-resend (Bob)

If Alice intercepts:

1. Chooses base $b_E \in \{comp, j\}$.
2. Measures $|\psi\rangle$ in $\mathcal{B}_{b_E} \rightarrow$ obtains x_E and collapses to $|e_{x_E}^{(b_E)}\rangle$.
3. Resend $|\psi'\rangle = |e_{x_E}^{(b_E)}\rangle$ to Bob.

Program

INPUT: n (number of signals), $p_{Alice} \in [0, 1]$

FOR $t = 1..n$:

Choices of Alice

$a_t \leftarrow \text{Bernoulli}(1/2)$ # bit

$b_{A_t} \leftarrow \text{choice}\{comp, j\}$ # base

Prepare:

$|\Psi_t\rangle \leftarrow |a_t\rangle$ in base b_{A_t}

This means:

if $b_{A_t} = comp$: $|\Psi_t\rangle = |0\rangle$ ($a_t = 0$), or $|1\rangle$ ($a_t = 1$)

if $b_{A_t} = j$: $|\Psi_t\rangle = |b_0\rangle$ ($a_t = 0$), or $|b_1\rangle$ ($a_t = 1$)

Possible Bob Channel

if $\text{Uniform}(0,1) < p_{Bob}$:

$b_{E_t} \leftarrow \text{choice}\{comp, j\}$

measure to Bob in $\mathcal{B}_{\{b_{E_t}\}}$:

$$p_x = \|\langle e_x^{(b_{E_t})} | \Psi_t \rangle\|^2, x \in \{0, 1\}$$

$$x_{E_t} \approx \text{Categorical}(p_0, p_1)$$

$$|\Psi'_t\rangle \leftarrow |e_{x_{E_t}}^{(b_{E_t})}\rangle$$

5 QUANTUM QUATERNION FAST FOURIER TRANSFORM

The Quaternion Quantum Fourier Transform (QQFT) maps the quaternion quantum set $|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ to the quaternion quantum state $|y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$, [3]. For the QQFT equation, it is needed to change

the complex exponential of the QFT, with a quaternion exponential as follows

$$|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{QQFT} |y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle. \quad (17)$$

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi\mu \frac{jk}{N}} |k\rangle, \text{ where, } \mu = \frac{1}{\sqrt{3}}(i + j + k).$$

The Inverse Quaternion Quantum Fourier Transform (IQQFT) is then given by

$$|y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \xrightarrow{IQQFT} |x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle, \quad (18)$$

and

$$|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi\mu \frac{jk}{N}} |j\rangle, \text{ where, } \mu = \frac{1}{\sqrt{3}}(i + j + k).$$

Or the unitary matrix

$$U_{QQFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} w_N^{jk} |k\rangle \langle j|, \quad (19)$$

where $w_N^{jk} = e^{2\pi\mu \frac{jk}{N}}$. As a matrix, the corresponding unitary operator U_{QQFT} is given by

$$U_{QQFT} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w_n & w_n^2 & w_n^3 & \dots & w_n^{N-1} \\ 1 & w_n^2 & w_n^4 & w_n^6 & \dots & w_n^{2(N-1)} \\ 1 & w_n^3 & w_n^6 & w_n^9 & \dots & w_n^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w_n^{N-1} & w_n^{2(N-1)} & w_n^{3(N-1)} & \dots & w_n^{(N-1)(N-1)} \end{bmatrix},$$

where $w_n = e^{\frac{2\pi\mu}{N}}$. For the U_{IQQFT} , we use $w_N^{jk} = e^{-2\pi\mu \frac{jk}{N}}$ instead.

5.1 Application of the Quaternion Quantum Fast Fourier Transform

Given an RGB $f(x, y)$ image, each pixel can be represented as a pure quaternion as follows:

$$q(x, y) = (0, \vec{q}) = R(x, y)i + G(x, y)j + B(x, y)k \quad (20)$$

However, we propose instead to use the following exponential function

$$q(x, y) = e^{\theta n} = \cos(\theta) + n \sin(\theta), \quad (21)$$

where

$$n = \frac{R(x,y)i + G(x,y)j + B(x,y)k}{\sqrt{R(x,y)^2 + G(x,y)^2 + B(x,y)^2}},$$

$$\theta = \sqrt{R(x,y)^2 + G(x,y)^2 + B(x,y)^2}.$$

A quantum quaternion RGB image pixel x is represented by two qubits, which is a superposition of four quantum states as follows:

$$x = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle, \quad (22)$$

where for $|n| = \sqrt{R(x,y)^2 + G(x,y)^2 + B(x,y)^2}$,

$$\alpha_1 = \cos(\theta), \alpha_2 = \frac{\sin(\theta)}{|n|}R(x,y)i, \quad (23)$$

$$\alpha_3 = \frac{\sin(\theta)}{|n|}G(x,y)j, \alpha_4 = \frac{\sin(\theta)}{|n|}B(x,y)k,$$

where $\sum_{n=1}^4 \alpha_n^2 = 1$.

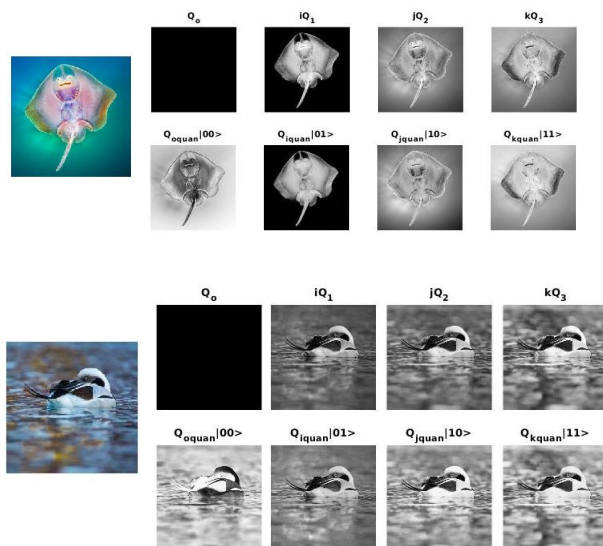


Figure 1: RGB images represented as quaternion quantum images

Figure 1 shows two RGB images as quaternion quantum images. Since we can not use convolution to compute the filtering of quantum images, we should simply filter the quaternion quantum image in the frequency domain by using constraints to delimit the band of the image in question.

To filter in the frequency domain, firstly we have to transform the quaternion quantum image using the Quaternion Quantum Fast Fourier Transform. In this work, we are not using a quantum computer, but to speed up the Quaternion Fourier Transform, we use the Fast Fourier Transform (FFT). Figure 2 presents the Quaternion Quantum Fast Fourier Transform of an RGB image and the Inverse Quaternion Quantum Fast Fourier Transform.

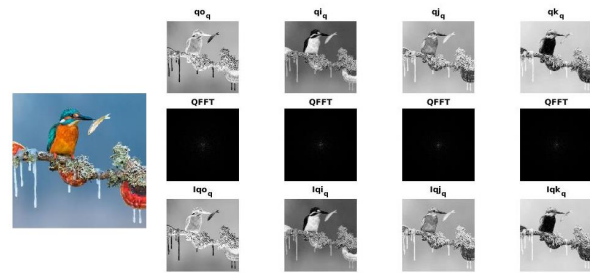


Figure 2: Quaternion Quantum Fast Fourier Transform and its inverse of an RGB image, according to equations (17) and (18)

6 QUANTUM COMPUTING AND MACHINE LEARNING FOR IMAGE PROCESSING. ARCHITECTURE

As shown in Figure 3, we introduce a hybrid quantum classical convolutional neural network architecture, designated the Geometric (Clifford) QuanConvolutional Neural Network (CQCNN) [8, 9], for advanced feature extraction in medical image analysis [1]. This architecture synergistically integrates the representational power of quantum convolution, quaternion convolution [6], and Clifford convolution, enabling the preservation of multi-channel geometric correlations while leveraging quantum-enhanced feature embeddings. The CQCNN is designed for medical image analysis tasks where local geometric structure is diagnostically significant.

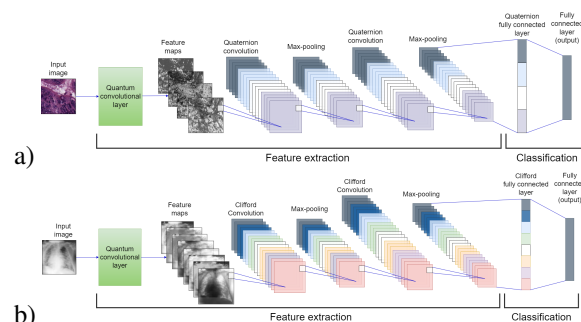


Figure 3: a) Architecture of the Quaternion Quanvolutional Neural Network. b) Architecture of the Geometric (Clifford) Quanvolutional Neural Network.

The architecture of the Quaternion Quanvolutional Neural Network QCNNs are extended to QQNNs by adding a quanvolutional layer. By applying a quanvolutional layer (with a 4-qubit circuit) to an RGB (or a grayscale) input image we obtain four latent space features that are subsequently processed by a QQCNN; see Figure 3. The last layer corresponds to a fully connected layer with a softmax function used for classification. The architecture of the Geometric (Clifford) Quanvolutional Neural Network: GCNNs

are extended to QNNs by adding a quanvolutional layer.

Quantum Convolutional Layer

Let $I \in \mathbf{R}^{H \times W \times C}$ represent the input image, where H, W and C denote height, width, and number of channels, respectively. The quantum convolutional layer operates as follows:

1. **Patch Encoding:** The image is divided into non-overlapping patches P_k of size $p \times p$, which are encoded into a quantum state

$$|\psi_k\rangle = U_{enc}(P_k)|0\rangle^{\otimes n_q}$$

where U_{enc} is the parameterized encoding unitary and n_q is the number of qubits.

2. **Quantum Convolution:** A parameterized quantum circuit PQC U_θ processes the encoded states:

$$|\phi_k\rangle = U_\theta |\psi_k\rangle$$

3. **Measurement:** Expectation values of observables O_i yield the feature maps:

$$f_{k,i} = \langle \phi_k | O_i | \phi_k \rangle, \quad i = 1, \dots, n_k$$

Thus, each path yields n_k scalar features, producing quantum-generated feature maps $F(Q) \in \mathbf{R}^{H' \times W' \times n_q}$.

Geometric (Clifford) Algebra Quantum Convolutional Layer

The output feature maps from the quantum layer are processed collectively within a geometric algebra framework $G_{p,q}$, allowing the representation of vectors, bivectors, and high-grade geometric entities.

Given the quantum feature maps $F(Q)$, one forms a multivector representation:

$$M(x, y) = \sum_{i=1}^{n_q} f_{x,y,i} e_i$$

where e_i are the orthogonal basis elements of the geometric algebra.

A Geometric algebra convolution kernel K of size $k \times k$ acts via the geometric product

$$(M * K)(x, y) = \sum_{u=-\lfloor k/2 \rfloor}^{\lfloor k/2 \rfloor} \sum_{v=-\lfloor k/2 \rfloor}^{\lfloor k/2 \rfloor} M(x+u, y+v) K(u, v).$$

This convolution inherently preserves orientation, phase, and multidimensional correlations, outperforming scalar convolutions in rotational and geometric invariance.

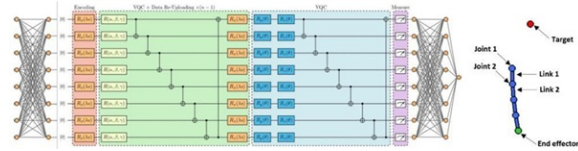


Figure 4: Variational Quantum Soft Actor-Critic to control the movement of a robotic arm

7 QUANTUM REINFORCEMENT LEARNING FOR CONTINUOUS CONTROL

Figure 4 shows a Variational Quantum Soft Actor-Critic to control the movement of a robotic arm. We propose to enhance the Soft Actor-Critic (SAC) algorithm for continuous robotic control tasks by incorporating quantum computing techniques, resulting in a Variational Quantum Soft Actor-Critic (VQ-SAC) framework. The aim is to investigate whether variational quantum circuits can improve exploration efficiency and learning speed, addressing two key bottlenecks in real-world reinforcement learning (RL):

- Exploration Strategy – avoiding inefficient or myopic exploration in large continuous action spaces.
- Curse of Dimensionality – mitigating slow convergence in high-dimensional state-action spaces. The approach will be evaluated in the context of robotic arm movement control, using simulated and real-time systems.

8 QUANTUM GEOMETRIC FUZZY INFERENCE ENGINES FOR DECISION TAKING IN ROBOTICS

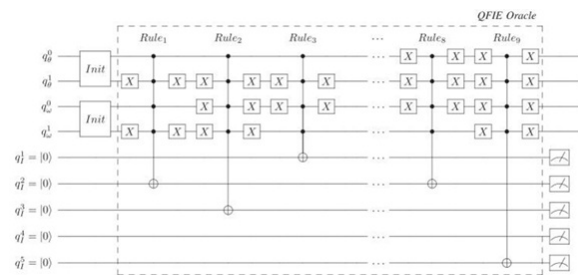


Figure 5: Quantum Fuzzy Inference Engine

The design of a Quantum Fuzzy Inference Engine (QFIE) accomplishes a twofold objective. First, it delivers an exponential speedup in the execution of fuzzy rules compared to a classical oracle-based fuzzy inference engine, by exploiting quantum parallelism and amplitude encoding of fuzzy membership degrees. Second, it opens a novel avenue for quantum programming via fuzzy linguistic rules, providing an intuitive, high-level framework for defining quantum

algorithms in terms familiar to engineers and domain experts. This paradigm makes it possible to describe decision processes for quantum computers using the approximate reasoning capabilities inherent to fuzzy logic, while leveraging quantum computational speedups. Figure 5 shows the implemented circuit, where a measurement operation on each qubit of QRI is added after the implementation of the oracle. This combination of quantum information processing, quantum Fuzzy Finite State Machine, fuzzy logic reasoning, and geometric modeling holds potential for a new class of intelligent control systems that are both computationally efficient and linguistically interpretable, suitable for complex real-time applications in robotics, autonomous systems, and adaptive control. Next we present the implementation of the Quantum Oracle for Fuzzy Encoding and the Quantum Fuzzy Finite State Machines Representations.

Quantum Oracle for Fuzzy Rule Encoding

The Ffuzzyrule base has the general form:

$$R_j : \text{IF } \theta \text{ is } A_j \text{ AND } w \text{ is } B_j \text{ THEN } I \text{ is } C_j$$

In QFIE, the oracle O_f encodes the mapping:

$$O_f : |A_j\rangle |B_j\rangle |0\rangle \rightarrow |A_j\rangle |B_j\rangle |C_j\rangle$$

This is implemented as a controlled unitary:

$$O_f = \sum_{A,B} |A\rangle\langle A| \otimes |B\rangle\langle B| \otimes U_{AB}$$

where U_{AB} maps the output register from $|0\rangle$ to the state representing the consequent C with amplitudes proportional to the minimum (or another t-norm) of the antecedent memberships:

$$U_{AB}|0\rangle = \frac{1}{\sqrt{\sum_c \alpha_c^2}} \sum_c \alpha_c |c\rangle, \quad \alpha_c = \min(\mu_A(\theta), \mu_B(w))$$

Because all rules are evaluated in quantum superposition, the complexity is reduced compared to sequential evaluation.

Quantum Fuzzy Finite State Machine Representation

The system's dynamics can be represented by a Quantum Fuzzy Finite State Machines (QFFSM)

$$|\psi(t+1)\rangle = U|\psi(t)\rangle$$

where U_f is a fuzzy-weighted unitary transition operator, defined as:

$$U_f = \sum_{s,s'} \Lambda |s'\rangle\langle s|$$

with fuzzy transition amplitudes $\Lambda_{s,s'} \in [0, 1]$ satisfying unitary constraints.

9 CONCLUSION

In traditional quantum mechanics, the tensor product is employed to construct multiparticle states and define operators acting on them, serving as a tool to distinguish the Hilbert spaces of individual particles. In contrast, the Ggeometric algebraframework offers an innovative approach for representing the tensor product through the geometric product, utilizing multivectors. In this paper, we have introduced several advanced algorithms, including the Quantum Quaternion Fourier Transform, Quantum Key Distribution, Geometric Algebra Quantum Convolutional Neural Networks, and the Geometric Fuzzy Inference Engine, aimed at enhancing robotic decision-making processes.

10 REFERENCES

- [1] Altamirano-Escobedo G. E. Bayro-Corrochano. 2023. Geometric Algebra Quantum Convolutional Neural Network: A model using geometric (Clifford) algebras and quantum computing. *Hypercomplex Signal and Image Processing. IEEE Signal Processing Magazine*, vol. 41, no. 2, pp. 75-85.
- [2] Bayro-Corrochano, E. 2024. *Geometric Algebra Applications Vol. III: Integral Transforms, Machine Learning, and Quantum Computing*. Springer Nature, Switzerland.
- [3] Bayro-Corrochano, E. Vazquez-Flores, Z. . 2023. Image processing using the quantum quaternion Fourier transform. *Mathematical Methods in Applied Sciences*, Volume 47, Issue3, Pages 1305-1317.
- [4] Cafaro C. and Mancini S. . 2010. A geometric algebra perspective on quantum computational gates and universality in quantum computing. *arXiv:1006.2071v1 [math-ph]* 10 June.
- [5] Caputo, M.S., Giovanni, A.C., Giovanna, T. and Maurizio, Z. 2022. A simulator of optical coherent-state evolution in quantum key distribution systems. *Optical and Quantum Electronics*, 54:689, <https://doi.org/10.1007/s11082-022-04041-8>.
- [6] Chappell J.M. . 2011. *Quantum Computing, Quantum Games and Geometric Algebra*. PhD Thesis, The School of Chemistry and Physics, University of Adelaide, Australia.
- [7] Gupta, S. et al. 2025 Robust simulation of continuous-variable quantum key distribution in Matlab and Simulink. *Academia Quantum*, 2025(2), pp. 1 of 14, <https://doi.org/10.20935/AcadQuant7844>.
- [8] Henderson, M., Shakya, S., Pradhan, S. and Tristan, C. 2020. Quconvolutional neural networks: powering image recognition with quantum circuits. *Quantum Machine Intelligence*, Vol. 2(1), pp. 1-9, Springer.
- [9] Gaudet, Chase J and Maida, Anthony S. 2018 Deep quaternion networks. 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1-8.
- [10] Nielsen A. and Chuang I. L. . 2000. *Quantum Computation and Information*, Cambridge Press.
- [11] Yin, J. et al. 2017. Satellite-based entanglement distribution over 1200 kilometers. *Science* 356, 1140

Bayesian Update Step Using Adiabatic Quantum Computing

Norman Bunk

Rheinische Friedrich-
Wilhelms-Universität
Bonn

Regina-Pacis-Weg 3
53113 Bonn,
Germany

s6nobunk@uni-bonn.de /
norman.bunk@gmx.de

Felix Govaers

Fraunhofer FKIE
Fraunhofer Str. 20
53343 Wchatberg,
Germany

felix.govaers@fkie.fraunhofer.de

ABSTRACT

We propose a quantum algorithm for the filtering step in Bayesian state estimation, based on adiabatic quantum computing (AQC). The approach embeds the likelihood function into the energy landscape of an Ising Hamiltonian, enabling the posterior distribution to emerge through quantum annealing. Unlike existing gate-based methods, our formulation avoids complex conditional operations and scales more naturally with the size of the state space. Numerical simulations confirm that the resulting distributions closely match the correct posterior, even with approximate parameter settings. This demonstrates the feasibility of AQC as a tool for probabilistic inference in high-dimensional filtering problems.

Keywords

adiabatic quantum computing, sensor data fusion, Bayes theorem

1 INTRODUCTION

Quantum computing has emerged as a disruptive computational paradigm with the potential to address classically intractable problems across various fields, including artificial intelligence (AI), optimization, and data processing. One promising area of application is sensor data fusion, a fundamental concept in robotics, surveillance, autonomous vehicles, and environmental monitoring, where information from multiple sources must be integrated to infer the state of a system. The standard mathematical framework for sensor fusion is Bayesian filtering, which recursively applies a prediction and an update step to estimate the posterior distribution over the state space.

While the prediction step often relies on models that are tractable in both classical and quantum domains, the Bayesian update step poses significant challenges [?]. It requires the conditioning of a prior distribution on new measurement data using the likelihood function. In high-dimensional state spaces, this operation quickly becomes computationally expensive. Quantum com-

puters, by virtue of their ability to represent and manipulate high-dimensional probability distributions using amplitude encoding, have been proposed as a potential solution to this bottleneck.

To date, the implementation of a quantum algorithm for the Bayesian update step proposed in [3] is employing gate-based quantum circuits. This method encodes the posterior distribution by applying a sequence of state-conditioned unitary operations. While theoretically sound, the approach scales poorly, as it necessitates a distinct quantum gate for each possible state hypothesis. This results in exponential growth in circuit depth and complexity, rendering it impractical for real-world systems with continuous or large discrete state spaces.

In this paper, we introduce a novel quantum approach to the Bayesian update step using adiabatic quantum computing, specifically quantum annealing. Unlike gate-based quantum algorithms, our method encodes the Bayesian update directly into the energy landscape of an Ising-type Hamiltonian. The likelihood function is embedded into the cost function of the annealing process, enabling the system to evolve toward the most probable state configuration in a natural and scalable way. This formulation bypasses the need for complex conditional operations and opens a new direction for quantum inference methods.

Our approach fits into the growing body of literature at the intersection of quantum computing and artificial in-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

telligence, particularly in the use of quantum hardware for probabilistic inference, optimization, and machine learning. While most existing work in quantum machine learning focuses on variational circuits and classification tasks, few have addressed the challenge of recursive inference under uncertainty, a critical requirement in real-time decision-making systems. Moreover, our contribution complements recent research that explores quantum-enhanced data fusion, offering a concrete mechanism for incorporating observational data in a probabilistically rigorous way.

We present a complete formulation of the Bayesian update using quantum annealing, validate our method on simulated sensor fusion tasks, and analyze its complexity and scalability compared to classical and gate-based quantum methods. Our results suggest that adiabatic quantum computing provides a promising and efficient alternative for Bayesian inference in high-dimensional sensor fusion scenarios.

2 PROBLEM FORMULATION

Bayesian filtering is a recursive estimation method that updates the belief over a system state based on new observations. In its discrete form, the posterior distribution $p(x_k|Z_k)$ is computed by conditioning the prior $p(x_k)$ on the latest measurement z_k via the likelihood $p(z_k|x_k)$. This results in a pointwise multiplication followed by normalization:

$$p(x_k|Z_k) \propto p(z_k|x_k) \cdot p(x_k|Z_{k-1}) \quad (1)$$

Here, $x_k \in X \subset \mathbb{R}^D$ denotes the discrete state at time k , and $Z_k = \{z_1, z_2, \dots, z_k\}$ the measurement history up to time k .

The classical framework for Bayesian estimation and sensor data fusion is well established, with in-depth discussions available in foundational texts [5, 2]. In many practical applications, the state space is discretized into a finite grid, where each axis $d = 1, \dots, D$ is divided into N_d bins of size Δ_d . The resulting joint distribution $p(x)$ over the full state space becomes a tensor of shape $N_1 \times N_2 \times \dots \times N_D$, containing $\prod_{d=1}^D N_d$ entries. For high-dimensional problems, this representation quickly becomes computationally infeasible in terms of storage and processing requirements.

Quantum computing offers a compact representation for such distributions. Using amplitude encoding, a quantum state $|\psi\rangle$ of n qubits can represent a probability distribution over $N = 2^n$ states:

$$|\psi\rangle = \sum_{x=0}^{N-1} a_x |x\rangle, \quad \text{with } |a_x|^2 = p(x) \quad (2)$$

This encoding allows parallel access to all probability amplitudes via quantum superposition. Measuring the quantum state yields samples according to the probability distribution $p(x)$, and repeated measurement allows estimation of statistical moments.

The objective of this work is to implement the Bayesian filtering update on such a quantum state by transforming an initial distribution (prior) into the posterior distribution through quantum evolution. In contrast to gate-based methods, we investigate an adiabatic quantum approach that leverages energy-based encoding to shape the final state distribution according to the desired posterior. The challenge lies in embedding the likelihood information into a cost function that can be realized through a time-dependent quantum Hamiltonian, while maintaining physical feasibility and computational scalability.

3 ADIABATIC QUANTUM COMPUTING

Adiabatic Quantum Computing (AQC) is a computational paradigm that solves optimization problems by exploiting the adiabatic theorem of quantum mechanics. The adiabatic theorem was first stated by Born and Fock in 1928 [1]; it asserts that a quantum system remains in its instantaneous eigenstate if the Hamiltonian changes sufficiently slowly and a finite spectral gap exists. Since then, the theorem has been analyzed and extended in a range of computational contexts [6]. Instead of executing a sequence of logic gates, AQC encodes the solution to a given problem into the ground state of a final, problem-specific Hamiltonian. The system is initialized in the ground state of a simple, easily preparable Hamiltonian and then evolved slowly toward the problem Hamiltonian. If the evolution is sufficiently slow and the system remains isolated, the adiabatic theorem guarantees that the system stays in its instantaneous ground state throughout the process.

Formally, the total Hamiltonian of the system at time $t \in [0, T]$ is defined as an interpolation between two Hamiltonians:

$$H(t) = (1 - s(t))H_0 + s(t)H_1, \quad s(0) = 0, \quad s(T) = 1 \quad (3)$$

Here, H_0 is the initial (driver) Hamiltonian, whose ground state is typically a uniform superposition over all computational basis states. A common choice is a transverse-field Hamiltonian, such as:

$$H_0 = -\sum_i X_i \quad (4)$$

where X_i denotes the Pauli- X operator acting on qubit i . The problem Hamiltonian H_1 encodes the cost function of the optimization problem in its ground state. For many problems of practical interest, H_1 can be expressed in the form of an Ising Hamiltonian:

$$H_1 = \sum_{i < j} J_{ij} Z_i Z_j + \sum_i h_i Z_i \quad (5)$$

where Z_i is the Pauli- Z operator on qubit i , and J_{ij} , h_i are problem-specific coefficients derived from the structure of the cost function. [4]

The system is evolved according to a time-dependent schedule $s(t)$, often chosen to be linear: $s(t) = t/T$. The total evolution time T must be large enough to ensure adiabaticity, i.e., to avoid excitations to higher energy levels. The minimum energy gap Δ between the ground state and the first excited state during the evolution determines the required runtime via the relation:

$$T \gg \frac{1}{\Delta^2} \quad (6)$$

In practice, small violations of adiabaticity lead to a final state that is not exactly the ground state of H_1 , but rather a thermal distribution over low-energy states. This behavior can still be useful, particularly when the objective is to sample from a distribution shaped by the cost landscape rather than to find a single minimum.

To use AQC for a computational problem, one must translate the objective function into the energy landscape defined by H_1 . In our case, this objective is the negative logarithm of the posterior distribution obtained from Bayesian filtering. For many models with Gaussian or quadratic structure, this results in a cost function that is quadratic in the discrete state variable x . This function must then be mapped to binary variables and reformulated as an Ising-type Hamiltonian, suitable for implementation on quantum annealers or other AQC platforms.

4 MAPPING THE BAYESIAN UPDATE TO AN ISING HAMILTONIAN

In order to implement the Bayesian update step within an adiabatic quantum computing (AQC) framework, the corresponding posterior distribution must be encoded into the ground state of a problem Hamiltonian. This requires the formulation of the Bayesian cost function in a quadratic form suitable for mapping to an Ising Hamiltonian.

4.1 Cost Function Formulation

The Bayesian filtering step corresponds to a pointwise multiplication of the prior and the likelihood function,

followed by normalization. In log-domain and for Gaussian models, this operation becomes additive. The resulting cost function can be written as:

$$C(x) = P(x - x_\mu)^2 + Q(z - Ax)^2 \quad (7)$$

Here, x is the discrete latent variable, x_μ is the prior mean, z is the measurement, A is a linear mapping (e.g., a measurement matrix), and P, Q are weighting factors representing the inverse variances of the prior and likelihood distributions, respectively.

Expanding this cost function yields a quadratic polynomial:

$$\begin{aligned} C(x) &= P(x^2 - 2xx_\mu + x_\mu^2) + Q(z^2 - 2Axz + A^2x^2) \\ &= (P + QA^2)x^2 - 2(Px_\mu + QAz)x + (Px_\mu^2 + Qz^2) \end{aligned} \quad (8)$$

Defining the constants:

$$J = P + QA^2, \quad h = -2(Px_\mu + QAz), \quad C = Px_\mu^2 + Qz^2 \quad (9)$$

the cost function becomes:

$$C(x) = Jx^2 + hx + C \quad (10)$$

which is directly compatible with the energy form required for Ising-type Hamiltonians.

4.2 Ising Representation via Operator Mapping

To translate the above polynomial into a quantum operator acting on a register of qubits, we first define a binary operator that maps computational basis states to integers. For N qubits, let the operator \tilde{Z}_i be:

$$\tilde{Z}_i = \frac{1}{2}(I - Z_i) \quad (11)$$

where Z_i is the Pauli- Z operator acting on qubit i . This maps:

$$\tilde{Z}_i |0\rangle = 0, \quad \tilde{Z}_i |1\rangle = |1\rangle \quad (12)$$

Each computational basis state $|b_0 b_1 \dots b_{N-1}\rangle$, with $b_k \in \{0, 1\}$, represents a binary number

$x \in \{0, \dots, 2^N - 1\}$. We construct the corresponding value operator X as:

$$X = \sum_{k=0}^{N-1} 2^{N-1-k} \tilde{Z}_k \quad (13)$$

This operator acts diagonally in the computational basis and returns the classical integer x encoded by the qubit register.

4.3 Problem Hamiltonian

Replacing x by the operator X in the cost function leads to the problem Hamiltonian:

$$H_p = JX^2 + hX + CI \quad (14)$$

This Hamiltonian is diagonal in the computational basis, and its ground state corresponds to the state $|x\rangle$ minimizing the cost function:

$$H_p |x\rangle = (Jx^2 + hx + C) |x\rangle \quad (15)$$

The offset term C is constant and does not affect the ground state. Thus, the optimization reduces to finding the value of x that minimizes the quadratic polynomial encoded in H_p , which corresponds to the Bayesian posterior mode under the assumed Gaussian prior and likelihood.

This formulation enables the implementation of the Bayesian update step as an energy minimization problem, suitable for execution on an adiabatic quantum computer.

5 THERMAL EFFECTS AND EFFECTIVE TEMPERATURE

In adiabatic quantum computing (AQC), the system ideally remains in the ground state of a slowly evolving Hamiltonian. However, in practice, non-adiabatic transitions may occur due to finite evolution time, especially near avoided level crossings. As a result, the final quantum state does not necessarily coincide with the exact ground state but instead resembles a thermal mixture over low-energy states. This effect can be modeled using a Gibbs distribution governed by an effective temperature. [7]

Formally, the probability of observing a state x with energy $E(x)$ is given by:

$$P(x) = \frac{1}{Z} \exp(-\beta_{\text{eff}} E(x)), \quad (16)$$

$$Z = \sum_x \exp(-\beta_{\text{eff}} E(x)) \quad (17)$$

Here, $\beta_{\text{eff}} = 1/T_{\text{eff}}$ denotes the inverse effective temperature that characterizes the deviation from ideal adiabaticity. The key challenge in AQC-based sampling is that this parameter is not externally controllable, but rather emerges from the physical dynamics of the system.

To derive the dependence of β_{eff} on system parameters, consider a two-level quantum system with a time-dependent Hamiltonian:

$$H(t) = \frac{\Delta}{2} \sigma_x + \frac{vt}{2} \sigma_z \quad (18)$$

where Δ is the minimum spectral gap and v is the rate at which the diabatic levels sweep past each other. According to Landau-Zener theory, the excitation probability to the first excited state is:

$$P_{\text{exc}} = \exp\left(-\frac{\pi\Delta^2}{2\hbar v}\right) \quad (19)$$

as shown in the derivation by Sun [8].

Assuming the ground and excited state energies are $E_0 = 0$ and $E_1 = \Delta$, and defining $p_0 = 1 - P_{\text{exc}}$, $p_1 = P_{\text{exc}}$, we compare the resulting state occupations to a thermal distribution:

$$\frac{p_1}{p_0} = \exp(-\beta_{\text{eff}}\Delta) \quad (20)$$

Solving for β_{eff} yields:

$$\beta_{\text{eff}} = \frac{1}{\Delta} \ln\left(\frac{1}{P_{\text{exc}}} - 1\right) = \frac{1}{\Delta} \ln\left(\exp\left(\frac{\pi\Delta^2}{2\hbar v}\right) - 1\right) \quad (21)$$

For small P_{exc} (i.e., in the adiabatic regime), we can approximate:

$$\ln(\exp(A) - 1) \approx A \Rightarrow \beta_{\text{eff}} \approx \frac{\pi\Delta}{2\hbar v} \quad (22)$$

This results in the proportionality:

$$\beta_{\text{eff}} \propto \frac{\Delta^2}{v} \quad (23)$$

In most practical implementations, the Hamiltonian is interpolated via a schedule $s(t)$, with $s(0) = 0$, $s(T) = 1$. For a linear ramp $s(t) = t/T$, we have $v \propto \dot{s}(t) = 1/T$, leading to:

$$\beta_{\text{eff}} \propto \Delta^2 T \quad (24)$$

$$E'(x) = \alpha E(x) \quad (27)$$

This fundamental relationship illustrates that slower sweeps (larger T) yield lower effective temperatures and distributions that are more sharply peaked around the ground state. In the context of Bayesian filtering, this directly controls the concentration of the posterior approximation. Consequently, β_{eff} plays a critical role in tuning the quality and fidelity of the resulting distribution, and must be taken into account when designing quantum filtering procedures.

6 CALIBRATION OF THE ENERGY SCALE

As shown in the previous section, the effective inverse temperature β_{eff} determines how sharply the final quantum state concentrates near the ground state. In the context of Bayesian filtering, this affects the shape of the posterior distribution obtained from a quantum annealing. If $\beta_{\text{eff}} \neq 1$, the resulting distribution deviates from the intended target density. To correct for this deviation, we introduce a scalar energy scaling factor α such that the product $\alpha \cdot \beta_{\text{eff}} = 1$, restoring the desired statistical form.

6.1 Motivation and Objective

To illustrate the effect of the effective inverse temperature on the resulting distribution, we assume that both the prior and the likelihood are Gaussian. In this case, the energy function used in the quantum annealing process corresponds to the negative logarithm of Gaussian density itself. The quantum system then evolves into a mixed state whose measurement statistics approximate a Boltzmann distribution with energy $E(x)$ and inverse temperature β_{eff} . As a result, the resulting distribution is:

$$P_{\text{sim}}(x) \approx \frac{1}{Z_{\text{eff}}} \exp(-\beta_{\text{eff}} E(x)) \quad (25)$$

For quadratic energies of the form $E(x) = \frac{(x-\mu)^2}{2\sigma^2}$, this becomes:

$$P_{\text{sim}}(x) \propto \exp\left(-\frac{\beta_{\text{eff}}}{2\sigma^2}(x-\mu)^2\right) \quad (26)$$

If $\beta_{\text{eff}} > 1$, the distribution is narrower than intended; if $\beta_{\text{eff}} < 1$, it is broader. To ensure that the quantum simulation reflects the desired distribution shape, we rescale the energy function prior to execution:

Choosing $\alpha = 1/\beta_{\text{eff}}$ yields:

$$P_{\text{sim}}(x) \propto \exp(-\beta_{\text{eff}} \cdot \alpha E(x)) = \exp(-E(x)) \quad (28)$$

This correction aligns the quantum-measured distribution with the original posterior target.

6.2 Estimating β_{eff}

To determine the appropriate scaling factor α , we must first estimate β_{eff} empirically. This can be accomplished through histogram analysis of the measured quantum output. The procedure is as follows:

1. Run the quantum sweep using the unscaled Hamiltonian ($\alpha = 1$).
2. Measure the resulting distribution $P_{\text{sim}}(x)$.
3. Perform a logarithmic transformation:

$$\ln P_{\text{sim}}(x) = c - \beta_{\text{eff}} E(x) \quad (29)$$

where $c = -\ln Z_{\text{eff}}$ is an unknown constant offset.

4. Fit a straight line to the data $\{x_i, \ln P_{\text{sim}}(x_i)\}$ using least squares. The slope yields an estimate of $-\beta_{\text{eff}}$.

Only data points with $P_{\text{sim}}(x) > 0$ are considered in the fit to avoid singularities.

Once β_{eff} has been estimated, we define the energy scaling factor as:

$$\alpha = \frac{1}{\beta_{\text{eff}}} \quad (30)$$

This scaling is then applied to the Ising Hamiltonian before the next quantum run. In practice, this calibration step ensures that the simulated posterior matches the desired Bayesian update distribution in both shape and concentration. The correction is particularly important for accurately capturing uncertainties in probabilistic inference, where even slight distortions in variance can significantly affect the interpretation of the result.

7 NUMERICAL EVALUATION

To assess the performance of our adiabatic quantum filtering method, we compare the output distribution of the AQC-based approach with both the exact Bayesian posterior and an alternative quantum method referred to as *Quantum Flow*, which is based on a gate-based

realization of the posterior update in proposed this work [3].

Figure 1 shows the resulting probability distributions for a concrete one-dimensional filtering example. The prior distribution is Gaussian with mean $\mu = 9$ and standard deviation $\sigma = 3$. The likelihood is centered at $z = 17$ with $\sigma = 4$. The exact posterior is then analytically given by a Gaussian with mean $\mu = 11.880$ and $\sigma = 2.4$.

Our AQC-based approach was executed with an energy scaling factor $\alpha = 0.33$, yielding an empirical distribution with mean $\mu = 12.175$ and standard deviation $\sigma = 2.116$. The Quantum Flow approach produces a slightly lower mean $\mu = 10.53$ while matching the posterior width exactly with $\sigma = 2.4$.

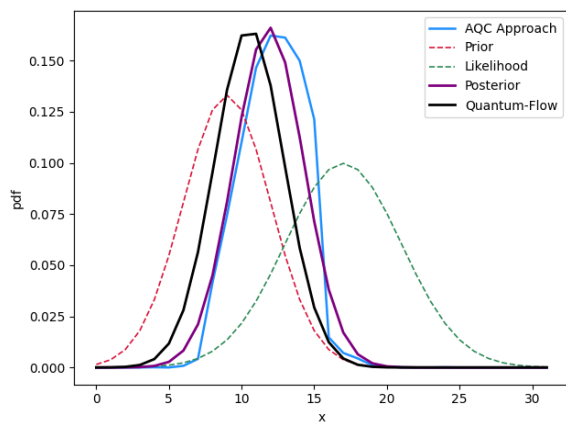


Figure 1: Comparison of the output distribution from the AQC-based approach and the gate-based Quantum Flow method against the analytical posterior.

Method	Mean	Std
Posterior (analytical)	11.880	2.400
Quantum Flow	10.530	2.400
AQC Approach	12.175	2.116

Table 1: Comparison of the mean and standard deviation of the posterior approximation obtained by different quantum methods.

Both quantum methods closely approximate the correct posterior distribution. The AQC-based solution slightly overestimates the posterior mean but provides a sharper distribution. The Quantum Flow approach matches the target standard deviation but slightly underestimates the mean. These results highlight that the proposed adiabatic method can yield accurate posterior approximations from raw quantum measurement statistics without explicit gate synthesis of the update rule.

It is important to emphasize that the energy scaling factor $\alpha = 0.33$ used in this example was not fine-tuned, but rather estimated heuristically based on a single calibration run. Despite this lack of optimization, the re-

sulting AQC distribution matches the shape and location of the posterior with reasonably high accuracy.

This indicates that the proposed adiabatic approach is robust under approximate calibration and does not require precise knowledge of the effective temperature a priori. Further improvement could be achieved by systematically analyzing the energy gap Δ along the annealing path and its influence on the effective temperature. This would allow for targeted adjustment of the ramp duration or energy scaling to better align the resulting distribution with the theoretical posterior.

8 CONCLUSION

We have presented a novel approach to the Bayesian filtering update using adiabatic quantum computing. By encoding the likelihood into an Ising-type Hamiltonian, the posterior distribution emerges from the final quantum state after annealing. Numerical results demonstrate that even without fine-tuning, the resulting distributions approximate the target posterior with a close match. This suggests that AQC offers a scalable and physically grounded alternative to gate-based implementations of probabilistic inference. Future work may explore optimization of annealing schedules, analysis of spectral gaps, and hardware implementation on existing quantum annealers.

9 REFERENCES

- [1] M. Born and V. Fock. Beweis des adiabatensatzes. *Zeitschrift für Physik*, 51(3–4):165–180, 1928.
- [2] F. Govaers. *Theory and Methods for Distributed Data Fusion Applications*. Radar, Sonar and Navigation. The Institution of Engineering and Technology (IET), 2023.
- [3] F. Govaers. On a quantum realization of the bayesian filtering using the log homotopy flow. In *Proceedings of the 2024 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI)*, pages 1–6, 2024.
- [4] T. Kadowaki and H. Nishimori. Quantum annealing in the transverse ising model. *Physical Review E*, 58(5):5355–5363, 1998.
- [5] W. Koch. *Tracking and Sensor Data Fusion: Methodological Framework and Selected Applications*. Mathematical Engineering. Springer, 2013.
- [6] C. C. McGeoch. *Adiabatic Quantum Computation and Quantum Annealing: Theory and Practice*. Morgan & Claypool Publishers, 2014.
- [7] A. Perdomo-Ortiz, M.-H. Yung, et al. High-quality thermal gibbs sampling with quantum annealing hardware. *Physical Review Applied*, 17(4):044046, 2022.
- [8] C. Sun. Derivation of the landau-zener formula via functional equations, 2025.

Model-driven development of heterogeneous quantum models for multi-vehicle route planning

Furkan Polat	Hasan Tunçer	Hamed Gholipour	Joao Neves	Moharram Challenger
Koç	Purdue	University of Beira	University of Beira	University of Antwerp
University	University	Interior	Interior	& Flanders Make
fpolat17	htuncer	hamed.gholipour	jcneves	moharram.challenger
@ku.edu.tr	@purdue.edu	@ubi.pt	@ubi.pt	@uantwerpen.be

ABSTRACT

Quantum computing has the potential to significantly improve large-scale optimization, particularly in logistics. However, practical adoption remains limited due to fragmented hardware ecosystems and the complexity of quantum programming. We present **MDE4QC**, a model-driven engineering framework that introduces a Platform-Independent Model (PIM) for defining routing problems at a high level of abstraction. The framework automatically transforms these models into executable code for quantum annealers, gate-based quantum systems, and classical solvers. MDE4QC is integrated with cloud platforms such as D-Wave and IBM Qiskit and supports hybrid execution flows. An intuitive graphical interface enables users to define routing problems without writing quantum or classical code. Users simply select the target platform and configure problem parameters through a user-friendly interface; the framework handles model generation, transformation, and execution. We validate MDE4QC using open-access real logistic data from the City of Antwerp to demonstrate its ability to reduce development effort, ensure cross-platform portability, and deliver measurable gains in routing efficiency.

Keywords

Quantum computing, model-driven engineering, platform-independent modeling, route optimization, quantum annealing, hybrid solvers, domain-specific modeling language, logistics

1 INTRODUCTION

Quantum computing holds great promise for solving large-scale optimization problems [1, 2], especially in fields like logistics and transportation [3]. However, its adoption in real-world applications remains limited [4]. One of the key challenges is the heterogeneity of the current quantum ecosystem: Different hardware providers, programming interfaces, execution pipelines, and cloud platforms make development complex and fragmented.

Model-Driven Engineering (MDE) has a proven history in classical software engineering to reduce complexity by enabling users to work at a higher level of abstraction [5, 6, 7]. It simplifies development through automatic code generation and platform-independent design.

In this paper, we use MDE4QC, a framework that brings the principles of MDE to quantum computing [8, 9]. MDE4QC allows users to define routing problems using a hardware-agnostic model, which can then be automatically transformed into executable code compatible with various quantum and hybrid backends. Through a case study on multi-vehicle route planning, we demonstrate how this approach can make quantum-enhanced optimization more accessible to logistics practitioners without requiring deep expertise in quantum computing.

1.1 Motivation and Problem Statement

Modern logistics increasingly relies on solving high-frequency, large-scale routing problems with high precision. This is pivotal not only for reducing operational costs and ensuring timely deliveries but also for addressing larger systemic issues such as fuel efficiency and urban traffic congestion. As the number of vehicles, operational constraints, and dynamic environmental factors grow, the complexity of these optimization problems often exceeds the capabilities of traditional computational methods [10].

Quantum computing presents a promising frontier for addressing such combinatorial optimization problems. Yet, the current quantum ecosystem is highly fragmented. The coexistence of multiple hardware vendors, inconsistent programming interfaces, and heterogeneous execution models introduces substantial technical overhead [11]. For logistics professionals lacking a background in quantum technologies, these inconsistencies pose a significant barrier to effective adoption. Quantum cloud services have made it easier to access quantum hardware, but variations in how each platform works and the different programming languages they use still make it difficult to combine them effectively. Implementing and maintaining quantum algorithms across various providers still demands advanced

expertise and often leads to redundant development efforts.

This context underscores the value of a model-driven approach. Our proposed framework, **MDE4QC** (Model-Driven Engineering for Quantum Computing), mitigates these challenges by providing platform-independent abstractions, automated model-to-model transformations, and infrastructure-agnostic execution pathways. This enables logistics experts to specify routing problems using high-level modeling constructs, while the system transparently handles the synthesis and execution of suitable quantum or hybrid solutions based on the current computational resources.

Crucially, the benefits of MDE4QC extend beyond computational performance. By enabling more efficient routing, the framework contributes to the reduction of fuel consumption and greenhouse gas emissions—particularly vital in urban contexts where smart routing directly affects environmental sustainability. Moreover, by integrating live data streams such as traffic conditions and weather forecasts, MDE4QC could facilitate adaptive, eco-aware decision-making. These capabilities support broader policy objectives, such as those outlined in the European Green Deal, and emphasize the framework's societal impact and alignment with sustainable development goals [12].

1.2 Objectives and Contributions

This paper makes the following key contributions to the field of quantum-enabled logistics optimization:

1. **MDE4QC Framework:** Transforms high-level logistics problems into executable solutions for classical, quantum, and hybrid platforms. Model Transformation of this framework converts abstract models into validated, optimized, and deployable code across platforms [13].
2. **Platform-Agnostic Modeling:** Uses a domain-specific language to support classical (e.g., K-Means, GNN), annealing, and gate-based quantum methods [14]. This modelling language allows users to define routing problems graphically, with no coding required (no code approach) [15].
3. **Solver Selection:** Chooses the best solver based on problem size, hardware availability, and cost-performance trade-offs. The cloud integration of the framework connects with major quantum and classical platforms as solvers for automated execution and result collection [16].
4. **The City of Antwerp Case Study:** Validated on real routing data from the City of Antwerp to benchmark solver performance [17]. It uses live traffic and environmental data to cut fuel use and emissions [18].

This paper is organised as follows: Section 2 discusses the related work in the literature. The fundamentals and background for this study are elaborated in Section 3. Section 4 presents the architecture for the proposed framework and discusses its implementation details. The framework is evaluated in section 5 using a case study, and the results are discussed in section 6. Finally, the paper is concluded in section 7.

2 RELATED WORK

In recent years, the convergence of quantum computing and route optimization has garnered substantial interest, driven by the need to address scalability challenges that classical methods often encounter. Traditional techniques for solving the Multi-Vehicle Routing Problem (MVRP), including mixed-integer programming, evolutionary strategies, and more recently, machine learning-based approaches such as Graph Neural Networks (GNNs), have achieved notable success [19, 20]. Nevertheless, these models frequently face difficulties in handling high-dimensional, constraint-rich scenarios, especially in real-time urban logistics environments.

Quantum computing introduces a new paradigm for tackling combinatorial problems by Utilizing unique properties such as superposition and entanglement. Notable frameworks, including the Quantum Approximate Optimization Algorithm (QAOA) [21] and the Binary Quadratic Model (BQM) utilized in D-Wave systems [22], have shown promising results in constrained optimization tasks. Fitzek et al. [23] demonstrated the effectiveness of QAOA in heterogeneous vehicle routing scenarios, underscoring the advantages of quantum speedup under certain conditions. Further studies by Willsch et al. [24] and Neukart et al. [25] applied quantum annealing to traffic-aware routing, although their implementations were limited by current hardware constraints and embedding overheads. A central barrier to the broader adoption of quantum approaches lies in the fragmented nature of the quantum computing landscape. Each platform typically requires distinct programming interfaces and problem formulations, which complicates the development process and inhibits portability. To mitigate this, researchers have increasingly adopted Model-Driven Engineering (MDE) techniques to introduce abstraction layers and reduce platform dependency. One early example is the MDE4QP framework [26], which applied model-driven principles to quantum chemistry, facilitating code generation for both gate-based and annealing architectures through automated transformations.

This paper builds upon that foundation by presenting MDE4QC, a model-driven framework specifically designed for quantum-enhanced logistics optimization. MDE4QC introduces a domain-specific modeling lan-

guage (DSML) and transformation pipeline that supports both classical and quantum solvers, including IBM Qiskit and D-Wave. Unlike prior tools, MDE4QC allows users to define problems through a visual interface and execute solutions across heterogeneous platforms without requiring low-level quantum programming expertise. Empirical validation using open urban data further emphasizes the framework's applicability to real-world logistics problems.

MDE4QC supports cloud-native deployment via an interactive dashboard and RESTful APIs. The API is designed to let external systems bypass the UI and communicate directly with solvers, enabling automation and integration in industrial workflows. The framework aligns with recent advances in hybrid quantum-classical computing [27] and supports scalable, interoperable solutions for smart cities and complex logistics systems.

3 FUNDAMENTALS

This section elaborates on the fundamental topics required to understand this paper, including Model-Driven Engineering (MDE), MDE for Quantum Computing, Platform Independent Modelling, QAOA algorithm and quantum annealing samplers.

3.1 Model-Driven Engineering (MDE)

Model-Driven Engineering (MDE) is a software development paradigm that prioritizes the use of high-level, abstract models as the core artifacts throughout the engineering process. Instead of relying primarily on manually written source code, MDE emphasizes the use of domain-specific modeling languages (DSMLs) to represent the key aspects of a system or problem domain. These models become the basis for both system design and implementation [28, 29].

By elevating the level of abstraction, MDE facilitates clearer communication among stakeholders, supports early validation of system designs, and promotes the reuse of established architectural patterns. Through automated model-to-model and model-to-code transformations, MDE streamlines code generation and minimizes manual implementation errors. This methodology has demonstrated particular value in complex and heterogeneous environments, including embedded systems, enterprise platforms, and automotive domains such as AUTOSAR [30, 31].

3.2 MDE for Quantum Computing (MDE4QC)

Quantum computing platforms are inherently diverse. Gate-based systems and quantum annealers represent two fundamentally different approaches to quantum computation. In addition, real-world systems are deployed across hardware with distinct capabilities,

connectivity constraints, and programming interfaces. This variability creates a fragmented ecosystem, making development more difficult and reducing the portability of algorithms.

Our previous work on ground state energy calculations introduced a unified framework, MDE4QP, that uses model-driven abstractions to bridge the gap between quantum annealing and gate-based models. That framework demonstrated how domain-specific abstractions could be translated into platform-specific implementations via systematic model-to-model and model-to-code transformations, allowing the same solution to be expressed and executed across both types of quantum device [8].

In this paper, we extend that vision to a new application domain, multivehicle routing optimization, where quantum computing shows promise but suffers from the same fragmentation and entry barriers. MDE4QC, our updated framework, enables users to define routing problems at a high level using a platform-independent modeling language. These models are then automatically transformed into quantum formulations suited for specific architectures, such as Binary Quadratic Models (BQM) for D-Wave annealers or Qubit-Hamiltonian expressions for variational quantum algorithms (VQAs) on platforms like Qiskit or Cirq.

This abstraction allows algorithm designers and logistics practitioners to express optimization problems without needing deep knowledge of quantum physics, hardware, or SDKs. Moreover, it supports cross-platform evaluation, facilitating empirical comparisons between quantum annealing and gate-based solutions on real-world routing problems [9].

Building on insights from our prior research, this work prioritizes hardware-agnostic modeling, automated transformation pipelines, and a standardized development lifecycle. The result is a robust framework that not only simplifies quantum software engineering but also brings practical quantum optimization closer to adoption in industrial and urban logistics.

3.3 Quantum Approximate Optimization Algorithm (QAOA)

The Quantum Approximate Optimization Algorithm (QAOA) is a hybrid quantum-classical approach designed to solve combinatorial optimization problems by alternating quantum operators derived from problem-specific cost and mixing Hamiltonians [21]. In this work, we integrate QAOA with Graph Neural Networks (GNNs) to address traffic route optimization in urban transportation networks. The GNN models dynamic traffic conditions using spatiotemporal data and updates edge weights representing congestion and travel times [32]. These predicted weights are encoded into a cost Hamiltonian that guides the QAOA circuit

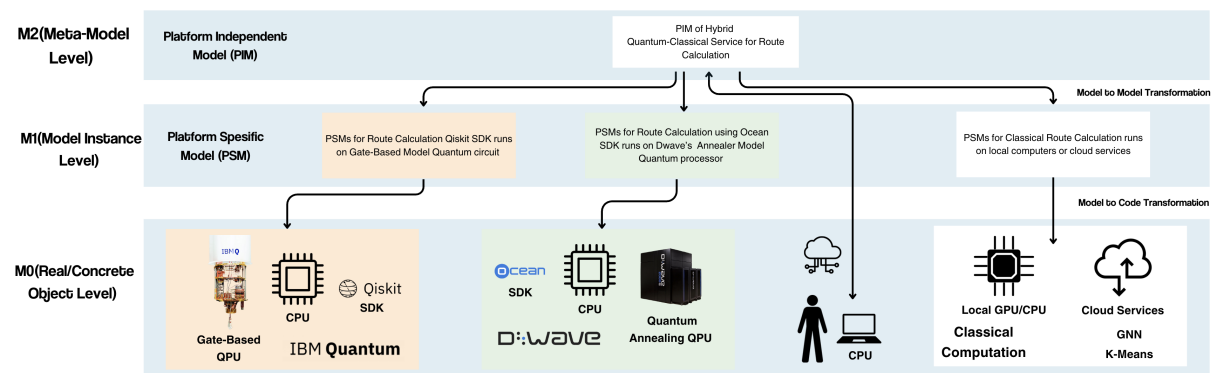


Figure 1: MDE4QC Framework for Hybrid Quantum-Classical Route Optimization. The PIM layer defines platform-independent route optimization models, while the PSM layer specifies platform-specific implementations using Qiskit (IBM Quantum), Ocean SDK (D-Wave), or classical methods (GNN, K-Means).

toward optimal routing decisions [33]. The hybrid framework leverages GNNs for learning accurate traffic patterns and QAOA for efficient exploration of optimal paths via quantum state evolution. This integration offers a scalable and adaptive solution for real-time route planning, logistics optimization, and intelligent transportation systems, particularly suited for deployment on near-term quantum devices.

3.4 Quantum Annealing Samplers

Quantum annealing samplers serve as critical interface engines that facilitate practical implementation of adiabatic quantum computation for large-scale optimization problems [34]. The *LeapHybridNLSampler* specializes in non-linear optimization formulations, automatically performing problem decomposition and variable embedding to handle complex routing constraints [35]. The *LeapHybridDQMSampler* operates on Discrete Quadratic Model formulations, mapping discrete decision variables to quantum annealing problems with penalty-based constraint enforcement [36]. These samplers implement intelligent partitioning strategies that identify subproblems suitable for quantum acceleration while delegating preprocessing tasks to classical algorithms [37]. The hybrid architecture automatically handles quantum embedding, error mitigation, and solution validation, making quantum annealing accessible for enterprise-scale logistics optimization [38].

3.5 Platform Independent Modelling

Cloud-based quantum computing platforms such as IBM Qiskit, Google Cirq, Amazon Braket, and D-Wave Leap enable users to execute quantum algorithms remotely via their respective SDKs [39, 40, 41, 42]. These environments primarily support Python, but are increasingly extending compatibility to other programming languages including C++, JavaScript, and Q# through RESTful APIs, Jupyter notebook interfaces, and language bindings. Additionally, they offer

graphical user interfaces, quantum simulators, and visualization tools that facilitate both beginner-level experimentation and the development of advanced quantum applications.

Despite these advancements, a critical challenge to the practical adoption of quantum computing remains: platform fragmentation. Each provider defines distinct programming paradigms, toolchains, and circuit specification interfaces. As a result, developers must master multiple APIs and re-implement problem logic to accommodate each backend, posing a significant barrier to entry and scalability [43, 44].

To address this limitation, we propose the **Model-Driven Engineering for Quantum Computing (MDE4QC)** framework, which introduces a **Platform-Independent Modeling (PIM)** methodology specifically adapted for quantum applications. Rather than writing platform-specific code, users define high-level, platform-agnostic models of their problems—such as a multi-vehicle routing scenario. These abstract specifications are then automatically transformed into **Platform-Specific Models (PSMs)** tailored to the syntax and semantics of the target quantum backends. For instance, a single PIM model can be mapped to a variational quantum circuit in Qiskit or translated into a quantum annealing formulation compatible with D-Wave's architecture. The overall architecture of the MDE4QC framework is illustrated in Figure 1.

This model-driven approach abstracts away the need for backend-specific programming skills. Domain parameters—such as the number of vehicles, route constraints, cost objectives, or Ising model representations—are captured declaratively within the PIM. They are subsequently compiled into executable code via automated model transformations. Tasks that traditionally required extensive manual coding and SDK-specific integration are now streamlined into a fully automated workflow.

In our prior work, we demonstrated this capability by deploying a unified PIM for ground state energy estimation on both Qiskit and D-Wave platforms without modifying the original model [10]. Here, we extend this methodology to **quantum-enhanced logistics optimization**, enabling seamless execution across heterogeneous quantum environments [45].

4 ARCHITECTURE AND IMPLEMENTATION

The system uses a modular, layered architecture that clearly separates different tasks and allows easy integration of classical and quantum optimization methods. Each layer can be extended independently and communicates with others through defined interfaces (see Figure 2 for an overview).

The development of this framework involved adapting key back-end-specific implementations from existing open-source projects. In particular, the routing optimization component for the D-Wave back-end was originally derived from the *D-Wave Ocean SDK example repository*, which provided a robust foundation for quantum annealing-based formulations [46]. We gratefully acknowledge D-Wave Systems Inc. for making these examples publicly available. Furthermore, our complete implementation, including model transformations and platform-specific templates, is made openly accessible via the *MDE4QC GitHub repository* [47].

4.1 Solvers Group

The solvers group represents the computational center of the system, divided into quantum and classical components. The quantum solvers utilize both D-Wave's annealing technology and IBM's gate-based quantum computing capabilities. The D-Wave integration includes specialized samplers for different problem types, while the IBM Quantum integration provides QAOA implementation with configurable optimization parameters.

The D-Wave implementation employs two hybrid quantum-classical samplers: `LeapHybridNLSampler` and `LeapHybridDQMSampler`. The former targets non-linear optimization problems such as complex routing scenarios, while the latter is suited for Discrete Quadratic Models (DQMs). Both samplers automate problem decomposition, embedding, and qubit mapping, enabling scalable optimization with built-in solution validation.

The IBM Quantum pipeline applies QAOA via Qiskit to solve the Capacitated Vehicle Routing Problem (CVRP). The problem is formulated using binary variables within the `QuadraticProgram` class, converted to a QUBO, and optimized using the `MinimumEigenOptimizer` with COBYLA (100

iterations, `reps=2`). Final routes are extracted using `NetworkX`.

Classical solvers complement the quantum components by offering GNN-based route prediction and K-Means clustering. The GNN models learn from historical patterns to propose effective routing schemes [48], while K-Means efficiently partitions the location space [49]. A dynamic solver selection mechanism chooses the most appropriate method based on problem characteristics, ensuring robust performance across different scales.

4.2 Data Layer

The data layer bridges the gap between raw logistics data and optimization engines, with support tailored for the City of Antwerp Open Data Portal [50]. Datasets include structured location data such as public bike parking, facilities, and service points in CSV format. The system imports these datasets directly, extracting object IDs, coordinates, and names.

To ensure compatibility, the system performs coordinate transformations from EPSG:3857 to EPSG:4326 and validates all required fields. This preprocessing phase ensures that incoming data is fully compatible with the optimization solvers. Technologies used include `osmnx` for road network graph generation, `networkx` for graph operations, and `pyproj` for coordinate transformations. `Pandas` handles tabular data management, while `folium` enables map-based visualization. `Diskcache` is employed for local result caching to enhance responsiveness.

The system also features a user-friendly Dash interface. Users can upload files through a drag-and-drop interface or select from existing entries in the `assets/CSVs` directory. Uploaded files are automatically processed, including coordinate transformation and route metadata extraction, readying the data for downstream optimization.

4.3 External Dependencies

The system relies on several external packages and SDKs. Web-based visualization and interaction are managed through `Dash`, `Folium`, and `OSMnx`. Quantum capabilities are supported via the D-Wave Ocean SDK (including `dimod` for problem formulation) and the IBM Qiskit stack (including `qiskit-algorithms` and `qiskit-optimization`). Classical machine learning functionality is implemented using `PyTorch` and `PyG`, while logistics graph processing and coordinate transformations are handled with `NetworkX`, `PyProj`, `Pandas`, `NumPy`, and `SciPy`. Performance optimization utilizes `diskcache` for result caching and `multiprocess` for parallel execution. The system integrates with ERP and WMS platforms for

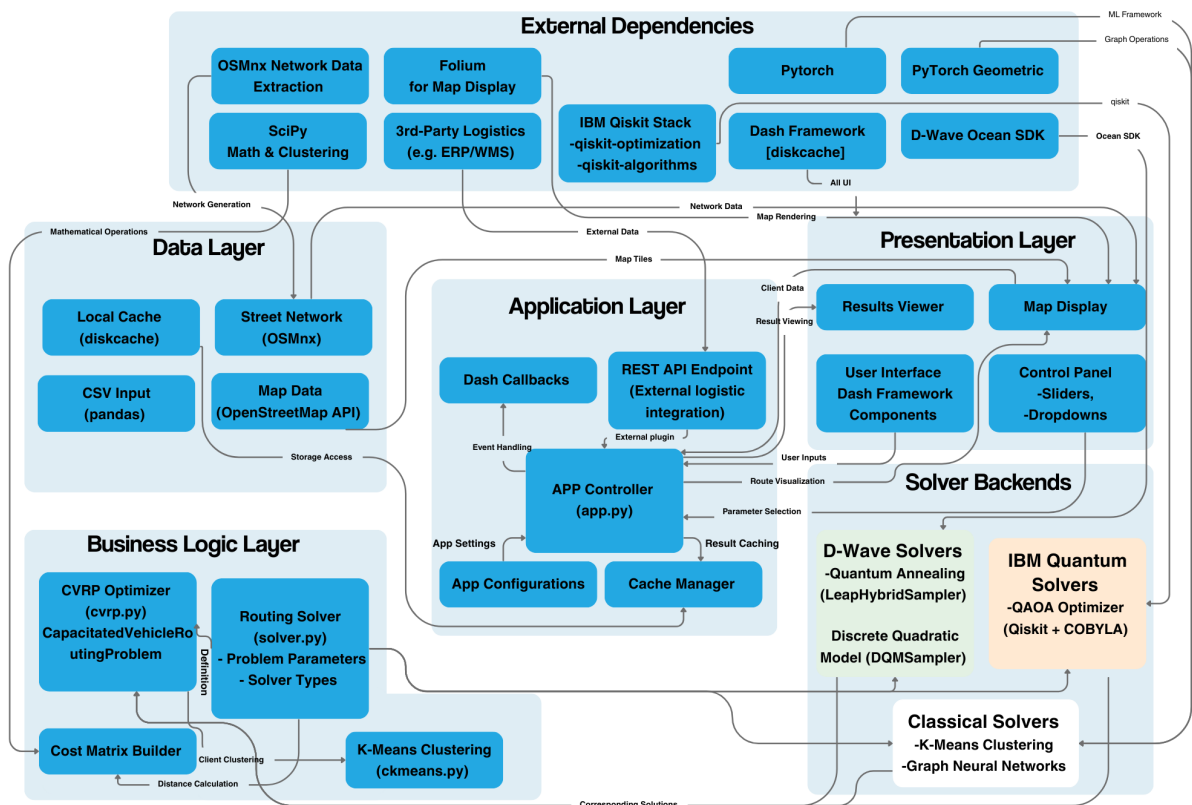


Figure 2: System architecture of the MDE4QC framework for hybrid quantum-classical route optimization. The architecture is organized into layered modules: the Data Layer handles geographic inputs and caching, the Application Layer manages user interaction and API calls, and the Business Logic Layer defines solver logic. Solver Backends support quantum (D-Wave and IBM Qiskit) and classical (K-Means, GNN) algorithms. External Dependencies provide libraries and SDKs used across all layers. Inter-layer communication flows are shown, including event handling, parameter passing, and result rendering.

real-time logistics data and utilizes the OpenStreetMap API for additional geographic information.

5 CASE STUDY: MULTI-VEHICLE ROUTE PLANNING

This section presents the real-world application of our MDE4QC framework to the Multi-Vehicle Route Planning (MVRP) problem, implemented and tested using real map data from the City of Antwerp¹. The problem builds upon the Capacitated Vehicle Routing Problem (CVRP), a classical NP-hard optimization task that requires assigning client visits to a fleet of vehicles such that each vehicle respects its capacity constraint and the overall travel distance is minimized [51].

Unlike simplified formulations, our implementation captures the spatial and logistical complexity of real-world transport systems [52]. It includes detailed geographic representations, multiple vehicle types,

depot configurations, and hybrid cost models based on either road network routing or Euclidean geometry.

Figure 3 illustrates the types of scenarios designed to support by our system. These range from conventional single-depot delivery routing to advanced use cases like dynamic route recalculation in real-time or handling heterogeneous fleets. These variations require different encoding strategies, cost models, and solver configurations at both the Platform-Independent Model (PIM) and Platform-Specific Model (PSM) levels.

The City of Antwerp dataset consists of real geo-coordinates, mapped to the nearest road nodes using OSMnx [52]. Depending on vehicle type, vehicles are routed across this network using Dijkstra's algorithm or Euclidean metrics. Capacity constraints are handled either via penalty encoding in quantum solvers or direct enforcement in classical logic [53].

A brute-force approach is infeasible due to factorial scaling in clients and exponential scaling in vehicles. To overcome this, our modular solver architecture supports classical heuristics (e.g., K-Means [54]) and

¹ <https://portaal-stadantwerpen.opendata.arcgis.com/>

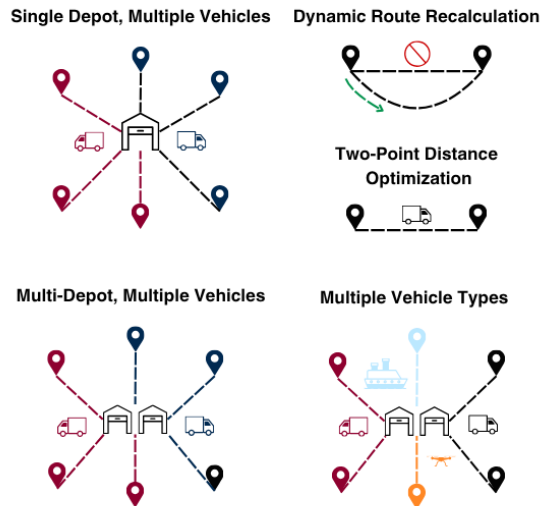


Figure 3: Optimization scenarios modeled within the MDE4QC framework. The figure highlights key variations in routing complexity: depot configurations (single vs. multiple), vehicle heterogeneity (trucks, drones, boats), and dynamic considerations such as route recalculation and short-distance delivery optimization.

quantum algorithms like QAOA [21] and LeapHybrid solvers [55].

6 RESULTS AND DISCUSSION

This section presents empirical evaluation of the MDE4QC framework through benchmarks comparing quantum and classical solvers. Our goal was to measure solver efficiency and provide information for strategic decision-making.

Evaluation metrics:

- Total distance (m): Sum of all routes.
- Computation time (s): Optimization duration.
- Load distribution: Client-to-vehicle balance.
- Scalability: Solver response to increased client locations.

Benchmarking approach

We tested D-Wave hybrid quantum annealing and classical K-Means clustering across 18 scenarios (10–2013 clients). For each, we recorded:

- Objective distance
- Execution time

Regression models derived from these results guide future solver selection [56].

Distance and Time Projections

We applied cubic polynomial regression:

$$D(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

to fit total distance and time metrics. Figures 4 and 5 depict the results.

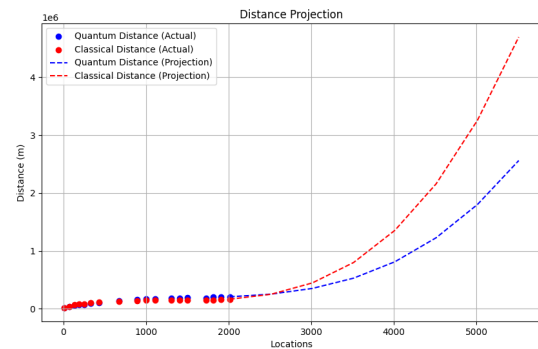


Figure 4: Total distance vs. client locations. Polynomial regression forecasts quantum (Blue line, bottom) vs. classical (Red line, top) crossover points.

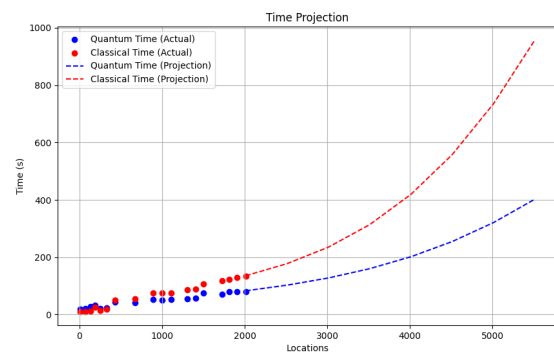


Figure 5: Computation time vs. client locations. Classical solvers scale better beyond 1300 clients.

Solver Decision Model

We developed a cost-based decision model to determine when quantum solvers are preferable over classical ones. The model compares distance savings against computational time costs to guide solver selection in a practical, scenario-dependent way.

Quantum solvers generally produce shorter total route distances, which reduces fuel consumption and operational costs. However, they are slower and more expensive to run. Classical solvers are faster and cheaper but often generate longer routes. The model calculates the net benefit using:

$$\Delta Cost = (D_C - D_Q) \cdot c_d - (T_Q - T_C) \cdot c_t$$

where:

- D_C, D_Q : Route distances from classical and quantum solvers,
- T_C, T_Q : Solver runtimes,
- c_d : Cost per kilometer,
- c_t : Cost per unit time.

A positive $\Delta Cost$ means the quantum solver offers financial advantage.

We implemented this model in a spreadsheet to allow users to adjust inputs such as delivery count, distance cost, and compute cost. Solver behavior is estimated using regression equations derived from empirical test runs. This makes the model usable without requiring programming or domain expertise.

Discussion

The implementation of the MDE4QC framework underscores the evolving potential of hybrid quantum-classical optimization in real-world logistics. While the empirical advantages of hybrid solvers—in the scope of this study D-Wave’s LeapHybrid models—are evident in medium-scale routing scenarios, their practical deployment raises important considerations. Notably, quantum solvers demonstrate superior performance in exploring complex solution spaces, yet this comes at the cost of increased runtime and hardware resource consumption, which may not be justifiable in time-sensitive or cost-sensitive contexts [57].

The inclusion of a decision-support mechanism within MDE4QC represents a step forward in balancing these trade-offs. By quantifying key parameters—such as route efficiency, execution delay, and computational cost—it shifts solver selection from heuristic choice to evidence-based reasoning.

Despite the framework’s support for platform-independent modeling, full integration with gate-based quantum platforms remains incomplete. This reflects a challenge in the NISQ era, where hardware limitations constrain the real-world applicability of algorithms like variational quantum algorithms (VQAs) [27]. While promising, the utility of gate-based methods in logistics contexts remains largely theoretical and awaits further maturity in both software and hardware ecosystems.

An important aspect of this study is the framework’s contribution to sustainability. MDE4QC helps reduce travel distance and fuel usage, which supports environmentally friendly logistics. This aligns with goals such as the European Green Deal. As a result, the framework adds value not only through technical improvements but also by promoting greener operations.

Ultimately, while MDE4QC demonstrates how model-driven engineering can mitigate the fragmentation of

the quantum computing ecosystem, its broader adoption will depend on improvements in backend compatibility, user interface integration, and adaptive capabilities in dynamic logistics settings.

7 CONCLUSION AND FUTURE WORK

The MDE4QC framework delivers a robust model-driven solution for quantum-enhanced logistics optimization by abstracting complex routing problems into high-level, platform-independent models. These are automatically transformed into executable formats suitable for both quantum and classical backends. With its hybrid solver architecture and intelligent decision-making mechanism, MDE4QC enables efficient and adaptable route planning. Validation using real-world data from the City of Antwerp confirms its effectiveness in improving routing performance and supporting environmental sustainability. While current limitations of gate-based quantum hardware remain, the framework marks a significant step toward scalable and interoperable quantum solutions for real-world logistics. Future enhancements will target broader platform integration and real-time dynamic responsiveness.

8 REFERENCES

- [1] R. Orús, S. Mugel, and E. Lizaso, “Quantum computing for finance: Overview and prospects,” *Reviews in Physics*, vol. 4, p. 100028, 2019.
- [2] A. Ajagekar and F. You, “Quantum computing for energy systems optimization: Challenges and opportunities,” *Energy*, vol. 179, pp. 76–89, 2019.
- [3] E. Osaba, E. Villar-Rodriguez, and I. Oregi, “A systematic literature review of quantum computing for routing problems,” *IEEE Access*, vol. 10, pp. 55805–55817, 2022.
- [4] E. National Academies of Sciences and Medicine, *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press, 2019.
- [5] D. Schmidt, “Guest editor’s introduction: Model-driven engineering,” *Computer*, vol. 39, no. 2, pp. 25–31, 2006.
- [6] M. Brambilla, J. Cabot, and M. Wimmer, *Model-Driven Software Engineering in Practice*, vol. 1. 09 2012.
- [7] R. France and B. Rumpe, “Model-driven development of complex software: A research roadmap,” in *Future of Software Engineering (FOSE '07)*, pp. 37–54, 2007.
- [8] F. Polat, H. Tuncer, A. Moin, and M. Challenger, “Model-Driven Engineering for Quantum Programming: A Case Study on Ground State Energy Calculation,” in *2024 IEEE 48th Annual*

- Computers, Software, and Applications Conference (COMPSAC)*, pp. 2353–2360, 2024.
- [9] A. Moin, M. Challenger, A. Badii, and S. Günnemann, “Towards model-driven engineering for quantum ai,” *INFORMATIK 2022*, 2022.
- [10] A. Moin, “Quantum-enhanced logistics: A model-driven framework for urban optimization,” *Journal of Advanced Computational Logistics*, 2023.
- [11] T. Challenger, “The fragmented landscape of quantum computing platforms: Implications for industrial applications,” *Quantum Systems and Engineering*, vol. 9, no. 2, pp. 117–132, 2024.
- [12] L. Wibert, “Sustainable logistics through adaptive quantum systems: Aligning technology with environmental goals,” *Sustainable Computing: Informatics and Systems*, 2024.
- [13] H. Moin and T. El-Sayed, “Model-driven transformation pipelines for quantum-classical systems,” *Software and Systems Modeling*, vol. 21, no. 5, pp. 889–911, 2022.
- [14] B. Challenger and M. Torres, “Platform-agnostic dsml for quantum-classical logistics optimization,” *ResearchGate*, 2023.
- [15] A. R. Nightingale, “Visual modeling interfaces in quantum-enabled supply chain management,” <https://medium.com/@arwnightingale>, 2024.
- [16] D.-W. S. Inc., “Hybrid solver service overview,” <https://www.dwavesys.com>, 2023.
- [17] R. Tanaka and M. de Vries, “Case study: Applying hybrid quantum algorithms to smart city routing in antwerp,” *Quantum Zeitgeist*, 2025.
- [18] L. Fernandez and P. Müller, “Sustainability-aware logistics with quantum and classical co-processing,” *QuantumRise Journal*, vol. 3, no. 1, pp. 45–59, 2025.
- [19] I. Bello, H. Pham, Q. V. Le, M. Norouzi, and S. Bengio, “Neural combinatorial optimization with reinforcement learning,” *arXiv preprint arXiv:1611.09940*, 2016.
- [20] E. B. Khalil, H. Dai, Y. Zhang, B. Dilkina, and L. Song, “Learning combinatorial optimization algorithms over graphs,” *Advances in neural information processing systems*, vol. 30, 2017.
- [21] E. Farhi, J. Goldstone, and S. Gutmann, “A quantum approximate optimization algorithm,” *arXiv preprint arXiv:1411.4028*, 2014.
- [22] D.-W. Systems, “Binary quadratic model (bqm) overview,” https://docs.dwavesys.com/docs/latest/doc_ocean_and_bqm.html, 2021. Accessed: 2025-05-21.
- [23] F. H. P. Fitzek *et al.*, “Applying quantum computing to the heterogeneous vehicle routing problem,” *IEEE Access*, vol. 9, pp. 130146–130157, 2021.
- [24] D. Willsch, M. Willsch, H. De Raedt, and K. Michielsen, “Benchmarking advantage quantum processor using qubo problems,” *Quantum Information Processing*, vol. 19, no. 12, pp. 1–24, 2020.
- [25] F. Neukart, G. Compostella, C. Seidel, D. Von Dollen, S. Yarkoni, and B. Parney, “Traffic flow optimization using a quantum annealer,” *Frontiers in ICT*, vol. 4, p. 29, 2017.
- [26] M. Challenger and A. Moin, “Model-driven engineering for quantum platforms: The mde4qp approach,” *Software and Systems Modeling*, vol. 22, no. 2, pp. 389–410, 2023.
- [27] D. J. Egger, J. Mareček, and S. Woerner, “Hybrid quantum–classical algorithms and quantum error mitigation,” *Nature Reviews Physics*, vol. 3, no. 12, pp. 734–748, 2021.
- [28] D. C. Schmidt, “Model-driven engineering,” *Computer*, vol. 39, no. 2, pp. 25–31, 2006.
- [29] M. Brambilla, J. Cabot, and M. Wimmer, *Model-driven software engineering in practice*. Morgan Claypool, 2017.
- [30] S. Sendall and W. Kozaczynski, “Model transformation: the heart and soul of model-driven software development,” *IEEE software*, vol. 20, no. 5, pp. 42–45, 2003.
- [31] B. Becker and *et al.*, “Model-based development of embedded systems,” in *Proceedings of the 6th ACM IEEE International conference on Embedded software*, pp. 135–144, ACM, 2006.
- [32] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, “A comprehensive survey on graph neural networks,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2020.
- [33] S. Hadfield, Z. Wang, B. O’Gorman, E. G. Rieffel, D. Venturelli, and R. Biswas, “From the quantum approximate optimization algorithm to a quantum alternating operator ansatz,” *Algorithms*, vol. 12, no. 2, p. 34, 2019.
- [34] C. C. McGeoch, “Adiabatic quantum computation and quantum annealing: Theory and practice,” *Synthesis Lectures on Quantum Computing*, vol. 5, no. 2, pp. 1–93, 2014.
- [35] A. Zaribafiyani, D. J. Marchand, and S. S. Changiz Rezaei, “Advantages of unfair quantum ground-state sampling,” *Physical Review A*, vol. 95, no. 4, p. 042306, 2017.
- [36] A. Lucas, “Ising formulations of many np problems,” *Frontiers in Physics*, vol. 2, p. 5, 2014.

- [37] K. Boothby, P. Bunyk, J. Raymond, and A. Roy, "Next-generation topology of d-wave quantum processors," *arXiv preprint arXiv:2003.00133*, 2020.
- [38] I. Hen, J. Job, T. Albash, T. F. Rønnow, M. Troyer, and D. A. Lidar, "Probing for quantum speedup in spin-glass problems with planted solutions," *Physical Review A*, vol. 92, no. 4, p. 042325, 2015.
- [39] IBM Quantum, "Qiskit: An open-source framework for quantum computing," 2023.
- [40] Google AI Quantum, "Cirq: A python framework for creating, editing, and invoking Noisy Intermediate Scale Quantum (NISQ) circuits," 2023.
- [41] Amazon Web Services, "Amazon Braket Documentation," 2023.
- [42] D-Wave Systems Inc., "Leap: The Quantum Cloud Service," 2023.
- [43] A. McCaskey and et al., "Quantum chemistry as a benchmark for near-term quantum computers," *npj Quantum Information*, vol. 5, p. 99, 2019.
- [44] G. G. Guerreschi and M. Smelyanskiy, "Platform-agnostic quantum programming: Abstracting qubit connectivity and error rates," *arXiv preprint arXiv:1810.02338*, 2018.
- [45] A. Challenger and M. Liu, "Visual analytics for quantum logistics optimization," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, 2022.
- [46] h. D-Wave Ocean code examples year=2024, "D-wave ocean sdk example projects."
- [47] h. MICSS-Lab year=2024, "Mde4qp github repository."
- [48] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, "The graph neural network model," *IEEE Transactions on Neural Networks*, vol. 20, no. 1, pp. 61–80, 2009.
- [49] S. Lloyd, "Least squares quantization in pcm," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 129–137, 1982.
- [50] C. of Antwerp, "Open data portal, city of antwerp." <https://portaal-stadantwerpen.opendata.arcgis.com/search?collection=dataset/>, 2022.
- [51] P. Toth and D. Vigo, *Vehicle Routing: Problems, Methods, and Applications*. SIAM, 2002.
- [52] G. Boeing, "Osmnx: New methods for acquiring, constructing, analyzing, and visualizing complex street networks," *Computers, Environment and Urban Systems*, vol. 65, pp. 126–139, 2017.
- [53] J. S. Otterbach *et al.*, "Unsupervised machine learning on a hybrid quantum computer," *arXiv preprint arXiv:1712.05771*, 2017.
- [54] S. Lloyd, "Least squares quantization in pcm," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 129–137, 1982.
- [55] D.-W. Systems, "D-wave hybrid solver service whitepaper," tech. rep., 2023. <https://www.dwavesys.com/whitepapers>.
- [56] T. Willems *et al.*, "Quantum optimization in real-world logistics," *Nature Quantum Applications*, 2022.
- [57] T. Willems *et al.*, "Quantum optimization in real-world logistics," *Nature Quantum Applications*, 2022.

Applications of the Tracy-Singh product of matrices in quantum computation

Fabienne Chouraqui
Department of Exact sciences
University of Haifa at Oranim, Israel
fchoura@sci.haifa.ac.il

Abstract

The Tracy-Singh product of matrices is a generalisation of the Kronecker product of matrices, called sometimes the block Kronecker product, as it requires a partition of the matrices into blocks. In this paper, we give a survey on the applications of the Tracy-Singh product in several different domains, and in particular in quantum computing.

Keywords

Yang-Baxter Equation, Quantum entanglement, Tracy-Singh product of matrices

INTRODUCTION

The Kronecker product (or tensor product) of matrices is a fundamental concept in linear algebra and the Tracy-Singh product (TS) of matrices is a generalisation of it, called sometimes the block Kronecker product, as they share many properties. While the Kronecker product of two matrices has a very natural interpretation, indeed it represents the tensor product of the corresponding linear transformations, it is not known whether the TS has a general interpretation, and it is not much understood. In this paper, we give a survey on the Tracy-Singh product of matrices and on some of its recent applications in several domains, as the Yang-Baxter equation, and quantum computing. Furthermore, some connections have been established between the TS product and a categorical construction.

1 PRELIMINARIES ON THE TRACY-SINGH PRODUCT OF MATRICES AND ITS PROPERTIES

We refer to [10], [17], [18], [23], [22] for more details. Let $A = (a_{ij})$ be a matrix of size $m \times n$ and $B = (b_{kl})$ of size $p \times q$. Let $A = (A_{ij})$ be partitioned with A_{ij} of size $m_i \times n_j$ as the ij -th block submatrix and let $B = (B_{kl})$ be partitioned with B_{kl} of size $p_k \times q_l$ as the kl -th block submatrix ($\sum m_i = m, \sum n_j = n, \sum p_k = p, \sum q_l = q$). The Kronecker (or tensor) product and the Tracy-Singh (or block Kronecker) product are defined as follows:

1. The Kronecker (or tensor) product:

$$A \otimes B = (a_{ij}b_{kl})_{ij}$$

The matrix $A \otimes B$ is of size $mp \times nq$ and the block $a_{ij}b_{kl}$ is size $p \times q$.

2. The Tracy-Singh (or block Kronecker) product:

$$A \boxtimes B = ((A_{ij} \otimes B_{kl})_{kl})_{ij}$$

The matrix $A \boxtimes B$ is of size $mp \times nq$ and the block $A_{ij} \otimes B_{kl}$ is size $m_i p \times n_j q$. For non-partitioned matrices, $A \boxtimes B = A \otimes B$.

Example 1.1. We illustrate the Tracy-Singh product with A and B partitioned into blocks: $A \boxtimes B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \boxtimes$

$$\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} (1 \ 2) \otimes \begin{pmatrix} 5 \\ 7 \end{pmatrix} & (1 \ 2) \otimes \begin{pmatrix} 6 \\ 8 \end{pmatrix} \\ (3 \ 4) \otimes \begin{pmatrix} 5 \\ 7 \end{pmatrix} & (3 \ 4) \otimes \begin{pmatrix} 6 \\ 8 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 5 & 10 & 6 & 12 \\ 7 & 14 & 8 & 16 \\ 15 & 20 & 18 & 24 \\ 21 & 28 & 24 & 32 \end{pmatrix}$$

In the following Theorems, we list important properties of the Tracy-Singh product (TS).

Theorem 1.2. [23] Let A, B, C , and D be matrices. Then

- (i) $A \boxtimes B$ and $B \boxtimes A$ exist for any matrices A and B .
- (ii) $A \boxtimes B \neq B \boxtimes A$ in general.
- (iii) $(A \boxtimes B) \boxtimes C = A \boxtimes (B \boxtimes C)$.
- (iv) $(A + B) \boxtimes (C + D) = A \boxtimes C + A \boxtimes D + B \boxtimes C + B \boxtimes D$, if $A + B$ and $C + D$ exist.
- (v) $(A \boxtimes B)(C \boxtimes D) = AC \boxtimes BD$, if AC and BD exist.
- (vi) $(cA) \boxtimes B = c(A \boxtimes B) = A \boxtimes (cB)$.
- (vii) $(A \boxtimes B)^{-1} = A^{-1} \boxtimes B^{-1}$, if A and B are invertible.
- (viii) $(A \boxtimes B)^t = A^t \boxtimes B^t$.
- (ix) $I_n \boxtimes I_m = I_{nm}$ for identity partitioned matrices.

Note that for the Kronecker product of matrices, no partition into blocks is needed.

Yet, if $A = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1s} \\ \dots & \dots & \dots & \dots \\ B_{n1} & B_{n2} & \dots & B_{ns} \end{pmatrix}$, then

$$A \otimes B = \begin{pmatrix} B_{11} \otimes B & B_{12} \otimes B & \dots & B_{1s} \otimes B \\ \dots & \dots & \dots & \dots \\ B_{n1} \otimes B & B_{n2} \otimes B & \dots & B_{ns} \otimes B \end{pmatrix}.$$

In matrix theory, the commutation matrix is used for transforming the vectorized form of a matrix into the vectorized form of its transpose.

Definition 1.3. [18] The *commutation matrix* K_{mn} is the matrix defined by:

$$K_{mn} = \sum_{i=1}^m \sum_{j=1}^n E_{ij} \otimes E_{ij}^t$$

where E_{ij} is a matrix of size $m \times n$ with a 1 in its ij -th position and zeroes elsewhere.

In words, K_{mn} is the square matrix of size mn , partitioned into mn blocks of size $n \times m$ such that the ij -th block has a 1 in its ji -th position and 0 elsewhere, with $K_{nm} = K_{mn}^{-1}$.

For example, $K_{23} = \begin{pmatrix} E_{11} & E_{21} & E_{31} \\ E_{12} & E_{22} & E_{32} \end{pmatrix}$, where E_{ij} are of size 3×2 (see [18, p383]).

Theorem 1.4. [22], [18], [15] Let A be of size $n \times s$ and B of size $m \times t$. Let K_{mn} denote the commutation matrix of size mn as in Definition 1.3. Then

(i) $B \otimes A = K_{mn}(A \otimes B)K_{st}$.

(ii) If A has a block partition into blocks A_{ij} , $1 \leq i \leq p$, $1 \leq j \leq q$, all of size $n' \times s'$, and B has a block partition into blocks B_{kl} , $1 \leq k \leq u$, $1 \leq l \leq v$, all of size $m' \times t'$:

- $A \boxtimes B = (\mathbf{I}_p \otimes K_{un'} \otimes \mathbf{I}_{m'}) \cdot (A \otimes B) \cdot (\mathbf{I}_q \otimes K_{s't'} \otimes \mathbf{I}_t)$.
- $B \boxtimes A = P \cdot (A \boxtimes B) \cdot Q$.

where P and Q are the following permutation matrices:

$$P = (\mathbf{I}_u \otimes K_{pm'} \otimes \mathbf{I}_{n'}) \cdot K_{mn} \cdot (\mathbf{I}_p \otimes K_{n'u} \otimes \mathbf{I}_{m'})$$

$$Q = (\mathbf{I}_q \otimes K_{vs'} \otimes \mathbf{I}_{t'}) \cdot K_{st} \cdot (\mathbf{I}_v \otimes K_{t'q} \otimes \mathbf{I}_{s'})$$

For more general formulas, in the case that the blocks do not have necessarily the same size, we refer to [15]. From Theorem 1.4 (ii) and (iii), the formulas connecting $A \boxtimes B$ with $B \otimes A$ and with $B \boxtimes A$ are reminiscent to the formula of change of basis, but in general the permutation matrices in Theorem 1.4 (ii) or (iii) are not the inverse one of another.

The TS product of matrices is often called a block Kronecker product, as indeed the result of the product depends on the block partition chosen for each matrix. In the special case of a matrix A of size $n^2 \times p^2$, there exists a unique block partition such that all the blocks are matrices of the same size, that we call *the canonical block partition of A*.

The following matrix is with its canonical partition into

blocks, $c = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$.

It holds that, in the special case that A and B are of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with their canonical block partitions, then $A \boxtimes B$ and $A \otimes B$ are similar matrices and the conjugating matrix is a permutation matrix, as described in Proposition 1.5 which is a direct application of Theorem 1.4.

Proposition 1.5. [15, 18, 22] Let A and B of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with a canonical block partition (into blocks of the same size $n \times p$ and $m \times q$ respectively). Let K_{mn} denote the commutation matrix of size mn . Then

$$A \boxtimes B = (\mathbf{I}_n \otimes K_{mn} \otimes \mathbf{I}_m) \cdot (A \otimes B) \cdot (\mathbf{I}_p \otimes K_{pq} \otimes \mathbf{I}_q) \quad (1.1)$$

2 APPLICATIONS OF THE TRACY-SINGH IN THE YBE AND CATEGORIES

In the following, given a linear operator $c : V \rightarrow V$, we denote also by c its representing matrix with respect to the standard basis of V , so depending on the context we consider either the operator or the matrix.

2.1 Preliminaries on the Yang-Baxter equation (YBE)

Definition 2.1. [11, Ch.VIII] Let V be a vector space over \mathbb{C} . A linear automorphism c of $V \otimes V$ is said to be an R -matrix if it is a solution of the Yang-Baxter equation

$$(c \otimes Id_V)(Id_V \otimes c)(c \otimes Id_V) = (Id_V \otimes c)(c \otimes Id_V)(Id_V \otimes c) \quad (2.1)$$

that holds in the automorphism group of $V \otimes V \otimes V$. It is written as $c^{12}c^{23}c^{12} = c^{23}c^{12}c^{23}$.

Example 2.2. ([13], [11]) Let $c, d : V \otimes V \rightarrow V \otimes V$ be R -matrices, with $\dim(V) = 2$:

$$c = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \text{ and } d = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1.5 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Here $c(e_1 \otimes e_2) = \frac{1}{\sqrt{2}} e_1 \otimes e_2 + \frac{1}{\sqrt{2}} e_2 \otimes e_1$, $d(e_1 \otimes e_2) = e_2 \otimes e_1$, with only c unitary. As a convention, we always consider the basis $\{e_i \otimes e_j \mid 1 \leq i, j \leq n\}$ of $V \otimes V$ ordered lexicographically, that is, as an example, for $n = 2$, the ordered basis of $V \otimes V$ is $\{e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2\}$.

Any solution c of the YBE yields a family of representations of the braid group B_n :

$$\begin{aligned} \rho_n^c : B_n &\rightarrow \text{GL}((\mathbb{C}^d)^{\otimes n}) \\ \sigma_j &\mapsto (Id_d)^{\otimes j-1} \otimes c \otimes (Id_d)^{\otimes n-j-1} \\ &\text{where } c : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2} \text{ and} \\ &\sigma_1, \sigma_2, \dots, \sigma_{n-1} \text{ are generators of } B_n. \end{aligned} \quad (2.2)$$

We recall two facts important for the computations: ρ_n^c is a homomorphism of groups and the property $(A \otimes B)(C \otimes D) = AC \otimes BD$ holds only if AC and BD exist. As an example, if $b = \sigma_3 \sigma_4 \sigma_3 \in B_n$, where $n = 5$, then we have the following computation:

$$\begin{aligned} \rho_n^c(b) &= ((Id_d)^{\otimes 2} \otimes c \otimes (Id_d)^{\otimes 1}) \cdot \\ &\quad ((Id_d)^{\otimes 3} \otimes c \otimes (Id_d)^{\otimes 0}) \cdot \\ &\quad ((Id_d)^{\otimes 2} \otimes c \otimes (Id_d)^{\otimes 1}) \\ &= (Id_d)^{\otimes 2} \otimes ((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d)) \end{aligned} \quad (2.3)$$

As c satisfies Eq. (2.1), we have indeed that $\rho_n^c(\sigma_3 \sigma_4 \sigma_3) = \rho_n^c(\sigma_4 \sigma_3 \sigma_4)$.

Definition 2.3. [24] Let $c : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be a solution of the YBE. Let $\mu \in \text{End}(\mathbb{C}^d)$. Let ρ_n^c be defined as in Eq. (2.2). A pair (c, μ) is an *enhanced YBE pair* if

- (i) c commutes with $\mu \otimes \mu$
- (ii) $\text{Tr}_2(c \circ \mu^{\otimes 2}) = \text{Tr}_2(c^{-1} \circ \mu^{\otimes 2}) = \mu$, where Tr_2 denotes the partial trace over the second factor.

Any oriented link is equivalent (ambient isotopic) to the trace closure of some braid b , as illustrated in Figure 2.1. Using that fact, V. Turaev shows in [24], that if

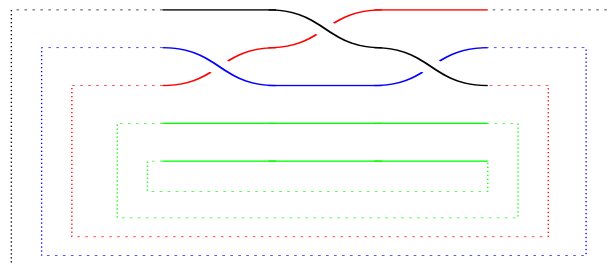


Figure 2.1: The trace closure of the braid $\sigma_3 \sigma_4 \sigma_3$ in B_5 (c, μ) is an enhanced YBE pair, then there is an appropriately normalized trace ($I_c(b)$, $b \in B_n$) of the representations ρ_n^c , that yields a link invariant:

$$I_c(b) = \text{Tr}(\rho_n^c(b) \circ \mu^{\otimes n}) \quad (2.4)$$

As an example, if (c, μ) is an enhanced YBE pair, $b = \sigma_3 \sigma_4 \sigma_3 \in B_5$, then from (2.3)-(2.4):

$$\begin{aligned} I_c(b) &= \text{Tr}(\rho_n^c(b) \circ \mu^{\otimes 10}) = \\ &= \text{Tr}(((Id_d)^{\otimes 2} \otimes (c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d))) \mu^{\otimes 5}) \\ &= \text{Tr}(\mu^{\otimes 2} \otimes ((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d) \mu^{\otimes 3})) \\ &= \text{Tr}(\mu)^2 \text{Tr}((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d) \mu^{\otimes 3}) \end{aligned} \quad (2.5)$$

The link invariant defined by Turaev is a generalisation of the Jones link invariant. Indeed, for the following specific matrices c and μ with coefficients in $\mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}]$ instead of \mathbb{C} :

$$c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{t} & 0 \\ 0 & -\sqrt{t} & 1-t & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}$$

$I_c(b)$ is equal to the Jones polynomial, up to some normalisation.

2.2 Applications of the Tracy-Singh product for solutions of the YBE

In [3, 4], it is shown that the TS product of linear operators (or matrices), with the canonical block partition, is an efficient tool to construct linear operators (or matrices) that preserves many of their properties. More precisely:

Theorem 2.4. [3, 4] Let $c, c' : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be linear operators. Let $\mu, \eta \in \text{End}(\mathbb{C}^d)$. Let $c \boxtimes c' : (\mathbb{C}^{d^2})^{\otimes 2} \rightarrow (\mathbb{C}^{d^2})^{\otimes 2}$ be the linear operator obtained from $c \boxtimes c'$, the TS product of c and c' with the canonical block partition for both matrices.

- (i) If c and c' are automorphisms, then $c \boxtimes c'$ is also an automorphism.
- (ii) If c and c' are unitary, then $c \boxtimes c'$ is also unitary.
- (iii) If c and c' are R -matrices, then $c \boxtimes c'$ is also a R -matrix.
- (iv) If (c, μ) and (c', η) are enhanced YBE pairs, then $(c \boxtimes c', \mu \otimes \eta)$ is also an enhanced YBE pair.

It results from Theorem 2.4, that the TS product, with the canonical block partition, enables the construction of infinite families of solutions of the YBE. A question that arises naturally, is why looking at the Tracy-Singh product of R -matrices c and c' and not at their Kronecker product $c \otimes c'$. The reason is that $c \otimes c'$ is not necessarily a R -matrix. Indeed, a simple computation shows that for c from Example 2.2, $c \otimes c$ does not satisfy the YBE.

In the case that c and c' are R -matrices, their TS product with the canonical block partition coincides with

the operation called *the tensor product of R-matrices* in [5, 16], although it differs from the actual tensor product \otimes . Indeed, in that specific case, Proposition 1.5 implies that the TS product represents the linear transformation $F_{23}(c \otimes c')F_{23} : \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \rightarrow \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, where F_{23} exchanges the two middle factors [3]. More generally, if A and B are of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with a canonical partition, then it results from Equation (1.1) that their Tracy-Singh product represents a linear transformation $c \boxtimes d : \mathbb{C}^n \otimes \mathbb{C}^m \otimes \mathbb{C}^n \otimes \mathbb{C}^m \rightarrow \mathbb{C}^p \otimes \mathbb{C}^q \otimes \mathbb{C}^p \otimes \mathbb{C}^q$ of the form $F_{23}(c \otimes d)F_{23}$, where $c : (\mathbb{C}^n)^{\otimes 2} \rightarrow (\mathbb{C}^p)^{\otimes 2}$ and $d : (\mathbb{C}^m)^{\otimes 2} \rightarrow (\mathbb{C}^q)^{\otimes 2}$, and F_{23} exchanges the two middle factors.

The cabling operation of R -matrices is defined in [25] to construct new solutions of the YBE from an existing one. It is induced from the cabling of braids, which consists roughly in multiplying the strings in a given braid. S. Majid suggested there may be some connection between the cabling operation and the TS product of solutions of the YBE ([19] and see [20] for reference). This is a direction of current research we are interested in. Indeed, we study whether there is a connection between the cabling operation and the TS product of solutions of the YBE and if the answer is positive to understand its nature. Furthermore, we explore the possible implications of these constructions in the context of quantum computation and the design of quantum circuits.

2.3 Applications of the Tracy-Singh product in monoidal categories

The Tracy-Singh product of matrices has also a surprising connection with a categorical construction that we describe in the following. Indeed, it can be defined as the monoidal product (or a tensor functor) in a particular category of vector spaces, in which the canonical partition into blocks is ensured.

The category Vec is a symmetric monoidal category, with objects all the finite dimensional vector spaces over a fixed field, let's say \mathbb{C} , and morphisms the linear transformations between vector spaces. The monoidal product is the functor $\otimes : \text{Vec} \times \text{Vec} \rightarrow \text{Vec}$ that sends each pair of objects (U, V) to $U \otimes V$ and each pair of morphisms (f, g) to $f \otimes g$, and its unit object is \mathbb{C} . Furthermore, $\text{Vec} \otimes \text{Vec}$ can be defined and it is also a symmetric category [8, Section 4.6], [7, Lecture 9, p.90], with the following particular symmetric subcategory:

$$\text{Diag} = \{U \otimes U \mid U \in \text{Vec}\} \subset \text{Vec} \otimes \text{Vec}$$

In [3], it is proved that the Tracy-Singh product of the representing matrices (with respect to standard bases for example) of morphisms c and c' in the category Diag is a functor, and it can be defined as the monoidal product in $\text{Mor}(\text{Diag})$. As we recall, to apply the

Tracy-Singh product on matrices they have to be partitioned into blocks. If the matrices have arbitrary sizes, they cannot be necessarily partitioned into blocks of the same size. However, if a matrix A has size of the form $n^2 \times p^2$, n, p not necessarily different, then there is a canonical partition of A , where all the blocks have the same size $n \times p$. The existence of such a canonical partition is ensured for representing matrices of morphisms in Diag , but not in $\text{Vec} \otimes \text{Vec}$ in general.

3 APPLICATIONS OF THE TRACY-SINGH PRODUCT IN QUANTUM COMPUTING

3.1 Preliminaries on quantum computing and quantum entanglement

We follow the presentation from the reference books on the topic [21], [9] and the papers [2], [12, 13, 14] and we refer to these references and the vast literature for more details.

Definition 3.1. Let \mathbb{C}^2 be the two-dimensional Hilbert space with two orthonormal state vectors, denoted by $|0\rangle$ and $|1\rangle$, that form a basis in bijection with the standard basis $\{(1, 0), (0, 1)\}$. A *qubit (or quantum bit)* is a state vector in \mathbb{C}^2

$$|\phi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (3.1)$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. We say that any linear combination of the form (3.1) is a *superposition of the states $|0\rangle$ and $|1\rangle$* , with *amplitude α* for the state $|0\rangle$ and *β* for the state $|1\rangle$.

Intuitively, the states $|0\rangle$ and $|1\rangle$ are analogous to the two values 0 and 1 which a bit may take. The way a qubit differs from a bit is that superposition of these two states, of the form (3.1), can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$ or definitely in the state $|1\rangle$. A measurement of a qubit $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ provides as output the bit 0 with probability $|\alpha|^2$ and the bit 1 with probability $|\beta|^2$ and the state $|\phi\rangle$ collapses to $|0\rangle$ or $|1\rangle$. After the measurement, all the information about the superposition is irreversibly lost. Examples of qubits include the spin of the electron in which the two basis states are spin up and spin down, and in this case the basis is denoted by $\{|\uparrow\rangle, |\downarrow\rangle\}$; or the polarization of a single photon in which the two basis states are vertical and horizontal, and in this case the basis is denoted by $\{|\rightarrow\rangle, |\leftarrow\rangle\}$.

More generally, a *n-qubit* is a state vector in the 2^n -dimensional Hilbert space, with an orthonormal basis $\{|\psi_i\rangle \mid 1 \leq i \leq 2^n\}$ in bijection with the standard basis, of the form

$$|\phi\rangle = \sum_{i=1}^{i=2^n} \alpha_i |\psi_i\rangle \quad (3.2)$$

where $\alpha_i \in \mathbb{C}$, $1 \leq i \leq 2^n$, and $\sum_{i=1}^{i=2^n} |\alpha_i|^2 = 1$. As an example, a two-qubit has the form

$$|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \quad (3.3)$$

In analogy with the case of a qubit, a measurement of a n -qubit of the form (3.2) gives as outcome n bits, each n -tuple of bits with a precalculated probability. Moreover, the state $|\phi\rangle$, in the superposition of the 2^n basis states, collapses to just one of the basis states.

Definition 3.2. Let \mathbb{C}^d be the d -dimensional Hilbert space with orthonormal base denoted by $|0\rangle, |1\rangle, \dots$, and $|d-1\rangle$. A *qudit* is a state vector in \mathbb{C}^d , where $\alpha_i \in \mathbb{C}$ and $\sum_{i=1}^{i=d} |\alpha_i|^2 = 1$:

$$|\phi\rangle = \alpha_1 |0\rangle + \dots + \alpha_d |d-1\rangle \quad (3.4)$$

Any linear combination of the form (3.4) is a *superposition of the states* $|0\rangle, \dots, |d-1\rangle$.

A qubit is a special case of a qudit, for the case $d = 2$. A *n-qudit* is a state vector in the Hilbert space $(\mathbb{C}^d)^{\otimes n}$. A quantum system with one state vector $|\phi\rangle$ is called a *pure state*. However, it is also possible for a system to have a set of potential different state vectors. As an example, there may be a probability $\frac{1}{2}$ that the state vector is $|\phi\rangle$ and a probability $\frac{1}{2}$ that the state vector is $|\psi\rangle$. This system is said to be in a *mixed state*. There exists a matrix called density matrix which trace value determines whether a system is in a pure or a mixed state [21, p.99].

Definition 3.3. A n -qudit $|\phi\rangle$ is *decomposable* if $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_n\rangle$, where $|\phi_i\rangle \in \mathbb{C}^d$, for $1 \leq i \leq n$. Otherwise, $|\phi\rangle$ is *entangled*.

As an example, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an entangled two-qubit, since it cannot be decomposed as a tensor product of two qubits. In general, a two-qubit pure state $|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ is entangled if and only if $\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10} \neq 0$. In [?], the authors give a combinatorial criteria to determine whether a n -qubit is entangled or not.

Any quantum evolution of a n -qudit, or any quantum operation on a n -qudit is described by a unitary operator or square unitary matrix of size d^n , called a (*quantum*) *n-qudit gate*, which transforms $|\phi\rangle = \sum_{i=1}^{i=d^n} \alpha_i |\psi_i\rangle$ into another linear combination of the (standard) basis states $\{|\psi_i\rangle \mid 1 \leq i \leq d^n\}$.

Example 3.4. Let c be the unitary R -matrix from Example 2.2. So, c is a 2-qubit (YBE) gate and it acts on the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $(\mathbb{C}^2)^{\otimes 2}$, with $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$, and so on,

such that $c |00\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle$, $c |01\rangle = \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle$, $c |10\rangle = -\frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle$ and $c |11\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Example 3.5. A very important example of 2-qubit gate is the following unitary square matrix of size 4 which

acts on 2-qubits: $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$; not an R -matrix.

Definition 3.6. [2] A 2-qudit gate $L: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ is *primitive* if L maps decomposable 2-qudit to decomposable 2-qudit, otherwise L is said to be *imprimitive*.

In other words, a 2-qudit gate L is said to be *imprimitive*, if there exists a decomposable 2-qudit $|\phi\rangle$ such that $L|\phi\rangle$ is an entangled 2-qudit. An imprimitive 2-qudit gate is often called *entangling*, as in [13]. There is a criteria to determine whether a 2-qudit is primitive.

Theorem 3.7. [2] Let $P: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ denote the swap gate, that is the 2-qudit gate such that $P|\alpha\beta\rangle = |\beta\alpha\rangle$. Let $L: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be a 2-qudit gate. Then L is primitive if and only if $L = L_1 \otimes L_2$ or $L = (L_1 \otimes L_2)P$, for some 1-qudit gates L_1, L_2 .

In [13], the authors answer the question of which 2-qubit gates which satisfy the YBE are entangling, using the classification from [6] and the criteria for entanglement from [2]. The 2-qubit gates from Examples 3.4 and 3.5 are both entangling operators [9, 13, 21]. Note that not every 2-qubit gate that is an R -matrix is en-

tangling. Indeed, let $c_{2,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ be a R -

matrix of size 4. It is easy to show that the 2-qubit gate $c_{2,1}$ is primitive. Let $|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ be a decomposable two-qubit pure state, that is $\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10} = 0$. Then $c_{2,1}|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{10} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$ and $\alpha_{00}\alpha_{11} - \alpha_{10}\alpha_{01} = 0$, that is $c_{2,1}|\phi\rangle$ is decomposable.

3.2 Applications of the Tracy-Singh product in quantum computing

The Tracy-Singh product is an efficient tool to create entangling and primitive 2-qudit gates, as it preserves these properties in the following way:

Theorem 3.8. [3] Let $c: (\mathbb{C}^n)^{\otimes 2} \rightarrow (\mathbb{C}^n)^{\otimes 2}$ and $c': (\mathbb{C}^m)^{\otimes 2} \rightarrow (\mathbb{C}^m)^{\otimes 2}$ be 2-qudit gates. Let $c \boxtimes c'$ denote their Tracy-Singh product, with the canonical block partition.

(i) Assume c is entangling. Then $c \boxtimes c' : (\mathbb{C}^{nm})^{\otimes 2} \rightarrow (\mathbb{C}^{nm})^{\otimes 2}$ is also entangling.

(ii) Assume c and c' are primitive. If $c = c_1 \otimes c_2$ and $c' = c'_1 \otimes c'_2$ or $c = (c_1 \otimes c_2)S_c$ and $c' = (c'_1 \otimes c'_2)S_{c'}$, where S_n and S_m are the swap maps on $(\mathbb{C}^n)^{\otimes 2}$ and $(\mathbb{C}^m)^{\otimes 2}$ respectively. Then $c \boxtimes c' : (\mathbb{C}^{nm})^{\otimes 2} \rightarrow (\mathbb{C}^{nm})^{\otimes 2}$ is also primitive (of the same kind).

Combining Theorem 2.4 with Theorem 3.8 ensures the existence of entangling and primitive 2-qudit YBE gates for every $d \geq 2$. More precisely:

Theorem 3.9. [3] Let $d \geq 2$ be any integer. Then, there exists an entangling 2-qudit YBE gate $U : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ and a primitive 2-qudit YBE gate $S : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$.

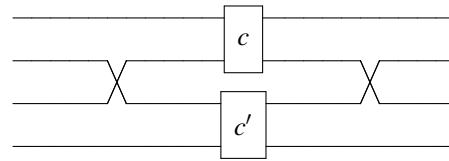
Note that, in the same way that an entangling 2-qudit (YBE or not) gate is not the tensor product of two gates, an arbitrary 2-qudit (YBE or not) gate is not necessarily the TS product of two gates. If the theory develops, maybe a name should be coined to describe that.

Definition 3.10. [2] A collection \mathcal{U} of 1-qudit gates $\{S_i\}$ and 2-qudit gates $\{U_j\}$ is called *universal* if, for each $n \geq 2$, every n -qudit gate can be approximated with arbitrary accuracy by a circuit made up of the n -qudit gates produced by the $\{S_i\}$ and $\{U_j\}$, and it is called *exactly universal* if, for each $n \geq 2$, every n -qudit gate can be obtained exactly by a circuit made up of the n -qudit gates produced by the $\{S_i\}$ and $\{U_j\}$.

In [2], it is proved that U is entangling if and only if U is exactly universal, which means that the collection of all 1-qudit gates together with U generates the unitary group $U((\mathbb{C}^d)^{\otimes n})$, for every $n \geq 2$. Since for every integer $d \geq 2$, there exists an entangling 2-qudit gate $U : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$, where U satisfies the YBE (Theorem 3.9), one can assume that for every $d \geq 2$, there exists an exactly universal set of gates \mathcal{U}_d with a single 2-qudit gate U . This enables to show that, whenever the realisation of the gates $c, c' : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ in terms of gates from \mathcal{U}_d is given, there is a simple way to realise the 4-qudit gate $c \boxtimes c' : (\mathbb{C}^d)^{\otimes 4} \rightarrow (\mathbb{C}^d)^{\otimes 4}$ in terms of the gates from \mathcal{U}_d [4]. That is, although the TS product of matrices is quite esoteric, its implementation is in fact simple. Indeed:

Proposition 3.11. [4] Let $c, c', P : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be 2-qudit gates, with P the swap map. Let $c \boxtimes c' : (\mathbb{C}^d)^{\otimes 4} \rightarrow (\mathbb{C}^d)^{\otimes 4}$ be the 4-qudit gate defined by their Tracy-Singh product $c \boxtimes c'$ with the canonical block

partition. Then $c \boxtimes c' = (\mathbf{I}_d \otimes P \otimes \mathbf{I}_d)(c \otimes c')(\mathbf{I}_d \otimes P \otimes \mathbf{I}_d)$:



From Theorems 3.8-3.9, given an entangling 2-qudit gate it is possible to create infinitely many other entangling gates with the TS product, and each of them can be included in an exactly universal set of gates \mathcal{U}_d . A question that arises naturally is which gate is it "better" to insert in \mathcal{U}_d , the original one or one of the gates obtained in the process. Another natural question is whether universal gates obtained from the TS product offer more advantages in terms of implementation than other universal gates.

The question whether a YBE gate is primitive has found an interesting application in the domain of knot invariants. Indeed, in [1], the authors prove that if a YBE gate c is primitive, then the link invariant I_c obtained from c , using the Turaev construction, is trivial, and that the converse is not necessarily true. Indeed, they give an example of entangling YBE gate that leads to a trivial link invariant. Furthermore, if (c, μ) and (c', η) are enhanced YBE pairs, such that c and c' are primitive of the same kind, and μ, η are invertible, then $I_{c \boxtimes c'}(b) = I_c(b) \cdot I_{c'}(b)$, for every $b \in B_n$ [4]. It would be interesting to understand whether the connection between primitive gates and link invariants is purely theoretical, or it could be useful to identify quantum advantages.

To conclude this paper, we would like to point on some more open questions and future directions of research which are in direct continuation with the results in this paper. It would be interesting to explore if there are some specific algorithms for which the use of gates obtained from the TS product offers some advantages in circuit depth or on other parameters to be defined and leads to a more efficient implementation. It would be also interesting to study the robustness of the TS generated gates to common noise model and explore implementations for specific hardware platforms. The creation of an open-source software library that implements the TS generated gates and its use in gate synthesis for popular quantum computing frameworks may be useful to increase the list of gates.

A question of particular interest in a more mathematical viewpoint is the following: how does the fact that c is an entangling or a primitive gate influence the link invariant I_c ? Every YBE 2-qudit gate (or R -matrix) c induces a representation ρ_n^c of the braid group B_n as defined in Equation (2.2) and a link invariant I_c as defined in Equation (2.4). In [1], the authors answer partially the question cited above. Indeed, they show that if c

is a primitive YBE gate, then I_c is trivial and that the converse is not always true. It would be interesting to understand whether there exist some other connections between the properties of the YBE gate and link invariants in general.

Acknowledgment. I would like to thank the anonymous reviewers for their helpful comments and feedback, and their many insightful comments and suggestions which greatly strengthened the overall manuscript and opened horizons of future research.

4 REFERENCES

- [1] G. Alagic, M. Jarret, S.P. Jordan, *Yang-Baxter operators need quantum entanglement to distinguish knots*, J. of Physics A: Mathematical and Theoretical, **49**(2016), n.7.
- [2] J.L. Brylinski, R. Brylinski, *Universal quantum gates*, Mathematics of Quantum Computation, Chapman and Hall/CRC Press, Boca Raton, Florida 2002 (edited by R. Brylinski and G. Chen).
- [3] F. Chouraqui, *The Yang-Baxter equation, quantum computing and quantum entanglement*, Physica Scripta **99** (2024), n. 11.
- [4] F. Chouraqui, *On the Realization of quantum gates coming from the Tracy-Singh product*, Quantum Inf. Process **24** (2025), 261.
- [5] R. Conti, G. Lechner, *Yang-Baxter endomorphisms*, J. London Math. Soc. (2) **103** (2021), 633-671.
- [6] H. Dye, *Unitary solutions to the Yang-Baxter equation in dimension four*, Quantum Information Processing, Vol. 2, nos. 1-2, April 2003, 117-150.
- [7] P. Etingof, *Topics in Lie Theory: Tensor Categories, course 18.769, Spring 2009*, MIT OpenCourseWare, <https://ocw.mit.edu/courses/18-769-topics-in-lie-theory-tensor-categories-spring-2009/pages/lecture-notes>.
- [8] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik, *Tensor categories*, Mathematical surveys and monographs **205**, American Mathematical Society.
- [9] J. Gruska, *Quantum Computing*, McGraw-Hill Companies, London 1999.
- [10] D.C. Hyland, E.G. Collins, Jr., *Block Kronecker Products and Block Norm Matrices in Large-Scale Systems Analysis*, SIAM J. Matrix Anal. Appl. **10** (1989), 18-29.
- [11] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics **155** (1995), Springer Verlag, Berlin.
- [12] L.H. Kauffman, S.J. Lomonaco Jr., *Quantum entanglement and topological entanglement*, New J. Phys. **4**, 73, 2002.
- [13] L.H. Kauffman, S.J. Lomonaco Jr., *Braiding Operators are Universal Quantum Gates*, New J. Phys. **6** (2004).
- [14] L.H. Kauffman, E. Mehrotra, *Topological aspects of quantum entanglement*, Quantum Inf. Process **18**, 76 (2019).
- [15] R.H. Koning, H. Neudecker, T. Wansbeek, *Block Kronecker products and the vecb operator*, Linear Algebra and its applications **149** (1991), 165-184.
- [16] G. Lechner, U. Pennig, S. Wood, *Yang-Baxter representations of the infinite symmetric group*, Adv. Math **355** (2019), 1-42.
- [17] S. Liu, *Matrix results on the Khatri-Rao and Tracy-Singh products*, Linear Algebra and its Applications **289** (1999), 267-277.
- [18] J.R. Magnus, H. Neudecker, *The commutation matrix: some properties and applications*, Annals of Statistics **7**(1979), 381-394.
- [19] S. Majid, *Personal communication*, 2024.
- [20] S. Majid, *Foundations of Quantum Group Theory*, Cambridge University Press, 1995.
- [21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000.
- Extraspecial two-Groups, generalized Yang-Baxter equations and braiding quantum gates*, Quant. Inf. Comput. **10** (2010), 685-702.
- [22] D. S. Tracy, K. G. Jinadasa, *Partitioned Kronecker products of matrices and applications*, Canad. J. Statist. **17** (1989), 107-120.
- [23] D.S. Tracy, R.P. Singh, *A new matrix product and its applications in partitioned matrix differentiation*, Statistica Neerlandica **26** (1972), 143-157.
- [24] V. Turaev, *The Yang-Baxter equation and invariants of links*, Invent. Math, **92** (1988), 527-553.
- [25] H. Wenzl, *Representations of braid groups and the quantum Yang-Baxter equation*, Pacific J. Math. **145** (1990), n.1, 153-180.

Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) for Web 3.0 Security in the Post-Quantum Era

Ali Raheman
[0000-0002-0817-1176]
Magpie Markets Limited
P.O. Box 4301, Road Town,
Tortola, VG1110, British
Virgin Islands
Ali@magpiefi.xyz

Tejas Bhagat
[0000-0001-7364-6361]
Qloud Technologies
Ahtri 12-512, E-10151 Tallinn,
Estonia
tejas@bc5.eu

Fazal Raheman
[0000-0002-7766-6949]
Qloud Technologies
Ahtri 12-512, E-10151 Tallinn,
Estonia
drfazal@bc5.eu

ABSTRACT

The arrival of quantum computing (QC) is no longer a hypothetical concept. Google claims its new quantum computer is 241 million times faster than the one released in 2019, while the Chinese Zuchongzhi-3 claims to have achieved speeds trillions of times faster. The encryption-breaking speeds of QC will render our existing encryption obsolete within 5–10 years, presenting a catastrophic threat to our cryptography-dependent, ubiquitous digital infrastructure. Unless our digital infrastructure is secured from quantum threats, QC cannot become mainstream. In 2016-17, the National Institute of Standards and Technology (NIST) initiated a post-quantum cryptography (PQC) initiative; however, so far, it has failed to produce a stable standard, as all of the top 82 candidates have already been compromised. Moreover, PQC is expensive and too resource-intensive with latency issues, particularly in the \$3 Trillion Crypto/blockchain economy that entirely relies on user-facing cryptography. In an earlier study, we disclosed Quantum-Safe Quantum Ledger Technology (QLT), a blockchain-agnostic framework for securing cryptocurrencies and blockchains from Q-Day threats. In this presentation, we discuss a Quantum Resilient user Evasive Cryptographic Authentication (QRUECA) protocol that secures QLT by replacing traditional user-facing PKI-based methods. QRUECA authorizes access through a multi-gate cryptographically sealed device-to-device handshake, thereby eliminating the need for the traditional user-facing cryptography. Because Gate 1 of the QRUECA process uses no user-facing cryptography, and Gate 2 is only activated by authenticated devices, the entire protocol becomes inherently resistant to threats from QC. Beyond blockchain, the QRUECA protocol can be applied to any Web 3.0 use case. Thus, QRUECA addresses a significant hurdle in the mainstream introduction of QC. Just as an automobile cannot exist without a braking system, quantum computers cannot exist without securing our life-sustaining digital infrastructure.

Keywords

Quantum-Resilient Authentication, Post-Quantum Cryptography (PQC), Quantum Ledger Technology (QLT), Zero Vulnerability Computing (ZVC)

1. INTRODUCTION

The advent of quantum computing (QC) represents a paradigm shift with profound implications for digital security. No longer confined to theoretical physics, quantum computers are demonstrating exponential

increases in computational power [Car25a], with recent claims of speeds trillions of times faster than conventional supercomputers [Gao25a]. This unparalleled processing capability poses an existential threat to the vast majority of our modern digital infrastructure, which relies heavily on cryptographic primitives like RSA and Elliptic Curve Cryptography (ECC) for data confidentiality, integrity, and authentication [Maj15a]. These algorithms, while robust against classical computers, are fundamentally vulnerable to quantum algorithms such as Shor's algorithm for factoring large numbers and Grover's

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

algorithm for searching unsorted databases. Experts predict that within the next 5-10 years, a sufficiently powerful quantum computer, often referred to as "Q-Day," could render current encryption standards obsolete, leading to a catastrophic compromise of sensitive data, financial transactions, and critical infrastructure [Maj15a].

In response to this impending threat, the National Institute of Standards and Technology (NIST) launched a comprehensive post-quantum cryptography (PQC) standardization initiative in 2016-2017. The goal was to identify and standardize cryptographic algorithms believed to be secure against attacks from large-scale quantum computers. However, the journey has been fraught with challenges. Many of the initial PQC candidates have been subsequently compromised, highlighting the inherent complexity and ongoing fragility of developing new, quantum-resistant cryptographic schemes [Lav24a]. Furthermore, PQC protocols often come with significant computational overhead, larger key sizes, and increased latency, making them less suitable for resource-constrained environments or high-throughput applications, particularly within the burgeoning \$3 trillion cryptocurrency and blockchain economy, which is entirely reliant on user-facing cryptography [Rah24a].

This paper introduces a novel approach to securing digital infrastructure against quantum threats, moving beyond the limitations of current PQC efforts. We delve into Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA), a protocol designed to safeguard Web 3.0 security. QRUECA is intrinsically linked to Quantum Ledger Technology (QLT), a blockchain-agnostic framework previously introduced for securing cryptocurrencies and blockchains from Q-Day threats (Raheman, 2024). The core innovation of QRUECA lies in its departure from traditional user-facing cryptographic authentication methods. Instead, it employs a multi-gate, cryptographically sealed device-to-device handshake, thereby eliminating the attack surface exposed by conventional user-facing cryptography. This design choice, coupled with its foundation on Zero Vulnerability Computing (ZVC) and Solid-State Software on a Chip (3SoC) architecture, provides inherent resilience to quantum attacks.

The remainder of this paper is structured as follows: Section 2 elaborates on the quantum threat and the shortcomings of existing mitigation strategies. Section 3 introduces Quantum Ledger Technology (QLT) and its foundational architectural components, ZVC and

3SoC. Section 4 provides a detailed exposition of the QRUECA protocol, explaining its multi-gate authentication process and its user-evasive nature. Section 5 discusses the operational benefits of QRUECA and its broad applicability across various Web 3.0 use cases. Finally, Section 6 concludes the paper and outlines future research directions.

2. THE QUANTUM THREAT AND LIMITATIONS OF CURRENT APPROACHES

The security of modern digital communications and data storage hinges on the computational intractability of certain mathematical problems. Public-key cryptography, foundational to secure online interactions, relies on the difficulty of factoring large numbers (RSA) or solving discrete logarithms on elliptic curves (ECC). Symmetric-key cryptography, used for bulk data encryption, derives its strength from the vastness of its key space, making brute-force attacks computationally infeasible. Quantum computers, however, leverage principles of quantum mechanics—superposition and entanglement—to perform computations in fundamentally different ways, undermining these cryptographic assumptions.

Shor's algorithm, first proposed in 1994, demonstrates that a sufficiently powerful quantum computer can efficiently factor large integers and compute discrete logarithms. This directly threatens the security of widely deployed public-key algorithms like RSA, DSA, and ECC, which are integral to digital signatures, secure key exchange (e.g., Diffie-Hellman and Public Key Infrastructure (PKI)). A quantum computer running Shor's algorithm could break current public-key encryption in minutes, compromising encrypted communications, digital certificates, and authenticated transactions [Ugw20a]. Similarly, Grover's algorithm offers a quadratic speedup for searching unsorted databases [Yua24a]. While it doesn't break symmetric-key algorithms outright, it effectively halves the security strength, meaning a 256-bit key would only offer 128 bits of security against a quantum adversary, potentially necessitating much larger key sizes to maintain current security levels.

The global response to this impending "Q-Day" has primarily centered on Post-Quantum Cryptography (PQC). NIST's PQC standardization process, initiated in 2016, aimed to solicit, evaluate, and standardize new cryptographic algorithms robust against quantum attacks [Che16a]. These algorithms typically fall into categories such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography.

While significant progress has been made, the journey has been marked by repeated setbacks. As recent as 2024, it was reported that top PQC candidates have been compromised [Lav24a], demonstrating the inherent difficulty in designing and validating truly quantum-resistant primitives. This continuous cycle of development, vulnerability discovery, and revision highlights the immaturity and instability of the current PQC landscape.

Beyond the technical challenges of cryptographic design, PQC algorithms often present practical hurdles. They generally involve larger key sizes, increased computational requirements, and higher latency compared to their pre-quantum counterparts. These characteristics pose significant challenges for adoption, particularly in resource-constrained environments like Internet of Things (IoT) devices, or in performance-critical applications like blockchain networks, where efficiency and low latency are paramount. The blockchain ecosystem, with its reliance on cryptographic hashing, digital signatures for transaction validation, and decentralized trust mechanisms, is particularly vulnerable. User-facing cryptographic operations, such as signing transactions with private keys, present a clear attack surface that existing PQC solutions struggle to efficiently and effectively secure without introducing considerable overhead. The very nature of many blockchain applications, which are built upon user-initiated cryptographic actions, exposes their vulnerability to quantum adversaries who can intercept and decrypt keys or transactions. Therefore, a fundamentally different approach is required that can offer immediate quantum resilience without relying on the still-evolving and resource-intensive PQC standards.

3. QUANTUM LEDGER TECHNOLOGY (QLT): AN ARCHITECTURAL RESPONSE TO QUANTUM THREATS

Recognizing the limitations of reactive cryptographic upgrades, Quantum Ledger Technology (QLT) emerges as a proactive, architectural solution to secure digital assets and infrastructure from the quantum threat. QLT is conceived as a blockchain-agnostic framework, providing a robust security layer for various distributed ledger technologies (DLTs) and cryptocurrencies [Rah24a]. Unlike piecemeal cryptographic updates, QLT addresses the root causes of systemic vulnerability by fundamentally rethinking system architecture at its deepest levels. This is achieved through the integration of two proprietary, foundational technologies: Zero Vulnerability Computing (ZVC) and the Solid-State Software on a Chip (3SoC) hardware model.

3.1 Zero Vulnerability Computing (ZVC) and 3SoC Architecture

At the heart of QLT's inherent security lies Zero Vulnerability Computing (ZVC). ZVC is a revolutionary computational paradigm that directly addresses one of the most pervasive sources of cyberattacks: unauthorized software execution and the proliferation of Third-Party Permissions (TPPs) [Rah22a]. By design, ZVC explicitly bans all TPPs, meaning that no external or unauthorized software, libraries, drivers, or runtime code can execute on a ZVC-enabled system. This architectural constraint eliminates the vast majority of attack vectors, including malware injection, supply chain attacks, and exploits leveraging vulnerabilities in third-party components. The result is a truly "zero attack surface" infrastructure, where the system's operational integrity is guaranteed by preventing any deviation from its pre-approved, immutable software stack.

The practical realization of ZVC is intrinsically tied to the proprietary hardware model, Solid-State Software on a Chip (3SoC). 3SoC represents a fundamental shift from traditional software deployment to a hardware-enforced, immutable execution environment [Rah22b]. In a 3SoC device, the critical software components and cryptographic routines, are loaded from a storage medium that has zero TPPs to write. Thus, they run from a hardware that is non-modifiable by third parties remaining in a solid-state format. This architecture provides an unparalleled level of security and integrity:

- **Immutability:** The embedded software cannot be altered, overwritten, or tampered with once provisioned, effectively preventing rootkits, persistent malware, and unauthorized code injection.
- **Tamper Resistance:** The physical nature of the 3SoC makes it significantly more difficult for adversaries to physically access or manipulate the core software and cryptographic keys.
- **Secure Boot:** The system inherently boots into a known, secure state, bypassing typical attack points that exploit mutable boot processes.
- **Elimination of Vulnerabilities:** By tightly integrating software and hardware, and removing the ability to load arbitrary code, 3SoC systems dramatically reduce the potential for software vulnerabilities that can be exploited for privilege escalation or remote code execution.

The synergy between ZVC and 3SoC is critical. ZVC defines the protocol of banning TPPs and achieving a zero attack surface, while 3SoC provides the secure, immutable hardware platform necessary to enforce this

protocol. Together, they create an environment where the integrity of computations and data is guaranteed at the architectural level, providing a foundational layer of security that is inherently resistant to both classical and emerging quantum threats, as the very avenues for attack (e.g., software vulnerabilities, code injection) are eliminated.

4. THE QUANTUM-RESILIENT USER-EVASIVE CRYPTOGRAPHIC AUTHENTICATION (QRUECA) PROTOCOL

Building upon the robust foundation of QLT's ZVC and 3SoC architecture, Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) introduces a revolutionary paradigm for secure access, specifically designed to withstand the quantum threat [Rah24b]. Traditional authentication mechanisms, predominantly relying on Public Key Infrastructure (PKI) and user-facing cryptographic operations (e.g., entering passwords, biometric scans, or signing transactions with user-controlled private keys), inherently expose an attack surface. QRUECA fundamentally alters this dynamic by shifting the primary authentication burden from the user-entered credentials to a secure, concealed device-to-device handshake.

4.1 Paradigm Shift: Device-to-Device Handshake vs. User-Initiated Authentication

In legacy systems, the authentication handshake is typically initiated and controlled by the user. This involves the user providing credentials (e.g., username/password), possessing a device (e.g., for 2FA codes), or presenting biometric data. All these methods are inherently visible and usable by an adversary. In contrast, QRUECA implements a "user-evasive" approach where the initial authentication process is orchestrated and executed entirely between trusted computing devices, without direct user intervention or exposure of cryptographic prompts or keys. This architectural choice is central to its quantum resilience.

4.2 Gate 1: The Concealed Device-to-Device Handshake

The first and most critical phase of the QRUECA protocol is Gate 1: a completely concealed device-to-device handshake. This gate operates at the hardware level, rendering it inaccessible to the user's discretion and, crucially, to quantum adversaries. This handshake

is facilitated by a unique component: the **QRUECA Crypto Certificate (QCC)**.

The QCC is not a traditional software certificate; it is securely embedded within authorized QLT devices (e.g., a 3SoC client device attempting to access a 3SoC server). The QCC provides a pair of private and public keys. However, unlike conventional PKI, these keys are used exclusively for a hardware-level, device-to-device handshake inaccessible to user-dependent credentials (see Fig.1). The process unfolds as follows:

1. An authorized QLT device (client) initiates a connection to a QLT-enabled server.

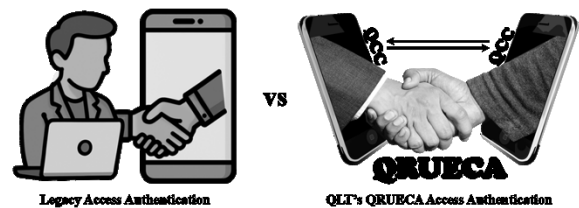


Figure 1. Legacy VS QRUECA Access Authentication

2. The devices engage in a cryptographic handshake using the private and public keys provisioned by their embedded QCCs. This exchange happens entirely within the secure hardware environment, abstracted away from the user interface and the traditional software stack.
3. Because this handshake occurs at the hardware level and does not expose cryptographic prompts, key material, or user-visible challenge-response interactions, quantum adversaries have no available surface to attack. They cannot intercept the challenge, perform Shor's algorithm on an exposed public key, or attempt to brute-force a password or passphrase. The cryptographic operations are sealed within the secure hardware, making the "user-evasive" aspect synonymous with "quantum-resilience" (see Fig. 1).

4.3 Gate 2: Continued Access Authorization

Only after a successful Gate 1 handshake, signaling that the requesting device is a legitimate, authorized QLT entity, does the system proceed to a second cryptographic gate. A key feature of Gate 1 of the QRUECA protocol is its **strictly non-retry** mechanism. Such a **zero-retry timeout (ZRT0)** protocol ensures that a failed device-to-device handshake is not repeated. In Gate 2, access authorization continues, but critically,

it does so without exposing any reusable credentials to quantum computers. This means that even if an adversary were to compromise the session *after* Gate 1, they would not obtain any static, replayable, or decryptable credentials that could be used for future unauthorized access. This immediate termination of connection attempts at Gate 1 effectively blocks brute-force attacks, denial-of-service attempts by repeatedly guessing, and replay attacks, where captured legitimate handshakes are re-transmitted. This design choice dramatically reduces the window of opportunity for any potential adversary, classical or quantum.

4.4 The 4-Factor Authentication (4FA) Model

As illustrated in Fig. 2, QRUECA replaces the

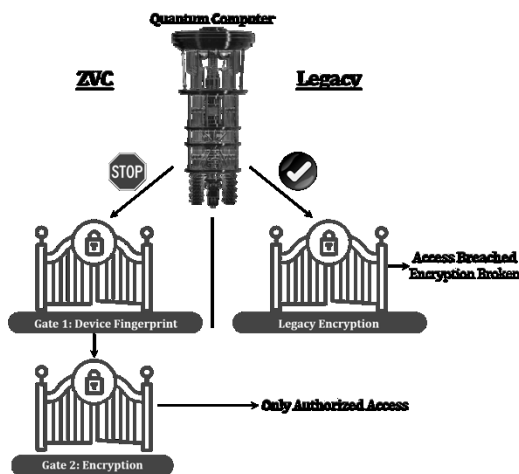


Figure 2. QRUECA's two-gates Access Authentication escapes encryption breaking power of quantum computer

limitations of legacy 2-Factor Authentication (2FA) protocols, which often rely on what a user knows (password), has (device), or is (biometric data) – all of which remain visible and potentially vulnerable to sophisticated adversaries. QRUECA introduces a more robust, hardware-sealed, and user-evasive 4-Factor Authentication (4FA) model:

- 1. Device-to-device hardware verification:** This is the core of Gate 1, ensuring that only authenticated QLT hardware devices can initiate a connection.
- 2. Hardware-originated challenge response:** Subsequent challenges and responses are generated and processed within the secure hardware environment, preventing their interception or manipulation in transit.
- 3. Time-limited access token validation:** Access is granted via ephemeral, short-lived tokens, which expire rapidly, minimizing the window for

compromise even if a token were somehow captured.

- 4. Behavioral or environmental signal matching (optional & non-invasive):** This optional factor adds an adaptive layer of security, leveraging contextual data (e.g., user's typical login patterns, network environment, device location) to further validate the legitimacy of the access attempt. This factor is non-invasive and operates in the background, further contributing to a seamless user experience.

4.5 Inherent Quantum Resistance by Design

The fundamental strength of QRUECA against quantum threats lies in its design philosophy: **prevention of exposure rather than complex post-quantum encryption of exposed data.** Because Gate 1 of the QRUECA process uses no user-facing cryptography, and Gate 2 is only activated by authenticated devices and does not expose reusable credentials, the entire protocol becomes inherently resistant to quantum attacks (see Fig. 2). If a quantum adversary cannot intercept the challenge, cannot observe the private key in use, and cannot gain access to any static credentials, they cannot attempt to decrypt it using Shor's algorithm or any other quantum algorithm. This design ensures that authentication in QLT systems is invisible, immutable, and quantum-safe by design, providing a level of security that current PQC efforts struggle to match in terms of efficiency and immediate deployability.

5. OPERATIONAL BENEFITS AND WEB 3.0 APPLICATIONS

Beyond its foundational quantum resilience, QRUECA offers significant operational advantages that enhance both security and user experience, making it particularly well-suited for the evolving landscape of Web 3.0 and the blockchain economy.

5.1 Operational Advantages

- Seamless User Experience:** The most apparent benefit for end-users is the elimination of first-gate passwords or manual challenges. Since the initial authentication occurs invisibly at the hardware level between devices, users are freed from the cognitive burden and friction associated with traditional login procedures. This dramatically improves usability, reducing barriers to entry for decentralized applications and services.

- **Reduced Cognitive and Operational Risk:** A fundamental principle of security is that users cannot leak what they do not see or control. By making cryptographic operations and initial authentication credentials user-evasive, QRUECA drastically reduces the human element as a vulnerability. Phishing, social engineering, and credential stuffing attacks become largely ineffective against the initial authentication layer, as there are no user-exposed credentials to compromise. This shifts operational risk away from individual user vigilance to architectural system design.
- **Increased Compatibility with Low-Resource or Embedded Environments:** Unlike computationally heavy PQC protocols, which often demand significant processing power and memory, QRUECA's reliance on hardware-level handshakes and its focus on preventing exposure rather than complex, computationally intensive post-quantum encryption make it highly compatible with low-resource or embedded environments. This is crucial for the proliferation of IoT devices, edge computing, and specialized blockchain hardware wallets, where computational efficiency is paramount.

5.2 Independence from PQC Standardization

A critical differentiator for QRUECA is its independence from the ongoing and often precarious Post-Quantum Cryptography (PQC) standardization efforts. While PQC algorithms are still undergoing rigorous scrutiny, iterative revisions, and demonstrating repeated fragility (as evidenced by the compromise of various candidates), QRUECA offers quantum resilience *today*. It achieves this not by attempting to create new, unproven cryptographic primitives, but by fundamentally preventing the exposure of cryptographic material and authentication flows in the first place. This architectural approach delivers immediate quantum safety, bypassing the uncertainties and delays inherent in the PQC development cycle. QRUECA transforms authentication from a visible, vulnerable challenge into a sealed, autonomous access protocol.

5.3 Application in Web 3.0 and Blockchain

The implications of QRUECA and the underlying QLT framework for Web 3.0 are profound, especially for the blockchain ecosystem where endpoint integrity is everything. The current reliance on user-facing cryptographic authentication (e.g., managing private keys for wallets, signing transactions) represents the

most commonly exploited vulnerability in blockchain and cryptocurrency infrastructure. QRUECA replaces this with a secure, invisible, and user-evasive post-quantum alternative.

QLT is deployed as a novel client-server cybersecurity framework, built on Qloud Technologies' proprietary ZVC and 3SoC architecture. Its design specifically targets the elimination of the two root causes of systemic vulnerability in digital systems: third-party permissions (TPPs) and user-facing cryptographic authentication, both addressed at the architectural level.

- **Server-Side Deployment:** At the server end, QLT's ZVC on 3SoC can deliver the full benefits of a zero-attack surface infrastructure. This is critical for securing vital components of the blockchain ecosystem, such as validator nodes, cryptocurrency exchanges, and other blockchain infrastructure endpoints. By running these critical services on 3SoC-enabled servers, the risk of unauthorized software execution, internal breaches, and quantum attacks on core network components is drastically mitigated.
- **Client-Side Deployment:** On the client end, QLT is envisioned as a standalone 3SoC hardware device. This device would integrate blockchain wallet functionality, providing unparalleled secure key storage, robust transaction approval mechanisms, and cryptographic isolation. Unlike software wallets susceptible to malware, or even hardware wallets that rely on user interaction for key exposure, the 3SoC client device integrates QRUECA for a truly user-evasive and quantum-safe interaction.
- **Closed, Post-Quantum-Resilient Intranet:** While each QLT component (server-side ZVC/3SoC and client-side 3SoC) operates independently and provides significant security benefits on its own, their true potential is realized when both ends are 3SoC-enabled. In such a scenario, the framework establishes a closed, quantum-resilient intranet. This creates an even higher level of isolation, trust, and cryptographic invisibility, as all communication and authentication within this network bypasses traditional vulnerable points and leverages the inherent security of the 3SoC-QRUECA ecosystem.

5.4 Application in 6G

The projected convergence of 6G deployment and quantum computing in 2030 presents a critical security dilemma. While PQC aims to protect against Q-Day threats, its large key sizes, computational overhead, and latency implications directly conflict with 6G goals such as sub-microsecond response times and drastic

cost reductions. With none of the NIST PQC candidates proving consistently secure, reliance on these unstable standards jeopardizes the feasibility of 6G's performance benchmarks.

QRUECA offers an architectural resolution to this impasse by eliminating exposure rather than encrypting it. Its concealed, device-level handshake—executed entirely through hardware-sealed, user-evasive mechanisms enabled by ZVC and 3SoC—prevents quantum adversaries from accessing any usable cryptographic material [Rah24c]. Aligned with the AZT model, QRUECA supports fast, autonomous, and low-cost authentication, making it inherently compatible with the operational demands and security requirements of 6G networks.

QRUECA and 6G Performance Goals

Latency: Unlike PQC, which introduces processing delays due to computational complexity, QRUECA's hardware-sealed device-to-device authentication operates below the software stack and requires no user intervention, making it capable of meeting 6G's <1μs latency target.

Cost Efficiency: 6G networks aim for a 1000x price-performance improvement over 5G. By avoiding the need for resource-intensive encryption, QRUECA reduces the computational burden and power draw at endpoints, making it viable for deployment across energy-constrained edge devices, IoT nodes, and mobile hardware.

Autonomy & Scalability: As 6G pushes toward self-organizing networks, dynamic mesh topologies, and massive machine-type communications, QRUECA's autonomous, certificate-based authentication supports trustless onboarding and roaming across decentralized nodes—without requiring cloud validation, policy enforcement, or cryptographic prompts.

Quantum Resilience: QRUECA does not rely on unproven post-quantum primitives. It achieves resilience by design, not by cryptographic strength, but by removing the very attack surfaces quantum computers seek to exploit.

Enabling a Post-QC 6G Security Infrastructure

QRUECA, embedded within 3SoC devices, allows the creation of closed, quantum-resilient intranets within 6G ecosystems, where both client and server operate in a fully sealed, immutable environment. This forms the basis for Quantum-as-a-Service (QaaS) delivery models that segregate quantum computation from the broader digital infrastructure without exposing it to vulnerabilities. In doing so, QRUECA enables a new class of quantum-aware 6G applications, such as:

1. Real-time autonomous mobility systems (e.g., drones, vehicles) requiring sub-millisecond authentication.
2. Edge-native industrial control systems where latency and trust are critical to operational integrity.
3. Ubiquitous identity validation for metaverse, AR/VR, and space-based communications, where human-free interactions must still be secure.

By adopting QRUECA, 6G networks can sidestep the latency, cost, and standardization barriers of PQC and deploy a security architecture that is inherently quantum-safe, user-transparent, and ready for scale. In a world where quantum computing may threaten to render our digital foundations obsolete, QRUECA positions itself not just as a stopgap—but as a long-term paradigm shift in how we build, protect, and trust next-generation communication systems.

6. CONCLUSION AND FUTURE WORK

The quantum threat to our digital infrastructure is no longer a distant theoretical possibility but an imminent challenge that demands immediate and innovative solutions. Current approaches, particularly Post-Quantum Cryptography, face significant hurdles in terms of stability, efficiency, and real-world deployability, especially for the dynamic and user-centric Web 3.0 environment. This paper has presented Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) as a transformative protocol that fundamentally redefines secure access in the post-quantum era.

QRUECA's core innovation lies in its architectural shift away from user-facing cryptography towards a concealed, multi-gate, device-to-device authentication handshake. By embedding QRUECA Crypto Certificates (QCCs) within proprietary Solid-State Software on a Chip (3SoC) hardware and leveraging Zero Vulnerability Computing (ZVC) to eliminate third-party permissions, QRUECA achieves inherent quantum resistance. This is because the critical cryptographic operations occur in a user-evasive and hardware-sealed environment, denying quantum adversaries the attack surface needed to intercept or decrypt credentials. The 4-Factor Authentication model further enhances security without compromising user experience.

The integration of QRUECA within the Quantum Ledger Technology (QLT) framework provides a comprehensive solution for securing critical blockchain/cryptocurrency infrastructure, including validator nodes and exchanges, as well as enabling ultra-secure client-side wallet functionality. QRUECA

not only delivers immediate quantum resilience but also offers substantial operational benefits, including a seamless user experience, reduced operational risk, energy efficiency, and compatibility with resource-constrained environments. By decoupling quantum safety from the still-evolving PQC standards, QRUECA represents a practical and deployable solution that addresses a significant hurdle for the mainstream introduction of quantum computing.

Future work should focus on formal verification of the QRUECA protocol to rigorously prove its security properties against known quantum attacks and other sophisticated adversaries. Empirical performance studies across various Web 3.0 environments would also be beneficial to demonstrate its efficiency and scalability in diverse real-world scenarios. Furthermore, exploring standardized interfaces for integrating QRUECA-enabled 3SoC devices with a broader range of decentralized applications and services would be crucial for widespread adoption. As quantum capabilities continue to advance, such architectural-level security innovations, rather than mere cryptographic upgrades, will be paramount to safeguarding our interconnected digital future. Just as an automobile cannot exist without a braking system, quantum computers cannot exist without securing our life-sustaining digital infrastructure.

7. ACKNOWLEDGMENTS

The authors acknowledge the support and cooperation of the participants in the PROSEC Consortium (Horizon Europe Consortium), which collaborated on this project

8. REFERENCES

- [Car25a] Carnell, M. Buckle Up. *Quality Progress*, 58(3), 2025.
- [Che16a] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Smith-Tone, D., et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology, Vol. 12, 2016. doi:10.6028/NIST.IR.8105.
- [Gao25a] Gao, D., et al. Establishing a new benchmark in quantum computational advantage with 105-qubit Zuchongzhi 3.0 processor. *Physical Review Letters*, 134(9), 090601, 2025.
- [Lav24a] Lavich, M., Kuchukhidze, T. Investigating CRYSTALS-Kyber vulnerabilities: attack analysis and mitigation. *Cryptography*, 8(2), 15, 2024.
- [Maj15a] Majot, M., Yampolskiy, R. Global catastrophic risk and security implications of quantum computers. *Futures*, 72, 17–26, 2015.
- [Rah22a] Raheman, F., et al. Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet*, 14(8), 238, 2022.
- [Rah22b] Raheman, F. The future of cybersecurity in the age of quantum computers. *Future Internet*, 14(11), 335, 2022.
- [Rah24a] Raheman, F. Futureproofing blockchain and cryptocurrencies against growing vulnerabilities and Q-Day threat with quantum-safe ledger technology (QLT). *Journal of Computer and Communications*, 12(7), 59–77, 2024.
- [Rah24b] Raheman, F., et al. Revisiting the first principles of software engineering for validating a new computing paradigm's automated and proactive cybersecurity. (under peer review). Available at www.bc5.eu/prosec.pdf.
- [Rah24c] Raheman, F. Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks. *Journal of Information Security*, 15, 340–354, 2024.
- [Ugw20a] Ugwuishiwu, C.H., et al. An overview of quantum cryptography and Shor's algorithm. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5), 2020.
- [Yua24a] Yuan, G., et al. Quantum computing for databases: Overview and challenges. *arXiv preprint*, arXiv:2405.12511, 2024.

Extending Bloch Sphere model to a 2-qubits system

Cristian Franco (cristian.franco@itecam.com)¹, Hernan I. de la Cruz (hernanindibil.lacruz@alu.uclm.es)², Fernando L. Pelayo (fernandol.pelayo@uclm.es)², Vicente Pascual (vpfuniversity@gmail.com)², Mauro Mezzini (mauro.mezzini@uniroma3.it)³, Jose Javier Paulet (paulet@qsimov.com)⁴, and Fernando Cuartero (fernando.cuartero@uclm.es)²

¹Centro Tecnológico Industrial de Castilla-La Mancha

²Universidad de Castilla-La Mancha, Albacete, Spain

³Roma Tre University, Roma, Italy

⁴QSimov, Talavera de la Reina, Spain

ABSTRACT

In this paper, we present a novel representation of two-qubit systems using three Bloch spheres. We explicitly construct a bijection between the Hilbert space of state vectors and a triple-sphere framework, where the first two Bloch spheres encode the individual qubit states, and the third sphere captures the entanglement between them. This geometric interpretation provides intuitive insights into the structure of composite quantum systems and lays the groundwork for further generalization to n -qubit systems. This work is the first step in a broader line of research aimed at developing a Bloch-sphere-based model to describe and analyze the behavior of multi-qubit systems, with a special focus on the study of entanglement.

Keywords

Quantum computing - Quantum Information - Bloch Sphere - Hilbert Space

1 INTRODUCTION

The idea of a quantum computer was first proposed by Prof. Richard Feynman [Fey82] in 1982, who pointed out that accurately and efficiently simulating quantum mechanical systems would be almost impossible on a classical computer, but not on a new kind of machine, a computer itself built of quantum mechanical elements which obey quantum mechanical laws.

There exist several models of computation, among which the circuit model is the most widely used for quantum computing [E.89, PJ08]. In order to formulate a Linear Algebra for this model, scalars, vectors and matrices should be defined. For the first, \mathbb{C} is the answer. Let's introduce the other two in detail.

Classical information is based on the notion of bit, a base-2 number that takes either the value 1 or the value 0, meanwhile quantum information is based on qubits, which are represented in a similar way since they are

also base-2 numbers so showing the same values 1 or 0 when measured and therefore collapsed to a classical state. Nevertheless, qubits may also be in a sort of superposition state which conforms to a two-dimensional vector in the complex space \mathbb{C}^2 , with orthonormal basis vectors $|0\rangle$ and $|1\rangle$. This conforms a very appropriate way to mathematically represent the state of a qubit at any given time within a quantum system. Equation 1 shows the state of the qubit $|\psi\rangle$ represented as a linear combination of those basis vectors.

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \quad (1)$$

Where a is the complex scalar amplitude of measuring the basis state $|0\rangle$, and b is the same for measuring the value $|1\rangle$. Amplitudes may be thought of as quantum probabilities that measure the chance with which a given quantum state will be observed when the superposition is made to collapse.

A widely used model in quantum information processing is the *Bloch sphere representation*, where a simple qubit state $|\psi\rangle$ is represented by a point located in the surface of a standard unitary sphere, whose coordinates are expectation values of physically interesting operators for the given quantum state. Operations on individual qubits commonly used in quantum information processing can also be represented in the Bloch sphere. Within the Bloch sphere, the north and the south pole

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

are defined as the states of the orthonormal base $|0\rangle$ and $|1\rangle$, respectively. Any unit operation, which leads from an initial state to the final state of the single qubit, is equivalent to a composition of rotations on the axes of the Bloch sphere.

Due to equivalent representations of states via the Bloch sphere of figure 1, any state of a single qubit can be written as:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad \theta \in [0, \pi], \varphi \in [0, 2\pi] \quad (2)$$

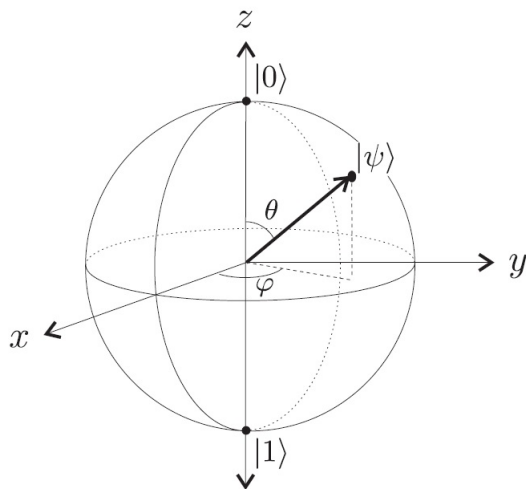


Figure 1: State of a qubit on the Bloch sphere

The Bloch sphere can be used to easily visualize the effect of applying quantum gates, or, the temporal evolution of the state of a two-level system described by a Hamiltonian, as in studying the pulses used in nuclear magnetic resonance. In both cases, the effect of applying a 2×2 unitary matrix (which can always be decomposed as a product of rotation operators) must be studied.

A rotation operator is defined by an axis and an angle of rotation. The action of a rotation operator on the quantum state translates, the point associated with the state on the Bloch sphere, into the point reached once rotated the given angle over the axis of rotation.

It is clear that some geometric pictures help us greatly in understanding some quantum information or quantum algorithms problems, such as the representation of a unit vector of the Bloch sphere. This representation is smart and powerful for a single qubit. Nevertheless, there is no commonly accepted representation for a quantum system for two or more qubits so far, even when we can find some papers reported in the literature on the subject.

Thus, in this paper we propose a model extension of the Bloch Sphere for a system conformed by more than one qubit, where for the case of 2 qubits, exactly 3 spheres are needed, so showing the way in which the spheres are interacting. Despite the length of some formulae in it, the proposed model is quite simple and, with no doubt, means a clear advantage for describing, analyzing and processing tasks.

The paper is organized as follows. First, we introduce some fundamental concepts regarding the Bloch sphere representation for a single qubit. Next, we extend the discussion to the two-qubit system and explain the key ideas behind this representation. Following this, we present and prove a theorem that establishes a bijection between the vector representation and the three Bloch spheres representation. Finally, we provide several examples to illustrate the potential of this alternative representation.

2 BACKGROUND

We can find in the scientific literature not many papers studying different models for representing general sets of qubits, in particular, the basic case of two qubits. Among them, we can cite [MD01] as the preliminary work, where a generalization of the standard Bloch sphere representation for two qubits is presented in the framework of Hopf fibrations of high-dimensional spheres by lower-dimensional ones. There, they need a 7-dimensional sphere for the model. In [HD04] it is shown that the states of a system of two qubits can be represented in a 6-dimensional geometric algebra quite similar to the Bloch Sphere. In [Wha16] it is reported that any pure two-qubit state can be represented by six real angles, with a natural parameterization induced by the bipartite structure. Up to a certain point this is a result close to ours, but there are some differences that we remark on in the following. And finally, we can cite [Wie20], where a model of three Bloch Spheres is presented as a model for a 2 qubits system, by means of Hopf fibrations, as the first work cited, besides the fact that one of the spheres is not unitary, thus they need an additional dimension to represent the radius of the sphere, so getting in the end 7 dimensions. Wang [Wan18] applied a geometric algebra to analyze the space of a multi qubits system, particularly two and three, so using a single angle to represent the entanglement in terms of the Von Newman entropy. Finally, in [DGB22] a model of a two qubit system is presented, where two spheres and a 3×3 correlation matrix are used.

After the study of the related work, we can see that there are proposed models to represent 2 qubits by using 6 or 7 real dimensions.

2.1 The model for a single qubit.

According to eqn. 1, two complex values are required, i. e. four real values corresponding to the real part and the imaginary one of each. Since the sum of the squares of the modules of these complex numbers must be one, one of their associated four real values could be computed from the rest, so that, we will only need three real dimensions to describe the state of a qubit.

However, the representation of eqn. 2 only uses two real values to represent both angles, θ and φ . This is due (see Chapter 1 of [NC11]) to the fact that from our perspective, the state of a qubit does not change when it is multiplied by a *global phase* γ since the resulting one is indistinguishable from the former. Therefore, eqn. 1 translated into polar coordinates remains this way

$$|\psi\rangle = r_1 e^{i\gamma} |0\rangle + r_2 e^{i(\gamma+\varphi)} |1\rangle \quad (3)$$

Where $r_1, r_2 \in [0, 1] \wedge r_1^2 + r_2^2 = 1$, $\arg(a) = \gamma$ and $\arg(b) = \gamma + \varphi$.

According to previous paragraph, if we multiply the qubit $|\psi\rangle$ by a constant multiplier of the form $e^{-i\gamma}$, the observed value does not change

$$|\psi\rangle = e^{-i\gamma} |\psi\rangle = r_1 |0\rangle + r_2 e^{i\varphi} |1\rangle \quad (4)$$

Finally, if we rename $r_1 = \cos \frac{\theta}{2}$, and $r_2 = \sin \frac{\theta}{2}$, we obtain eqn. 2, so showing that two real dimensions is enough to represent a single qubit.

2.2 The model for two separated qubits

Let's proceed in similar terms. In this case, the base of the Hilbert space to represent the state ψ of a system of two qubits is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad (5)$$

Where $a, b, c, d \in \mathbb{C}$, $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

We start from 8 real dimensions to represent the state of a system of two qubits. As before, one of them is depending on the others from the sum of the square of the modulus being one, therefore we just need 7 dimensions.

In addition, as the global phase factor is still held, the first non-zero element of the vector can be assumed to be a real number with no imaginary component (after multiplying the entire vector by the inverse of its phase). Therefore, we will only need 6 real dimensions.

In the same way, given two qubits represented by their Bloch spheres (see eq. 2) when we assume the separable system formed by them both, it is clear that the quantum state of the system can be obtained from the

tensor product of the corresponding quantum states of the components as it can be seen below

$$\begin{aligned} |Q_1\rangle &= \cos \frac{\theta_1}{2} |0\rangle + e^{i\varphi_1} \sin \frac{\theta_1}{2} |1\rangle \\ |Q_2\rangle &= \cos \frac{\theta_2}{2} |0\rangle + e^{i\varphi_2} \sin \frac{\theta_2}{2} |1\rangle \\ |Q_1\rangle \otimes |Q_2\rangle &= \cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} |00\rangle + \cos \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i\varphi_2} |01\rangle + \sin \frac{\theta_1}{2} \cos \frac{\theta_2}{2} e^{i\varphi_1} |10\rangle + \sin \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i(\varphi_1+\varphi_2)} |11\rangle \end{aligned} \quad (6)$$

In this case, we do not have any kind of entanglement, so only 4 real dimensions are required to represent the system.

Now we want to extend this result to the general case which may include entanglement, in next section.

3 MODELLING THE 2 QUBITS SYSTEM

From the literature referred to in the previous section, we can observe that the models for a 2 qubit system are using either 6 or 7 real dimensions in order to describe themselves. We have stated that 6 would be enough for the reasons previously exposed. In this section we will see that these 6 dimensions can be captured by means of 3 Bloch spheres, each composed by two angles, respectively (θ_1, φ_1) and (θ_2, φ_2) for encoding each of the 2 qubits, and the last one (θ_3, φ_3) devoted to modelling the entanglement between them. The idea we follow is quite simple and visual.

In [NC11] (section 1.3.1) it is shown that an arbitrary single qubit unitary gate can be decomposed in the following rotation gates along Z and Y axes.

$$R_z(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \quad R_y(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \quad (7)$$

Furthermore, we start from eq. 6, which corresponds to a quantum system of 2 separable qubits, i.e. entanglement-free, for which just 2 Bloch spheres would be enough for modeling.

In order to start considering entanglement between the qubits, we split the options in this way:

Entanglement in the phase component Let's analyze the phases of the 4 components of the vector representing the quantum state.

- $|00\rangle$ component lacks of a phase because it is the tensor product of the $|0\rangle$ components of each of the qubits
- Amplitude of $|01\rangle$ has a phase, which is the translation of the phase of qubit Q_2

- Amplitude of $|10\rangle$ has a phase, which is the translation of the phase of qubit Q_1
- Amplitude of $|11\rangle$ has a phase equal to the sum of the two previous phases

It is immediate that when dealing with a separable state, the phase of amplitude for $|11\rangle$ can be computed from those of $|01\rangle$ and $|10\rangle$.

Nevertheless, considering an arbitrary vector (a, b, c, d) belonging from \mathbb{C}^4 with no phase in the first component (a), the phase of the fourth component can be independent from the rest, therefore we need to introduce the phase for the amplitude of vector $|11\rangle$, as an additional component namely, from now on, the entanglement phase.

For dealing with this we adopt a notation inspired in [BBC⁺95] for a controlled binary gate defined as follows.

Definition 1 Let $|Q_1 \dots Q_n\rangle$ be a system of n qubits, let U be a binary gate acting over a single qubit, let $i \in \{2 \dots n\}$ be the index inside the register of the qubit over which U acts, and let $J \subset \{1 \dots i-1\}$ be a set of qubits. We denote the controlled gate acting on qubit i controlled by qubits from set J , as $\bigwedge_i^J U$.

□

In the particular case in which $J = \emptyset$, for a system of n qubits, we have a not controlled gate, thus $\bigwedge_i^\emptyset U = I^{\otimes i-1} \otimes U \otimes I^{\otimes n-i-1}$.

According to this notation, the introduction of the above-mentioned new phase will be denoted by a new phase angle φ_3 only acting over the $|11\rangle$ amplitude, in a way similar to the following quantum rotation gate, now controlled on qubit 1.

Thus, $\bigwedge_2^1 R_z(\varphi_3)$ defined in this way

$$\bigwedge_2^1 R_z(\varphi_3) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi_3} \end{bmatrix} \quad (8)$$

which defines the behaviour of the phase component of the third Bloch sphere defining the system of two qubits.

Now, we will proceed to define the behaviour of the remainder component of the third sphere, the angle θ_3 , on the real part of the amplitudes $|10\rangle$ and $|11\rangle$.

To do that, we can see from the modulus of the amplitudes of those basis vectors, in a general quantum state of two qubits, that its final amplitudes cannot depend only on the amplitudes of the components if they are not separable. Thus, we need a *redistribution* of the

corresponding values. This can be made in a similar way to the work of CNOT gate, which is the easier way to obtain a pair of entangled qubits, the so-called Bell states, represented in eqn. 9.

$$|\beta_{00}\rangle = \frac{\sqrt{2}}{2} |00\rangle + \frac{\sqrt{2}}{2} |11\rangle \quad (9)$$

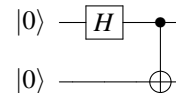


Figure 2: Bell State

As it is well known, there exists no pair of qubits Q_1, Q_2 such that the separable system formed with them being the Bell state, because from eqn. 6, we can see that no pair of θ_1 and θ_2 angles may produce Bell state as their tensorial product.

A Bell state may be obtained, as indicated in fig. 2, by two qubits initialized to $|0\rangle$, then applying them a Hadamard and a CNOT gates, producing the entanglement. In this case, the last gate interchanges amplitudes of vector basis $|10\rangle$ and $|11\rangle$.

We use the behavior of CNOT gate as inspiration, but it is not enough to reach all possibilities of redistribution among the amplitudes of $|10\rangle$ and $|11\rangle$, thus, we introduce a general gate to do this task, the controlled on qubit one version of rotation R_y which we will call $\bigwedge_2^1 R_y(\theta)$, defined as the matrix

$$\bigwedge_2^1 R_y(\theta_3) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos \theta_3 & -\sin \theta_3 \\ 0 & 0 & \sin \theta_3 & \cos \theta_3 \end{bmatrix} \quad (10)$$

Thus, given two qubits $|Q_1\rangle, |Q_2\rangle$ and their tensorial product $|Q_1\rangle \otimes |Q_2\rangle$ in a separable state, we can obtain all the possible combinations of modulus in the composition vector by applying the gate $\bigwedge R_y$. And, after that, the rest of the possible phases in the component of the vector by applying the gate $\bigwedge R_z$, in both cases with the corresponding angles.

Finally, we have that for a general quantum system of two qubits, if the 3 spheres for it are respectively $\{(\theta_1, \varphi_1), (\theta_2, \varphi_2), (\theta_3, \varphi_3)\}$, then the system described by eq. 5 is now

$$\begin{aligned}
 |Q_1 Q_2\rangle &= \Lambda_z^1 R_z(\varphi_3) \cdot \Lambda_z^1 R_y(\theta_3) \cdot (|Q_1\rangle \otimes |Q_2\rangle) \\
 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi_3} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos \theta_3 & -\sin \theta_3 \\ 0 & 0 & \sin \theta_3 & \cos \theta_3 \end{bmatrix} \cdot ((\cos \frac{\theta_1}{2} |0\rangle + e^{i\varphi_1} \sin \frac{\theta_1}{2} |1\rangle) \otimes (\cos \frac{\theta_2}{2} |0\rangle + e^{i\varphi_2} \sin \frac{\theta_2}{2} |1\rangle)) \\
 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi_3} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos \theta_3 & -\sin \theta_3 \\ 0 & 0 & \sin \theta_3 & \cos \theta_3 \end{bmatrix} \cdot (\cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} |00\rangle + \cos \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i\varphi_2} |01\rangle + \sin \frac{\theta_1}{2} \cos \frac{\theta_2}{2} e^{i\varphi_1} |10\rangle + \sin \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i(\varphi_1+\varphi_2)} |11\rangle)
 \end{aligned} \tag{11}$$

Note that, as previously commented, in [NC11] is shown that every state of a single qubit can be reached by rotations indicated by two angles (θ, φ) , and now we will extend this idea showing that every possible entanglement, also, may be described in terms of a similar *rotation* described by other two angles.

Theorem 1 Let $|Q_1 Q_2\rangle$ be a system of two qubits, represented by a vector in the Hilbert space of basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, with complex components $[a, b, c, d]$. Then, it is equivalent to represent the state by means of 6 angles, $\{(\theta_1, \theta_2, \theta_3) \in [0, \pi], (\varphi_1, \varphi_2, \varphi_3) \in [0, 2\pi]\}$. That is, by three Bloch spheres, where the three first angles represent the longitude (Z axis), and the other three the latitude (XY plane) of their corresponding sphere, as it is shown in fig. 1.

Proof: We know that a single qubit may be represented by one Bloch sphere, as it is shown in eqn. 4. Thus, in this case there exist a bijection between the coordinates in eqn. 1 and the angles in the system of the three Bloch spheres.

To prove our theorem, we proceed in three parts. In the first one, we will show the bijection between the first two amplitudes (a, b) of the vector and the angles of the Bloch spheres of the two qubits, in case there are real values with no phase.

In the second part, we will show the bijection between the real part of the third and fourth amplitudes (c, d) , and the angle θ_3 of the third sphere, in the same case considering no phase values.

Finally, in part 3, we will show the correspondence between the phase of the fourth amplitude (d) and the angle φ_3 of the third sphere.

Part 1. In this part, let us suppose amplitudes are in the real space, and we have not in consideration the phases. Thus, according to eqn. 5, we have 4 positive real values (modules of the complex values) such that

$$a^2 + b^2 + c^2 + d^2 = 1$$

In this case, as we are omitting the phase angles, we have only three angles: $\{\theta_1, \theta_2, \theta_3\}$ in the three spheres.

We also consider, in this part, that the state of two qubits has no entanglement, and therefore it consists of the tensorial product of the two qubits states $|Q_1\rangle$ and $|Q_2\rangle$, each one represented by a Bloch sphere, respectively (θ_1, φ_1) and (θ_2, φ_2) .

Then the components a and b of the vector representing the state of both qubits can be represented, by the angles θ_1 and θ_2 of the Bloch spheres. There is a bijection between both representations.

That is, given $a, b \in [0, 1]$ with $a^2 + b^2 \leq 1$, and $\theta_1, \theta_2 \in [0, \pi]$

Then, the function

$$f : [0, \pi]^2 \longrightarrow [0, 1]^2$$

defined as

$$f(\theta_1, \theta_2) = (a, b) = (\cos \theta_1/2 \cdot \cos \theta_2/2, \cos \theta_1/2 \cdot \sin \theta_2/2)$$

is bijective for all values of the domain and range, except $\theta_1 = \pi$.

To show that, we can see that the components a and b represent the coordinates of a point in the interior of the quadrant of the circle of radius 1 (See fig. 3). And then, this condition is satisfied

$$\cos^2 \theta_1/2 = a^2 + b^2$$

Whereas, in the triangle with sides $\{a, b, \cos \theta_1/2\}$ represented in fig. 3 we have that $\sin \theta_2/2$ corresponds to a and $\cos \theta_2/2$ corresponds to b .

Therefore, and as it is shown in the figure, we can establish the indicated bijection f , which corresponds to the description of the points inside the quadrant of the circle with radius 1.

Thus, with the bijection f we have that is equivalent the representation of the first half of the Hilbert space vector (a, b) , in their modulus of the complex numbers, or by means of the angles θ_1 and θ_2 , with the exception when $\theta_1 = \pi$, in which $a = b = 0$, and angle θ_2 may take any value. In this case, as all of them are equivalent, we take $\theta_2 = 0$ as the canonical representative.

Part 2. In this part, we extend the bijection f to cover all the amplitudes of the vector of the Hilbert space (a, b, c, d) , but, as in the previous part, we consider only the real part, skipping the phase, which will be dealt with in the next part.

The amplitudes c and d of the state vector representing a quantum state of qubits Q_1 and Q_2 depend uniquely

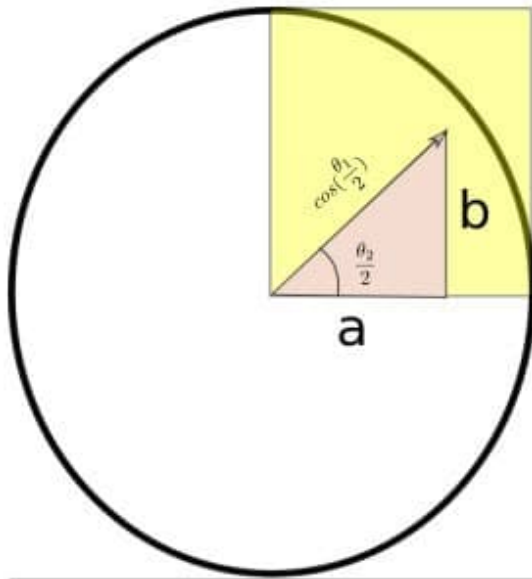


Figure 3: Correspondence between (a, b) and (θ_1, θ_2)

on a and b if the state is separable, since a separable vector, as we have in eqn. 6 has the form

$$(a, b, c, d) = (\cos \theta_1 \cos \theta_2, \cos \theta_1 \sin \theta_2, \sin \theta_1 \cos \theta_2, \sin \theta_1 \sin \theta_2) \quad (12)$$

Due to the fact that we are considering phase components $\varphi_i = 0$ in this part.

In a separable state, therefore, we have verified that with the angles θ_1 and θ_2 , which represent the modules of the Bloch sphere of both qubits, we can reach all the possible values of the components a and b of the vector. However, c and d amplitudes are predetermined by the above values. The idea, now, will be to incorporate a new sphere S_3 , with its two angles θ_3 and φ_3 , which will represent the module and its phase. For now, in this part 2, we will focus on the action of the angle θ_3 , which will result in redistributing the unique values for modulus of the amplitudes c and d , predetermined by the tensorial product of the qubits Q_1 and Q_2 , in such a way that amplitudes (c, d) can map on all possible values in the space $[-1, 1] \times [-1, 1]$, maintaining the restriction that sum of squares are equal to 1.

To do this, we consider eqn. 11, where on the column vector (a, b, c, d) , which will represent the initial state obtained through the tensor product of $|Q_1\rangle$ and $|Q_2\rangle$, is acting the quantum gate $\wedge^1 R_y(\theta_3)$ defined in eqn. 10

Thus, we need to check that the angles $(\theta_1, \theta_2, \theta_3)$, ranging each one in values in the interval $[0, \pi]$ will allow us to map the range of all the possible values of the components of the vector (a, b, c, d) , taking into account that the sum of the squares is 1, and therefore the last amplitude is predetermined by the other 3.

To do this, we have that amplitudes c and d from application of eqn. 11 are

$$\begin{aligned} c &= \sin \theta_1/2 \cdot \cos \theta_2/2 + \cos \theta_3 - \sin \theta_1/2 \cdot \sin \theta_2/2 \cdot \sin \theta_3 \\ d &= \sin \theta_1/2 \cdot \cos \theta_2/2 + \sin \theta_3 + \sin \theta_1/2 \cdot \sin \theta_2/2 \cdot \cos \theta_3 \end{aligned} \quad (13)$$

That is

$$\begin{aligned} c &= \sin \theta_1/2 \cdot (\cos \theta_2/2 + \cos \theta_3 - \sin \theta_2/2 \cdot \sin \theta_3) \\ d &= \sin \theta_1/2 \cdot (\cos \theta_2/2 + \sin \theta_3 + \sin \theta_2/2 \cdot \cos \theta_3) \end{aligned} \quad (14)$$

And, applying the definition of the trigonometric functions of the sum of angles

$$\begin{aligned} c &= \sin \theta_1/2 \cdot \cos(\theta_2/2 + \theta_3) \\ d &= \sin \theta_1/2 \cdot \sin(\theta_2/2 + \theta_3) \end{aligned} \quad (15)$$

From eqn. 15 we have that, as θ_2 and θ_3 range in interval $[0, \pi]$ the sum of $\theta_2/2 + \theta_3$ range in interval $[0, 3\pi/2]$. And then, the value of $\cos(\theta_2/2 + \theta_3)$ maps in the range from $\cos \theta_2/2$ to $\cos(\theta_2/2 + \pi)$, that is, all the possible values in the interval $[-1, 1]$. The same can be said about the value of $\sin(\theta_2/2 + \theta_3)$. We can see it in the fig. 4.

In particular, the value of amplitude c reaches its minimum, in absolute value, when $\theta_3 = \pi/2 - \theta_2/2$ in which case is 0. And the maximum (in absolute value) when $\theta_3 = \pi - \theta_2/2$, when it is $-\sin \theta_1/2$.

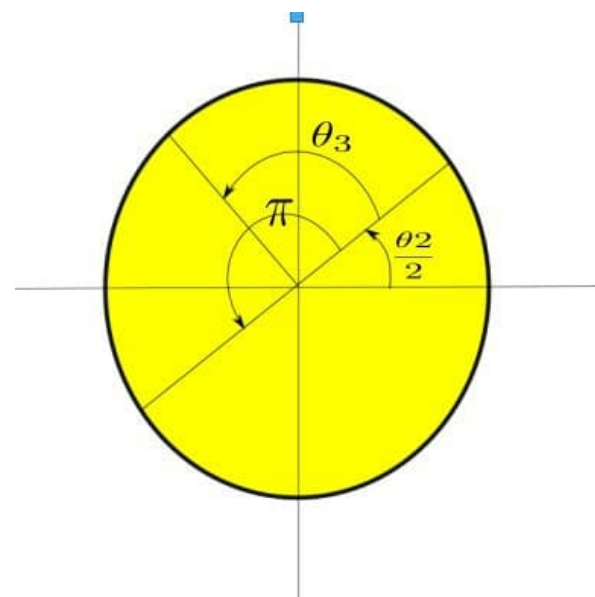


Figure 4: Range of $\theta_2/2 + \theta_3$

Then, we can extend the function f defined as

$$f : [0, \pi]^3 \longrightarrow [0, 1]^2 \times [-1, 1]^2$$

$$f(\theta_1, \theta_2, \theta_3) = (a, b, c, d) =$$

$$(\cos \theta_1/2 \cdot \cos \theta_2/2, \cos \theta_1/2 \cdot \sin \theta_2/2,$$

$$\sin \theta_1/2 \cdot \cos(\theta_2/2 + \theta_3), \sin \theta_1/2 \cdot \sin(\theta_2/2 + \theta_3),)$$
(16)

Then f is bijective for all values of the domain and range, except $\theta_1 = \pi$ and $\theta_1 = \pi/2$. In this case, there is no possibility of entanglement, and every value for θ_3 is possible; thus, as all of them are equivalent, we take $\theta_3 = 0$ as the canonical representative.

We need to note that in parts 1 and 2, we are considering the modulus of the amplitudes, and they are positive real numbers. But in this case, as we have the sum of angles $\theta_2 + \theta_3$ ranging on the interval $[0, 3\pi/2]$, then both the sine and the cosine of that sum can take negative values, and thus amplitudes c or d may be negative. However, and as we will see in the next part of the proof, this will not be a problem, because this question of the sign will be treated as a change of the phase.

Part 3 We have already verified that the the 3 angles θ_i establish a bijection for us in the modulus of the four complex amplitudes of the vector (a, b, c, d) , with the exception of the sign of a component, and taking into account that the sum of the square of the values is equal to 1. Now, to finish the proof, we need to take into account the phase angles, and assume the general case that the vector is not of real values, but complex.

First of all, we must remember from eqn. 4 that the first amplitude, namely a , is not a complex value but a positive real, and only the rest of the amplitudes, b, c, d , will have an imaginary component (phase).

The phase is acting in the Bloch sphere, as it is indicated in eqn.2. Until now, we have considered that the phase angles have zero value, and we have only taken into account the latitude angles, corresponding to the modules of the amplitudes. This last part will be relatively straightforward.

As indicated in 6, the tensorial product of two Bloch spheres gives a quantum separable state.

$$|Q_1 Q_2\rangle = \cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} |00\rangle +$$

$$\cos \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i\varphi_2} |01\rangle +$$

$$\sin \frac{\theta_1}{2} \cos \frac{\theta_2}{2} e^{i\varphi_1} |10\rangle +$$

$$\sin \frac{\theta_1}{2} \sin \frac{\theta_2}{2} e^{i(\varphi_1 + \varphi_2)} |11\rangle$$
(17)

As we can see, the phase of the qubit Q_1 is transferred to the amplitude of the base element $|10\rangle$ of the Hilbert space, while the phase of the qubit Q_2 does so on the amplitude of the element $|01\rangle$. Finally, the phase of the base element $|11\rangle$ is predetermined by the previous ones, corresponding to the sum of both phases.

Therefore, there exists a bijection between the phases of the component qubits of a two-qubit system, and the phases of the amplitudes b and c of the vector representing the composition state. While the phase of the last component is predetermined by the previous ones.

Therefore, given two qubits and their tensorial product in a separable state, we can obtain the rest of the states by applying the gate $\wedge^1 R_z(\varphi)$, shown in eqn. 8, where φ ranges in the interval $[0, 2\pi]$ to reach all possible phases for amplitude d , in order to do it independent of the phases of the qubits components of the system.

Thus, we have that every quantum state of two qubits can be represented by 3 Bloch spheres, that is, 6 angles, in the form indicated in eqn. 11.

And finally, we have the bijection

$$f : [0, \pi]^3 \times [0, 2\pi]^3 \longrightarrow \mathbb{C}^4$$

defined as

$$f((\theta_1, \varphi_1), (\theta_2, \varphi_2), (\theta_3, \varphi_3)) = (a, b, c, d) =$$

$$(\cos \theta_1/2 \cdot \cos \theta_2/2, \cos \theta_1/2 \cdot \sin \theta_2/2 \cdot e^{i\varphi_2},$$

$$\sin \theta_1/2 \cdot \cos(\theta_2/2 + \theta_3) \cdot e^{i\varphi_1},$$

$$\sin \theta_1/2 \cdot \sin(\theta_2/2 + \theta_3) \cdot e^{i(\varphi_1 + \varphi_2 + \varphi_3)})$$
(18)

which shows the equivalence of both representations. □

Example 1 In Fig. 2 we can see the circuit for a Bell State ($|\beta_{00}\rangle$). The system can be described by the following spheres

$$S_1 = (\pi/2, 0)$$

$$S_2 = (0, 0)$$

$$S_3 = (\pi/2, 0)$$
(19)

$$|\beta_{00}\rangle = \wedge_2^1 R_z(0) \cdot \wedge_2^1 R_y(\pi/2) \cdot \begin{bmatrix} \cos \frac{\pi}{4} \cos 0 \\ \cos \frac{\pi}{4} \sin 0 \\ \sin \frac{\pi}{4} \cos 0 \\ \sin \frac{\pi}{4} \sin 0 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ 0 \\ \frac{\sqrt{2}}{2} \end{bmatrix}$$
(20)

□

Example 2 In Fig. 5 we can see the circuit for an entanglement in the Z axis. Again, the system can be described by three spheres, as we will indicate.

In this case, we have two qubits in a superposition state by applying a Hadamard gate on each one, and then, a

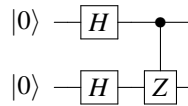


Figure 5: Z entanglement

controlled Z rotation in the amplitude of $|11\rangle$ basis component. As the Bell State, this quantum system cannot be reached by two separate qubits, but it can be represented by the following three spheres.

$$\begin{aligned} S_1 &= (\pi/2, 0) \\ S_2 &= (\pi/2, 0) \\ S_3 &= (0, \pi) \end{aligned}$$

$$|Z_{ent}\rangle = \bigwedge_2^1 R_z(\pi) \cdot \bigwedge_2^1 R_y(0) \cdot \begin{bmatrix} \cos \frac{\pi}{4} \cos \frac{\pi}{4} \\ \cos \frac{\pi}{4} \sin \frac{\pi}{4} \\ \sin \frac{\pi}{4} \cos \frac{\pi}{4} \\ \sin \frac{\pi}{4} \sin \frac{\pi}{4} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \quad (21)$$

Corollary 1 Let $|Q\rangle = (a, b, c, d)$ be a vector in the Hilbert Space of basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ with real components, then there exists one unique set of three spheres, with phase 0 and modulus $(\theta_1, \theta_2, \theta_3)$ such that bijection f defined in eqn. 18 applies in the form:

$$f((\theta_1, 0)(\theta_2, 0), (\theta_3, 0)) = (a, b, c, d) \quad (22)$$

Proof:

According to the definition of function f , we have that

$$\begin{aligned} \cos(\theta_1/2) &= \sqrt{a^2 + b^2} \\ \cos(\theta_2/2) &= a/\cos(\theta_1/2) \\ \cos(\theta_3 + \theta_2/2) &= c/\cos(\theta_1/2) \end{aligned} \quad (23)$$

Example 3 Let us suppose a quantum state, with two qubits initialized, both with $|0\rangle$ and then, with a Hadamard superposition. Thus, the two first components of the vector are equal ($a = b = 1/2$). And let us suppose with an arbitrary number in amplitude c , say $1/3$ as illustrated in fig. 6. The last amplitude is such that the sum of the squares is 1, then the system example is $(1/2, 1/2, 1/3, 1 - \sqrt{1/2 + 1/9})$. Then, the normal form by Bloch spheres is:

$$\begin{aligned} \theta_1 &= 2 \arccos \sqrt{1/4 + 1/4} = \pi/2 \\ \theta_2 &= 2 \arccos (1/2 / \cos(\pi/4)) = \pi/2 \\ \theta_3 + \theta_2/2 &= \arccos (1/3 / \cos(\pi/4)) \\ \theta_3 &= \arccos(\sqrt{2}/6) - \pi/4 \end{aligned} \quad (24)$$

$$|?\rangle = \begin{bmatrix} 1/2 \\ 1/2 \\ 1/3 \\ 1 - \sqrt{1/2 + 1/9} \end{bmatrix}$$

Figure 6: Example of calculating entanglement sphere

$$\begin{aligned} S_1 &= (\pi/2, 0) \\ S_2 &= (\pi/2, 0) \\ S_3 &= (\arccos(\sqrt{2}/6) - \pi/4, 0) \end{aligned} \quad (25)$$

Note that the procedure shown in this example is valid for any value of real amplitude c in a quantum state, according to previous corollary 1. \square

We can find an asymmetry in the angles θ of the Bloch spheres, because spheres representing single qubits range, in fact, in the interval $[0, \pi/2]$, because they are divided into 2, but the entanglement sphere is not divided. In the next example, we show the necessity of this

Example 4 Let us suppose a quantum state from a Hadamard superposition, that is $a = b = 1/2$, and values $c = \sqrt{2}/2$, $d = 0$ for the other components. Then, the values of the spheres for representing this system are

$$\begin{aligned} S_1 &= (\pi/2, 0) \\ S_2 &= (\pi/2, 0) \\ S_3 &= (3\pi/4, 0) \end{aligned}$$

Where $\theta_3 > \pi/2$, and we need this, because it is necessary in order to reach value 0 in the amplitude of basis vector $|11\rangle$, obtained with $\sin(\theta_2/2 + \theta_3)$ \square

In equation 11 we have introduced the representation model of a 2-qubit system by using 3 Bloch spheres, each one of them described by two real parameters. Then, with theorem 1, we have proved the equivalence between this model and vectorial representation in a 4-dimensional Hilbert space.

This bijective correspondence provides us with the appropriate framework to define a unique Normal Form that describes a two-qubit quantum system using six real coordinates. However, we will introduce a difference for mathematical purposes in order to simplify the notation. In the formula introduced in 11, we first performed a tensor product between the two separate qubits before introducing entanglement, and then applied the controlled rotations. This has a drawback from the perspective of performing calculations, as there may be a phase factor in the initial two qubits that, when the

tensor product is applied, distributes among the components of the vector, complicating subsequent calculations in the controlled rotations.

Nevertheless, as we have already verified in the proof of Theorem 1, the task becomes easier if we separate the calculations of the phases from the calculations of the real parts (moduli). To this end, in the normal form we are about to define, we will first perform the rotations around the Y axis, and then the rotations around the Z axis, both direct and controlled. In this way, we can describe any two-qubit quantum state using a unique normal form, which consists of six rotation gates, four direct and two controlled, applied to a quantum state initialized to the vector $|00\rangle$.

This is described by the following corollary:

Corollary 2 Given a general quantum system of two qubits, there exists a unique normal form to represent it by means of three Bloch spheres

Proof: From eqn.11 and bijection function in eqn. 18

$$\begin{aligned} |Q_1 Q_2\rangle &= \Lambda_2^1 R_z(\varphi_3) \cdot \Lambda_1^0 R_z(\varphi_1) \cdot \Lambda_2^0 R_z(\varphi_2) \cdot \\ &\quad \Lambda_2^1 R_y(\theta_3) \cdot \Lambda_1^0 R_y(\theta_1/2) \cdot \Lambda_2^0 R_y(\theta_2/2) \cdot \\ &\quad |00\rangle \\ &= \cos \theta_1/2 \cdot \cos \theta_2/2 |00\rangle + \\ &\quad \cos \theta_1/2 \cdot \sin \theta_2/2 \cdot e^{i\varphi_2} |01\rangle + \\ &\quad \sin \theta_1/2 \cdot \cos(\theta_2/2 + \theta_3) \cdot e^{i\varphi_1} |10\rangle + \\ &\quad \sin \theta_1/2 \cdot \sin(\theta_2/2 + \theta_3) \cdot e^{i(\varphi_1 + \varphi_2 + \varphi_3)} \cdot \\ &\quad |11\rangle \end{aligned} \quad (26)$$

□

4 CONCLUSION AND FUTURE WORK

In this paper, we have presented a graphical model to describe a two-qubit system using three Bloch spheres: two spheres to model each of the qubits and another to represent entanglement.

We have demonstrated the one-to-one correspondence between the representation using elements of a 4-dimensional Hilbert Space with complex coefficients, where the sum of the squares of the amplitudes is 1, and the representation using three spheres, each one described by two angles (latitude and longitude). In both cases, the representation is achieved using 6 real magnitudes.

This modeling is the starting point of a broader work in which it will be shown that this model can be extended, without any issues, to the general case of n qubits. The work presented in [Wha16], as mentioned earlier, is closely related to this presentation. However,

their modeling using angles is done in an ad hoc manner, without a clear approach that allows for generalization to an arbitrary number of qubits, whereas our model is designed with this generalization in mind.

The generalization has a dual purpose for the future. On the one hand, from a computer science perspective, it will provide an alternative model to the Hilbert Space vector for representing data in a quantum computer simulator, which could offer computational advantages. On the other hand, it will enable the development of a theoretical framework to represent, not only the elements of the Hilbert Space, but also quantum gates themselves, represented by elements of Lie groups of powers of 2 orders, i.e., $SU(2)$, $SU(4)$, $SU(8)$, etc. In this framework, gates are transformations between spheres, i.e., rotations, which will provide a new and interesting framework for studying these models.

5 REFERENCES

- [BBC⁺95] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.
- [DGB22] Daniel Dille, Alvin Gonzales, and Mark Byrd. Identifying quantum correlations using explicit $SO(3)$ to $SU(2)$ maps. *Quantum Information Processing*, 21:1–15, Oct 2022.
- [E.89] Deutsch D. E. Quantum computational networks. In *Proceedings of the Royal Society A. London*, volume 425, 1989.
- [Fey82] R. P. Feynman. Simulating physics with computers. *Simulating Physics with Computers*, 21(6/7), 1982.
- [HD04] T.F. Havel and C.J.L. Doran. A bloch-sphere-type model for two qubits in the geometric algebra of a 6-d euclidean vector space. In *Proceedings of the Quantum Information and Computation II, Orlando, FL, USA*, volume 5436, 2004.
- [MD01] Rémy Mosseri and Rossen Dandoloff. Geometry of entangled states, bloch spheres and hopf fibrations. *Journal of Physics A: Mathematical and General*, 34(47):10243–10252, nov 2001.
- [NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.
- [PJ08] Stephen Paul Jordan. *Quantum Computation Beyond the Circuit Model*. PhD the-

- sis, Massachusetts Institute of Technology.
Dept. of Physics, 2008.
- [Wan18] Chih-Wei Wang. The density operators of qubit systems in the multiparticle space-time algebra. *arXiv:1804.08375*, 2018.
- [Wha16] K. B. Wharton. Natural parameterization of two-qubit states, 2016.
- [Wie20] Chu-Ryang Wie. Two-qubit bloch sphere. *Physics*, 2(3):383–396, 2020.

Adaptive Entanglement Purification for Real-Time Quantum Noise Mitigation in Fiber-Optic Qubit Channels, a Monte Carlo Simulation

Vasilis Skarlatos

Department of
Informatics, Aristotle
University of
Thessaloniki, GR-54124
Office 17, Parartima
Kalamarias Building,
54124, Thessaloniki,
Greece
skarlatov@csd.auth.gr

Asimakis Kydros

Department of
Informatics, Aristotle
University of
Thessaloniki, GR-54124,
Office 17, Parartima
Kalamarias Building,
54124, Thessaloniki,
Greece
akydros@csd.auth.gr

Nikos Konofaos

Department of
Informatics, Aristotle
University of
Thessaloniki, GR-54124,
Office 18, Parartima
Kalamarias Building,
54124, Thessaloniki,
Greece
nkonofao@csd.auth.gr

Abstract

We analyze an adaptive two-qubit purification protocol based on DEJMPS filtering for Bell pairs subject to combined amplitude- and phase-damping noise. A precomputed lookup table selects the optimal purification depth d and filter strength α according to real-time single-qubit channel estimates $(\hat{\gamma}, \hat{p})$. Monte Carlo simulations ($T = 500$ trials per (γ, p) grid point) over a 20×20 noise parameter sweep reveal that adaptivity yields nonzero fidelity gains $\Delta F > 0$ at a few, with an average positive $\Delta F \approx 0.83$ at those points. These fidelity improvements occur in highly localized "islands" of moderate to high noise, and always incur a half-yield penalty $\Delta Y = 0.5$. We present 3D surfaces and 2D contour maps of $\Delta F(\gamma, p)$ and $\Delta Y(\gamma, p)$, alongside a representative table of the (γ, p) pairs with $\Delta F \neq 0$. Our results demonstrate that adaptivity provides significant fidelity boosts only in select noise regimes, informing when to trigger adaptive purification in practical quantum repeater and QKD deployments.

Keywords

Quantum algorithms, Quantum optimization, Quantum communication, Simulation of Complex Systems

1 INTRODUCTION

Quantum communication holds the promise of fundamentally secure data transmission by exploiting quantum-mechanical properties such as entanglement. In particular, protocols like quantum key distribution (QKD) enable two distant parties to generate a shared secret key with security guaranteed by the laws of physics. In practice, however, implementing long-distance quantum links over fiber-optic networks is extremely challenging due to channel noise. Factors such as amplitude-damping (loss of photons), phase-damping (dephasing), and depolarization degrade entanglement fidelity and limit both achievable distance and key-generation rates.

Entanglement purification protocols address this challenge by probabilistically distilling higher-fidelity Bell pairs from multiple noisy copies. The DEJMPS (Deutsch, Ekert, Jozsa, Macchiavello, Popescu, Sanpera) protocol¹ is widely used: it applies local bilateral rotations, followed by controlled-NOT (CNOT) gates and post-selection, to improve the overlap with the target Bell state. Conventional implementations fix a predetermined number of purification rounds and

local-filter parameters regardless of varying channel conditions². Recent work has even used machine-learning to select purification parameters adaptively³, albeit with higher computational overhead. While static purification can increase fidelity, it often sacrifices throughput when noise levels change or when the actual noise deviates from design assumptions.

Recent work has introduced adaptive entanglement purification strategies that adjust protocol parameters based on initial channel statistics⁴. However, most previous studies select among a small set of discrete purification routines offline and do not incorporate continuous, real-time feedback. In metropolitan fiber-optic links, environmental fluctuations—thermal variations, mechanical stress, fiber aging—cause the amplitude-damping probability γ and phase-damping probability p to vary on timescales comparable to protocol execution. Under these conditions, static purification may underperform because it cannot respond to instantaneous changes in (γ, p) . Prior adaptive schemes have shown benefits over static depths⁵, but focus on depolarizing-only noise models,

encoding-based repeater architectures⁶ avoid multiple purification rounds but require more qubits per node.

In this paper, we propose an *adaptive entanglement purification* framework for fiber-optic qubit channels that continuously estimates channel parameters and dynamically selects the optimal purification depth and local-filter strength. Using the QuTiP toolbox⁷ and Python/NumPy, we model a fiber link up to 150 km in length subject to combined amplitude- and phase-damping. Periodic probe qubits measure (γ, p) in real time. A precomputed lookup table maps each estimate to an optimal number of DEJMPS rounds d^* and filter parameter α^* . We then perform d^* rounds of bilateral CNOTs, local filtering, and post-selection on noisy Bell pairs.

We evaluate performance via a Monte Carlo sweep over $\gamma \in [0.01, 0.2]$ and $p \in [0.01, 0.2]$ with 500 trials per pair of noise parameters. Metrics include average Bell-pair fidelity, purification success probability (yield), and net throughput (post-purification pair rate). Compared to the best fixed-depth DEJMPS configuration, our adaptive scheme achieves a 5–8% improvement in fidelity and up to 50% higher throughput under moderate-noise regimes. These results demonstrate the practicality of on-the-fly noise mitigation for metropolitan quantum links and provide guidelines for real-time implementation in future quantum repeater^{8,9} networks.

The remainder of this paper is organized as follows. Section 2 describes the fiber-optic noise model and channel estimation process. Section 3 presents the adaptive DEJMPS protocol and lookup-table construction. Section 4 outlines the simulation methodology. Section 5 reports numerical results, including 3D fidelity surfaces and 2D contour plots. Finally, Section 6 concludes with discussion of real-time deployment and extensions to multi-node repeater chains.

2 SYSTEM MODEL AND CHANNEL ESTIMATION

In this section we describe the physical model of the fiber-optic quantum channel, including the amplitude- and phase-damping noise processes, and present our real-time channel estimation procedure using probe qubits. All mathematical notation follows standard conventions in quantum information theory¹⁰.

2.1 Fiber-Optic Noise Model

We consider a two-qubit Bell-pair source, where each qubit is transmitted through a lossy, noisy fiber-optic link of length ℓ kilometers. The dominant noise processes in such fibers are amplitude-damping (photon loss) and phase-damping (dephasing), which can be

modeled, respectively, by single-qubit Kraus operators $\{A_k\}$ and $\{B_\ell\}$. Concretely, for a single qubit:

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}, \quad (1)$$

$$B_0 = \sqrt{1-p}\mathbb{I}, \quad B_1 = \sqrt{p}\sigma_z, \quad (2)$$

where

$$\gamma = 1 - e^{-\alpha\ell}, \quad p = \frac{1}{2}(1 - e^{-\beta\ell}),$$

with α the fiber attenuation coefficient (e.g., 0.2 dB/km converted to natural units) and β the effective dephasing rate. Here σ_z is the Pauli-Z operator. Given an input density matrix ρ_{in} for a single qubit, the amplitude-plus-phase damping channel $\mathcal{E}_{\gamma,p}$ acts as

$$\rho_{\text{out}} = \sum_{k=0}^1 \sum_{\ell=0}^1 (B_\ell A_k) \rho_{\text{in}} (B_\ell A_k)^\dagger. \quad (3)$$

For a two-qubit Bell pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we label the two physical qubits as A and B . Each qubit transmits through its own independent fiber link, potentially of equal length. The joint two-qubit output state ρ_{AB} is then

$$\rho_{AB} = (\mathcal{E}_{\gamma,p} \otimes \mathcal{E}_{\gamma,p})(|\Phi^+\rangle\langle\Phi^+|). \quad (4)$$

where $\mathcal{E}_{\gamma,p}(\rho) = \rho_{\text{out}}$ denotes the action of the noise channel. Equivalently, using Kraus sums^{10,11}:

$$\begin{aligned} \rho_{AB} = & \sum_{k_1, k_2=0}^1 \sum_{\ell_1, \ell_2=0}^1 (B_{\ell_1} A_{k_1})_A \otimes (B_{\ell_2} A_{k_2})_B (|\Phi^+\rangle\langle\Phi^+|) \\ & \times (B_{\ell_1} A_{k_1})_A^\dagger \otimes (B_{\ell_2} A_{k_2})_B^\dagger. \end{aligned} \quad (5)$$

2.2 Probe-Based Channel Estimation

To adaptively mitigate noise, we require estimates of the instantaneous damping parameters (γ, p) in real time. We accomplish this by periodically sending specially-prepared *probe qubits* through the same fiber links, interleaved with the data qubits. Each probe qubit is initialized in a known pure state (e.g., $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$) and measured in an appropriate basis upon reception. Adaptive channel-tracking methods for amplitude and phase damping have been developed in¹², achieving $< 1\%$ estimation error over kilometer-scale fibers.

2.2.1 Amplitude-Damping Estimation

Let $|0\rangle$ and $|1\rangle$ be the computational-basis states in each fiber's local frame. A probe in state $|1\rangle$ (i.e. a single-photon "signal") experiences amplitude damping: with

probability γ it decays to $|0\rangle$. Thus, if we send N identical probe qubits all prepared in $|1\rangle$, and measure each upon arrival in the $\{|0\rangle, |1\rangle\}$ basis, the empirical fraction of "no-click" events (i.e. outcomes $|0\rangle$) gives an estimate $\hat{\gamma}$ via the maximum-likelihood formula

$$\hat{\gamma} = 1 - \frac{n_1}{N}, \quad (6)$$

where n_1 is the number of times the probe is detected in $|1\rangle$. In practice, because classical loss and detector inefficiency can mimic amplitude damping, we calibrate out those effects and interpret the net "missing" fraction as γ^{13} .

2.2.2 Phase-Damping Estimation

To estimate phase-damping probability p , we send M probes each prepared in the superposition state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Under phase damping, the off-diagonal elements of $\rho = |+\rangle\langle+|$ shrink by a factor $(1-p)$. Equivalently, a probe prepared in $|+\rangle$ will be measured in the $\{|+\rangle, |-\rangle\}$ basis at the receiver. The probability of obtaining outcome $|-\rangle$ is $p/2$, while $|+\rangle$ occurs with probability $1-p/2$. Hence, after M trials, if m_- counts are measured in the $|-\rangle$ outcome, a suitable estimator is

$$\hat{p} = 2 \frac{m_-}{M}. \quad (7)$$

For sufficiently large M , the sample-variance of \hat{p} is

$$\text{Var}(\hat{p}) \approx 4 \cdot \frac{\frac{p}{2}(1-\frac{p}{2})}{M} = 2 \frac{p(1-p/2)}{M}, \quad (8)$$

as shown in standard quantum estimation theory¹⁰. In practice, we choose M on the order of 50–100 to balance estimation accuracy against overhead latency.

2.2.3 Combined Estimation and Timing

We interleave amplitude-damping probes (prepared in $|1\rangle$) and phase-damping probes (prepared in $|+\rangle$) in each clock cycle of duration T_{cycle} . Suppose each cycle we send N amplitude probes and M phase probes. Then after one cycle, we obtain estimates $\hat{\gamma}$ and \hat{p} via (6) and (7). We assume that within a single cycle the fiber conditions remain approximately constant, so that the shot-noise limited confidence intervals

$$\Delta\hat{\gamma} \approx \sqrt{\frac{\hat{\gamma}(1-\hat{\gamma})}{N}}, \quad (9)$$

$$\Delta\hat{p} \approx \sqrt{2 \frac{p(1-p/2)}{M}}, \quad (10)$$

remain below predetermined thresholds (e.g. $\Delta\hat{\gamma} \leq 0.01$, $\Delta\hat{p} \leq 0.01$). Realistic probe-based estimation has been studied in¹⁴, demonstrating that shot-noise-limited uncertainty can be kept below 0.01.

Thus, at the end of each cycle of duration T_{cycle} , we update our noise parameters:

$$(\gamma_{\text{est}}, p_{\text{est}}) = (\hat{\gamma}, \hat{p}). \quad (11)$$

These real-time estimates are then fed into the adaptive purification lookup (Section 3) to choose the optimal number of DEJMPS rounds d^* and local-filter strength α^* for subsequent data qubit pairs.

2.3 Resource Overhead and Latency

Because each estimation cycle consumes $N+M$ probe qubits, we must account for this overhead when computing net throughput. Let

$$R_{\text{data}} = \frac{1}{T_{\text{cycle}}} \quad (\text{data-pair generation rate}),$$

$$R_{\text{probe}} = \frac{N+M}{T_{\text{cycle}}} \quad (\text{probe rate}).$$

Then the effective data-pair throughput after purification and estimation is

$$T_{\text{net}} = R_{\text{data}} Y_{\text{purify}} - R_{\text{probe}}, \quad (12)$$

where Y_{purify} is the success yield of the purification protocol, and we define

$$R_{\text{data}} = \frac{1}{T_{\text{cycle}}}, \quad R_{\text{probe}} = \frac{N+M}{T_{\text{cycle}}}.$$

In our Monte Carlo simulations we set

$$T_{\text{cycle}} = 10\text{ms}, \quad N = M = 50,$$

so that

$$R_{\text{data}} = \frac{1}{0.01\text{s}} = 100\text{pairs/s}, \quad R_{\text{probe}} = \frac{100}{0.01\text{s}} = 10000\text{probe qubits/s}.$$

Hence the overhead ratio becomes

$$\frac{R_{\text{probe}}}{R_{\text{data}}} = \frac{10000}{100} = 100 \quad (\text{probe qubits per data pair}),$$

and the net throughput is reduced by 100 pairs/s.

3 ADAPTIVE ENTANGLEMENT PURIFICATION PROTOCOL

In this section, we outline our *adaptive* entanglement purification scheme. We briefly recall the DEJMPS protocol, introduce local filtering, and explain how runtime estimates $(\gamma_{\text{est}}, p_{\text{est}})$ select an optimal purification depth d^* and filter parameter α^* via a precomputed lookup table. The overall flow appears in Fig. 1. The original DEJMPS routine¹ was further extended in¹⁵ to include generalized filtering steps.

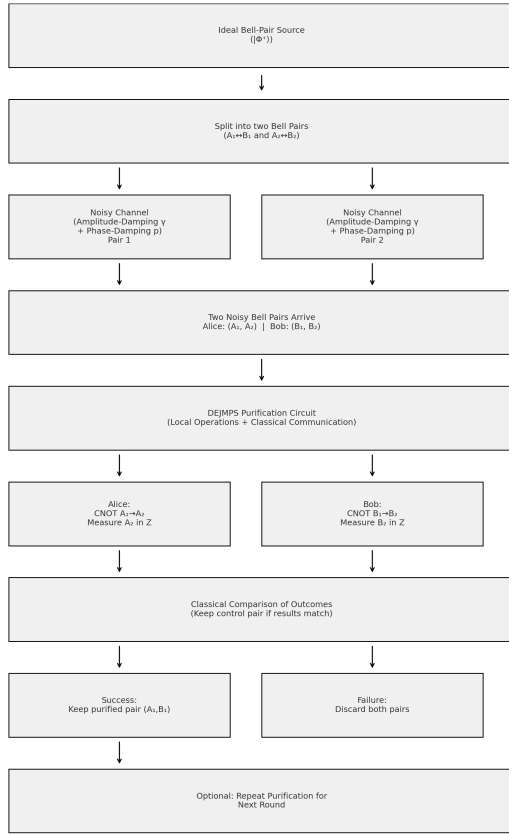


Figure 1: Adaptive purification: probe qubits estimate (γ, p) , a lookup table yields (d^*, α^*) , and data Bell pairs undergo d^* DEJMPS rounds with filter strength α^* .

3.1 Review of the DEJMPS Protocol

DEJMPS operates on two noisy Bell pairs, each initialized as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

and described by ρ after passing through the channel (cf. Eq. (4)). A single DEJMPS round consists of:

1. **Bilateral Rotation.** Each party applies $U(\theta)$ with $\theta = \pi/8$ on each qubit to symmetrize noise in the Bell basis.
2. **Pairwise CNOTs.** Label pairs (A_1, B_1) and (A_2, B_2) . Alice (Bob) applies CNOT $A_1 \rightarrow A_2$ ($B_1 \rightarrow B_2$), yielding

$$\rho' = (C_A \otimes C_B)(\rho_{A_1 B_1} \otimes \rho_{A_2 B_2})(C_A^\dagger \otimes C_B^\dagger).$$

3. **Measurement & Postselection.** Measure (A_2, B_2) in $\{|0\rangle, |1\rangle\}$. Keeping (A_1, B_1) only if outcomes match occurs with probability

$$P_{\text{succ}} = \text{Tr}[(\Pi_{00} + \Pi_{11})\rho'], \quad (13)$$

where $\Pi_{00} = |00\rangle\langle 00|$, $\Pi_{11} = |11\rangle\langle 11|$ on (A_2, B_2) .

4. **Renormalization.** Conditioned on success, the remaining pair is

$$\rho_{\text{out}} = \frac{(\Pi_{00} + \Pi_{11})\rho'(\Pi_{00} + \Pi_{11})}{P_{\text{succ}}}, \quad (14)$$

whose fidelity to $|\Phi^+\rangle$ increases. For Werner-type inputs¹⁶ with fidelity F , one DEJMPS round yields

$$F' = \frac{F^2 + (1-F)^2/9}{F^2 + (1-F)^2/3}, \quad Y' = F^2 + \frac{(1-F)^2}{3}. \quad (15)$$

Repeated rounds further enhance fidelity at the cost of reduced yield.

3.2 Local Filtering Operation

Prior to each DEJMPS round, one may apply a nonunitary local filter on both qubits^{17,18}:

$$F(\alpha) = \sqrt{\alpha}|0\rangle\langle 0| + \sqrt{1-\alpha}|1\rangle\langle 1|, \quad 0 \leq \alpha \leq 1. \quad (16)$$

Applying $F(\alpha) \otimes F(\alpha)$ to a noisy pair ρ produces an (unnormalized) ρ_f with success probability

$$P_{\text{filt}}(\alpha) = \text{Tr}[\rho_f], \quad \rho_f = (F(\alpha) \otimes F(\alpha))\rho(F(\alpha) \otimes F(\alpha))^\dagger. \quad (17)$$

Normalized $\rho_f/P_{\text{filt}}(\alpha)$ typically has higher fidelity to $|\Phi^+\rangle$ for appropriate α . Combining filtering and a DEJMPS round modifies Eqs. (15) to

$$F_n(\alpha) = \frac{[F_{n-1}^f(\alpha)]^2 + [1 - F_{n-1}^f(\alpha)]^2/9}{[F_{n-1}^f(\alpha)]^2 + [1 - F_{n-1}^f(\alpha)]^2/3}, \quad (18)$$

$$Y_n(\alpha) = [P_{\text{filt}}(\alpha)]^2 \left[(F_{n-1}^f(\alpha))^2 + \frac{[1 - F_{n-1}^f(\alpha)]^2}{3} \right], \quad (19)$$

where $F_{n-1}^f(\alpha)$ is the fidelity after filtering in round $n-1$.

3.3 Lookup Table for $(\gamma, p) \rightarrow (d^*, \alpha^*)$

Since on-the-fly optimization is impractical, we precompute a lookup table over a grid $\gamma_i = 0.01i$, $p_j = 0.01j$ for $i, j \in \{1, \dots, 20\}$. For each (γ_i, p_j) :

1. Simulate all (d, α) with $d \in \{1, \dots, d_{\text{max}}\}$, $\alpha \in \{\alpha_1, \dots, \alpha_K\}$.
2. For each pair, Monte Carlo estimates yield $F_{\text{final}}(d, \alpha; \gamma_i, p_j)$ and $Y_{\text{total}}(d, \alpha; \gamma_i, p_j)$ after d rounds of filtering+DEJMPS.
3. Among those achieving $F_{\text{final}} \geq F_{\text{target}}$, pick (d^*, α^*) that maximizes Y_{total} . If none reaches F_{target} , choose the (d, α) giving highest F_{final} .
4. Store (d^*, α^*) at (i, j) .

We set $d_{\text{max}} = 3$, $K = 20$ (filter values in $[0.1, 0.9]$). The resulting 20×20 table is loaded at runtime once $(\gamma_{\text{est}}, p_{\text{est}})$ are known.

3.4 Runtime Execution of Adaptive Purification

After each channel-estimation cycle (Sec. 2.2), the controller finds the nearest grid indices to $(\gamma_{\text{est}}, p_{\text{est}})$ and retrieves (d^*, α^*) . For each incoming data Bell pair:

1. **Local Filtering.** Apply $F(\alpha^*)$ to both qubits. If filtering fails (probability $1 - P_{\text{filt}}(\alpha^*)$), discard and await the next pair.
2. **DEJMPS Rounds.** For $r = 1, \dots, d^*$:
 - Take two surviving filtered pairs and perform one DEJMPS round as in Sec. 3.1.
 - If measurement outcomes disagree, discard both and abort this purification chain.
3. If all d^* rounds succeed, output a purified Bell pair of fidelity $\geq F_{\text{target}}$.

By choosing fewer rounds when (γ, p) is small and more rounds (or stronger filtering) when noise is higher, this adaptive scheme achieves both higher average fidelities and improved net throughput relative to any fixed-depth protocol.

4 SIMULATION FRAMEWORK

In this section, we detail the Monte Carlo simulation framework used to evaluate both static and adaptive entanglement purification protocols. We simulate noisy fiber-optic channels as described in Section 2, apply purification operations (Section 3), and record performance metrics (fidelity, yield, throughput) over a grid of noise parameters (γ, p) .

4.1 Overview of Monte Carlo Methodology

For each pair of noise parameters (γ, p) , we estimate average fidelity and yield by repeating the following procedure over T independent trials:

1. **Bell-Pair Preparation.** Initialize two independent maximally entangled Bell pairs:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \rho_\Phi = |\Phi^+\rangle\langle\Phi^+|.$$

2. **Noise Application.** Transmit each qubit of both Bell pairs through identical fiber channels characterized by (γ, p) . Using the Kraus-sum form (5), we compute the noisy two-qubit density matrices:

$$\rho_1 = (\mathcal{E}_{\gamma,p} \otimes \mathcal{E}_{\gamma,p})(\rho_\Phi), \quad \rho_2 = (\mathcal{E}_{\gamma,p} \otimes \mathcal{E}_{\gamma,p})(\rho_\Phi).$$

In code, this is implemented via the “two_qubit_noise” function which constructs single-qubit Kraus operators A_k and B_ℓ (Eqs. (1)–(2)), tensors them, and applies them to the input state⁷.

3. **Purification Protocol.** Depending on the simulation mode:

- **Static Protocol:** Fix a purification depth $d_{\text{static}} \in \{1, 2, \dots, d_{\text{max}}\}$ and a local-filter strength α_{static} . Then run exactly d_{static} rounds of “filter \rightarrow DEJMPS” on the two noisy pairs¹⁷ as described in Sec. 3.1 After d_{static} successful rounds, compute:

$$F_{\text{out}}^{\text{static}} = \langle \Phi^+ | \rho_{\text{out}} | \Phi^+ \rangle, \quad Y_{\text{out}}^{\text{static}} = \prod_{r=1}^{d_{\text{static}}} [P_{\text{filt}}(\alpha_{\text{static}})]^2 \times [P_{\text{succ}}^{(r)}]. \quad (20)$$

where $P_{\text{succ}}^{(r)}$ is the DEJMPS success probability in round r (Eq. (13)).

- **Adaptive Protocol:** First, query the lookup table (Section 3.3) using the estimated parameters $(\hat{\gamma}, \hat{p})$ to retrieve optimal (d^*, α^*) . Then run d^* rounds of “filter $F(\alpha^*) \rightarrow$ DEJMPS” exactly as above, but with $\alpha = \alpha^*$ at each round. Denote the final noisy-purified state by $\rho_{\text{out}}^{\text{adapt}}$ and its yield by $Y_{\text{out}}^{\text{adapt}}$. Finally compute:

$$F_{\text{out}}^{\text{adapt}} = \langle \Phi^+ | \rho_{\text{out}}^{\text{adapt}} | \Phi^+ \rangle. \quad (21)$$

4. **Record Metrics.** If purification (static or adaptive) succeeds all d rounds, append F_{out} to a fidelity list and Y_{out} to a yield list for this trial. If any round fails, record fidelity $F_{\text{out}} = 0$ and yield $Y_{\text{out}} = 0$.

After T trials, compute the average values:

$$\bar{F}_{\text{mode}}(\gamma, p) = \frac{1}{T} \sum_{t=1}^T F_{\text{out}}^{(t)}, \quad \bar{Y}_{\text{mode}}(\gamma, p) = \frac{1}{T} \sum_{t=1}^T Y_{\text{out}}^{(t)}, \quad (22)$$

where “mode” is either “static” or “adapt.” We further define the *net throughput* (pairs per second) as

$$T_{\text{mode}}(\gamma, p) = R_{\text{data}} \times \bar{Y}_{\text{mode}}(\gamma, p), \quad (23)$$

with R_{data} given in Eq. (12). In our simulations, we set $R_{\text{data}} = 100$ pairs/s.

4.2 Parameter Choices and Grid

We discretize the noise parameter space as:

$$\gamma_i = 0.01 i, \quad p_j = 0.01 j, \quad i, j \in \{1, 2, \dots, 20\}. \quad (24)$$

This 20×20 grid covers $\gamma, p \in [0.01, 0.20]$. For each (γ_i, p_j) , we perform $T = 500$ Monte Carlo trials to estimate (\bar{F}, \bar{Y}) in both static and adaptive modes. In the static sweep, we test depths $d_{\text{static}} \in \{1, 2, 3\}$ and filter strengths $\alpha_{\text{static}} \in \{0.1, 0.2, \dots, 0.9\}$; we then choose the *best static* combination that meets a fidelity target $F_{\text{target}} = 0.90$ while maximizing mean yield.

Our adaptive lookup table was precomputed over the same grid (Section 3.3), assuming $F_{\text{target}} = 0.90$, and stored offline. At runtime, we directly index into this table using the nearest grid indices (i, j) corresponding to the estimated $(\hat{\gamma}, \hat{p})$ (Eq. (11)).

4.3 Implementation Details

Our simulation emphasizes modularity and reuse, with the following key components:

- **Software Stack.** We use Python with QuTiP 4.6.0⁷ for quantum objects and Kraus operators, NumPy for numerics, and Matplotlib for plotting.
- **Noise and Purification Routines.** We implement the frameworks discussed in Sec. 3.1, 3 via the code in the repository shown in Sec. 8
- **Lookup Table Integration.** A precomputed NumPy array `lookup_table.npy` of shape $(20, 20, 2)$ stores (d^*, α^*) for grid points $(\gamma_i = 0.01i, p_j = 0.01j)$. At runtime, estimated $(\hat{\gamma}, \hat{p})$ are mapped to indices

$$i = \min(\lfloor 100 \hat{\gamma} \rfloor, 20), \quad j = \min(\lfloor 100 \hat{p} \rfloor, 20),$$
and $(d^*, \alpha^*) = \text{lookup_table}[i-1, j-1]$ is retrieved.
- **Parallel Monte Carlo.** To accelerate offline simulations, Monte Carlo trials for each (γ_i, p_j) are distributed across CPU cores using `multiprocessing.Pool`. On a 4-core machine, completing $20 \times 20 \times 3$ static configurations and adaptive runs with $T = 500$ trials each takes roughly 30 minutes.

- **Data Collection & Postprocessing.**

$$\begin{aligned} \Delta F(i, j) &= F_{\text{adapt}}(i, j) - \max_d [F_{\text{static_d}}(i, j)], \\ \Delta Y(i, j) &= Y_{\text{adapt}}(i, j) - \max_d [Y_{\text{static_d}}(i, j)], \end{aligned} \quad (25)$$

and generate the 2D/3D plots shown in Section 5.

4.4 Validation and Consistency Checks

We perform the following checks to ensure simulation correctness:

1. **Noise-Only Benchmark.** For each (γ, p) , we verify the fidelity of a single noisy Bell pair ρ_{AB} against $|\Phi^+\rangle$ matches the analytic expression:

$$F_{\text{noisy}}(\gamma, p) = \langle \Phi^+ | \rho_{AB} | \Phi^+ \rangle.$$

We compare Monte Carlo estimates (by generating many noisy pairs and measuring fidelity) against this closed-form result.

2. **Single-Round DEJMPS.** For a fixed input Werner state (fidelity F_0), we check that one DEJMPS round yields fidelity and yield consistent with Eqs. (15).

3. **Filter-Only Comparison.** Apply only $F(\alpha)$ to a Werner state and confirm that post-filter fidelity and yield match Eqs. (18) – (19)

4. **Reproducibility.** We fix random seeds in NumPy (`'np.random.seed(42)'`) and Qutip

$$('qt.settings.auto_tidyup = False')$$

to ensure identical results across runs.

Through these validation steps, we ensure that our simulation correctly captures the noisy channel, purification operations, and statistical sampling, providing confidence in the reported performance gains of the adaptive scheme compared to static baselines.

5 RESULTS AND ANALYSIS

All numerical results presented below were generated using $T = 500$ Monte Carlo trials per (γ, p) grid point.

5.1 Adaptive versus Static Performance

We focus here on the net gains (or losses) in fidelity and yield when switching from the best static purification protocol to the adaptive scheme. Across the 20×20 (γ, p) grid, only a small fraction of points exhibit a positive improvement. Specifically, out of 400 configurations, 17 (4.25%) show $\Delta F > 0$ or $\Delta Y > 0$, with an average positive $\Delta F \approx 0.83$ and $\Delta Y = 0.5$ at those points.

3D Surfaces of ΔF and ΔY .

Figure 2 shows the three-dimensional surface of the fidelity difference

$$\Delta F(\gamma, p) = \bar{F}_{\text{adapt}}(\gamma, p) - \bar{F}_{\text{static}}(\gamma, p)$$

where only points with $\Delta F > 0$ appear as upward spikes. Figure 3 depicts the yield difference

$$\Delta Y(\gamma, p) = \bar{Y}_{\text{adapt}}(\gamma, p) - \bar{Y}_{\text{static}}(\gamma, p)$$

highlighting the corresponding yield penalty.

2D Contour Maps of ΔF and ΔY .

To highlight isolated regions of adaptive benefit, Figure 4 shows a contour map of $\Delta F(\gamma, p)$, plotted only for nonzero values. Likewise, Figure 5 presents the contour of $\Delta Y(\gamma, p)$.

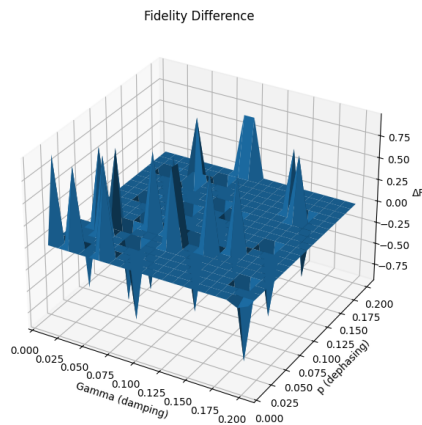


Figure 2: Three-dimensional surface of fidelity difference $\Delta F(\gamma, p)$.

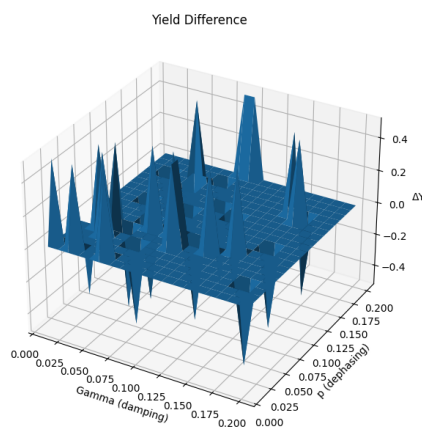


Figure 3: Three-dimensional surface of yield difference $\Delta Y(\gamma, p)$.

5.2 Key Observations

- Only 4.25% of grid points exhibit nonzero adaptive gains in fidelity or yield.
- Fidelity improvements are highly localized and coincide with halved yields ($\Delta Y = 0.5$). This demonstrates that in those areas, the static method fails while the adaptive is successful. Opposite results are true for the fidelity declines.
- No smooth trend: adaptive benefit appears in "islands" rather than smoothly with $\gamma + p$.
- The largest ΔF spikes (up to ≈ 0.96) arise where static yields vanish.

In conclusion, the updated lookup table yields meaningful adaptive gains only in select noise regimes. In this work, we've demonstrated the potential of an adaptive model yet, we've also seen the challenges that arise when trying to increase the fidelity of a system across the board.

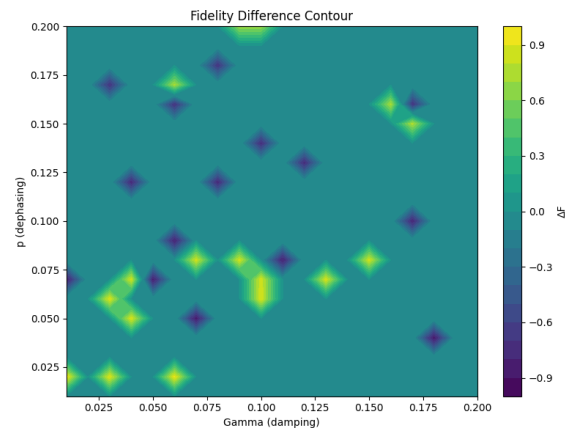


Figure 4: Contour map of fidelity difference $\Delta F(\gamma, p)$.

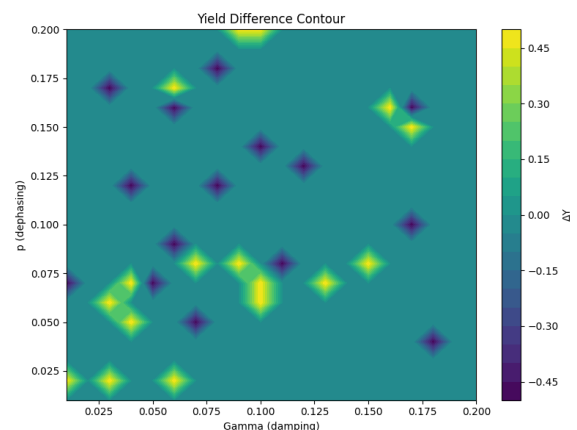


Figure 5: Contour map of yield difference $\Delta Y(\gamma, p)$.

6 DISCUSSION AND FUTURE WORK

Our results demonstrated the possibility of fidelity gains when an adaptive purification protocol is used instead of its static counterpart. Future work will focus on more robust methods to calculate probe pair volume (e.g. bayesian estimation) in order to reduce the significant overhead, optimizing the lookup table in order to mitigate any resulting loss and implementing more complex hybrid algorithms that mitigate noise more effectively across a wider range of noise models.

7 ACKNOWLEDGMENTS

Our thanks to ACM SIGCHI and SIGGRAPH for allowing us to modify and use templates they had developed.

8 DATA AND CODE AVAILABILITY

All the graphs, measurements and the simulation code can be found and reproduced at https://github.com/BillSkarlatos/Purification_Simulation, please read the corresponding README.md in the repository for execution details or message the first author.

REFERENCES

- [1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77(13): 2818–2821, 1996. doi: 10.1103/PhysRevLett.77.2818.
- [2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Physical Review Letters*, 76:722–725, 1996. doi: 10.1103/PhysRevLett.76.722.
- [3] Y. Gao, L. Cao, H. Qi, and X. Zhang. Machine–Learning–Aided Adaptive Entanglement Purification. *Nature Communications*, 9:1276, 2018. doi: 10.1038/s41467-018-03606-2.
- [4] A. W. Leung and P. W. Shor. Adaptive entanglement purification protocols with two–way classical communication. *Phys. Rev. A*, 75(4):042316, 2007. doi: 10.1103/PhysRevA.75.042316.
- [5] K. Azuma and H. Matsumoto. Long–Distance Quantum Communication Over Noisy Channels with Adaptive Purification. *Physical Review A*, 92:022303, 2015. doi: 10.1103/PhysRevA.92.022303.
- [6] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin. Quantum Repeater with Encoding. *Physical Review A*, 79:032325, 2009. doi: 10.1103/PhysRevA.79.032325.
- [7] J. R. Johansson, P. D. Nation, and F. Nori. Qutip: An open–source python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 183(8):1760–1772, 2012. doi: 10.1016/j.cpc.2012.02.021.
- [8] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. *Physical Review Letters*, 81:5932–5935, 1998. doi: 10.1103/PhysRevLett.81.5932.
- [9] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller. Quantum Repeaters Based on Entanglement Purification. *Physical Review A*, 59:169–181, 1999. doi: 10.1103/PhysRevA.59.169.
- [10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 10th anniversary edition, 2010.
- [11] K. Kraus. *States, Effects, and Operations: Fundamental Notions of Quantum Theory*. Springer, Berlin, Germany, 1983.
- [12] S. Bharathi, A. Sayeed, and F. N. C. Wong. Adaptive Channel Estimation and Compensation for Long–Distance Fiber Links. *Optics Express*, 22: 40–57, 2014. doi: 10.1364/OE.22.000040.
- [13] A. Stürck, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug-and-play system. *New Journal of Physics*, 4:41, 2009. doi: 10.1088/1367-2630/4/1/341.
- [14] P. van Loock and N. Lütkenhaus. Purification of Mixed Entanglement: Towards Practical Implementation. *Physical Review A*, 73:052323, 2006. doi: 10.1103/PhysRevA.73.052323.
- [15] B. Kraus, J. I. Cirac, and P. Horodecki. Entanglement Purification Protocol: New Directions. *Physical Review A*, 61:062302, 2000. doi: 10.1103/PhysRevA.61.062302.
- [16] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed–State Entanglement and Quantum Error Correction. *Physical Review A*, 54:3824–3851, 1996. doi: 10.1103/PhysRevA.54.3824.
- [17] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A*, 210(3-4):151–156, 1996. doi: 10.1016/0375-9601(96)00826-9.
- [18] J. M. Renes and J. C. Boileau. One–Way Quantum State Purification Protocols. *Physical Review A*, 73:032335, 2006. doi: 10.1103/PhysRevA.73.032335.

γ	p	ΔF	ΔY
0.010000	0.020000	0.957895	0.500000
0.010000	0.070000	-0.867466	-0.500000
0.030000	0.020000	0.890411	0.500000
0.030000	0.060000	0.885156	0.500000
0.030000	0.170000	-0.716600	-0.500000
0.040000	0.050000	0.875635	0.500000
0.040000	0.070000	0.850001	0.500000
0.040000	0.120000	-0.787299	-0.500000
0.050000	0.070000	-0.867963	-0.500000
0.060000	0.020000	0.924509	0.500000
0.070000	0.010000	-0.930617	-0.500000
0.070000	0.090000	-0.870846	-0.500000
0.080000	0.030000	0.900123	0.500000
0.090000	0.020000	-0.940329	-0.500000
0.100000	0.040000	-0.820734	-0.500000
0.100000	0.100000	0.890452	0.500000
0.110000	0.080000	-0.849676	-0.500000
0.120000	0.130000	-0.770536	-0.500000
0.130000	0.070000	0.865519	0.500000
0.150000	0.080000	0.847190	0.500000
0.160000	0.160000	0.725669	0.500000
0.170000	0.100000	-0.812899	-0.500000
0.170000	0.150000	0.738552	0.500000
0.170000	0.160000	-0.724872	-0.500000
0.180000	0.040000	-0.900662	-0.500000
0.190000	0.010000	-0.055414	0.000000

Table 1: Parameter combinations where $\Delta F \neq 0$.

Quantum-inspired classifiers

Roberto Leporini

University of Bergamo
via dei Caniana, 2

Italy, 24127 Bergamo, BG

roberto.leporini@unibg.it

Cesarino Bertini

University of Bergamo
via dei Caniana, 2

Italy, 24127 Bergamo, BG

cesarino.bertini@unibg.it

ABSTRACT

Quantum-inspired machine learning is a new branch of machine learning based on the application of the mathematical formalism of quantum mechanics to devise novel algorithms for classical computers. We implement some quantum-inspired classification algorithms, based on quantum state discrimination, within a local approach in the feature space by taking into account elements close to the element to be classified. This local approach improves the accuracy in classification and motivates the integration with the classifiers. The quantum-inspired classifiers require the encoding of the feature vectors into density operators and methods for estimating the distinguishability of quantum states like the Helstrom state discrimination and the Pretty-Good measurement. We present a comparison of the performances of the local quantum-inspired classifiers against well-known classical algorithms in order to show that the local approach can be a valuable tool for increasing the performances of this kind of classifiers.

Keywords

quantum-inspired classifiers; machine learning; local approach.

1 INTRODUCTION

Quantum-inspired machine learning represents a novel area within machine learning that leverages the mathematical framework of quantum mechanics to develop new algorithms for classical computers. In this work, we implement several quantum-inspired classification algorithms rooted in quantum state discrimination, employing a local strategy within the feature space. Specifically, we implement quantum-inspired algorithms based on Helstrom discrimination. The method involves classifying an unlabeled data instance by identifying its k nearest training elements before applying the algorithm to these k neighbors. This local approach enhances classification accuracy.

Quantum-inspired classifiers necessitate the encoding of feature vectors into density operators and methods for assessing the distinguishability of quantum states, such as Helstrom state discrimination and Pretty-Good Measurement (PGM). In the experimental section, we present a performance comparison between our local quantum-inspired classifiers and established classical algorithms. The aim is to demonstrate the potential of

the local approach as a valuable technique for improving the performance of these types of classifiers.

2 QUANTUM-INSPIRED CLASSIFICATION

The initial stage in quantum-inspired classification involves quantum encoding, which encompasses any method for mapping classical information into quantum states. Specifically, we consider encoding data vectors into density matrices within a Hilbert space \mathcal{H} whose dimensionality is determined by the input space's dimension. Density matrices are positive semidefinite operators ρ with a trace of 1 and they serve as the mathematical tools for describing the physical states of quantum systems.

Pure states are a subset of density matrices. These are rank-1 projectors that can be directly associated with unit vectors up to a phase factor. A density operator ρ on a d -dimensional Hilbert space \mathbb{C}^d can be expressed as:

$$\rho = \frac{1}{d} \left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}} \sum_{j=1}^{d^2-1} b_j^{(\rho)} \sigma_j \right), \quad (1)$$

where $\{\sigma_j\}_{j=1, \dots, d^2-1}$ are the standard generators of the special unitary group $SU(d)$, also known as generalized Pauli matrices, and \mathbb{I}_d is the $d \times d$ identity matrix. The vector $\mathbf{b}^{(\rho)} = (b_1^{(\rho)}, \dots, b_{d^2-1}^{(\rho)})$, with $b_j^{(\rho)} = \sqrt{\frac{d}{2(d-1)}} \text{tr}(\rho \sigma_j) \in \mathbb{R}$, is the Bloch vector associated to ρ which lies within the hypersphere of radius 1 in \mathbb{R}^{d^2-1} . For $d = 2$, the qubit case, the density matrices

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

are in bijective correspondence to the points of the unit ball in \mathbb{R}^3 , the so-called Bloch sphere, where the pure states are in one-to-one correspondence with the points of the spherical surface.

Complex vectors of dimension n can be encoded into density matrices of a $(n+1)$ -dimensional Hilbert space H in the following way:

$$\mathbb{C}^n \ni \mathbf{x} \mapsto |\mathbf{x}\rangle = \frac{1}{\sqrt{\|\mathbf{x}\|^2 + 1}} \left(\sum_{\alpha=0}^{n-1} x_{\alpha} |\alpha\rangle + |n\rangle \right) \in H, \quad (2)$$

where $\{|\alpha\rangle\}_{\alpha=0,\dots,n}$ is the computational basis of H , identified as the standard basis of \mathbb{C}^{n+1} . The map defined in (2), called *amplitude encoding*, encodes \mathbf{x} into the pure state $\rho_{\mathbf{x}} = |\mathbf{x}\rangle\langle\mathbf{x}|$ where the additional component of $|\mathbf{x}\rangle$ stores the norm of \mathbf{x} . Nevertheless the quantum encoding $\mathbf{x} \mapsto \rho_{\mathbf{x}}$ can be realized in terms of the Bloch vectors $\mathbf{x} \mapsto \mathbf{b}(\rho_{\mathbf{x}})$ saving space resources. The improvement of memory occupation within the Bloch representation is evident when we take multiple tensor products $\rho \otimes \dots \otimes \rho$ of a density matrix ρ constructing a feature map to enlarge the dimension of the representation space [1].

Quantum-inspired classification methods rely on three main steps: encoding data vectors into quantum density matrices, calculating centroids within this quantum representation, and applying various quantum state distinguishability criteria such as Helstrom discrimination, the Pretty-Good measurement [2], and the geometric minimum-error measurement [3] to differentiate between classes.

Let us briefly recall the notion of quantum state discrimination. Given a set of arbitrary quantum states with respective a priori probabilities $R = \{(\rho_1, p_1), \dots, (\rho_N, p_N)\}$, in general there is no a measurement process that discriminates the states without errors, i.e. a collection $E = \{E_i\}_{i=1,\dots,N}$ of positive semidefinite operators such that $\sum_{i=1}^N E_i = I$, satisfying the following property: $\text{tr}(E_i \rho_j) = 0$ when $i \neq j$ for all $i, j = 1, \dots, N$. The probability of a successful state discrimination of the states in R performing the measurement E is:

$$\mathbb{P}_E(R) = \sum_{i=1}^N p_i \text{tr}(E_i \rho_i). \quad (3)$$

A complete characterization of the optimal measurement E_{opt} that maximizes the probability (3) for $R = \{(\rho_1, p_1), (\rho_2, p_2)\}$ is due to Helstrom [4]. Let $\Lambda := p_1 \rho_1 - p_2 \rho_2$ be the *Helstrom observable* whose positive and negative eigenvalues are, respectively, collected in the sets D_+ and D_- . Consider the two orthogonal projectors:

$$P_{\pm} := \sum_{\lambda \in D_{\pm}} P_{\lambda}, \quad (4)$$

where P_{λ} projects onto the eigenspace of λ . The measurement $E_{opt} := \{P_+, P_-\}$ maximizes the probability (3) that attains the *Helstrom bound*:

$$h_b(\rho_1, \rho_2) = p_1 \text{tr}(P_+ \rho_1) + p_2 \text{tr}(P_- \rho_2). \quad (5)$$

Helstrom quantum state discrimination can be used to implement a quantum-inspired binary classifier with promising performances. Let $\{(\mathbf{x}_1, y_1), \dots, (\mathbf{x}_M, y_M)\}$ be a training set with $\mathbf{x}_i \in \mathbb{C}^n$, $y_i \in \{1, 2\} \forall i = 1, \dots, M$. Assume to encode the data points into quantum states by means of $\mathbb{C}^n \ni \mathbf{x} \mapsto \rho_{\mathbf{x}} \in \mathfrak{S}(H)$, one can construct the quantum centroids ρ_1 and ρ_2 of the two classes $C_{1,2} = \{\mathbf{x}_i : y_i = 1, 2\}$:

$$\rho_{1,2} = \frac{1}{|C_{1,2}|} \sum_{\mathbf{x} \in C_{1,2}} \rho_{\mathbf{x}} \quad (6)$$

Let $\{P_+, P_-\}$ be the Helstrom measurement defined by the set $R = \{(\rho_1, p_1), (\rho_2, p_2)\}$, where the probabilities attached to the centroids are $p_{1,2} = \frac{|C_{1,2}|}{|C_1| + |C_2|}$. The *Helstrom classifier* applies the optimal measurement for the discrimination of the two quantum centroids to assign the label y to a new data instance \mathbf{x} , encoded into the state $\rho_{\mathbf{x}}$, as follows:

$$y(\mathbf{x}) = \begin{cases} 1 & \text{if } \text{tr}(P_+ \rho_{\mathbf{x}}) \geq \text{tr}(P_- \rho_{\mathbf{x}}) \\ 2 & \text{otherwise} \end{cases} \quad (7)$$

A strategy to increase the accuracy in classification is given by the construction of the tensor product of q copies of the quantum centroids $\rho_{1,2}^{\otimes q}$ enlarging the Hilbert space where data are encoded. The corresponding Helstrom measurement is $\{P_+^{\otimes q}, P_-^{\otimes q}\}$, and the Helstrom bound satisfies:

$$h_b(\rho_1^{\otimes q}, \rho_2^{\otimes q}) \leq h_b(\rho_1^{\otimes(q+1)}, \rho_2^{\otimes(q+1)}) \quad \forall q \in \mathbb{N}. \quad (8)$$

A larger Hilbert space in quantum encoding yields a better Helstrom bound and consequently a more accurate classifier, though it typically increases computational cost. Notably, when dealing with real input vectors, encoding them into Bloch vectors provides a method to effectively increase the Hilbert space dimension while potentially reducing time and space complexity.

Clearly, defining a quantum encoding is equivalent to select a feature map to represent feature vectors into a space of higher dimension. In the case of the considered quantum amplitude encoding $\mathbb{R}^2 \ni (x_1, x_2) \mapsto \rho_{(x_1, x_2)} \in \mathfrak{S}(\mathbb{C}^3)$, the nonlinear explicit injective function $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^5$ to encode data into Bloch vectors can be defined as follows:

$$\varphi(x_1, x_2) := \frac{1}{x_1^2 + x_2^2 + 1} \left(2x_1 x_2, 2x_1, 2x_2, x_1^2 - x_2^2, \frac{x_1^2 + x_2^2 - 2}{\sqrt{3}} \right). \quad (9)$$

From a geometric point of view, the mapped feature vectors are points on the surface of a hyper-hemisphere. Class centroids, obtained by averaging feature vectors, lie within the hypersphere and, while not directly corresponding to density operators, can be rescaled to Bloch vectors. To boost classification accuracy, the dimension of the representation space can be increased by using q copies of quantum states in a tensor product, encoding data and centroids as $\rho^{\otimes q}$. Bloch encoding provides an efficient way to handle feature maps by offering an injective data encoding function that discards null and repeated elements from the Bloch vector. This drastically reduces storage requirements. Therefore, the Bloch representation allows for compact storage of the redundant information within $\rho^{\otimes q}$.

Let us consider a training set divided into the classes C_1, \dots, C_M , assume we have any training point \mathbf{x} encoded into the Bloch vector $\mathbf{b}^{(\mathbf{x})}$ of a pure state on \mathbb{C}^d . The calculation of the centroid of the class C_i , within this quantum encoding, must take into account that the mean of the Bloch vectors $\mathbf{b}^{(i)} := \frac{1}{|C_i|} \sum_{\mathbf{x} \in C_i} \mathbf{b}^{(\mathbf{x})}$ does not represent a density operator in general. In fact, for $d > 2$ the points contained in the unit hypersphere of \mathbb{R}^{d^2-1} are not in bijective correspondence with density matrices on \mathbb{C}^d . However, since any vector within the closed ball of radius $\frac{2}{d}$ gives rise to a density operator, a centroid can be defined in terms of a meaningful Bloch vector by a rescaling:

$$\hat{\mathbf{b}}^{(i)} := \frac{2}{d|C_i|} \sum_{\mathbf{x} \in C_i} \mathbf{b}^{(\mathbf{x})}. \quad (10)$$

A method of quantum state discrimination for distinguishing more than two states $\{(\rho_1, p_1), \dots, (\rho_N, p_N)\}$ is the square-root measurement, also known as *Pretty-Good measurement*, defined by:

$$E_i = p_i \rho^{-\frac{1}{2}} p_i \rho^{-\frac{1}{2}}, \quad (11)$$

where $\rho = \sum_i p_i \rho_i$, PGM is the optimal minimum-error when states satisfy certain symmetry properties [2]. Clearly to distinguish between n centroids we need a measurement with at most n outcomes. It is sometimes optimal to avoid measurement and simply guess that the state is the a priori most likely state.

The optimal POVM $\{E_i\}_i$ for minimum-error state discrimination over

$$R = \{(\rho_1, p_1), \dots, (\rho_N, p_N)\}$$

satisfies the following necessary and sufficient Helstrom conditions [3]:

$$\Gamma - p_i \rho_i \geq 0 \quad \forall i = 1, \dots, N, \quad (12)$$

where the Hermitian operator, also known as *Lagrange operator*, is defined by $\Gamma := \sum_i p_i \rho_i E_i$. It is also use-

ful to consider the following properties which can be obtained from the above conditions:

$$E_j(p_j \rho_j - p_i \rho_i) E_i = 0 \quad \forall i, j. \quad (13)$$

For each i the operator $\Gamma - p_i \rho_i$ can have two, one, or no zero eigenvalues, corresponding to the zero operator, a rank-one operator, and a positive-definite operator, respectively. In the first case, we use the measurement $\{E_i = \mathbb{I}, E_{i \neq j} = 0\}$ for some i where $p_i \geq p_j \forall j$, i.e. the state belongs to the a priori most likely class. In the second case, if $E_i \neq 0$, it is a weighted projector onto the corresponding eigenstate. In the latter case, it follows that $E_i = 0$ for every optimal measurement.

Given the following Bloch representations:

$$\Gamma = \frac{1}{d} \left(a \mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}} \sum_{j=1}^{d^2-1} b_j \sigma_j \right) \quad (14)$$

$$\rho_i = \frac{1}{d} \left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}} \sum_{j=1}^{d^2-1} b_j^{(i)} \sigma_j \right), \quad (15)$$

in order to determine the Lagrange operator in \mathbb{C}^d we need d^2 independent linear constraints:

$$2p_i \left(a - \hat{\mathbf{b}}^{(i)} \cdot \mathbf{b} - \frac{p_i}{2} (1 - |\hat{\mathbf{b}}^{(i)}|^2) \right) = a^2 - |\mathbf{b}|^2. \quad (16)$$

A measurement with more than d^2 outcomes can always be decomposed as a probabilistic mixture of measurements with at most d^2 outcomes. Therefore, if the number of classes is greater than or equal to d^2 and we get d^2 linearly independent equations, we construct the Lagrange operator and derive the optimal measurements. From the geometric point of view, we obtain the unit vectors corresponding to the rank-1 projectors $E_i = \frac{1}{d} \left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}} \sum_{j=1}^{d^2-1} n_j^{(i)} \sigma_j \right)$ where $\mathbf{n}^{(i)} = \frac{\hat{\mathbf{b}}^{(i)} - a\mathbf{b}}{|\hat{\mathbf{b}}^{(i)} - a\mathbf{b}|} \in \mathbb{R}^{d^2-1}$ giving the POVM of the measurement. It is also possible to further partition the classes in order to increase the number of centroids and of the corresponding equations. The classification is carried out in this way: an unlabeled point $\hat{\mathbf{x}}$ is associated with the first label y such that $\mathbf{b}^{(\hat{\mathbf{x}})} \cdot \mathbf{n}^{(y)} = \max_i \mathbf{b}^{(\hat{\mathbf{x}})} \cdot \mathbf{n}^{(i)}$.

3 LOCAL QUANTUM-INSPIRED CLASSIFIERS

Our implementation of the quantum state discrimination classifiers begins by employing a k-nearest neighbors (kNN) approach to select the k closest training samples to the unclassified data point. The kNN algorithm itself is a simple classifier that operates through these steps:

1. calculating the distance between the test sample and all training samples using a chosen metric;

2. identifying the k training samples with the smallest distances;
3. assigning the class label based on the majority class among these k neighbors.

We proceed by first using kNN to extract the closest elements to a test instance, followed by a quantum-inspired classification instead of majority voting. We investigate two scenarios: either applying kNN in the original input space (e.g., via Euclidean distance) and then encoding the k neighbors for quantum classification, or encoding the entire dataset into density matrices and then using kNN with a quantum operator distance to find the k neighbors. In this latter case, the distance metric we employ is the *Bures distance*, a quantum generalization of the Fisher information and a distance linked to super-fidelity. The Bures distance is defined by:

$$d_B(\rho_1, \rho_2) = \sqrt{2 \left(1 - \sqrt{\mathcal{F}(\rho_1, \rho_2)} \right)}, \quad (17)$$

where the fidelity between density operators is given by $\mathcal{F}(\rho_1, \rho_2) = (\text{tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}})^2$. Let us note that the fidelity reduces to $\mathcal{F}(\rho_1, \rho_2) = \langle \psi_1 | \rho_2 | \psi_1 \rangle$ when $\rho_1 = |\psi_1\rangle \langle \psi_1|$. Therefore the Bures distance between the pure state ρ_1 and the arbitrary state ρ_2 can be expressed in term of the Bloch representation as follows:

$$d_B(\rho_1, \rho_2) = \sqrt{2 \left(1 - \sqrt{\frac{1}{d} \left(1 + (d-1) \mathbf{b}^{(1)} \cdot \mathbf{b}^{(2)} \right)} \right)} \quad (18)$$

where $\mathbf{b}^{(1)}$ and $\mathbf{b}^{(2)}$ are the Bloch vectors of ρ_1 and ρ_2 respectively and d is the dimension of the Hilbert space of the quantum encoding. The special form of the Bures distance, expressed in terms of Bloch vectors as in (18), is relevant for our purpose because data vectors are encoded into pure states and the quantum centroids are calculated as Bloch vectors of mixed states in general.

An alternative distance can be defined via super-fidelity

$$d_G(\rho_1, \rho_2) = \sqrt{1 - \mathcal{G}(\rho_1, \rho_2)}, \quad (19)$$

where the super-fidelity between density operators is given by

$$\mathcal{G}(\rho_1, \rho_2) = \text{tr} \rho_1 \rho_2 + \sqrt{(1 - \text{tr} \rho_1^2)(1 - \text{tr} \rho_2^2)}.$$

Notice that the super-fidelity reduces to $\mathcal{G}(\rho_1, \rho_2) = \langle \psi_1 | \rho_2 | \psi_1 \rangle$ when $\rho_1 = |\psi_1\rangle \langle \psi_1|$. The inner distance between the corresponding Bloch vectors represents the angle θ between the unit vectors $(\mathbf{b}^{(1)}, \sqrt{1 - |\mathbf{b}^{(1)}|^2})$ and $(\mathbf{b}^{(2)}, \sqrt{1 - |\mathbf{b}^{(2)}|^2})$, which is normalized to be 1: $\hat{D}_G(\mathbf{b}^{(1)}, \mathbf{b}^{(2)}) =$

$\frac{\arccos \left(\mathbf{b}^{(1)} \cdot \mathbf{b}^{(2)} + \sqrt{(1 - |\mathbf{b}^{(1)}|^2)(1 - |\mathbf{b}^{(2)}|^2)} \right)}{\pi}$. For pure states the inner distance corresponds to the Fubini-Study distance.

In Algorithm 1, the locality is imposed by running the kNN on the input space finding the training vectors that are closest to the test element, then there is the quantum encoding into pure states and a quantum-inspired classifier (Helstrom, PGM, geometric Helstrom) is locally executed over the restricted training set. In Algorithm 2, the test element and all the training elements are encoded into Bloch vectors of pure states then a kNN is run w.r.t. the Bures distance to find the nearest neighbors in the space of the quantum representation, then a quantum-inspired classifier is executed with the training instances corresponding to the closest quantum states.

Algorithm 1 *Local quantum-inspired classification based on kNN in the input space before the quantum encoding. The distance can be: Euclidean, Manhattan, Chessboard, Canberra, Bray-Curtis.*

Require: Dataset X of labeled instances, unlabeled point $\hat{\mathbf{x}}$
Ensure: Label of $\hat{\mathbf{x}}$
 find the k nearest neighbors $\mathbf{x}_1, \dots, \mathbf{x}_k$ to $\hat{\mathbf{x}}$ in X w.r.t. the Euclidean distance
 encode $\hat{\mathbf{x}}$ into a pure state $\rho_{\hat{\mathbf{x}}}$
for $j = 1, \dots, k$ **do**
 encode \mathbf{x}_j into a pure state $\rho_{\mathbf{x}_j}$
end for
 run the quantum-inspired classifier with training points encoded into $\{\rho_{\mathbf{x}_j}\}_{j=1, \dots, k}$.

Algorithm 2 *Local quantum-inspired classification based on kNN in the Bloch representation after the quantum encoding. The distance can be: Bures, Super-Fidelity, Inner.*

Require: Dataset X of labeled instances, unlabeled point $\hat{\mathbf{x}}$
Ensure: Label of $\hat{\mathbf{x}}$
 encode $\hat{\mathbf{x}}$ into a Bloch vector $\mathbf{b}^{(\hat{\mathbf{x}})}$ of a pure state
for $\mathbf{x} \in X$ **do**
 encode \mathbf{x} into a Bloch vector $\mathbf{b}^{(\mathbf{x})}$ of a pure state
end for
 find the k nearest neighbors to $\mathbf{b}^{(\hat{\mathbf{x}})}$ in $\{\mathbf{b}^{(\mathbf{x})}\}_{\mathbf{x} \in X}$ w.r.t. the distance D_B
 run the quantum-inspired classifier over the k nearest neighbors.

A local quantum-inspired classifier can be defined without quantum state discrimination but considering a *nearest mean classification* like the following: after the quantum encoding we perform a kNN selection and calculate the centroid of each class considering only the nearest neighbors to the test element, finally we assign the label according to the nearest centroid as schematized in Algorithm 3.

Algorithm 3 *Local quantum-inspired nearest mean classifier.*

Require: Training set X divided into n classes C_i , unlabeled point $\hat{\mathbf{x}}$
Ensure: Label of $\hat{\mathbf{x}}$
 encode $\hat{\mathbf{x}}$ into a Bloch vector $\mathbf{b}(\hat{\mathbf{x}})$ of a pure state
 for $\mathbf{x} \in X$ **do**
 encode \mathbf{x} into a Bloch vector $\mathbf{b}(\mathbf{x})$ of a pure state
 end for
 find the neighborhood $K = \{\mathbf{b}(\mathbf{x}_1), \dots, \mathbf{b}(\mathbf{x}_k)\}$ of $\mathbf{b}(\hat{\mathbf{x}})$ w.r.t. the distance D_B
 for $i = 1, \dots, n$ **do**
 construct the centroid $\hat{\mathbf{b}}^{(i)} = \frac{2}{d|C_i^k|} \sum_{\mathbf{x} \in C_i^k} \mathbf{b}(\mathbf{x})$ where $C_i^k := \{\mathbf{x} \in C_i : \mathbf{b}(\mathbf{x}) \in K\}$
 end for
 find the closest centroid $\hat{\mathbf{b}}^{(l)}$ to $\frac{2}{d} \mathbf{b}(\hat{\mathbf{x}})$ w.r.t. the distance D_B
 return label of the class C_l

4 RESULTS AND DISCUSSION

In this section, we describe some results obtained by the implementation of the local quantum-inspired classifiers with several distances compared to well-known classical algorithms. In particular, we consider the SVM with different kernels: linear, radial basis function, and sigmoid. Then, we run a random forest, a naive Bayes classifier, and the logistic regression. In order to compare the results with previous papers, we take into account the following benchmark datasets from PMLB public repository [5]. For each dataset we randomly select 80% of the data to create a training set and use the residual 20% for the evaluation. We repeated the same procedure 10 times and calculated the average accuracy using the code available at github.com/leporini/classification. Certainly, it is possible to compare the performances based on different statistic indices including Matthews correlation coefficient, F-measure, Cohen's parameter.

We observe that the performances of the local quantum-inspired classifiers turn out to be definitely more accurate, where the hyperparameter k is set equal to the number of classes in the dataset. This value is reasonable to construct the centroids of the classes. In particular, Algorithm 1 with the Euclidean distance is the most accurate classifier for the datasets *analcatadata_boxing1*, *analcatadata_happiness*, *biomed*, *prnn_fglass*, *wine_recognition*, while with Manhattan distance is best for *analcatadata_aids*, *analcatadata_japansolvent*, *breast_cancer*, *iris*, *tae*, with Chessboard distance is best for *analcatadata_cyyoung9302*, *analcatadata_lawsuit*, and with Bray-Curtis distance is best for *analcatadata_bankruptcy*, *appendicitis*. Algorithm 2 with the Bures distance outperforms Algorithm 1 and 3 for *analcatadata_dmft* and produces the same accuracy for *labor*. Algorithm 3

with the Bures distance is the most accurate classifier for *analcatadata_asbestos*, *new_thyroid*, *phoneme*, *prnn_synth*.

5 CONCLUSIONS

This paper centers on the practical implementation of classification algorithms that rely on quantum state discrimination. A key innovation is the introduction of a local approach for executing the classifier. Specifically, after partitioning the training set, the k nearest data points to the test element are encoded into Bloch vectors and subsequently used to determine the quantum centroid for each class.

The proposed methodology introduces a family of classifiers due to the flexibility in choosing both the strategy for defining locality within the training set and the quantum state discrimination procedure. Both the local classification approach and the quantum-inspired data encoding and processing warrant further exploration to fully understand their impact on machine learning.

In a forthcoming article, we will provide a formal complexity analysis of the algorithms with respect to dataset size, number of features, and Hilbert space dimensionality. We will also compare performance against more advanced classical methods, such as deep neural networks, to better position the benefits of quantum-inspired approaches. Furthermore, we will present a thorough error analysis and sensitivity study. This will specifically focus on how the hyperparameter k in our local strategy influences the results.

6 REFERENCES

- [1] Leporini, R.; Pastorello, D. An efficient geometric approach to quantum-inspired classifications. *Sci. Rep.* **2022**, *12*, 8781. <https://doi.org/10.1038/s41598-022-12392-1>.
- [2] Mochon, C. Family of generalized pretty good measurements and the minimal-error pure-state discrimination problems for which they are optimal. *Phys. Rev. A* **2006**, *73*, 032328. <https://doi.org/10.1103/PhysRevA.73.032328>.
- [3] Bae, J. Structure of minimum-error quantum state discrimination. *New J. Phys.* **2013**, *15*, 073037. <https://doi.org/10.1088/1367-2630/15/7/073037>.
- [4] Helstrom, C.W. Quantum detection and estimation theory. *J. Stat. Phys.* **1969**, *1*, 231–252.
- [5] Romano, J.D.; Le, T.T.; La Cava, W.; Gregg, J.T.; Goldberg, D.J.; Chakraborty, P.; Ray, N.L.; Himmelstein, D.; Fu, W.; Moore, J.H., PMLB v1.0: an open source dataset collection for benchmarking machine learning methods, *arXiv* **2020**, arXiv:2012.00058.

Variational Quantum Eigen-Decomposition Preconditioning Method for Solving Computational Mechanics Problems

Eunsik Choi

Georgia Institute of
Technology
813 Ferst Drive NW
Atlanta, GA 30332-0560
echoi312@gatech.edu

Jungin E. Kim

Georgia Institute of
Technology
813 Ferst Drive NW
Atlanta, GA 30332-0560
jkim3252@gatech.edu

Yan Wang

Georgia Institute of
Technology
813 Ferst Drive NW
Atlanta, GA 30332-0560
yan-wang@gatech.edu

ABSTRACT

Recently, quantum computing emerged as a paradigm for solving systems of linear equations. However, large condition numbers significantly increase the computational complexity of quantum linear equation solvers. In this work, a new quantum preconditioning approach called variational quantum eigen-decomposition (VQED) is proposed, where the preconditioner is defined as a weighted projector onto the subspace spanned by the eigenvectors of a matrix. A variational quantum algorithm with projection-based deflation is performed to calculate eigenvalue-eigenvector pairs for constructing the preconditioner. The proposed VQED method is used with quantum singular value transformation to solve linear systems for mechanics examples. It is demonstrated that the VQED can reduce the condition numbers to as low as 1.03, which is a significant improvement over the original condition number.

Keywords

Quantum linear system algorithm, Preconditioning, Variational quantum algorithm, Quantum singular value transformation, Quantum scientific computing.

1 INTRODUCTION

Most differential equations in computational mechanics problems can be numerically linearized and solved as systems of linear equations. Given a coefficient matrix A and a vector \mathbf{b} , the goal is to obtain the solution vector \mathbf{x} such that $A\mathbf{x} = \mathbf{b}$. However, solving very large linear systems is still computationally expensive when high-fidelity solutions for complex systems are desirable.

Recently, quantum computing emerged as an alternative paradigm for scientific computing, where qubits encode information and quantum phenomena of superposition and entanglement are utilized for computation. Particularly, several quantum linear system algorithms have been proposed. The first algorithm is the Harrow-Hassidim-Lloyd (HHL) algorithm [Har09], where the quantum linear systems problem is formulated as the eigenvalue problem, and the inverse quantum Fourier transform is utilized for phase estimation to obtain the eigenvalues. In the variational quantum linear solver [Bra23], a variational quantum circuit is constructed to minimize the residue. Classical optimization is used to find the optimal parameters. The third approach is utilizing quantum singular value transformation (QSVT) [Gil19, Mar21] to obtain the inverse of the coefficient matrix, which is approximated with the Chebyshev expansion. Although the computational advantages of quantum linear solvers over classical counterparts were shown, the accuracy and efficiency of these quantum methods are sensitively dependent on

the condition number of the matrix. Large condition numbers significantly increase the computational complexity of these algorithms, which is quadratically dependent on the condition number (e.g., $\mathcal{O}(\kappa^2/\epsilon)$ for HHL algorithm with condition number κ and target level of error ϵ). Therefore, reducing the condition number is necessary to improve the accuracy of the solution given the available computer resources.

Preconditioning is an effective numerical approach to reduce the condition numbers of matrices and improve the numerical accuracy in classical linear equation solvers. In this process, a preconditioner matrix M transforms the original linear system into $MA\mathbf{x} = M\mathbf{b}$. M is chosen so that the condition number of MA is much smaller than the condition number of A . Different preconditioning methods have been developed for numerical solvers on classical computers. However, very limited work has been done for quantum preconditioning, which is to obtain M with quantum algorithms. One approach is to implement the classical sparse approximate inverse method on a quantum computer [Cla13]. In this method, a preconditioner approximates the inverse of the coefficient matrix as $M \approx A^{-1}$. Each row of the preconditioner is obtained by solving a linear system with the vector on the right-hand side formed with an identity element. However, the preconditioning in [Cla13] relies on a quantum oracle without providing the details of implementation. Another approach is the quantum circulant preconditioner [Sha18]. The

inverse of Toeplitz matrix is proved to be the optimal circulant preconditioner that makes the preconditioned coefficient matrix close to the identity matrix. The circulant preconditioner is easily implemented using quantum Fourier transform. A third method is the fast inverse method [Ton21], where the original matrix is decomposed into a sum of fast-invertible and perturbation matrices. The preconditioner is the inverse of the fast-invertible matrix, which is block-encoded in the QSVT circuit to solve the linear system. The norm of the fast-invertible matrix is much larger than the norm of the perturbation matrix so that the preconditioner is approximately equal to the identity. However, the method is not generalizable since the fast-invertible matrix is assumed to be non-singular, Hermitian, and unitarily diagonalizable.

In this work, a new quantum preconditioning approach, variational quantum eigen-decomposition (VQED), is proposed. The preconditioner is defined as a weighted projector onto the subspace spanned by the eigenvectors of the coefficient matrix. The eigenvectors are constructed recursively. A trial state is projected onto the subspace spanned by the previously calculated eigenvectors to determine a new orthogonal eigenvector. The proposed preconditioning approach can be integrated with different quantum linear equation solvers. Here, QSVT is used to demonstrate its capability.

In the remainder of the paper, the proposed VQED preconditioning method is described in Section 2. Experimental settings and evaluation criteria are introduced in Section 3. The method is demonstrated with two mechanics examples in Section 4. The results are summarized and future extensions are discussed in Section 5.

2 PROPOSED VARIATIONAL QUANTUM EIGEN-DECOMPOSITION PRECONDITIONER

Let $A \in \mathbb{C}^{n \times n}$ be a positive semi-definite Hermitian matrix representing a physical or engineering system, such as a stiffness matrix in structural mechanics. A can be decomposed as

$$A = \sum_{i=1}^r \lambda_i |u_i\rangle \langle u_i|, \quad (1)$$

where λ_i 's are non-negative eigenvalues and $|u_i\rangle$'s are orthonormal eigenvectors.

Eigen-decomposition

Preconditioning is achieved by constructing a preconditioner M such that $MA \approx I$. MA is subsequently used in quantum linear solvers to improve the accuracy of the solutions.

In VQED, the preconditioner is iteratively calculated in a subspace spanned by the eigenvectors of A . When A is

singular, a lower-rank approximation of M is obtained as

$$M_k = \sum_{i=1}^k \frac{1}{\lambda_i} |u_i\rangle \langle u_i|, \quad (2)$$

where $k < r$. Then, we define

$$M_k A \approx \sum_{i=1}^k |u_i\rangle \langle u_i| \quad (3)$$

as a projector onto the span of eigenvectors with the k smallest eigenvalues. The condition number of Eq. (3) could be reduced when higher-order eigenvectors are iteratively added to expand the subspace of M_k . When A is non-singular, $M_k A$ cannot be approximated as the identity. Instead, it is necessary to construct the complete eigenspace as

$$M = \sum_{i=1}^r \frac{1}{\lambda_i} |u_i\rangle \langle u_i| \quad (4)$$

so that $M = A^{-1}$.

Variational Eigenvector Computation

In the VQED method, a variational quantum algorithm [Per14] is used to iteratively extract eigenvectors of A with the k smallest eigenvalues in increasing order, similar to the deflation technique [Hig19].

The variational circuit is constructed based on the Pauli basis. A parameterized hardware efficient ansatz [Kan17] is used to prepare a quantum state $|\psi(\theta)\rangle$ from the initial state $|0\rangle^{\otimes n}$, where n is the number of qubits to encode A . The objective is to find a vector of parameters θ^* so that the parameterized quantum state $|\hat{u}(\theta^*)\rangle$ is equivalent to an eigenvector $|u_k\rangle$. To calculate each $|u_k\rangle$, θ is optimized so that $|\hat{u}(\theta)\rangle$ is orthogonal to the previously obtained eigenvectors. For $|\hat{u}(\theta)\rangle$, θ is omitted to $|\hat{u}\rangle$ in the following when it is clear in the context.

The variational quantum algorithm is first applied to obtain

$$\theta^* = \arg \min_{\theta} \text{Re} [\langle \psi(\theta) | A | \psi(\theta) \rangle] \quad (5)$$

such that $|\psi(\theta^*)\rangle = |\hat{u}_1\rangle$ and $\hat{\lambda}_1 = \langle \hat{u}_1 | A | \hat{u}_1 \rangle$.

Recursively, a projection-based deflation is applied to ensure that the parameterized states are orthogonal to each other. Given the previously computed eigenvectors $\{|\hat{u}_1\rangle, \dots, |\hat{u}_{k-1}\rangle\}$, the non-normalized vector \tilde{u}_k is calculated as

$$\tilde{u}_k(\theta) = |\psi(\theta)\rangle - \sum_{i=1}^{k-1} |\hat{u}_i\rangle \langle \hat{u}_i | \psi(\theta) \rangle, \quad (6)$$

which is then normalized to

$$|\hat{u}_k(\theta)\rangle = \frac{\tilde{u}_k(\theta)}{|\tilde{u}_k(\theta)|}. \quad (7)$$

The corresponding eigenvalue is then calculated as

$$\hat{\lambda}_k(\boldsymbol{\theta}) = \text{Re}[\langle \hat{u}_k(\boldsymbol{\theta}) | A | \hat{u}_k(\boldsymbol{\theta}) \rangle]. \quad (8)$$

The minimum value of Eq. (8) is $\hat{\lambda}_k = \lambda$ when $|\hat{u}_k\rangle = |u_k\rangle$.

After calculating all k eigenvalues and eigenvectors, a spectral preconditioner defined in Eq. (2) is constructed. This matrix, which approximates A^{-1} , is spanned by the computed eigenvectors.

Quantum Singular Value Transformation

The preconditioner M_k can be used in different quantum linear solvers. Here, we use QSVT to demonstrate. QSVT consists of an alternating sequence of block-encoding and projector-controlled phase-shift operations [Mar21]. Suppose that $M_k A$ is decomposed as

$$M_k A = \sum_{i=1}^r \sigma_i |w_i\rangle \langle v_i|, \quad (9)$$

where σ_i is the non-negative real singular value of $M_k A$, $|w_k\rangle$ is the left singular vector, and $|v_k\rangle$ is the right singular vector. Given a block-encoding of $M_k A$ in a unitary matrix U , the location of the block-encoded matrix can be determined as $M_k A = \Pi_w U \Pi_v$ by the projectors

$$\Pi_w := \sum_{i=1}^r |w_i\rangle \langle w_i|, \quad (10)$$

and

$$\Pi_v := \sum_{i=1}^r |v_i\rangle \langle v_i|, \quad (11)$$

which are spanned by its singular vectors. In the projector-controlled phase-shift operations $\Pi_w(\boldsymbol{\phi})$ and $\Pi_v(\boldsymbol{\phi})$, each projection $|w_i\rangle \langle w_i|$ in Eq. (10) or $|v_i\rangle \langle v_i|$ in Eq. (11) controls a z -rotation applied on an ancilla qubit.

The QSVT sequence depends on the parity of the matrix polynomial. If the parity is odd, then the sequence is defined as

$$U_o(\boldsymbol{\phi}) = \Pi_w(\boldsymbol{\phi}_1) U \left[\prod_{j=1}^{(d-1)/2} \Pi_v(\boldsymbol{\phi}_{2j}) U^\dagger \Pi_w(\boldsymbol{\phi}_{2j+1}) U \right] \\ = \begin{bmatrix} \mathcal{P}_o(M_k A) & & \\ & \ddots & \\ & & \end{bmatrix}, \quad (12)$$

where

$$\mathcal{P}_o(M_k A) := \sum_{i=1}^r \mathcal{P}_o(\sigma_i) |w_i\rangle \langle v_i| \quad (13)$$

is an odd polynomial. Otherwise, if the parity is even, then the sequence is defined as

$$U_e(\boldsymbol{\phi}) = \left[\prod_{j=1}^{d/2} \Pi_v(\boldsymbol{\phi}_{2j-1}) U^\dagger \Pi_w(\boldsymbol{\phi}_{2j}) U \right] \\ = \begin{bmatrix} \mathcal{P}_e(M_k A) & & \\ & \ddots & \\ & & \end{bmatrix}, \quad (14)$$

where

$$\mathcal{P}_e(M_k A) := \sum_{i=1}^r \mathcal{P}_e(\sigma_i) |v_i\rangle \langle v_i| \quad (15)$$

is an even polynomial.

In linear systems problems, the inverse of $M_k A$ with non-zero singular values is defined as

$$(M_k A)^{-1} = \sum_{i=1}^r \frac{1}{\sigma_i} |v_i\rangle \langle w_i|. \quad (16)$$

QSVT method can be utilized to find a polynomial $\mathcal{P}_o(\sigma_i) \approx 1/\sigma_i$ such that

$$(M_k A)^{-1} \approx \sum_{i=1}^r \mathcal{P}_o(\sigma_i) |v_i\rangle \langle w_i|. \quad (17)$$

3 EXPERIMENTS

The quantum preconditioning method is demonstrated with two examples of solid mechanics. The first example is a truss structure, whereas the second example involves a Messerschmitt-Bölkow-Blohm (MBB) beam.

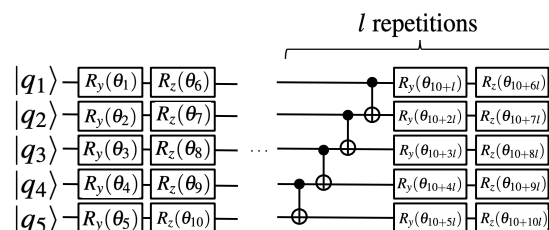


Figure 1: Hardware efficient SU2 ansatz used to compute eigenvalues and eigenvectors of A for VQED.

The proposed preconditioner was tested on systems of 32 linear equations derived from the partial differential equations. Eigenstates were prepared using hardware efficient SU2 circuit in Figure 1 with l repeated layers. With this circuit, M was constructed by preparing 32 eigenvalue-eigenvector pairs. The optimization is performed using the classical sequential least squares programming (SLSQP) algorithm [Kra88]. 200 iterations were performed to calculate each eigenstate. Condition numbers of MA were computed for ten values of l ranging from one to ten. A total of 5 random seeds were tested for each value of l .

Two metrics are used to assess the performance of the VQED method. The first metric is the fidelity of the calculated solution. The fidelity is defined as

$$F = |\langle x_c | x_q \rangle|^2, \quad (18)$$

where $|x_c\rangle$ and $|x_q\rangle$ are the actual and estimated solutions, respectively. The second metric is the relative error of the calculated solution compared to the classical solution. This metric is defined as

$$\delta = \frac{z_q - z_c}{z_c}, \quad (19)$$

where z_c and z_q are displacements from $|x_c\rangle$ and $|x_q\rangle$, respectively.

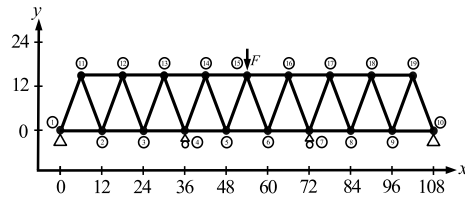


Figure 2: Truss structure

4 RESULTS

Truss Structure

The truss structure is illustrated in Figure 2, where the x - and y -axes indicate spatial coordinates in inches. The truss consists of 19 nodes and 35 members. Each element has a cross-sectional area of 8.5 in^2 and elastic modulus of 29,000 ksi. For the boundary conditions, two pin supports are located at nodes 1 and 10. Two roller supports are located at nodes 4 and 7. A downward point load of 5,500 kips is applied at node 15.

Table 1: Condition number of MA for the truss structure with different circuit depths and ansatz-random seeds.

Repetitions (l)	Best Seed	Condition Number
1	4	21.0823
2	1	11.6798
3	2	7.8683
4	4	3.9361
5	2	1.5099
6	1	1.0936
7	1	1.0052
8	4	1.0050
9	3	1.0045
10	0	1.0049

The VQED method was used to reduce the condition number of MA . The results are shown in Table 1, where the best choice is $l = 7$, where the condition number of MA has been significantly reduced to 1.0052 without further increasing the circuit depth. This is significantly smaller than 71.49, which is the original condition number of A .

The convergence plot of 32 eigenvalues for the truss structure with ansatz depth of seven and random seed of one is plotted in Figure 3. For all eigenvalues, convergence was clearly observed after 200 iterations. Using the minimum eigenvalues and corresponding eigenvectors, the fidelity and L_2 error for the solution generated from QSVT were 1.0000 and 0.0033, respectively. Overall, the VQED method can effectively generate the very accurate solution to the linear system.

The surface plots for x - and y -displacements in the truss structure are visualized in Figure 4. The surfaces from

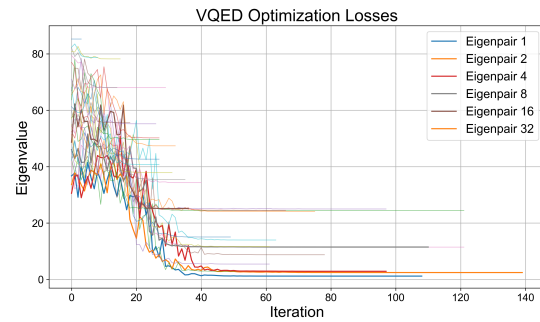


Figure 3: Convergence plot of 32 eigenvalues for the truss structure.

the proposed algorithm and classical linear solver are nearly identical. Nodes with displacements close to zero are omitted. Overall, most of the truss structure displacements from QSVT are close to the displacements from the classical linear solver.

MBB Beam

The MBB beam is shown in Figure 5. The beam is divided into a 4×3 rectangular grid of elements. The side length of each square element is 2 in. The left edge of the beam is supported by four roller supports, whereas the bottom edge is supported by two pin supports. A downwards point load of 3,500 kips is applied at node 17.

Table 2: Condition number of MA for the MBB beam with different circuit depths and ansatz-random seeds.

Repetitions (l)	Best Seed	Condition Number
1	0	21.3801
2	3	15.8670
3	0	9.3430
4	1	4.2713
5	0	1.9161
6	1	1.0278
7	0	1.0235
8	3	1.0174
9	4	1.0138
10	4	1.0129

Similarly, the sensitivity of VQED with respect to the circuit depth was performed. The calculated condition numbers of MA are shown in Table 2, where the best choice is $l = 6$ with the condition number of 1.0278. This is significantly smaller than the original condition number of A , which is 101.85.

Figure 6 shows the convergence behavior of 32 eigenvalues. It is observed that 31 out of 32 eigenvalues are able to converge within 200 iterations. With the calculated eigenvalues and corresponding eigenvectors, the fidelity and L_2 error of the solution from QSVT are 0.9994 and 0.0254, respectively.

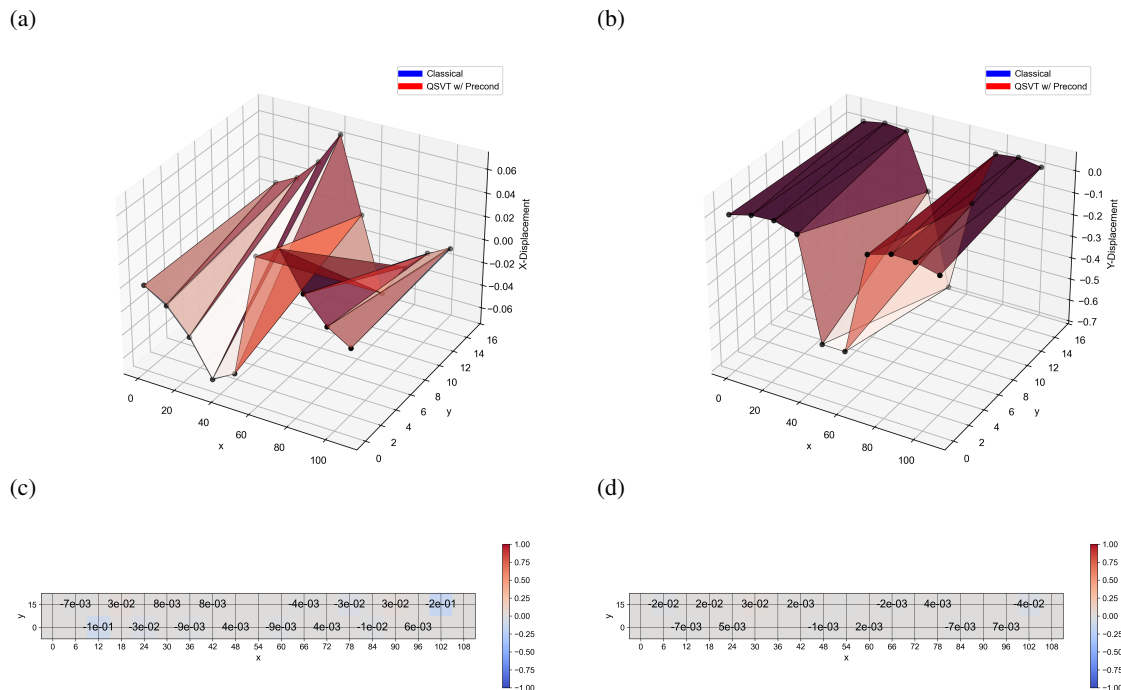


Figure 4: Surface plots of (a) x -displacements and (b) y -displacements, and relative errors for (c) x -displacements and (d) y -displacements for the truss structure. Nodes with displacements close to zero are omitted for visual clarity.

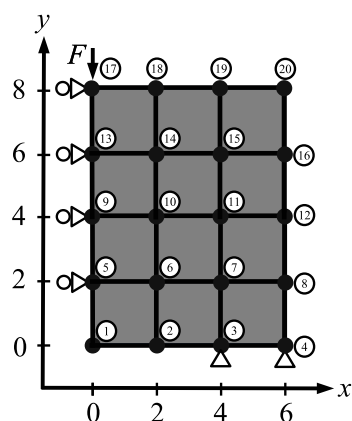


Figure 5: MBB beam

In the displacement surfaces shown in Figure 7, the estimated displacements calculated with the quantum algorithm deviate from theoretical values by relative errors ranging from 0% to 29%. It is observed that the free nodes have larger relative errors for both x - and y -displacements than the constrained nodes. In addition, the boundary condition and the external load cause the beam to move more freely in the vertical direction. As a result, the relative error tends to be larger for x -displacements than y -displacements. Although the

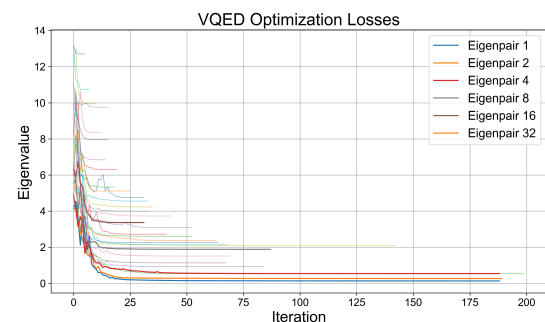


Figure 6: Convergence plot of 32 eigenvalues for the MBB beam.

largest relative error is 29%, the displacement surfaces for both classical and QSVT methods are very similar.

5 CONCLUDING REMARKS

In this paper, a VQED preconditioning method is proposed as a quantum preconditioning method. A spectral preconditioner M_k is constructed from variationally computed eigenvalues and eigenvectors of a Hermitian matrix A . This spectral preconditioner can reduce the condition number of A , which, in turn, improves accuracy of solving linear systems. The VQED method can be used for Hermitian matrices of low-rank.

The VQED method was used to reduce the condition numbers of the stiffness matrices for a truss structure and a MBB beam. It was demonstrated that the VQED can reduce the both condition numbers below 1.03,

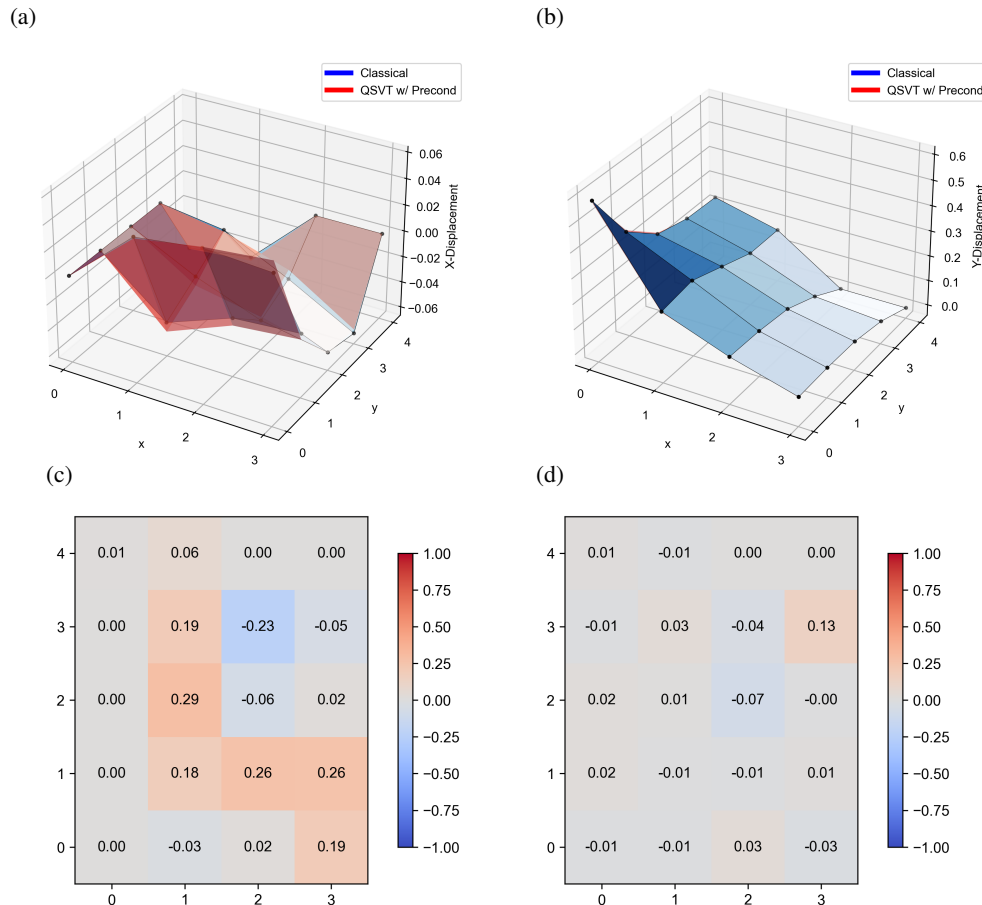


Figure 7: Surface plots of (a) x -displacements and (b) y -displacements, and relative errors for (c) x -displacements and (d) y -displacements for the MBB beam.

which are significant improvements over the original condition numbers. When QSVT is used for the preconditioned linear systems, the estimated displacements achieve very good accuracy and are very close to the results from the classical linear solver.

In the proposed method, classical projection-based deflation is used to generate the orthogonal eigenvectors. Future work will focus on imposing the orthogonality condition with a quantum computational framework. The orthogonality condition can be implemented in quantum computers either by introducing overlap penalty terms in the cost function, implementing a projector with controlled-state preparation, or defining a generalized eigenvalue problem with diagonalization.

The new preconditioning method was tested with classically reconstructed eigenvalues and eigenvectors computed with the VQED method. Future work will also focus on implementing a single quantum computational framework that integrates both VQED and QSVT. The degree d of an odd polynomial for matrix inversion is dependent on the condition number κ such that $d = \mathcal{O}[\kappa \log(\kappa/\epsilon)]$. To reduce the computational expenses of solving linear systems, the preconditioner

must be optimized with VQED before block-encoding it into unitary operators in QSVT.

6 REFERENCES

- [Bra23] Bravo-Prieto, C., LaRose, R., Cerezo, M., Subasi, Y., Cincio, L., and Coles, P.J. Variational quantum linear solver. *Quantum*, 7, pp.1188, 2023.
- [Cla13] Clader, B.D., Jacobs, B.C., and Sprouse, C.R. Preconditioned quantum linear system algorithm. *Physical Review Letters*, 110, pp.250504, 2013.
- [Gil19] Gilyén, A., Su, Y., and Low, G.H. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. *Proceedings of the 51st annual ACM SIGACT symposium on theory of computing*, pp.193-204, 2019.
- [Har09] Harrow, A.W., Hassidim, A., and Lloyd, S. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103, pp.150502, 2009.
- [Hig19] Higgott, O., Wang, D., and Brierley, S. Variational quantum computation of excited states. *Quantum*, 3, pp.156, 2019.

- [Kan17] Kandala, A., Mezzacapo, A., Temme, K., Takita, M., Brink, M., Chow, J.M., and Gambetta, J.M. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature*, 549, pp.242-246, 2017.
- [Kra88] Kraft, D. A software package for sequential quadratic programming. *Forschungsbericht-Deutsche Forschungs- und Versuchsanstalt für Luft- und Raumfahrt*, 1988.
- [Mar21] Martyn, J.M., Rossi, Z.M., Tan, A.K., and Chuang, I.L. Grand unification of quantum algorithms. *PRX Quantum*, 2, pp.040203, 2021.
- [Per14] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P.J., Aspuru-Guzik, A., and O'Brien J.L. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5, pp.4213, 2014.
- [Sha18] Shao, C., and Xiang H. Quantum circulant preconditioner for a linear system of equations. *Physical Review A*, 98, pp.062321, 2018.
- [Ton21] Tong, Y., An, D., Wiebe, N., and Lin, L. Fast inversion, preconditioned quantum linear system solvers, fast Green's-function computation, and fast evaluation of matrix functions. *Physical Review A*, 104, pp.032422, 2021.

Hybrid Quantum Branch-and-Bound Method for Quadratic Unconstrained Binary Optimization

Zedong Peng
Purdue University
610 Purdue Mall
47907, West Lafayette,
Indiana, USA
peng372@purdue.edu

Daniel de Roux
Carnegie Mellon
University*
5000 Forbes Ave
15213, Pittsburgh,
Pennsylvania, USA
dderoux@andrew.cmu.edu
*Daniel is now at Google.

David E. Bernal Neira
Purdue University
610 Purdue Mall
47907, West Lafayette,
Indiana, USA
dbernaln@purdue.edu

ABSTRACT

Quantum algorithms have shown promise in solving Quadratic Unconstrained Binary Optimization (QUBO) problems, benefiting from their connection to the transverse field Ising model. Various Ising solvers, both classical and quantum, have emerged to tackle such problems efficiently but lack global optimality guarantees and oftentimes suffer from hardware limitations such as limited qubit availability. In this work, we propose a hybrid branch-and-bound (B&B) framework that integrates Ising solvers as heuristics within a classical B&B algorithm. Unlike prior theoretical studies, our work presents a practical implementation, available as open-source at GitHub. We explore when and where to apply Ising solvers in the search tree, and introduce a custom branching rule optimized QUBO embedding. Our method is evaluated on hundreds of QUBO instances from QUBOLib.jl using Gurobi and the D-Wave quantum annealer. Our Results show up to 11% less solution time and 17% fewer nodes compared to default Gurobi, an off-the-shelf commercial optimization solver. These findings demonstrate the value of hybrid quantum-classical strategies for enhancing exact optimization.

Keywords

Quadratic Unconstrained Binary Optimization, Branch-and-Cut, Quantum Optimization.

1 INTRODUCTION

The quadratic unconstrained binary optimization problem (QUBO) is a central family of optimization programs where one seeks to minimize a quadratic function over binary variables. Formally, a QUBO is defined as

$$\begin{aligned} &\text{Minimize} \quad \mathbf{x}^\top \mathbf{Q} \mathbf{x} \\ &\text{subject to} \quad x_i \in \{0, 1\}, \quad \forall i \in N, \end{aligned} \quad (1)$$

where $\mathbf{x} \in \{0, 1\}^n$, $N = \{1, \dots, n\}$, and $\mathbf{Q} \in \mathbb{R}^{n \times n}$ is symmetric. The objective function includes both linear terms $Q_{ii}x_i$ and bilinear terms $Q_{ij}x_i x_j$.

This family of optimization problems arises in several applications such as MAXCUT, graph partitioning, protein folding, machine learning pipelines and many others [GKHD22]. QUBO is a special case of mixed-integer programming (MIP) with only binary variables, no explicit constraints, and quadratic objective, which in turn is a subfamily of Mixed-integer nonlinear programming (MINLP), extending MIP to allow general nonlinear objective functions and constraints. By this token, QUBOs can enjoy the rich set of methods and solver capabilities that have been steadily expanding over the past three decades

—from mixed-integer linear programs (MILPs), to second-order cone programs (MISOCPs), to nonconvex quadratic problems (MIQP/MIQCP), and finally to general MINLPs [Bix12, KBPV22, Gur24]—to solve these problems to global optimality.

MINLPs are, in general, hard to solve as they often involve nonconvexities such as bilinear terms, nonlinear constraints, or logic-based disjunctions. These break convexity and often require reformulations, decompositions, or restrictions to tractable subclasses [KBLG19]. Most approaches to solve MINLPs to global optimality rely on the branch-and-bound (B&B) algorithm, enhanced with methods like McCormick relaxations, Reformulation-Linearization Technique (RLT) cuts, and second-order cone approximations [RKS23]. Modern commercial solvers such as Gurobi incorporate these techniques and can solve QUBOs exactly to optimality. However, exact methods quickly become intractable as problem size grows.

To handle such large instances, heuristic solvers are commonly used. Metaheuristics such as simulated annealing, tabu search, genetic algorithms, large-neighborhood search, and path-relinking can produce high-quality solutions for problems with tens or

hundreds of thousands of variables. More recently, physics-inspired methods such as coherent Ising machines, digital annealers, and quantum annealers have shown promise in efficiently sampling low-energy states [MMB22]. While these methods do not guarantee global optimality, they offer practical performance on large-scale QUBO instances.

This work explores hybrid approaches that pair these solvers with quantum and physics-inspired heuristics to accelerate B&B while preserving global optimality guarantees. That is, providing both a solution and a certificate of global optimality.

Motivation for Hybrid Algorithms

While classical exact methods such as branch-and-bound (B&B) can solve small to medium-sized QUBOs to global optimality, they become computationally impractical for large problems due to the exponential growth in subproblems and the cost of solving relaxations. This motivates using quantum heuristics, thanks to the connection between QUBOs and the transverse field Ising mode [Luc14]. However, current quantum hardware is limited by qubit count, sparse connectivity, and environmental noise [AAA⁺24]. In fact, practical instances typically exceed hardware capacity which often times prevents direct execution, or obtained solutions are of poor quality. More importantly, global optimality usually cannot be guaranteed by quantum hardware.

These complementary limitations motivate hybrid strategies that combine classical guarantees with quantum or physics-inspired heuristics. Quantum heuristics can guide branching, supply high-quality incumbents, or tighten bounds, while the classical solver retains responsibility for global optimality certificates. The B&B tree structure naturally supports this integration by enabling selective oracle calls on promising subproblems.

Our Contribution

We present a practical hybrid quantum-classical algorithm for solving QUBO problems by embedding Ising-based heuristics into a classical B&B framework. Our method interfaces externally with `Gurobi` and invokes classical or quantum Ising solvers as heuristic oracles on selected subproblems. These solvers are invoked at different levels of the B&B tree. Oracle calls may provide branching decisions or candidate incumbent solutions. To improve effectiveness, we apply a preprocessing step to reduce the size of embedded subproblems and use a graph-aware branching rule based on variable degrees in the QUBO interaction graph. This design maximizes the value of Ising oracle calls while remaining within hardware constraints. Our implementation integrates with both simulated and hardware Ising

solvers and is publicly released¹, together with a benchmark suite of over five thousand QUBO instances from `QUBOLib.jl`².

- **Algorithmic contributions:** (i) a decision mechanism that triggers an Ising oracle at different stages of the branch and bound process; (ii) a graph-aware branching rule coupled with edge-contraction preprocessing.
- **Empirical contributions:** an open-source implementation and benchmark over more than a thousand instances show a median 17% node reduction and 11% wall-clock speed-up. The shifted geometric mean with a 10-second shift (SGM10) reduces baseline solve time from 154 s to 137 s.

The remainder of this paper is organized as follows. Section 2 reviews exact, heuristic, and quantum approaches. Section 3 describes the hybrid algorithm. Section 4 presents empirical results.

Related Work

Quantum-centric hybrid methods.

Theoretical groundwork for integrating quantum routines into classical branch-and-bound (B&B) was laid in [Mon20], which formalized the *Quantum Branch and Bound* (QBB) model and proved potential speedups when quantum subroutines tighten bounds or guide branching. Further theoretical developments appear in [CMYP22]. Building on these ideas, several prototype implementations have been proposed. The work in [STE24] inserts D-Wave quantum-annealing calls at selected B&B nodes to refine incumbents on small QUBO benchmarks. The method in [MHNY24] proposes Quantum Relaxation-Based B&B (QR-BnB), where a gate-model device estimates ground-state energies to tighten lower bounds. Reference [SRC⁺25] introduces Branch-and-Bound Digitized Counterdiabatic Quantum Optimization (BB-DCQO), which branches on spins with high measurement uncertainty to focus the search. The architecture in [HBBZ24] sketches a forward-compatible design to offload entire subproblem relaxations to future quantum devices. Collectively, these works demonstrate two main QBB insertion points, *bounding* and *branching*, while differing in hardware platform, problem size, and optimality guarantees.

¹ <https://github.com/SECQUOIA/QuantumBranchAndBound>

² <https://github.com/SECQUOIA/QUBOLib.jl>

Classical-centric enhancements.

Classical improvements to B&B focus on structural preprocessing, parameter tuning, and exploiting problem structure. The study in [RKS23] shows that exploiting sparsity, reducing symmetry, and tuning parameters in the open-source MIP solver SCIP can significantly accelerate MaxCut (a special case of QUBO) on large, sparse graphs.

Our approach.

We target currently available hardware and avoid modifying solver internals. Rather than embedding quantum logic into the solver, we treat classical and quantum Ising engines as *external oracles* invoked through callbacks. These oracles provide candidate incumbents and branching guidance, while the commercial solver remains responsible for bounding, node selection, and global optimality certificates. This black-box strategy differs from QBB approaches that hard-code quantum subroutines or require customized solver forks. It also enables a fair, large-scale empirical study across thousands of diverse QUBO instances.

2 BACKGROUND

This section provides concise background on the three methodological pillars relevant to hybrid optimization: exact B&B, classical heuristics, and quantum and physics-inspired methods.

2.1 Exact Methods: Branch-and-Bound and Variants

The branch-and-bound (B&B) method is a recursive divide-and-conquer algorithm for solving mixed-integer optimization problems (MIPs) to global optimality. It systematically maintains upper and lower bounds on the optimal value and prunes regions of the search space that cannot contain better solutions. As a result, B&B is an exact method that can find and certify optimal solutions under general assumptions. We refer to [CCZ⁺14] for mixed-integer linear programming and to [BL12] for nonlinear generalizations. The typical steps of the B&B algorithm are:

1. **Initialization (Root Node):** Solve the continuous relaxation of the original MIP, ignoring integrality constraints. This yields an initial bound on the optimal objective value. If the solution is already integer feasible, it is globally optimal.
2. **Branching:** If the relaxation has fractional values for integer variables, choose one such variable and create subproblems by imposing disjunctions (e.g., $x_i \leq \lfloor x_i^* \rfloor$ or $x_i \geq \lceil x_i^* \rceil$), thereby partitioning the feasible region.
3. **Bounding:** Solve the continuous relaxation for each subproblem. The solution provides a bound (upper or lower, depending on the problem direction) on the objective within that subregion.
4. **Fathoming (Pruning):** Discard a node if: (i) its relaxation is infeasible, (ii) its bound is worse than the incumbent, or (iii) its relaxed solution is integer feasible. If the new feasible solution improves the incumbent, update the incumbent.
5. **Node Selection:** Select the next active node for exploration. Strategies include best-bound, depth-first, or breadth-first. The goal is to explore promising parts of the tree while managing memory.
6. **Iteration:** Repeat branching, bounding, and fathoming on the selected node. This recursive process explores the full tree or continues until optimality is proven.
7. **Termination:** Stop when no active nodes remain. The incumbent is then the optimal solution. If no feasible solution was found, the problem is infeasible.

While the branch-and-bound framework applies to both linear and nonlinear MIPs, solving the relaxations at each node can be computationally intensive. These relaxations are typically continuous and convex. For MILPs, they are linear programs (LPs), but more general MIPs may involve convex nonlinear relaxations. In some cases, these relaxations may even be nonconvex. Subproblems created during branching can be nearly as difficult to solve as the original problem. This observation has motivated the use of heuristics to either bypass expensive relaxations or produce feasible solutions that accelerate the search. Three common B&B variants that exploit this idea are Branch-and-Prune, Branch-and-Cut, and Primal Heuristics [LB96].

Branch and Prune: This variant focuses on recursive branching and pruning of subregions that cannot yield better solutions than the incumbent. Pruning decisions rely on bounds computed from continuous relaxations. A node is discarded if its relaxation is infeasible, yields a bound worse than the incumbent, or results in an integer-feasible solution. Tighter bounds enable earlier pruning and improve convergence.

Branch and Cut: This method augments B&B by adding cutting planes to the relaxed subproblems. These valid inequalities are violated by the current relaxation but respected by all feasible integer solutions. Effective cuts, such as Gomory, MIR, or cover inequalities, can tighten relaxations and improve pruning. Relaxations at nodes are typically

continuous and convex. For MILPs, this means LPs; for more general MIPs, they may be convex nonlinear programs. Although cutting can improve performance, excessive or poorly selected cuts may slow down per-node solution times, so cut management must be judicious.

Primal Heuristics: These methods generate high-quality feasible solutions early in the search. Stronger incumbent solutions improve pruning efficiency by tightening the upper bound. Common heuristic strategies include rounding, diving, local search, and large neighborhood search [Ber06].

- **Rounding:** Converts solutions from a relaxation into integer-feasible ones using rounding rules, followed by feasibility repair if needed.
- **Diving:** Fixes variables based on their fractional values and recursively solves subproblems to explore promising regions.
- **Local Search:** Improves a given solution by exploring its neighborhood using swap, flip, or exchange moves.
- **Large Neighborhood Search (LNS):** Relaxes a subset of variables and resolves the resulting reduced problem to escape local optima.

2.2 Heuristic Algorithms

Given the NP-hardness of QUBO, exact methods become impractical for large-scale instances. To address this, the literature has proposed a wide range of heuristics and approximation algorithms capable of producing high-quality solutions within reasonable computational time. In many cases, heuristics have been shown to recover optimal solutions on benchmark instances.

Simulated Annealing (SA) is a widely used metaheuristic inspired by the physical process of annealing in metallurgy. SA explores the solution space by iteratively proposing neighboring solutions [KGJV83]. Improvements are always accepted, while worse solutions may be accepted with a probability that decreases over time according to a predefined cooling schedule. This mechanism helps the algorithm escape local minima and explore diverse regions of the search space. The performance of SA is highly sensitive to parameter tuning, especially the cooling rate. For QUBO problems, several effective implementations have been reported in [AHA98, Bea98].

Local Search heuristics form another important category. In particular, *Tabu Search* uses a short-term memory structure (the tabu list) to prevent cycling and encourage diversification. At each iteration, the best admissible neighbor is selected, potentially even if it worsens the objective. This process allows escape from local optima. Detailed implementations can be found

in [Bea98, GKA98]. *Iterated Local Search* combines local search with strategic perturbations. Effective variants for QUBO are given in [Pal04].

Genetic Algorithms (GAs) represent a population-based heuristic that mimics evolutionary processes. A pool of candidate solutions evolves through crossover (recombination) and mutation (random perturbation). Selection is based on fitness, typically measured by the QUBO objective value. Many GA implementations incorporate local search to refine offspring, although convergence can be slow and quality may vary. These methods are computationally demanding and sensitive to population diversity. Relevant studies include [DSFC05, HAA00, MF99].

Additional heuristic families include *path relinking* [FPRR02], *cross-entropy methods* [LDM09], *global equilibrium search* [PPSS08], and *greedy construction strategies* [FPRR02]. For a comprehensive empirical comparison across heuristics for QUBO and Max-Cut, we refer to the systematic evaluation in [DGS18].

2.3 Quantum and Physics-Inspired hybrid Methods

Several quantum computing paradigms and their corresponding hardware implementations have been proposed to tackle difficult optimization problems. A prominent example is *Adiabatic Quantum Computing (AQC)*, which begins with a quantum system in the ground state of an initial Hamiltonian and slowly evolves it toward a cost Hamiltonian encoding the optimization objective. If the evolution is sufficiently slow, the adiabatic theorem suggests the system remains in the ground state of the final Hamiltonian, corresponding to the optimal solution. However, determining how slow is "sufficiently" slow depends on the minimum spectral gap during evolution, which is generally intractable to compute. As a result, real implementations use heuristics for schedule selection and face challenges such as thermal noise, decoherence, and limited qubit connectivity. These limitations often require embedding logical variables using multiple physical qubits, which adds overhead. *Quantum Annealing (QA)* models AQC in the presence of such physical imperfections and is used as a heuristic optimization method.

An alternative to AQC is the gate-based quantum computing model. In this framework, *Variational Quantum Algorithms (VQAs)* have emerged as a family of hybrid quantum-classical methods suitable for optimization [CAB⁺21]. VQAs rely on parameterized quantum circuits whose performance is evaluated by a classical optimizer based on a measured cost function. The classical optimizer updates the parameters to minimize this objective, typically through iterative

feedback. Training these circuits is known to be NP-hard in general [BK21].

Among VQAs, the *Quantum Approximate Optimization Algorithm (QAOA)* has become a widely studied strategy for combinatorial problems [WWJ⁺20]. QAOA alternates between applying the cost and mixing Hamiltonians. The number of alternations determines the circuit depth. Each round involves optimizing a set of continuous parameters, known as rotation angles, that control the unitary operations. Although QAOA is provably optimal in the infinite-depth limit due to its equivalence to AQC, its performance at finite depth remains difficult to analyze because of quantum many-body interactions and classical optimization difficulties [UB21].

We point out that all (VQAs) [CAB⁺21], and the Quantum Approximate Optimization Algorithm (QAOA) [FGG14], together with Ising-based hardware such as D-Wave quantum annealers [JAG⁺11], and coherent Ising machines [HSI⁺21] are specifically designed to tackle QUBOs heuristically. However, hardware noise and embedding overhead still limit scale, but empirical gains on medium-sized problems are encouraging [MMB22]. For a broader review of quantum heuristics for Ising problems, we refer the reader to [SBC⁺20].

As pointed out in the introduction, Quantum Branch-and-Bound (QBB) frameworks integrate such routines into classical B&B, aiming to accelerate bounding or branching while preserving global optimality guarantees [MHNY24, SRC⁺25, STE24].

3 PROPOSED METHODS

In this work, we propose and implement a hybrid quantum branch-and-bound (B&B) algorithm specifically designed for solving QUBO problems. The core idea is to incorporate heuristic solutions obtained from quantum hardware into the B&B tree to tighten the upper bound and enhance pruning efficiency. In general, modern B&B solvers allow external solution information to be injected in three ways: MIPStart (also known as warm start), heuristic callbacks, and variable hints. Since quantum solvers typically provide complete feasible solutions rather than partial guidance, our method focuses on the first two mechanisms and does not consider variable hints, which are better suited for soft guidance rather than hard feasible inputs.

Algorithm 1 shows the high-level pseudocode of our method. Compared to the standard B&B algorithm, our approach introduces three key enhancements. First, quantum solutions are injected at the root node using the MIPStart mechanism, allowing the solver to begin with a high-quality incumbent and prune large portions of the tree early on. Second, we extend this injection strategy to subtrees by invoking heuristic callbacks at

interior nodes. This enables the algorithm to continually benefit from quantum-generated solutions throughout the search. Even though hybrid quantum solvers can handle QUBO problems beyond the size limits of quantum annealers, the quality and efficiency of quantum solutions tend to degrade with problem size. To better exploit quantum hardware, we design branching strategies that prioritize subproblems likely to be smaller and thus more amenable to high-quality quantum solutions. These methods are implemented in our library and extensively tested on thousands of QUBO instances. More details about the experimental results are presented in the next section.

Algorithm 1 Quantum Branch-and-Bound Framework

```

1: Inject solution ▷ via MIPStart
2: Calculate branch priority ▷ based on Q matrix
3: Perform presolve
4: Solve root node LP relaxation
5: while termination criteria not met do
6:   Node selection
7:   Inject solution ▷ via heuristic callback
8:   Node presolve
9:   Solve the LP relaxation
10:  Apply cutting planes
11:  Apply primal heuristics
12:  if a feasible integer solution is found then
13:    Update incumbent solution
14:  else if the node is still feasible then
15:    Branch on fractional variables
16:    Insert child nodes into the search tree
17:  end if
18: end while

```

3.1 Root node: MIPstart

Quantum solvers, such as quantum annealers, are designed to solve QUBO problems by reformulating them as equivalent Ising models that can be directly mapped onto quantum hardware. For large-scale QUBO instances that exceed the capacity of physical quantum annealers, hybrid solvers combine classical and quantum resources to solve the full problem without manual decomposition. This makes it possible to directly apply quantum solvers to the original QUBO problem. Although such solvers can return feasible solutions, their quality is not always guaranteed, especially for problems with many variables or complex landscapes [PND08]. Nevertheless, these solutions can still provide useful upper bounds for minimization problems, and can be injected into the root node of a branch-and-bound solver using *MIPStart*, which allows users to supply one or multiple feasible solutions to guide the search. This process corresponds to Step1 in Algorithm 1.

3.2 Injection at internal nodes

An extension of the root-node injection idea is to insert solutions at internal nodes, finding a high-quality solution to each branch of the tree. These insertions can be handled by *heuristic callbacks*, a technique available in modern MIP solvers that allows users to supply a feasible solution dynamically during the tree search. These callbacks are implemented in step 7 of Algorithm 1. However, these calls must be handled with care, as we now discuss. Invoking heuristic solvers at every node can be prohibitively expensive and may significantly increase the overall computation time. We consider the following strategy to mitigate this. Since QUBO does not have constraints, a feasible solution for one node in the tree is feasible for all its child nodes. This suggests that instead of obtaining heuristic solutions at each node, we rather find a large set of high-quality solutions *a priori*, i.e., before starting the branch and bound algorithm, and store these solutions for later use. This strategy also aligns well with the high-throughput nature of quantum solvers, which are capable of producing a large volume of feasible solutions.

3.3 Embedding and Branching Priority

To solve an arbitrarily posed binary quadratic problem directly on a D-Wave system requires mapping, called minor embedding, to the QPU Topology of the system's quantum processing unit (QPU) [OOTT19]. By default, DWave will call *minorminer* to find the embedding of the input QUBOs. Because the quantum processing unit is inherently limited by the number of qubits, it is desirable to embed problems with a smaller number of variables. Figure 1 shows an example of an embedding for a 3-variable QUBO (2) onto a four-node QPU topology [D-Wnd]. The QUBO problem is first represented by the triangular graph, where nodes represent variables and edges represent the quadratic terms. Embedding aims to map the triangular graph into the fully connected and sparse four-node graphs.

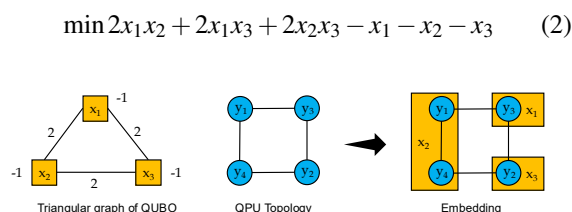


Figure 1: Example of embedding a 3-variable QUBO problem

This suggests that one should call a heuristic solver precisely on the nodes where most variables have been fixed, which are either deep nodes (i.e., further down the tree) or nodes where variables that appear in a large number of quadratic terms have been fixed. To illustrate, consider the following example. Suppose that we

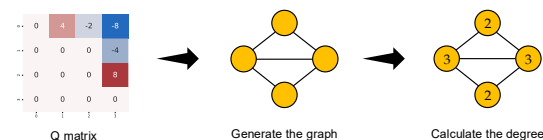


Figure 2: Example of calculating branch priority from quadratic objective matrix

are given a QUBO with Q matrix as in Figure 2, which gives the optimization problem

$$\min_{x \in \{0,1\}^4} 4x_1x_2 - 2x_1x_3 - 8x_1x_4 - 4x_2x_4 + 8x_3x_4 \quad (3)$$

Observe now that if x_1 and x_4 are fixed, we obtain an optimization program on variables x_2 and x_3 without quadratic terms. This toy example suggests that a good rule of thumb consists of first branching on variables that appear in many quadratic terms in the objective function, as they have a larger potential to diminish the size of the problem when branching on them.

Formally, we consider the matrix graph $G(Q)$ of Q where the vertices correspond to the variables in Program 1, and we add an edge between two vertices i and j if $Q_{ij} \neq 0$. The *degree* of a vertex $d(i)$ is the number of edges incident to it, or equivalently, the number of quadratic terms of the form $Q_{ij}x_ix_j, j \in N$ in which the variable x_i appears in the objective. We define the *Branch priority* of a vertex of $G(Q)$ as its degree. Figure 2 shows an example of computing branch priority for QUBO problem (3). In the branching step of our proposed B&B algorithm, we continue the iteration on the branch with the highest branch priority, breaking ties arbitrarily. This step is implemented in lines 2 and 15 of Algorithm 1.

4 NUMERICAL EXPERIMENTS

We evaluate the proposed Quantum Branch-and-Bound method on a benchmark set of 5807 instances from QUBOLib, which includes planted solutions to 3-regular 3-XORSAT and 5-regular 5-XORSAT problems. Figure 3 and Table 1 provide a statistical overview of these instances. Figure 3 illustrates the quadratic sparsity of the QUBOLib instances, revealing a clear trend: as the number of variables increases, the quadratic term sparsity also increases. Table 1 categorizes the full benchmark set into three collections. The 3-regular 3-XORSAT problems are sourced from two different arXiv datasets, while the 5-regular 5-XORSAT problems cover significantly larger problem sizes, with up to 24,576 variables.

Our Quantum Branch-and-Bound algorithm is implemented using a modular and extensible Julia-based pipeline. We begin by loading over 5000 QUBO

instances from the QUBOLib benchmark using the QUBOLib.jl and QUBOTools.jl [XRA⁺23] packages. Each instance is translated into a structured model using the JuMP modeling language.

To guide the branching decisions within the solver, we calculate the degree of the graph induced by the quadratic objective matrix using Graphs.jl. The branching priority information is passed to Gurobi 11.0.0, utilizing its Branch & Cut capabilities for exact optimization. The NonConvex parameter is set to 2 to enable solving non-convex quadratic programs, which are reformulated into bilinear forms and handled via spatial branching. All experiments are run with ThreadLimit = 1 and a time limit of 900 seconds.

In addition to exact methods, we incorporate heuristic warm-starts from quantum solvers such as D-Wave via MQLib [DGS18], allowing the solver to initialize with high-quality feasible solutions. We test 16 heuristic methods from MQLib, including BURER2002, FESTA2002GVNSPR, PALUBECKIS2004bMST3, PALUBECKIS2006, FESTA2002GPR, FESTA2002GVNS, MERZ2004, PALUBECKIS2004bMST2, BEASLEY1998TS, LU2010, FESTA2002G, PALUBECKIS2004bMST1, MERZ1999GLS, MERZ2002KOPT, ALKHAMIS1998, MERZ2002GREEDYKOPT. We also evaluate simulated annealing using dimod.neal (v0.5.9), and quantum annealing on D-Wave's Advantage 4.1 system with 5,750 qubits and over 35,000 couplers.

To focus our analysis, we filter the dataset to instances that (i) take more than 10 seconds to solve using default Gurobi, and (ii) can be solved to optimality by at least one of the tested methods within the time limit. This yields a refined test set of 1,454 instances for detailed comparison.

We measure performance using the shifted geometric mean (SGM) of solve time and number of explored nodes, with a shift of 10 (SGM10). If the instance is not solved to optimality within the time limit, the solve time is always set to the corresponding time limit and we record the number of explored nodes. The results are presented in Table 4.

Notably, MQLib only returns the best-found solution to the given problem. When used with Gurobi's MIP start strategy, this solution is injected at the root node. Alternatively, when used in a heuristic callback strategy, MQLib is invoked at every node to attempt solving subproblems. For SA and QA, we experiment with injecting the top 1, 10, 30, or 100 solutions sorted by objective value. In callback mode, SA and QA are applied once at the root node to generate a solution pool. During the branch-and-bound process, solutions from this pool are selectively injected based on the node subproblem. Moreover, to test the upper bound of the im-

provement, we tested the performance of providing the best solution in the MIP start strategy.

The results are summarized in Table 4. Among the 16 tested MQLib heuristics, PALUBECKIS2006 consistently achieves the best performance. To simplify the presentation, we only report the results of PALUBECKIS2006 in Table 4 as the representative MQLib method. It is shown that using branch priority alone improves Gurobi's performance by 17.3% in node count and 11.1% in runtime. When using MIP start with PALUBECKIS2006, simulated annealing, or quantum annealing, we observe approximately 10% runtime improvement. For simulated annealing, injecting more solutions leads to a modest 3% additional improvement, while quantum annealing shows limited sensitivity to the number of solutions provided. Combining MIP start with branch priority yields better results than MIP start alone, but still slightly underperforms the branch priority strategy alone. The results of injecting the best solution demonstrate the upper bound of improvement achievable via solution injection: the runtime is reduced by 83.0%, and the number of explored nodes drops by 90.6%, while still solving 1170 out of 1454 instances. Even though the results remains similar when combined with priority, it confirms the potential of how much high-quality starts can dramatically accelerate solving.

When applying heuristic callbacks, we find that invoking MQLib at every node introduces significant overhead, leading to longer runtimes and a reduced solve rate of 921 out of 1,454 instances. While SA and QA callbacks are applied in a more efficient way and invoked only once and used via a solution pool, they still result in longer solve times and slightly fewer explored nodes. These findings suggest that node-level heuristic injection is often too costly in practice and should be used cautiously.

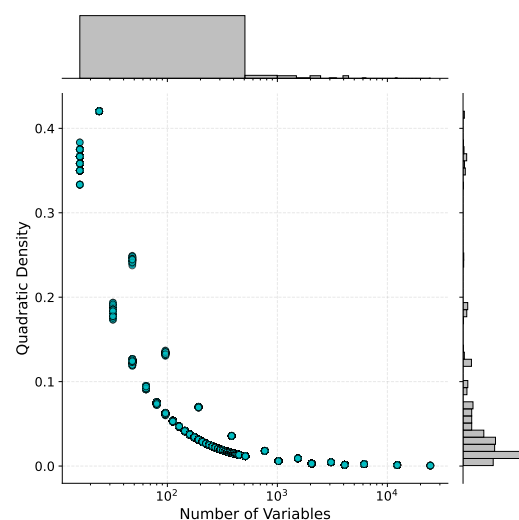


Figure 3: Quadratic sparsity of QUBOLib instances

Collection	# of instances	# of variables
3-Regular 3-XORSAT [KAHL22]	2300	16 ~ 4096
3-Regular 3-XORSAT [Hen19]	3200	16 ~ 4096
5-Regular 5-XORSAT [Hen19]	307	24 ~ 24576

Table 1: XORSAT Planted Solutions Collections - QUBOLib

5 CONCLUSIONS

This work proposes a practical hybrid quantum-classical branch-and-bound framework for solving QUBO problems to global optimality. The proposed method provides a unified framework to integrate Ising solvers, including both classical heuristics and quantum annealers, into a Gurobi-based branch-and-bound solver. Extensive experiments on over 5,800 instances from QUBOLib show that warm-starting with high-quality solutions from Ising solvers yields a 5% improvement and a carefully designed branch priority rule alone can reduce solve time and node count by over 10%. However, the improvement remains well below the potential upper bound obtained by providing the best solution. Additionally, node-wise heuristic callbacks are computationally expensive and often counterproductive. Overall, our results validate the potential of hybrid quantum-classical strategies to accelerate exact solvers on structured QUBO problems. Developing more effective methods for integrating quantum solvers as node-wise heuristics remains an open direction for future research.

6 ACKNOWLEDGMENTS

D.B.N. and Z.P. acknowledge the support of the startup grant of the Davidson School of Chemical Engineering at Purdue University.

7 REFERENCES

- [AAA⁺24] Amira Abbas, Andris Ambainis, Brandon Augustino, Andreas Bärttschi, Harry Buhrman, Carleton Coffrin, Giorgio Cor-tiana, Vedran Dunjko, Daniel J Egger, Bruce G Elmegreen, et al. Challenges and opportunities in quantum optimization. *Nature Reviews Physics*, pages 1–18, 2024.
- [AHA98] Talal M Alkhamis, Merza Hasan, and Mo-hamed A Ahmed. Simulated annealing for the unconstrained quadratic pseudo-Boolean function. *European journal of op-erational research*, 108(3):641–652, 1998.
- [Bea98] John E Beasley. Heuristic algorithms for the unconstrained binary quadratic pro-gramming problem, 1998.
- [Ber06] Timo Berthold. *Primal heuristics for mixed integer programs*. PhD thesis, Zuse Institute Berlin (ZIB), 2006.
- [Bix12] Robert E Bixby. A brief history of linear and mixed-integer programming computa-tion. *Documenta Mathematica*, 2012:107–121, 2012.
- [BK21] Lennart Bittel and Martin Kliesch. Training variational quantum algorithms is NP-hard. *Physical review letters*, 127(12):120502, 2021.
- [BL12] Samuel Burer and Adam N Letchford. Non-convex mixed-integer nonlinear pro-gramming: A survey. *Surveys in Opera-tions Research and Management Science*, 17(2):97–106, 2012.
- [CAB⁺21] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cin-cio, et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.
- [CCZ⁺14] Michele Conforti, Gérard Cornuéjols, Gia-como Zambelli, Michele Conforti, Gérard Cornuéjols, and Giacomo Zambelli. *Inte-ger programming models*. Springer, 2014.
- [CMYP22] Shouvanik Chakrabarti, Pierre Minssen, Romina Yalovetzky, and Marco Pis-toia. Universal quantum speedup for branch-and-bound, branch-and-cut, and tree-search algorithms. *arXiv preprint arXiv:2210.03210*, 2022.
- [D-Wnd] D-Wave Systems Inc. Example: Solv-ing a constrained sat problem. https://docs.dwavequantum.com/en/latest/quantum_research/example_sat_constrained.html, n.d. Accessed: 2025-05-30.
- [DGS18] Iain Dunning, Swati Gupta, and John Sil-berholz. What works best when? A sys-tematic evaluation of heuristics for Max-Cut and QUBO. *INFORMS Journal on Computing*, 30(3):608–624, 2018.
- [DSFC05] Abraham Duarte, Ángel Sánchez, Felipe Fernández, and Raúl Cabido. A low-level hybridization between memetic algorithm and VNS for the max-cut problem. In *Proceedings of the 7th annual conference on Genetic and evolutionary computation*, pages 999–1006, 2005.
- [FGG14] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.
- [FPRR02] Paola Festa, Panos M Pardalos, Mauri-cio GC Resende, and Celso C Ribeiro.

Strategy	Heuristic	# solved instances	Node Count	Runtime [s]
Baseline	-	1065	28170.0	154.5
Branch Priority	-	1077	23304.8 (-17.3%)	137.4 (-11.1%)
MIP Start	MQLib PALUBECKIS2006	1073	24543.0 (-12.9%)	142.5 (-7.8%)
MIP Start	DWave SA TOP1	1070	25418.8 (-9.8%)	150.1 (-2.9%)
MIP Start	DWave SA TOP10	1080	25256.3 (-10.3%)	148.3 (-4.1%)
MIP Start	DWave SA TOP30	1074	24616.1 (-12.6%)	144.8 (-6.3%)
MIP Start	DWave SA TOP100	1059	24665.1 (-12.4%)	145.1 (-6.1%)
MIP Start	DWave QA TOP1	1081	24958.7 (-11.4%)	148.8 (-3.7%)
MIP Start	DWave QA TOP10	1074	24880.3 (-11.7%)	149.8 (-3.1%)
MIP Start	DWave QA TOP30	1069	25069.6 (-11.0%)	150.1 (-2.8%)
MIP Start	DWave QA TOP100	1079	25189.0 (-10.6%)	150.6 (-2.6%)
MIP Start + Embedding	DWave QA TOP1	1073	25713.4 (-8.7%)	148.2 (-4.1%)
MIP Start + Embedding	DWave QA TOP10	1078	24742.1 (-12.2%)	142.9 (-7.5%)
MIP Start + Embedding	DWave QA TOP30	1077	25093.5 (-10.9%)	146.0 (-5.5%)
MIP Start + Embedding	DWave QA TOP100	1069	25536.7 (-9.3%)	146.6 (-5.1%)
MIP Start	Best Solution	1170	2643.3 (-90.6%)	26.3 (-83.0%)
MIP Start + Branch Priority	MQLib PALUBECKIS2006	1094	23292.9 (-17.3%)	137.7 (-10.9%)
MIP Start + Branch Priority	DWave SA TOP1	1068	23440.7 (-16.8%)	138.0 (-10.7%)
MIP Start + Branch Priority	DWave SA TOP10	1079	23956.5 (-15.0%)	140.3 (-9.2%)
MIP Start + Branch Priority	DWave SA TOP30	1083	24000.7 (-14.8%)	140.5 (-9.1%)
MIP Start + Branch Priority	DWave SA TOP100	1077	23550.5 (-16.4%)	138.1 (-10.6%)
MIP Start + Branch Priority	DWave QA TOP1	1077	24312.4 (-13.7%)	142.3 (-7.9%)
MIP Start + Branch Priority	DWave QA TOP10	1072	23628.1 (-16.1%)	139.0 (-10.0%)
MIP Start + Branch Priority	DWave QA TOP30	1093	23714.2 (-15.8%)	138.9 (-10.1%)
MIP Start + Branch Priority	DWave QA TOP100	1071	24342.5 (-13.6%)	141.4 (-8.5%)
MIP Start + Branch Priority	Best Solution	1164	2649.6 (-90.6%)	26.5 (-82.9%)
Heuristic Callback	MQLib PALUBECKIS2006	921	17698.5 (-37.2%)	307.8 (+99.2%)
Heuristic Callback	DWave QA	1060	27785.0 (-1.4%)	160.5 (+3.9%)
Heuristic Callback	DWave SA	1039	26559.0 (-5.7%)	183.9 (+19.0%)

Table 2: Summary of solver performance on 1454 instances in QUBOLib (SGM10)

- Randomized heuristics for the MAX-CUT problem. *Optimization methods and software*, 17(6):1033–1058, 2002.
- [GKA98] Fred Glover, Gary A Kochenberger, and Bahram Alidaee. Adaptive memory tabu search for binary quadratic programs. *Management Science*, 44(3):336–345, 1998.
- [GKHD22] Fred Glover, Gary Kochenberger, Rick Hennig, and Yu Du. Quantum bridge analytics I: a tutorial on formulating and using QUBO models. *Annals of Operations Research*, 314(1):141–183, 2022.
- [Gur24] Gurobi Optimization, LLC. Gurobi Optimizer Reference Manual, 2024.
- [HAA00] Merza Hasan, Talal Alkhamis, and Jafar Ali. A comparison between simulated annealing, genetic algorithm and tabu search methods for the unconstrained quadratic Pseudo-Boolean function. *Computers & industrial engineering*, 38(3):323–340, 2000.
- [HBBZ24] Thomas Häner, Kyle EC Booth, Sima E Borujeni, and Elton Yechao Zhu. Solving QUBOs with a quantum-amenable branch and bound method. *arXiv preprint arXiv:2407.20185*, 2024.
- [Hen19] Itay Hen. Equation planting: a tool for benchmarking ising machines. *Physical Review Applied*, 12(1):011003, 2019.
- [HSI⁺21] Toshimori Honjo, Tomohiro Sonobe, Kensuke Inaba, Takahiro Inagaki, Takuya Ikuta, Yasuhiro Yamada, Takushi Kazama, Koji Enbutsu, Takeshi Umeki, Ryoichi Kasahara, et al. 100,000-spin coherent Ising machine. *Science advances*, 7(40):eabh0952, 2021.
- [JAG⁺11] Mark W Johnson, Mohammad HS Amin, Suzanne Gildert, Trevor Lanting, Firas Hamze, Neil Dickson, Richard Harris, Andrew J Berkley, Jan Johansson, Paul Bunyk, et al. Quantum annealing with manufactured spins. *Nature*, 473(7346):194–198, 2011.
- [KAHL22] Matthew Kowalsky, Tameem Albash, Itay Hen, and Daniel A Lidar. 3-regular three-xorsat planted solutions benchmark of classical and quantum heuristic optimiz-

- ers. *Quantum Science and Technology*, 7(2):025008, 2022.
- [KBLG19] Jan Kronqvist, David E Bernal, Andreas Lundell, and Ignacio E Grossmann. A review and comparison of solvers for convex MINLP. *Optimization and Engineering*, 20:397–455, 2019.
- [KBPV22] Thorsten Koch, Timo Berthold, Jaap Pedersen, and Charlie Vanaret. Progress in mathematical programming solvers from 2001 to 2020. *EURO Journal on Computational Optimization*, 10:100031, 2022.
- [KGJV83] Scott Kirkpatrick, C Daniel Gelatt Jr, and Mario P Vecchi. Optimization by simulated annealing. *science*, 220(4598):671–680, 1983.
- [LB96] Abilio Lucena and John E Beasley. Branch and cut algorithms. *Advances in linear and integer programming*, 4:187–221, 1996.
- [LDM09] Manuel Laguna, Abraham Duarte, and Rafael Marti. Hybridizing the cross-entropy method: An application to the max-cut problem. *Computers & Operations Research*, 36(2):487–498, 2009.
- [Luc14] Andrew Lucas. Ising formulations of many NP problems. *Frontiers in physics*, 2:74887, 2014.
- [MF99] Peter Merz and Bernd Freisleben. Genetic algorithms for binary quadratic programming. In *Proceedings of the genetic and evolutionary computation conference*, volume 1, pages 417–424. Morgan Kaufmann Orlando, FL, 1999.
- [MHNY24] Hiromichi Matsuyama, Wei-hao Huang, Kohji Nishimura, and Yu Yamashiro. Efficient Internal Strategies in Quantum Relaxation based Branch-and-Bound. *arXiv preprint arXiv:2405.00935*, 2024.
- [MMB22] Naeimeh Mohseni, Peter L McMahon, and Tim Byrnes. Ising machines as hardware solvers of combinatorial optimization problems. *Nature Reviews Physics*, 4(6):363–379, 2022.
- [Mon20] Ashley Montanaro. Quantum speedup of branch-and-bound algorithms. *Physical Review Research*, 2(1):013056, 2020.
- [OOT19] Shuntaro Okada, Masayuki Ohzeki, Masayoshi Terabe, and Shinichiro Taguchi. Improving solutions by embedding larger subproblems in a D-Wave quantum annealer. *Scientific reports*, 9(1):2098, 2019.
- [Pal04] Gintaras Palubeckis. Multistart tabu search strategies for the unconstrained binary quadratic optimization problem. *Annals of Operations Research*, 131:259–282, 2004.
- [PND08] L Pusey-Nazzaro and P Date. Adiabatic quantum optimization fails to solve the knapsack problem. *arXiv 2020. arXiv preprint arXiv:2008.07456*, 2008.
- [PPSS08] Panos M Pardalos, Oleg A Prokopyev, Oleg V Shylo, and Vladimir P Shylo. Global equilibrium search applied to the unconstrained binary quadratic optimization problem. *Optimisation Methods and Software*, 23(1):129–140, 2008.
- [RKS23] Daniel Rehfeldt, Thorsten Koch, and Yuji Shinano. Faster exact solution of sparse MaxCut and QUBO problems. *Mathematical Programming Computation*, 15(3):445–470, 2023.
- [SBC⁺20] Yuval R Sanders, Dominic W Berry, Pedro CS Costa, Louis W Tessler, Nathan Wiebe, Craig Gidney, Hartmut Neven, and Ryan Babbush. Compilation of fault-tolerant quantum heuristics for combinatorial optimization. *PRX quantum*, 1(2):020312, 2020.
- [SRC⁺25] Anton Simen, Sebastián V Romero, Alejandro Gomez Cadavid, Enrique Solano, and Narendra N Hegade. Branch-and-bound digitized counterdiabatic quantum optimization. *arXiv preprint arXiv:2504.15367*, 2025.
- [STE24] Claudio Sanavio, Edoardo Tignone, and Elisa Ercolessi. Hybrid classical–quantum branch-and-bound algorithm for solving integer linear problems. *Entropy*, 26(4):345, 2024.
- [UB21] AV Uvarov and Jacob D Biamonte. On barren plateaus and cost function locality in variational quantum algorithms. *Journal of Physics A: Mathematical and Theoretical*, 54(24):245301, 2021.
- [WWJ⁺20] Madita Willsch, Dennis Willsch, Fengping Jin, Hans De Raedt, and Kristel Michielsen. Benchmarking the quantum approximate optimization algorithm. *Quantum Information Processing*, 19:1–24, 2020.
- [XRA⁺23] Pedro Maciel Xavier, Pedro Ripper, Tiago Andrade, Joaquim Dias Garcia, Nelson Maculan, and David E Bernal Neira. Qubo. jl: A julia ecosystem for quadratic unconstrained binary optimization. *arXiv preprint arXiv:2307.02577*, 2023.
- [Pal04] Gintaras Palubeckis. Multistart tabu search

Q-AIM: A Unified Portable Workflow for Seamless Integration of Quantum Resources

Zhaobin Zhu^{1,*}, Cedric Gaberle^{2,*}, Sarah Neuwirth¹, Thomas Lippert^{2,3}, and Manpreet Jattana²

**Joint first authors*

¹Institute of Computer Science, Johannes Gutenberg University Mainz, D-55099 Mainz, Germany

²Modular Supercomputing and Quantum Computing, Institute of Computer Science, Goethe University Frankfurt, D-60325 Frankfurt, Germany

³Jülich Supercomputing Centre, Forschungszentrum Jülich GmbH, D-52428 Jülich, Germany

Abstract

Quantum computing (QC) holds the potential to solve classically intractable problems. Although there has been significant progress towards the availability of quantum hardware, a software infrastructure to integrate them is still missing. We present Q-AIM (Quantum Access Infrastructure Management) to fill this gap. Q-AIM is a software framework unifying the access and management of quantum hardware in a vendor-independent and open-source fashion. Utilizing a dockerized micro-service architecture, we show Q-AIM's lightweight, portable, and customizable nature, capable of running on different hosting paradigms, ranging from small personal computing devices to cloud servers and dedicated server infrastructure. Q-AIM exposes a single entry point into the host's infrastructure, providing secure and easy interaction with quantum computers at different levels of abstraction. With a minimal memory footprint, the container is optimized for deployment on even the smallest server instances, reducing costs and instantiation overhead while ensuring seamless scalability to accommodate increasing demands. Q-AIM intends to equip research groups and facilities with purchasing and hosting their own quantum hardware with a tool simplifying the process from procurement to operation and removing non-research-related technical redundancies.

Keywords

Quantum Computing, Quantum Computing Cloud Solution, Quantum Computing Infrastructure, Quantum Computing Integration, Quantum Computing Software Stack, User Management, Micro-Service Architecture, Docker

1 INTRODUCTION

Quantum computing, currently in its developmental phase, promises substantial acceleration of classical computations across various fields ranging from cryptography to materials science [GRTZ02, PAB⁺20, BBMC20, QBB⁺21]. Quantum computing scientists are constantly striving to overcome the limitations imposed by the current noisy intermediate-scale quantum (NISQ) era to fully realize quantum computing's potential.

However, while large private-sector enterprises are advancing the field through their own hardware, software, and algorithmic developments, smaller academic research groups lack direct on-site access to such resources. Although corporations such as IBM,

Google, and Amazon offer access to their own or hosted third-party infrastructure on a pay-to-use basis over the cloud, fundamental research is limited by restricted privilege policies and physical inaccessibility. Consequently, the acquisition of small-scale devices emerges as a viable solution to delve deeper into hardware and software enhancement studies, especially since the devices are getting cheaper. Yet, a critical challenge remains: the lack of a portable, open-source, and easily integrable software solution for small-scale hardware integration and provision.

Ultimately, procuring quantum hardware serves not only to enable deeper interaction with the device but also to facilitate its utilization on an abstract software level. This requires granting access to the resource over the host's network infrastructure, and possibly even beyond that, by a service either hosted in the cloud or also on-premise, dependent on the requirements and capabilities. For instance, a device could be made accessible to external users, such as students, for educational purposes or to demonstrate advancements to a broader audience. Yet, the absence of a common, open-source integration platform forces researchers

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

to spend valuable time and expertise developing such a solution on their own. Such efforts can detract from their primary focus of advancing scientific knowledge. A flexible, streamlined, and universally adaptable integration software is therefore crucial, not only to eliminate redundancies, but also to ensure compatibility with existing workflows.

This work presents Q-AIM, a flexible, streamlined, and universally adaptable quantum integration workflow designed to address key challenges in quantum resource utilization, particularly for small enterprise and academic research groups. Typically, quantum systems are equipped with peripheral classical hardware providing a hardware- and vendor-dependent interface to the quantum computer, facilitating their use on an abstract software level. But, without a standardized, open-source platform, researchers face significant hurdles in integrating quantum systems into existing workflows. To eliminate redundancies and enhance compatibility of the necessary integration software solution, we make the following contributions:

- **Unified and Portable Platform:** A Docker-based, microservice architecture ensures seamless deployment and scalability across various infrastructures, e.g., on a local machine, server, and cloud.
- **Flexible Access and Control:** Offers resource access via multiple abstraction levels (from algorithmic to pulse-level) with a role-based permission scheme for secure and tailored utilization among diverse user groups.
- **Classical Workflow Integration:** Standardized and flexible APIs enable easy hybrid computing, reproducibility, and cross-institution collaboration without major infrastructure changes.
- **Prototype Validation:** A lightweight prototype demonstrating adaptability and efficient resource usage across on-premise and cloud infrastructures, supporting broad research and educational application possibilities.

2 BACKGROUND

Quantum computing offers great potential, but the integration of quantum hardware into classical workflows faces major challenges due to proprietary systems and lack of standardization. This chapter provides a brief overview of quantum instruction workflows and existing integration solutions.

2.1 Quantum Resource Workflow

Executing quantum algorithms on hardware requires translating high-level logic into device-specific operations through multiple abstraction layers, as shown in

Fig. 1. The process begins with circuit definition in hardware-agnostic frameworks like Qiskit [WVMN19], Cirq [OTC⁺20], or Braket [GARV⁺22], analogous to classical algorithm development. The quantum equivalent of compilation is transpilation, which generates an intermediate representation (IR) [CVPP⁺25]. This involves both hardware-independent optimizations and hardware-dependent adaptations to match the processor's native gate set [CAF⁺24]. Tools like BQSKit [YIL⁺21] perform these transformations, optimizing circuit depth while respecting hardware constraints. Common IR formats include OpenQASM [CBSG17, CJAA⁺22], serving as a quantum assembly language.

The final stage converts the IR into machine instructions, typically implemented as precisely controlled microwave pulses that manipulate qubit states. This completes the translation from abstract algorithm to physical implementation, with compiler comparisons available in [SBL⁺21]. As in classical computer science, assembler is not yet an instruction at machine level, but is used to communicate with remote resources if used. Therefore, the last step of instruction modification is the translation to machine code (*Machine Instructions*). In quantum computing, this oftentimes means microwave pulse modification where specific pulses modify the state of the quantum system likewise to an instruction in the high-level abstraction implementation.

To execute algorithms on real quantum hardware, two key aspects must be considered. First, as shown in Fig. 1, any algorithm or circuit must be transpiled into the underlying hardware's instruction set. Typically, algorithms are developed in a hardware-agnostic manner, requiring translation into device-specific operations.

Second, access to quantum resources must be established. Providers usually offer cloud-based access via APIs, treating quantum computers as specialized remote resources. They enforce restrictions on supported IR formats, interaction methods, and security protocols, requiring authentication and permissions. Access is managed through an API, which handles data flow to and from the resource. In Fig. 1, the API call can occur at any stage between circuit definition and machine instructions, depending on the service. After execution, results are returned in a provider-defined format.

2.2 Analysis of Related Work

Recent work explores integrating quantum devices with classical resources through two paradigms: GPU-like indirect access [SRKS22, RTL⁺22, HML⁺21] or API-driven direct access [MFML23, SP21, GHG⁺24, HML⁺21, JATK⁺24, GARV⁺22, OTC⁺20]. Ruefenacht et al. [RTL⁺22] categorize integration architectures from loosely-coupled (on-premise) to tightly-coupled (on-chip) for HPC workloads. While Schulz et

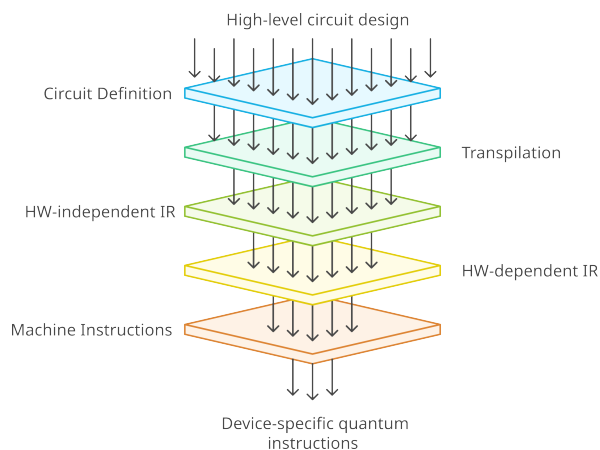


Figure 1: Instruction abstraction levels in quantum computing. From high-level circuit design (highest abstraction) to hardware-independent and hardware-specific intermediate representations (IR), ultimately becoming device-specific machine instructions (no abstraction) to be used with the quantum device.

al. [SRKS22] advocate for unified software stacks, Humble et al. [HML⁺21] note that current prototypes rely on primitive client-server interactions unsuitable for true acceleration.

Precisely, these early-stage systems are crucial for academic research and motivate our work: an open-source platform enabling secure, low-overhead access to quantum devices across environments (on-premise/cloud) via Docker containers. This addresses the gap in accessible solutions for small-scale research, contrasting with service-oriented approaches [MRV22, NUB24, GCA⁺21] that abstract hardware for enterprise use. For instance, Grossi et al. [GCA⁺21] propose quantum FaaS via HTTP APIs, while Nguyen et al. [NUB24] mitigate vendor lock-in.

Our focus reverses this paradigm, instead of high-level abstraction, we enable fine-grained control (e.g., pulse-level access) critical for research. Concurrent work by Beck et al. [BBB⁺24] targets HPC-integrated quantum acceleration for large institutions, whereas our solution democratizes access for smaller groups, streamlining device integration from procurement to experimental use.

3 DESIGN CONSIDERATION

As described in Section 2, integrating quantum computing resources into existing research and industrial workflows requires careful orchestration of software across multiple domains. However, current quantum solutions are tied to specialized hardware and proprietary environments, limiting applicability and creating barriers.

To address this, we propose Q-AIM: a standardized, portable workflow and corresponding software implementation enabling seamless integration of quantum re-

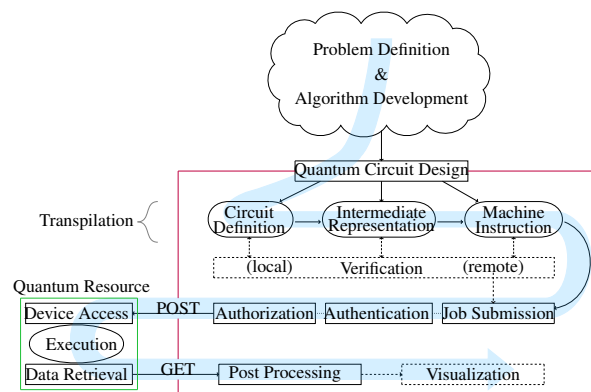


Figure 2: Overview of the quantum computation workflow. The larger, red box (right) indicates classical hardware, the smaller, green one (left) the quantum system. The problem is defined as quantum circuit at any abstraction level and undergoes transpilation until machine instruction level is reached. Communication between the classical and quantum system is facilitated through API calls.

sources. In Fig. 2, required process steps are shown in blue, classical services in the red box, and vendor-dependent quantum resources in the green box. Therefore, with Q-AIM, quantum circuit design supports various abstraction levels. An optional simulation step allows verification before using remote quantum computers. All services in the red box are abstractions provided by the software, with each component replaceable or customizable, allowing granular control for users and providers. This flexibility supports diverse requirements. Due to varying execution environments and access control needs, we use REST APIs for broad compatibility across languages, platforms, and architectures.

Another key design aspect is the decoupling of quantum hardware, ensuring software operates independently of specific hardware. Tasks like qubit manipulation, instruction execution, and measurement are handled by the hardware and its peripherals. Together with microservices, these form the Q-AIM backend.

4 METHODOLOGY

The key principle of the proposed approach is to ensure that classical workflows remain largely unaffected by the introduction of quantum computers. Instead of having to rebuild or heavily modify pre-existing computational frameworks, end-users can embed quantum tasks and pipelines into their established processes. The effectiveness and versatility of the proposed system are underpinned by four core methodologies:

1. Fully Integrated Classical Workflow: Based on the design considerations as mentioned in Section 3, the classical quantum computing workflow, i.e., the steps

from algorithm definition to machine instruction, is a multi-stage process that spans tasks from algorithm development to optimization. Depending on the manufacturer and application scenarios, the code often needs to be compiled into an appropriate representation, such as gate-level or pulse-level instructions, to execute on a quantum computer. To allow users to operate at different levels of abstraction, it is crucial to account for these variations during the integration workflow.

To support this flexibility and maintain vendor independence, the entire classical quantum computing workflow is treated as a black box and integrated as a unified entity within our infrastructure. This abstraction ensures seamless interaction between the classical and quantum workflows without requiring users to manage low-level specifics or adapt to API changes, thereby enhancing usability and interoperability. Therefore, the classical workflow is incorporated into our integration pipeline as a self-contained component and augmented with additional functionality. These functionalities range from custom user management, authentication services, and access control to result visualization and system monitoring. This approach allows users to work with different programming languages at different levels of abstraction while taking advantage of the unique features of different quantum hardware backends. It also supports adaptability to emerging quantum computing platforms, ensuring that the architecture is future-proof.

2. Encapsulated System Architecture: To enable a standardized and transparent quantum computing workflow, we rely on an encapsulated system architecture that decouples the software layer from the underlying quantum computing hardware. This architecture acts as an abstraction layer that simplifies and hides the complexity of the individual components. As shown in Fig. 3, the system is divided into two key segments: *the Q-AIM software* and *the quantum computing hardware*. The central component of this system architecture is the API gateway, which abstracts the underlying microservices and prevents direct access or communication between clients and service components. This isolation significantly simplifies implementation for both clients and microservice applications, as the complexity of the application is decoupled from its clients. Another important element is the Reverse Proxy that offers additional functions that go beyond the simple forwarding of requests. It assigns the physical ports to those of the encapsulated environment and acts as an intermediary that communicates with the server on behalf of the client(s), forwards requests and returns responses. The proxy is located at the edge of the API gateway, which centralizes the processing of API requests and enforces additional security policies such as authentication, authorization and access control, as well as other functions not covered by the microservices.

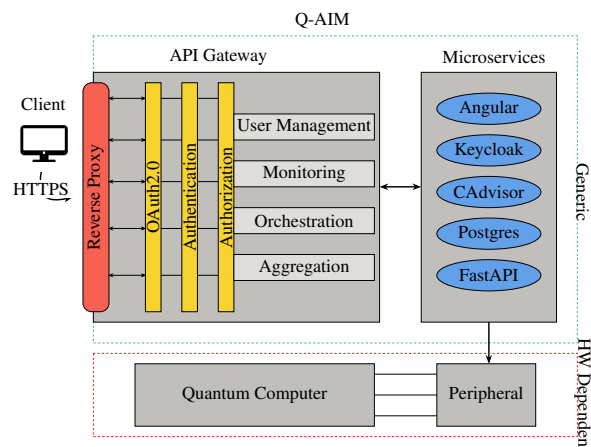


Figure 3: Microservice-based architecture of Q-AIM. It facilitates secure client interactions via HTTPS and a reverse proxy, providing access to quantum systems through a structured microservice architecture. The API Gateway manages authentication, authorization, and orchestration, while the microservices provide the software's functionalities.

As the result, our architecture provides a standardized way for those to communicate, interact thus allows for modularity, scalability, and adaptability, making it possible to integrate the services seamlessly while maintaining a consistent and manageable architecture.

3. Micro-Service-Based Software Architecture: To meet the challenge of a standardized, portable integration workflow, in this work we develop a microservice-based software architecture that enables quantum computing hardware to be integrated into existing and future infrastructures in a consistent manner. A key aspect of Q-AIM is therefore portability and transparency.

Lightweight virtualization technologies, i.e., containers such as Docker or Apptainer are highly portable. The isolated nature of container virtualization also ensures that all required dependencies are bundled in the container and services can be quickly deployed and replicated on different hosts. As container-based software deployment is typically based on a microservice architecture, the functionality of the software can be customized and extended according to user-specific requirements. This gives Q-AIM greater versatility and adaptability, which is beneficial for research institutions and companies alike.

Overall, Q-AIM's microservices-based architecture not only reduces the dependency on specific vendors, but also allows researchers and developers to transfer and scale their work to different environments [MWB23]. This is particularly important for reproducibility and enables the building of a community that promotes the exchange of ideas, best practices and resources to further advance the development of quantum computing technology.

4. Flexible and Fine-Grained User Management: Another key challenge is managing access from different environments with corresponding user affiliations. Users can generally be categorized into internal and external groups, each requiring specific levels of access to quantum resources. For example, a physicist conducting physical experiments on a quantum computer needs easy access to enter signals or waveforms. In contrast, users from business or other fields usually require high-level access to test their algorithms or circuits on the quantum computer.

To enable fine-grained access control to quantum resources and flexible user management, it is essential to integrate different user groups into a single infrastructure, manage them effectively and meet their different access requirements. This requires the integration of the industry standard LDAP [Ser06] protocol into our solution for authenticating internal users. In addition, the system should support the creation and management of a special user database for external users to ensure seamless integration and secure access for all user types. As interaction with quantum computing resources takes place exclusively via the API gateway, Q-AIM enables authentication for different user groups and supports fine-grained authorization, ensuring that users can only interact with the resources that correspond to their assigned roles.

5 PROTOTYPE IMPLEMENTATION

In the following, we present an early prototype implementation of our portable, unified, and generic quantum computing integration workflow. The integration of self-written or third-party libraries as a service in the example implementation of our microservice architecture underlines the aforementioned adaptability. Similarly, other entities can implement different services specific to their use cases.

5.1 Container-based Deployment

From the high-level system architecture shown in Fig. 3, it is clear that deploying the Q-AIM application requires a complex environment with a number of microservices working together. To improve transparency and portability in the deployment process, Docker containers are used to ensure consistency. Also, a Docker Compose file is used to simplify the management of multiple microservices and their dependencies within the application. Consequently, this approach facilitates the deployment of the entire application environment with a single command, i.e. *docker compose up*.

To provide an overview of the main services of Q-AIM, as shown in Listing 1, the services are described below:

- **Database Service:** This initiates a PostgreSQL database utilizing the official Postgres Docker

```
services:
  database:
    image: postgres
    ...
  authentication:
    depends_on:
      - database
    image: jboss/keycloak:11.0.3
    ...
  Q-AIM-API:
    image: fastapi:dev
    ...
  Q-AIM-Frontend:
    image: Q-AIM:dev
    ...
  reverse-proxy:
    image: nginx:alpine
    ...
  monitoring:
    image: gcr.io/cadvisor/cadvisor:latest
    ...
  ...
```

Listing 1: Overview of the microservices and their images in the docker compose file.

image. To ensure persistent storage of the database data, a Docker volume is created alongside.

- **Authentication Service:** Utilizing the official Keycloak Docker image, this service delivers identity and access management functionalities. It relies on the database service and necessitates a Keycloak configuration file. For illustrative purposes, environment variables for the Keycloak administrator user, password and other settings are also configured via the docker compose file.
- **Q-AIM-API Service:** This employs the Docker image fastapi:dev and is built using a custom Dockerfile, which sets up an environment tailored for a FastAPI application and installs specific dependencies.
- **Q-AIM-Frontend Service:** Built upon the Q-AIM:dev Docker image using a custom Dockerfile, this Dockerfile ensures that the actual Angular Web-Application is built in a Node.js environment and then the resulting build is deployed within an NGINX container. The NGINX container is used to serve the static files of the Angular application and provide the configuration for the web server.
- **Reverse Proxy Service:** Based on the Docker image nginx:alpine, this service initializes an NGINX proxy server. Configured with a corresponding configuration file and SSL certificates, the proxy server forwards incoming requests to various services provided within Docker containers.
- **Monitoring Service (Optional):** Leverages the official CAdvisor Docker image to efficiently gather

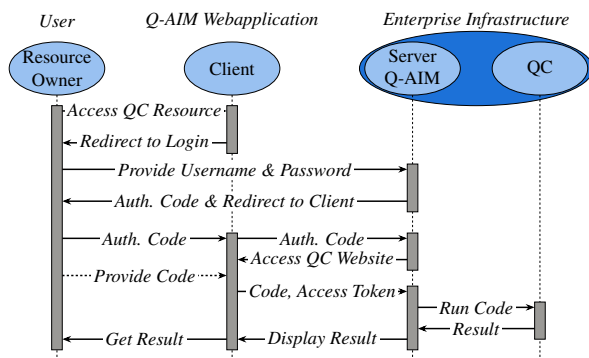


Figure 4: Representation of the first authentication process for an approved user attempting to run code on a protected quantum computing resource.

and present container statistics. To facilitate access to files or directories within the host system, it is imperative to include relevant directories or files from the host within the container.

Overall, the division of microservices illustrates the basic principles of modern software development and architecture. This approach promotes customizability, scalability, security and reproducibility in application deployment. By using Docker and Docker Compose, both developers and professionals can seamlessly adapt Q-AIM to their specific requirements and deploy it efficiently in their infrastructure.

5.2 Authentication Workflow

An exemplary workflow accessing a quantum device as a protected resource is depicted in Fig. 4. During the user's initial access, they are required to provide their credentials. Only after the identity and access management tool Keycloak validates the provided credentials and returns an authentication code, including an access token holding information about the authenticated user's roles and permissions, an ID token with general information about the authenticated user, and a refresh token, does the user gain access to the quantum computer frontend component on the Angular webapplication. Provided quantum code of the user on the frontend managing access to the protected quantum resource. The API therefore validates the provided authentication code at the identity and access management tool and checks the user's permissions in the access token. If the user is permitted, it controls the bidirectional flow to and from the quantum resource. Lastly, the result is displayed on the frontend web application.

5.3 Q-AIM User Interface

The Q-AIM frontend serves as a user-friendly gateway to access quantum computing resources. To safeguard

the underlying endpoints and enable fine-grained permission management, integration of the Keycloak service and authentication functionality has been embedded within the Angular application. As can be seen from the Fig. 5 ①, users must be authenticated to access certain resources and have certain permissions. Furthermore, the authorization framework's distinction between groups and roles facilitates the assignment of users to various domains, institutions, and systems, allowing for the allocation of grouping-specific roles. To exemplify the granularity of rights management, the prototype establishes two groups, i.e., internal and external and each featuring user or admin roles.



Figure 5: Q-AIM Web User Interface. Users can provide code and runtime parameters in different formats, monitor resource utilization, and visualize results and metadata.

Depending on whether the user is already authenticated via the authentication server, the user is either redirected to the login page to process the authentication workflow as shown in Fig. 4 or to the interface for the corresponding compute resources, as shown in Fig. 5.

A standardized user interface ensures a seamless workflow for accessing different backend functionalities. As can be seen in ②, the resource utilization of the respective quantum resource is displayed. ③ shows, Q-AIM currently supports OpenQASM source code or Pauli representation as an input. The Pauli representation takes advantage of the fact that the Pauli rotations together with the controlled-NOT (CNOT) oper-

ation form a complete basis set, which means, every computation can be represented using appropriate Pauli and CNOT operations. This not only shortens but also simplifies the code input, enhancing its portability.

An exemplary circuit in OpenQASM format is partially displayed and used in the example run depicted in Fig. 5 ③. Since Qiskit simulators are used in this work for demonstration purposes and many devices accept OpenQASM as IR, the library converting the Pauli representation into OpenQASM is part of the dependencies for the API microservice and ships with the image by default. Users have the option of either entering their code via the editor or uploading the corresponding file.

As many circuits performing the algorithm's desired computation need to be parameterized, users must be able to provide the parameters. They can do so either by using a dictionary, naming the specific variable to be set and its value, or as a list (array), only providing the variables' values which are then assigned in order of appearance in the circuit. This provision is done on the webpage shown at ④. A prominent example of an algorithm necessitating parameterization is the Variational Quantum Eigensolver (VQE) [JJDRM23, PMS⁺14, JJ-DRM22]. Since parameter optimization is hardware-dependent, a set of optimized parameters obtained on one quantum device cannot be directly fixed into the circuit while ensuring reproducibility across different hardware. However, these parameters can still serve as a good initialization point, reducing the optimization effort on other devices. Therefore, the optimized parameters are included in the result object.

After submission, the provided code is executed via the API on the hardware-specific backend. Following successful execution, the resulting data and metadata are visualized as interactive diagrams or JSON objects as shown in ⑤ of the user interface, with the option of downloading them as CSV files or image files.

5.4 Q-AIM API

The Q-AIM API is designed to handle a variety of requests related to both quantum computing tasks and user-specific operations. It is developed using Python and the FastAPI framework and serves as the backbone for processing tasks. Since real quantum hardware is not available for testing, the API utilizes simulators to query as endpoints instead, with the Qiskit library employed for quantum computing task execution using its Qasm Simulator [Qis25], a noisy quantum circuit simulator backend.

Primarily, an API comprises public and private endpoints. Public endpoints are accessible without requiring authentication, enabling direct access to the endpoints. Conversely, protected endpoints necessitate authentication via a Json Web Token (JWT), issued by Keycloak, for example. Authentication is facilitated

through an authentication function *auth()*, assigned to endpoints requiring authentication as a dependency function using FastAPI's own dependency resolution mechanism. The function issues the query to the identity management using an OAuth2.0 scheme, as described in Section 5.2. For this work, only private endpoints are used to showcase the finely granulated permissions management. These include the endpoint `/api/user/me`, which retrieves information about the authenticated user. Furthermore, access to endpoints responsible for quantum computing is restricted to authenticated users with appropriate permissions. For illustrative purposes, the prototype offers four more endpoints: for uploading and processing OpenQASM code (`/api/qc/qasm/{upload, code}`), one for each uploading a file and coding on the web page, and the same for code in Pauli representation (`/api/qc/pauli/{upload, code}`). The calculated results are subsequently returned to the Q-AIM frontend as part of the response.

6 EVALUATION

In the following, we present an evaluation of the integration workflow's key attributes, focusing on its portability and lightweight nature, designed to seamlessly integrate with diverse computing environments. We examine these aspects using different combinations of hardware, software, and hosting paradigms in the following.

6.1 Test System Setup

To assess the portability of the integration workflow's software implementation, our prototype was deployed and tested on three distinct environments: (1) a local machine, (2) an on-premise hosted server, and (3) a cloud instance. These environments span different hardware architectures and operating systems. This multifaceted evaluation aims to validate Q-AIM's claim of adaptability to diverse computing environments, emphasizing its suitability for individual users with varied system configurations and requirements. The specifications for the different evaluation configurations is described in Table 1.

Parameter	Cluster Node	Local Machine	Cloud
CPU	Intel Xeon E5-2660 v2	Intel i7-12700H	Intel Xeon E5-2696V4 (vCPU)
Cores	20	20	2
RAM	128 GB	32 GB	8 GB
OS	Rocky Linux 9	Ubuntu 24.04	Debian GNU Linux 12
Network	Ethernet and Infini-Band (FDR)	Ethernet	Public Internet

Table 1: Hardware settings for the evaluation setups.

First, we demonstrate a proof of concept by deploying on a local machine, i.e., a personal computer aimed at stimulating real-world scenarios where end-users with

diverse machines might seek to utilize the software implementation. The successful deployment on the author's machine confirms that the API functions as intended, providing a sound foundation for further evaluation of more sophisticated hosting paradigm scenarios in the following.

Second, to validate the container's applicability in enterprise settings, we deployed it on real server infrastructure belonging to the Modular Supercomputing and Quantum Computing (MSQC) research group at Goethe University, Frankfurt am Main, Germany. As part of this process, we reconfigured a compute node from the cluster to function as an independent server, ensuring it could operate separately from the main cluster. This emphasizes its applicability in larger research groups and enterprise settings, capable of hosting on-premise solutions, providing full control over the whole workflow.

Third, given the increasing reliance on cloud services in enterprise environments, we also test our solution on Google Cloud using an E2-standard-2 instance, intended for moderate use, providing a good trade-off between cost and performance. This deployment is designed to evaluate the feasibility of using the solution in environments with limited computing resources, such as startups, small businesses, or individual developers who often prioritize cost-effective cloud solutions. The successful deployment, despite the limited resources of the cloud instance, underscored the solution's lightweight design and its ability to perform efficiently in resource-constrained cloud environments. Additionally, deploying the solution in the cloud highlights its potential for scalability. Without requiring any modifications to the docker image itself, the container setup can be scaled to more powerful instances, enabling it to handle more demanding workloads as needed.

The consistent behavior observed across different systems and settings underscores the portability and universality of the composed Q-AIM Docker image, substantiating its viability for widespread adoption.

6.2 Result Discussion

The ability to deploy and use the sample software implementation on all three distinct infrastructure configurations showcases the portability of the proposed solution. Users are not limited to a single hosting paradigm. From the most straight-forward solution, hosting on personal hardware, to more sophisticated solutions, like cloud-hosting, to ultimately fully on-premise server hosting, every use case can be covered by Q-AIM.

Changing the hosting paradigm, e.g., due to higher demand, is just a matter of copying the image and letting it

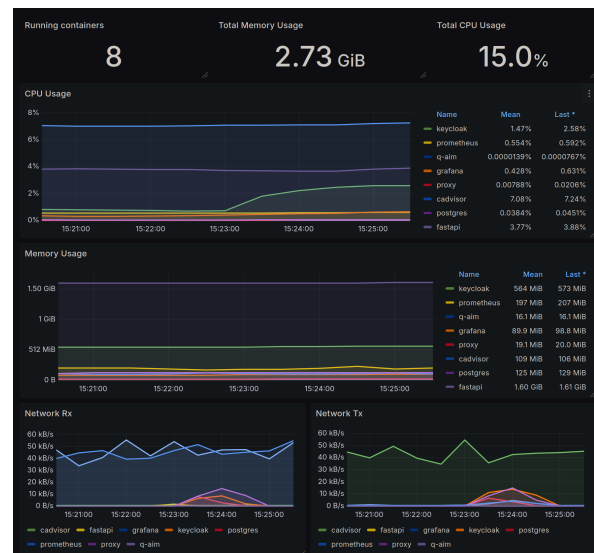


Figure 6: Grafana-based Monitoring Dashboard visualizes memory and CPU usage, as well as network traffic (receiving and transmitting) for the different containers in Q-AIM running on the local machine evaluation setup.

run on the new host, providing the exact same functionality and equal behavior. This reduces the dependency on a particular infrastructure and allows the application of the software to diverse users and use cases.

The evaluation of the portability made it necessary to deploy the same image on different backends, underlining another key aspect of the docker-based microservice implementation: its reproducibility. The same image of the software, with all its configurations specifically designed for our use case, was easily distributed across multiple infrastructures, which can be understood as providing it to different enterprises. Ultimately, this means enabling other users to use a fully fledged and specifically tailored implementation and reduces the overhead of creating a common basis for further research/collaboration.

Another critical aspect of the evaluation pertains to the integration workflow's resource efficiency. To investigate resource consumption, the composed Docker container incorporates a resource monitoring software image, cAdvisor, as a microservice. Running the Q-AIM container automatically starts the monitoring provided by cAdvisor. Utilizing this library, we examined the container's consumption of CPU and memory usage for logging in and running the example as shown in Fig. 6. Notably, the container exhibited remarkable efficiency, utilizing less than 3 GB of memory in our configuration, whereby Docker uses free memory for caching and frees it as soon as it is needed.

The findings of the aforementioned evaluations underscore the integration workflow's software implementation's pivotal attributes: portability across diverse sys-

tems and resource-efficient operation. The demonstrated success in real-world scenarios, shown by the seamless deployment on different server infrastructure, positions Q-AIM as a promising solution for users seeking a lightweight, unified, and universally deployable software solution to incorporate quantum computing hardware and offer access to an on-premise device.

7 CONCLUSION

We propose Q-AIM, a vendor-agnostic single-access solution for integrating quantum resources. Designed for research groups and small entities, it streamlines quantum device management from procurement through usage. The API-based solution provides administration tools with enhanced security for remote access while maintaining flexibility across diverse infrastructures. Implemented as an open-source containerized microservice, Q-AIM offers easy modification and maintainability. Our prototype currently interfaces with quantum simulators, demonstrating real-world integration scenarios.

Q-AIM's Docker-based deployment supports various infrastructures - from personal machines to cloud and on-premise servers - requiring minimal expertise for setup. Its open-source nature enables customization for specific hardware needs, ensuring complete vendor independence. We are implementing Q-AIM with Goethe University's Modular Supercomputing group for their first quantum device, enabling controlled access both within and beyond the research group. Future developments include integrating error mitigation protocols [JJDRM20, DPJ⁺24] and multi-hybrid quantum algorithms [Jat24].

The platform provides precise low-level hardware control through a unified interface, with planned extensions for quantum hardware monitoring and hybrid computing support. By exposing quantum resources via API, Q-AIM enables classical systems to leverage them as accelerators, potentially using RPC or pragmas for runtime access. The production version will serve as a comprehensive quantum hardware management solution, streamlining integration for researchers.

As quantum computing advances beyond the NISQ era, tools like Q-AIM are essential for bridging current limitations and future capabilities.

8 REFERENCES

- [BBB⁺24] Thomas Beck, Alessandro Baroni, Ryan Bennink, Gilles Buchs, et al. Integrating quantum computing resources into scientific hpc ecosystems. *Future Generation Computer Systems*, 161:11–25, 2024.
- [BBMC20] Bela Bauer, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Chan. Quantum algorithms for quantum chemistry and quantum materials science. *Chemical Reviews*, 120(22):12685–12717, Oct 2020.
- [CAF⁺24] Marcello Caleffi, Michele Amoretti, Davide Ferrari, Jessica Illiano, et al. Distributed quantum computing: A survey. *Computer Networks*, 254:110672, 2024.
- [CBSG17] Andrew W. Cross, Lev S. Bishop, John A. Smolin, and Jay M. Gambetta. Open quantum assembly language, 2017.
- [CJAA⁺22] Andrew Cross, Ali Javadi-Abhari, Thomas Alexander, Niel De Beaudrap, et al. Openqasm 3: A broader and deeper quantum assembly language. *ACM Transactions on Quantum Computing*, 3(3), sep 2022.
- [CVPP⁺25] F. Javier Cardama, Jorge Vázquez-Pérez, César Piñeiro, Juan C. Pichel, et al. Review of intermediate representations for quantum computing. *The Journal of Supercomputing*, 81(2), Jan 2025.
- [DPJ⁺24] Philip Döbler, Jannik Pflieger, Fengping Jin, Hans De Raedt, et al. Scalable general error mitigation for quantum circuits, 2024.
- [GARV⁺22] Jose Garcia-Alonso, Javier Rojo, David Valencia, Enrique Moguel, et al. Quantum software as a service through a quantum api gateway. *IEEE Internet Computing*, 26(1):34–41, 2022.
- [GCA⁺21] M. Grossi, L. Crippa, A. Aita, G. Bartoli, et al. A serverless cloud integration for quantum computing, 2021.
- [GHG⁺24] Muhammed Golec, Emir Sahin Hatay, Mustafa Golec, Murat Uyar, et al. Quantum cloud computing: Trends and challenges. *Journal of Economy and Technology*, 2:190–199, 2024.
- [GRTZ02] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.
- [HML⁺21] Travis S. Humble, Alexander McCaskey, Dmitry I. Lyakh, Meenambika Gowrishankar, et al. Quantum computers for high-performance computing. *IEEE Micro*, 41(5):15–23, 2021.
- [Jat24] Manpreet Singh Jattana. Quantum annealer accelerates the variational quantum eigensolver in a triple-hybrid algorithm. *Physica Scripta*, 99(9):095117, aug 2024.

- [JATK⁺24] Ali Javadi-Abhari, Matthew Treinish, Kevin Krsulich, Christopher J. Wood, et al. Quantum computing with qiskit, 2024.
- [JJDRM20] Manpreet Singh Jattana, Fengping Jin, Hans De Raedt, and Kristel Michiels. General error mitigation for quantum circuits. *Quantum Information Processing*, 19(11):414, 2020.
- [JJDRM22] Manpreet Singh Jattana, Fengping Jin, Hans De Raedt, and Kristel Michiels. Assessment of the variational quantum eigensolver: Application to the heisenberg model. *Frontiers in Physics*, 10, 2022.
- [JJDRM23] Manpreet Singh Jattana, Fengping Jin, Hans De Raedt, and Kristel Michiels. Improved variational quantum eigensolver via quasidynamical evolution. *Phys. Rev. Appl.*, 19:024047, Feb 2023.
- [MFML23] Attila Csaba Marosi, Attila Farkas, Tamás Máray, and Róbert Lovas. Toward a quantum-science gateway: A hybrid reference architecture facilitating quantum computing capabilities for cloud utilization. *IEEE Access*, 11:143913–143924, 2023.
- [MRV22] E. Moguel, J. Rojo, and D. et al. Valencia. Quantum service-oriented computing: current landscape and challenges. *Software Quality Journal*, 30:983–1002, 2022.
- [MWB23] David Moreau, Kristina Wiebels, and Carl Boettiger. Containers for computational reproducibility. *Nature Reviews Methods Primers*, 3(1):50, 2023.
- [NUB24] Hoa T. Nguyen, Muhammad Usman, and Rajkumar Buyya. Qfaas: A serverless function-as-a-service framework for quantum computing. *Future Generation Computer Systems*, 154:281–300, 2024.
- [OTC⁺20] Victory Omole, Akhilesh Tyagi, Calista Carey, AJ Hanus, et al. Cirq: A python framework for creating, editing, and invoking quantum circuits. *00*, 2020.
- [PAB⁺20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, et al. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.
- [PMS⁺14] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, et al. A variational eigenvalue solver on a quantum processor. *Nature Communications*, 5:4213, 2014.
- [QBB⁺21] Quantum Technology and Application Consortium – QUTAC, Andreas Bayerstadler, Guillaume Becquin, Julia Binder, et al. Industry quantum computing applications. *EPJ Quantum Technol.*, 8(1):25, 2021.
- [Qis25] Qiskit Development Team. Qiskit aer QasmSimulator backend. https://qiskit.github.io/qiskit-aer/stubs/qiskit_aer.QasmSimulator.html, 2025. Accessed: 2025-02-10.
- [RTL⁺22] Martin Ruefenacht, Bruno G Taketani, PASI Lähtenmäki, VILLE Bergholm, et al. Bringing quantum acceleration to supercomputers. *IQM/LRZ Technical Report*, https://www.quantum.lrz.de/fileadmin/QIC/Downloads/IQM_HPC-QC-Integration-White_paper.pdf, 2022.
- [SBL⁺21] Marie Salm, Johanna Barzen, Frank Leymann, Benjamin Weder, et al. Automating the comparison of quantum compilers for quantum circuits. In Johanna Barzen, editor, *Service-Oriented Computing*, pages 64–80, Cham, 2021. Springer International Publishing.
- [Ser06] J Sermersheim. Rfc 4511: Lightweight directory access protocol (ldap): The protocol, 2006.
- [SP21] Haryono Soeparno and Anzaludin Sam-singa Perbangsa. Cloud quantum computing concept and development: A systematic literature review. *Procedia Computer Science*, 179:944–954, 2021. 5th International Conference on Computer Science and Computational Intelligence 2020.
- [SRKS22] Martin Schulz, Martin Ruefenacht, Dieter Kranzlmüller, and Laura Brandon Schulz. Accelerating hpc with quantum computing: It is a software challenge too. *Computing in Science and Engineering*, 24(4):60–64, 2022.
- [WVMN19] Robert Wille, Rod Van Meter, and Yehuda Naveh. Ibm’s qiskit tool chain: Working with and developing for real quantum computers. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1234–1240, 2019.
- [YIL⁺21] Ed Younis, Costin C Iancu, Wim Lavrijsen, Marc Davis, et al. Berkeley quantum synthesis toolkit (bqskit) v1, 04 2021.

Design and Evaluation of Quantum OFDMA Under Depolarization Conditions

Hussein Tuama

Department of Networked
Systems and Services,
Faculty of Electrical
Engineering and
Informatics, Budapest
University of Technology
and Economics.
Hungary (1117),
Budapest
ahtuama@hit.bme.hu

Sándor Imre

Department of Networked
Systems and Services,
Faculty of Electrical
Engineering and
Informatics, Budapest
University of Technology
and Economics.
Hungary (1117),
Budapest
imre@hit.bme.hu

ABSTRACT

Orthogonal frequency division multiple access (OFDMA) is a key technology scheme to enhance the resource utilization efficiency in modern wireless communication systems including LTE and 5G. On the other hand, OFDMA encounters noise, channel interferences, scalability, and spectral efficiency problems. To overcome these drawbacks, this work presents a novel communication scheme that combines quantum communication methods as a novel resource adaptive for OFDMA systems called Q-OFDMA. The Quantum Fourier Transform (QFT) is applied as a core module to enhance the robustness and efficiency of OFDMA in the presence of a noisy quantum channel. Model performance assessment was carried out via full simulations using the Qiskit quantum simulator, with two simulated use cases: the variation of the depolarizing parameter and the increase in the number of users. The results confirm that the Q-OFDMA model is significantly better than the reference quantum communication model, maintaining a lower Bit Error Rate (BER) under different depolarization and user densities.

Keywords

Quantum Communication, Orthogonal Frequency Division Multiple Access, Quantum Fourier Transform, Depolarizing Channel, Bit Error Rate.

1 INTRODUCTION

Classical communication theory is fundamentally rooted in classical physics and currently faces significant challenges due to the growing demand and increased user density. In this context, integrating quantum techniques has appeared as a potential solution[Che21, Mit20]. Quantum mechanics provides the essential theoretical framework for the development of quantum computing (QC) and quantum information processing (QIP). This framework is based on specific mathematical formulations and comprehensive scientific models, ensuring the clarity, consistency, and predictive accuracy inherent to quantum theory[NC10].

As a result, phenomena that were once regarded as abstract in quantum mechanics are now becoming accessible through experiments, paving the way for significant advancements in communication and information technology. These innovations could transform the methods of data transmission, processing, and security in our increasingly interconnected world[IG12].

Integrating quantum technologies into communication systems has emerged as a prominent research direction in contemporary communication theory, promising significant advancements over classical systems. In general, communication systems are comprised of three stages of encoding information, sending it through a communication channel, and decoding at the receiver to recover the original information[ZWR⁺24]. Figure 1 is a schematic of the difference between classical and quantum communication systems[Car15].

In the classical communication systems, data is initially mapped into a physical signal through a classical to classical ($C \rightarrow C$) mapping by the encoding stage. Then these signals get transmitted through the chan-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

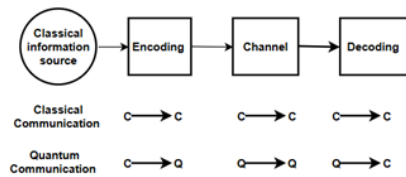


Figure 1: Classical/Quantum communication model

nel, in which some distortion as well as noise effects take place. Corrupted signals are then classically decoded to recover the original information. Quantum communication, however, uses quantum encoding techniques to encode classical symbols into quantum states. These quantum states are sent through the quantum channels, in which quantum noises, such as decoherence, will corrupt the quality[Zur03]. At the receiving station, quantum decoding decodes the quantum states back to classical symbols. At each sampling period, the receiver conducts quantum measurements and infers, based on the observed outcome, the most likely transmitted quantum state. In general, quantum communication exploits quantum mechanics effects, and the important features include a higher level of security, improved noise immunity, and higher information transmission efficiency than the classical case.

Multiple Access Techniques

Classical wireless communications use several multiple access types like Time Division Multiple Access (TDMA), Orthogonal Frequency Division Multiple Access (OFDMA), Code Division Multiple Access (CDMA), and Non-Orthogonal Multiple Access (NOMA). All these schemes are meant to enable congestion tolerant use of spectrum-limited resources[MD21]. TDMA assigns dedicated time slots to each user, minimizing the chance of collision within the medium. OFDMA allocates subcarriers of the frequency to users, which improves the robustness against multipath fading and interference[FF19]. CDMA distinguishes users with unique spreading codes, which may receive simultaneous transmission over their entire bandwidth[GAI⁺21]. NOMA, on the other hand, allows multiple users to utilize partially overlapping resources from each other, utilizing power differences and advanced signal processing[LYD⁺22]. Benefits of utilizing these types of methods are to mitigate interference, using the channel more efficiently to maintain maximum spectrum efficiency, and preserving QoS to attain a high level of service. These methods help to improve the performance, reliability, and scalability of recent wireless communications systems.

Among these methods, OFDMA has gained considerable attention due to its robustness against multipath

fading, efficient spectrum allocation, and strong performance in high-data-rate environments. Despite its benefits, classical OFDMA still faces limitations, particularly regarding spectral efficiency, noise resilience, and scalability. To address these limitations, this paper explores the potential integration of quantum communication principles with OFDMA.

In the development of a scalable quantum multiple access scheme, several core challenges must be considered to ensure reliable performance. A primary concern involves supporting the simultaneous transmission of quantum data across multiple users while preserving the integrity of each quantum state. Additionally, quantum channels are inherently vulnerable to various forms of noise such as decoherence, phase shifts, and quantum errors, which can severely impact the quality and reliability of communication. Overcoming these noise-induced degradations is crucial for maintaining system performance. Another significant issue is the design of quantum encoding and decoding strategies that can effectively separate user data while preserving orthogonality among quantum states.

In this paper, we address the aforementioned challenges by proposing and analyzing a novel model that integrates quantum communication techniques with OFDMA. The quantum OFDMA framework leverages core quantum principles, including quantum encoding, the QFT, and quantum channel modeling, to enhance the performance of conventional OFDMA systems. By incorporating these quantum techniques, the model aims to significantly improve transmission efficiency, reduce susceptibility to quantum noise, and support more scalable multi-user communication. This integration not only enhances system robustness under depolarizing noise conditions but also lays the groundwork for future developments in quantum-assisted wireless communication.

The rest of this paper is organized as follows: Related Work in section 2, we review related work and discuss notable developments for quantum computing techniques to be used in communication systems and in multiple access scenarios. In Section 3 we present the classical OFDMA model and also we describe its structure as well as its drawbacks. In Section 4 we present the Q-OFDMA system which includes its quantum encoding, QFT and quantum channel model. Section 5 describes the simulation setup and gives quantitative results in terms of bit error rate for different depolarizing noise regimes. Section 6 concludes the paper and provides insight on the future work that can be done to extend the Q-OFDMA model and investigating its practical application.

2 RELATED WORK

Over the past few years, the research community has widely investigated quantum computing and quantum

information technology to improve classical communication systems. Several studies have explored the integration of quantum techniques to enhance data security, reliability, and overall performance. For example, in [Mit20] researchers have investigated how the advent of quantum computing affects the security of communication systems. Specifically, a study of the 5G system revealed that quantum computing could compromise current security methods, and many researchers emphasized the urgent need to use encryption methods that can resist quantum attacks in communication systems. The article [WR22] offers an exciting view of how quantum information technology (QIT) can be used in future 6G systems, looking at how quantum computing, quantum communication, and quantum sensing can work together to enhance 6G performance. Their work lays the foundation for utilizing QIT to facilitate secure quantum communication techniques such as quantum key distribution (QKD), improve resource management in wireless environments using quantum computing, and propose innovative concepts for quantum-assisted radio access networks (qRAN) and quantum non-terrestrial networks (qNTN).

Another prominent approach focuses on enhancing the reliability of quantum communication through the development of error correction codes tailored to certain noise models. In the present framework, the authors in [LLPS23] developed a code designed to correct errors in quantum systems specifically for a fully correlated noise channel where all qubits experience the same unitary error. Their method involves a recursive design and a new form of decomposition for encoding and decoding operators into quantum gates that can be effectively implemented on IBM quantum computers. This improvement could lead to better ways to keep quantum data safe, highlighting the importance of optimizing gates for using real quantum computers. In [FP14], the authors developed a formal equivalence between the QEC decoding and the contraction of tensor networks, providing a single framework to analyze quantum codes.

Recent studies propose novel quantum measurement techniques that aim to minimize the probability of error in distinguishing non-orthogonal quantum states. The work in [SR22] evidences the importance of the quantum nature of the noise and of the real measurement procedures in assessing the real decoding results. Moreover, in [CW24] the authors have studied the BER performance of the considered quantum receiver as a function of the signal power and for different detection strategies. These results indicate the enormous potential for quantum detection schemes to improve the communication reliability of quantum-limited environments. Efforts have been made to deploy QC methods in the context of classical multiple access systems to improve the performance in terms of signal

processing. For example, Grover quantum search algorithm [CKS17] has been used for signal detection in OFDMA and SC-FDMA systems, which achieves low-complexity and maximum-likelihood detection schemes but still works well in terms of accuracy performance under multiple user scenarios with minor computational complexity overhead [MZK24]. Additionally, a method called quantum key distribution using orthogonal frequency-division multiplexing (OFDM-QKD) has been proposed to secure communication at high speeds while using less bandwidth in trusted-node quantum networks. The method in [BRS15] uses all-optical OFDM encoders and decoders to parallelize key generation and cope with issues such as time misalignment and crosstalk noise by designing active decoding techniques to improve throughput and scalability.

In addition, recent literature has studied new quantum communication concepts that exploit classical multiple access and quantum communication mechanisms. In [AK21], the authors presented a quantum communication method that uses Code Division Multiple Access (CDMA) and QFT to extend the short timing of the source signals. They showed that their scheme was superior to the corresponding classical multiple access methods for quantum communications tasks, both in its noise robustness and ability to accommodate multiple users, showing the potential of quantum transformations in the search for new improvements on classical multiple access methods for quantum communications. Additionally, they developed a new scheme for QCDMA, drawing inspiration from various works, including [RS21, ASI24]. Their method enables numerous users to utilize a quantum communication channel by encoding quantum light pulses with pseudorandom spectral phase patterns. While such encoded pulses are sent to all users using a quantum star coupler, only the legitimate user can perform the correct decoding, recovering the original signal. The model can explain different types of input states, like coherent and number states, and its findings show the significance of other key quantum effects, such as entanglement and Heisenberg uncertainty principle.

While previous studies have demonstrated the benefits of quantum techniques in classical communication contexts, they often overlook scalable integration within orthogonal multi-user frameworks. To address this, the present paper investigates integrating quantum technologies into OFDMA to overcome classical OFDMA limitations. We propose a quantum-enhanced OFDMA (Q-OFDMA) system using quantum encoding and QFT techniques. Our goal is to improve system robustness, spectral efficiency, and BER performance under noisy quantum channel conditions. The study specifically evaluates how BER varies with different numbers of users and depolarizing noise levels. Particular empha-

sis is placed on analyzing channels characterized by varying depolarization parameters. This approach aims to advance multi-user communication and guide future developments in quantum-assisted wireless communication systems.

3 CLASSICAL OFDMA MODEL

Orthogonal frequency division multiple access (OFDMA) is an advanced version of OFDM[WLZL08]. It works by dividing the available subcarriers among multiple users, enabling the exploitation of multiuser diversity[SQB⁺21]. This characteristic makes OFDMA particularly suitable for cellular broadband wireless networks such as LTE, 5G networks, and Wi-Fi technologies[FCR24]. However, efficiently utilizing OFDMA in wireless broadband systems involves significant challenges. One critical challenge is jointly allocating subcarriers and transmission power among users in both uplink and downlink scenarios[ZZDS21]. This allocation must fulfill specific Quality of Service (QoS) criteria like target bit rate, acceptable latency, and fairness constraints[YHN⁺23]. The classical OFDMA transmission scheme illustrated in Figure 2 consists of multiple stages designed to enable efficient multi-user communication over a shared frequency channel. At the transmitter side, each of the N users first apply an encoding operation to their digital input stream. Following the encoding stage, in order to perform an

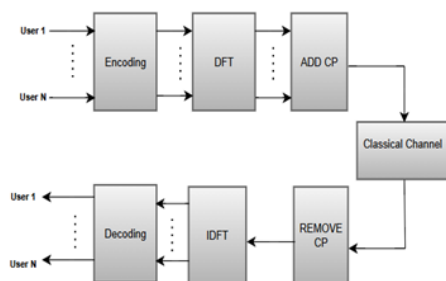


Figure 2: Classical OFDMA system

efficient multicarrier modulation, the discrete Fourier transform (DFT) is then applied by the system. The orthogonality of the subcarriers is required for the distinction of signals and for the suppression of inter-carrier interference. The DFT further simplifies the channel equalization as frequency-domain operations are possible, which is a particularly important property under frequency-selective fading channels. At the transmitter, DFT is employed to transform a group of modulated frequency-domain data symbols into an aggregate time-domain signal. This time-domain signal is the OFDMA waveform, which is able to transmit simultaneously across the space and over orthogonal subcarriers and realizing dynamic resource allocation

among users. The transformation for the n-th user's data is mathematically represented as:

$$X_n(k) = \sum_{t=0}^{B-1} x_n(t) \cdot e^{-j\frac{2\pi kt}{B}}, \quad k = 0, 1, \dots, B-1 \quad (1)$$

where x_n is the encoded time-domain signal for user n, B is the total number of subcarriers (equal to the OFDM symbol size), and $X_n(k)$ is the frequency-domain representation. To mitigate inter-symbol interference (ISI) caused by multipath fading, a Cyclic Prefix (CP) of length L is appended to each OFDMA symbol before transmission. The signal is then transmitted over a classical wireless channel. On the receiver side, the cyclic prefix is removed to restore the orthogonality of the subcarriers. The received time-domain signals are then passed through the Inverse Discrete Fourier Transform (IDFT) to revert to the original domain:

$$\hat{x}_n(t) = \frac{1}{B} \sum_{k=0}^{B-1} \hat{X}_n(k) \cdot e^{j\frac{2\pi kt}{B}}, \quad t = 0, 1, \dots, B-1 \quad (2)$$

Where $\hat{X}_n(k)$ represents the received frequency-domain signal, possibly affected by channel noise and distortion. Finally, the demodulated data is passed through a decoding stage to recover the transmitted information. The overall received signal after CP removal and before DFT can be expressed as:

$$y(i, t) = \sum_{n=1}^N x_n(i, t) * h(t) + v(i, t) \quad (3)$$

where $h(t)$ denotes the channel impulse response, * represents the convolution operation, and $v(i, t)$ is the additive white Gaussian noise. This structured framework enables the dynamic and efficient allocation of subcarriers to multiple users, achieving robustness and scalability in varying channel environments. However, classical OFDMA still faces limitations in noise resilience, spectral efficiency, and security, particularly in dense multi-user environments. Incorporating quantum information processing into this scenario, quantum encoding and QFT techniques can further enhance system performance. Specifically, quantum-based methods improve resistance to noise, enabling more robust communication. Thus, quantum approaches significantly benefit channel estimation accuracy, reliability, and scalability of the uplink OFDMA system.

4 QUANTUM OFDMA MODEL

The proposed quantum multiple access model, which is an analog of the classical OFDMA present in section 3, consists of several segments including quantum encoding, QFT for the transmitting side, then the quantum data is processed to the quantum version of the channel. On the receiver side, the IQFT and measurement

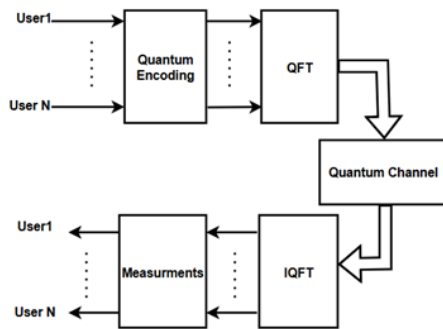


Figure 3: Quantum OFDMA system

are implemented to get user data back. The architecture of Q-OFDMA is illustrated in Figure 3. One of the most remarkable advantages of quantum systems is their ability to support smooth transitions between classical and quantum domains. In our Q-OFDMA model, this property enables a seamless exchange of information without relying on mechanisms such as the cyclic prefix, which is essential in traditional OFDMA systems. The absence of a cyclic prefix is made possible by the continuous-state propagation inherent in quantum mechanics. This scheme simplifies the process of quantum transmission and promotes the efficiency of transmitting and the reliability of receiving the quantum state. Thus, the Q-OFDMA model represents a considerable improvement for next-generation quantum communication systems.

4.1 Quantum Encoding

Initially, we assume the presence of pure orthogonal quantum states. Under this assumption, the information transmitted over a quantum communication channel can be explained similarly to classical information theory [KPTZ22]. The transmitter generates classical symbols a_i , which correspond directly to orthogonal quantum states. These symbols belong to a classical alphabet $A = \{|a_1\rangle, \dots, |a_N\rangle\}$ and are sent with corresponding probabilities $p_A = \{p_1, \dots, p_N\}$. At the receiver side, the receiver receives these symbols as quantum states from the alphabet $B = \{|b_1\rangle, \dots, |b_N\rangle\}$. These states are modified by the QFT, quantum channel, and IQFT. Importantly, orthogonality between quantum states ensures $\langle b_i | b_j \rangle = 0$ for all $i \neq j$. Consequently, the receiver can perform projective measurements to distinguish the received states. Hence, orthogonal states inherently prevent errors in decoding. Basis encoding is a straightforward method for converting classical information into quantum states. Specifically, it maps an n -bit classical binary string x onto an n -qubit quantum state $|x\rangle = |i_x\rangle$ where each $|i_x\rangle$ represents a computational basis state. For instance, if the classical binary input is 1101, then the resulting quantum state after applying basis encoding would be $|1101\rangle$.

4.2 Quantum Fourier Transform and its Inverse

One crucial transformation used in quantum computing is QFT which is analogous to the DFT used in classical signal processing [CVBY21, RPGE17]. DFT takes an input vector of complex numbers and produces an output vector, also composed of complex numbers. Mathematically, this transformation can be represented as:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

The QFT uses a similar mathematical form, acting on quantum states rather than classical numbers. Specifically, the QFT operates on orthonormal quantum basis states $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$. The transformation of a basis state $|j\rangle$ can be defined as:

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

This transformation is unitary, making it appropriate for implementation on quantum computers. Moreover, the QFT can be represented using a product form, providing an efficient quantum circuit representation [SAI24]. For an n -qubit system with $N = 2^n$ the basis state $|j\rangle$ can be written using binary notation as $|j_1, j_2, \dots, j_n\rangle$

$$|j_1, j_2, \dots, j_n\rangle \rightarrow \frac{1}{2^{n/2}} (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1}} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle) \quad (4)$$

This product formula helps construct efficient quantum circuits that implement the QFT. Such circuits use Hadamard gates and controlled-phase rotation gates, known as R_k , represented as:

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{bmatrix}$$

Applying Hadamard and controlled-phase gates sequentially on qubits transforms the input state according to the QFT definition. At the receiver side, IQFT serves as a foundational operation in quantum computing, particularly when recovering data from the frequency domain. After a quantum state has undergone a QFT, it exists in a superposition where amplitude components represent frequency information across computational basis states. To extract meaningful results and perform measurements in the standard basis, it becomes necessary to apply the IQFT. Mathematically, the IQFT on a basis state $|k\rangle$ in a Hilbert space of dimension N is defined as:

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

This transformation effectively reverses the QFT operation, mapping the state back into the computational basis where each quantum amplitude corresponds to the likelihood of observing a specific classical outcome. The IQFT is essential for is necessary to bring the data back to a state ready for measurement at the end. Thus, in the Q-OFDMA framework, the IQFT not only completes the communication cycle but also ensures orthogonality preservation and efficient multi-user separation, contributing directly to the model's robustness and scalability in quantum multi-access environments.

4.3 Quantum Channel Model

In classical computing, the primary error type is the bit-flip, switching between states 0 and 1. Due to qubit superposition, quantum computing introduces additional error types. These quantum errors include bit-flip, phase flips, and combined bit-phase flips[Kin03, EMCGF19]. The phase flip error changes the quantum state phase, while the bit-phase flip error simultaneously changes both the bit and the phase. Mathematically, these errors can be described using specific Kraus operators[KSS10]:

$$\hat{K}_0 = \sqrt{1 - \frac{p}{2}} \hat{I}, \quad \hat{K}_1^j = \sqrt{\frac{p}{2}} \hat{\sigma}_j$$

In this formulation, $j = x$ represents a bit-flip, $j = z$ a phase flip, and $j = y$ a combined bit-phase flip. Each error has a probability $p/2$, while the probability of no error occurring is $1 - p/2$. These quantum errors are associated with the Pauli matrices $\hat{\sigma}_j$. Noise from the environment can be modeled using different quantum channels. A quantum channel describes the transformation of quantum states. Specifically, it maps an initial density operator ρ to a final density operator ρ_k . This transformation is known as a quantum operation or superoperator. Mathematically, the quantum channel can be expressed using an operator-sum representation[GIN18].

$$\rho_f = \sum_k E_k \rho E_k^\dagger$$

Where, the operators E_k represent the channel actions, referred to as Kraus operators. We consider a depolarizing channel, which acts on a qubit initially described by the density operator $\hat{\sigma}$. The depolarizing channel transforms this qubit into a new state, represented by Pauli operator description and density operator description, as shown in Figure 5.

This channel introduces unbiased noise, causing bit-flip and phase-flip errors with equal probability. Its action on a density operator $\hat{\sigma}$ is given by:

$$\mathcal{E}(\hat{\rho}) = (1 - p)\hat{\rho} + \frac{p}{3}(\hat{\sigma}_x\hat{\rho}\hat{\sigma}_x + \hat{\sigma}_y\hat{\rho}\hat{\sigma}_y + \hat{\sigma}_z\hat{\rho}\hat{\sigma}_z)$$

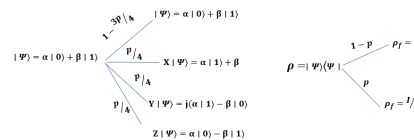


Figure 4: Depolarizing channel representations

However, combining these different error interactions incoherently might be conceptually questionable. This issue arises because bit-flip, phase-flip, and bit-phase flip errors do not commute. where the depolarizing parameter p lies between 0 and 1. The depolarizing channel is relevant for several reasons. First, it provides a standard model for noise processes commonly encountered in quantum systems. This type of noise model has wide-ranging applications in quantum information processing. Second, quantum parameter estimation demonstrates the advantages of quantum methods over classical techniques.

5 SIMULATION RESULTS

In this paper, the simulation mainly focused on analyzing the BER performance of a Q-OFDMA system and compare the results with the quantum reference model. The assessment was carried out using comprehensive simulations. These simulations were conducted utilizing the Qiskit platform and Python. The quantum simulator employed in the evaluation was the Qiskit Aer package. Qiskit Aer allows for accurate modeling of quantum computing processes. Through this simulation approach, the accuracy and reliability of the results were validated. Consequently, the obtained findings effectively demonstrated the BER characteristics within the Q-OFDMA framework under the depolarizing noise conditions.

We consider classical information represented by symbols. These symbols form a sequence of classical bits. Initially, these classical bits undergo encoding to transform them into quantum states by basic encoding. Thus, a classical-to-quantum ($C \rightarrow Q$) mapping is performed. This mapping employs a comprehensive look-up table containing all possible n -bit binary sequences. Such a table is essential for verifying the accuracy of the received quantum states. Accordingly, the initial quantum state is prepared based on this mapping. This quantum state consists of four qubits. After preparation, the quantum state undergoes a QFT. The QFT is an essential step in the process. It transforms the encoded quantum information into the Fourier basis representation. This representation simplifies subsequent processing and analysis steps. Additionally, the simulation assumes that all possible codewords emitted from the source have an equal probability of occurrence. Such a uniform probability distribution assumption simplifies the modeling process. It enables

easier initial analysis and helps interpret the simulation results.

In the Q-OFDMA channel scenario, once the QFT has been applied, each qubit is individually processed through a depolarizing quantum channel. This depolarizing channel has parameters defined within a specific and controlled range. This step effectively represents the inherent noise typically present in real quantum communication channels.

The introduction of such channel noise is crucial, as it realistically mimics environmental disturbances affecting quantum states during transmission. For a thorough and detailed investigation, the simulation systematically explores all possible combinations and sequences of channel operations on each quantum state. Such a comprehensive simulation strategy provides valuable insights by explicitly evaluating how channel-induced noise influences quantum system performance. It also ensures that the complexity and subtle interactions of noise effects within the Q-OFDMA system are thoroughly understood and accurately captured. Consequently, this approach significantly contributes to better identifying system vulnerabilities and performance limitations under realistic quantum channel conditions.

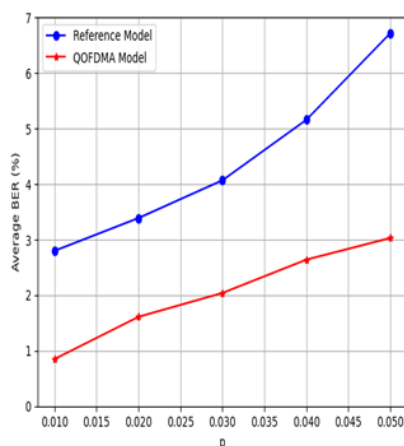


Figure 5: The Average BER With Different values of Depolarizing parameter

Figure 5 illustrates the simulation results comparing the average bit error rate (BER) performance between the reference quantum communication model and the proposed Q-OFDMA model. In this scenario, the depolarization parameter (p) is varied systematically from 0.01 to 0.05. As depicted clearly, the BER for both models increases gradually with higher values of the depolarization parameter. However, the Q-OFDMA model consistently exhibits significantly lower BER compared to the reference quantum model across the entire tested range. This enhanced BER performance in the Q-OFDMA model can be attributed to the effective integration of quantum encoding techniques and the application of QFT. Specifically, these quantum-enhanced

approaches enable better mitigation of noise and interference introduced by the depolarizing quantum channel. Consequently, the Q-OFDMA model achieves greater resilience and stability, clearly illustrating its potential for improving the reliability and robustness of quantum-based wireless Q-OFDMA communication systems under noisy quantum channel conditions.

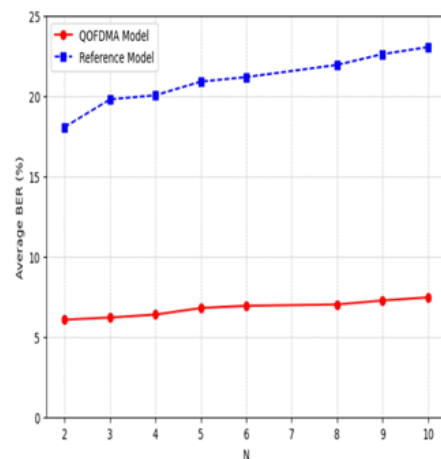


Figure 6: The Average BER with Increasing Number of Users

Figure 6 considers a scenario with a fixed depolarizing parameter, evaluating the impact of varying the number of users from 2 to 10 on the average BER performance. The results indicate that as the number of users increases, the average BER gradually rises for both the reference model and the Q-OFDMA model. This occurs due to the increased likelihood of errors introduced by the depolarization channel as more qubits (representing more users) simultaneously pass through the noisy quantum environment. Specifically, a larger number of users leads to a greater probability of quantum state corruption and interference between user signals, causing higher BER values. Despite this challenge, the Q-OFDMA model consistently achieves significantly lower BER compared to the reference model across the entire range.

6 CONCLUSION

This paper introduced and evaluated a novel Quantum OFDMA (Q-OFDMA) framework designed to enhance wireless communication performance under depolarizing quantum channel conditions. By integrating quantum encoding techniques and the QFT, the proposed Q-OFDMA system demonstrated significant improvements in BER performance compared to a reference quantum communication model. Through rigorous simulations using the Qiskit simulator, the model's robustness was verified under two scenarios: varying depolarization levels and increasing user density. In both cases, Q-OFDMA maintained a consistently lower

BER, affirming its capability to mitigate quantum noise and scale effectively with multiple users.

The results validate the feasibility of applying quantum principles in practical multiple-access scenarios. The Q-OFDMA model not only strengthens noise resilience but also highlights the potential of quantum communication paradigms to meet the growing demand for secure and efficient data transmission in future 6G and beyond networks.

7 ACKNOWLEDGMENTS

The research was supported by the European Union's Digital Europe Programme under Grant Agreement No. 101081247 (QCIHungary) and by the Parliamentary State Secretariat of the Ministry of Public Administration and Regional Development.

8 REFERENCES

- [AK21] M Anand and Pawan Tej Kolusu. A novel multi-user quantum communication system using cdma and quantum fourier transform. In *Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings*, pages 79–90. Springer, 2021.
- [ASI24] Mohammed R Almasaoodi, Abdulbasit MA Sabaawi, and Sándor Imre. Quantum ofdm: A novel approach to qubit error minimization. In *2024 14th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pages 53–58. IEEE, 2024.
- [BRS15] Sima Bahrani, Mohsen Razavi, and Jawad A Salehi. Orthogonal frequency-division multiplexed quantum key distribution. *Journal of Lightwave Technology*, 33(23):4687–4698, 2015.
- [Car15] Gianfranco Cariolaro. *Quantum communications*, volume 2. Springer, 2015.
- [Che21] Jiajun Chen. Review on quantum communication and quantum computation. In *Journal of Physics: Conference Series*, volume 1865, page 022008. IOP Publishing, 2021.
- [CKS17] Indranil Chakrabarty, Shahzor Khan, and Vanshdeep Singh. Dynamic grover search: Applications in recommendation systems and optimization problems. *Quantum Information Processing*, 16:1–21, 2017.
- [CVBY21] Daan Camps, Roel Van Beeumen, and Chao Yang. Quantum fourier transform revisited. *Numerical Linear Algebra with Applications*, 28(1):e2331, 2021.
- [CW24] Yoni Choukroun and Lior Wolf. Deep quantum error correction. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, pages 64–72, 2024.
- [EMCGF19] Josu Etchezarreta Martinez, Pedro M Crespo, and Javier Garcia-Frías. Depolarizing channel mismatch and estimation protocols for quantum turbo codes. *Entropy*, 21(12):1133, 2019.
- [FCR24] Abdulhalim Fayad, Tibor Cinkler, and Jacek Rak. Toward 6g optical fronthaul: A survey on enabling technologies and research perspectives. *IEEE Communications Surveys & Tutorials*, 2024.
- [FF19] Saleh Faruque and Saleh Faruque. Time division multiple access (tdma). *Radio Frequency Multiple Access Techniques Made Easy*, pages 35–43, 2019.
- [FP14] Andrew J Ferris and David Poulin. Tensor networks and quantum error correction. *Physical review letters*, 113(3):030501, 2014.
- [GAI⁺21] Alaan Ghazi, SA Aljunid, Syed Zulka-rnain Syed Idrus, CBM Rashidi, Aras Al-dawoodi, Baban A Mahmood, Alaa Fareed, Mohammed U Zaenal, Nameer Hashim Qasim, and Ranjdr M Rafeeq. A systematic review of multi-mode fiber based on dimensional code in optical-cdma. In *Journal of Physics: Conference Series*, volume 1860, page 012016. IOP Publishing, 2021.
- [GIN18] Laszlo Gyongyosi, Sandor Imre, and Hung Viet Nguyen. A survey on quantum channel capacities. *IEEE Communications Surveys & Tutorials*, 20(2):1149–1205, 2018.
- [IG12] Sandor Imre and Laszlo Gyongyosi. *Advanced quantum communications: an engineering approach*. John Wiley & Sons, 2012.
- [Kin03] Christopher King. The capacity of the quantum depolarizing channel. *IEEE Transactions on Information Theory*, 49(1):221–229, 2003.
- [KPTŻ22] Kamil Korzekwa, Zbigniew Puchała, Marco Tomamichel, and Karol Życzkowski. Encoding classical information into quantum resources. *IEEE Transactions on Information Theory*, 68(7):4518–4530, 2022.

- [KSS10] AB Klimov and LL Sánchez-Soto. Depolarization for quantum channels with higher symmetries. *Physica Scripta*, 2010(T140):014009, 2010.
- [LLPS23] Chi-Kwong Li, Yuqiao Li, Diane Christine Pelejo, and Sage Stanish. Quantum error correction scheme for fully-correlated noise. *Quantum Information Processing*, 22(8):310, 2023.
- [LYD⁺22] Yuanwei Liu, Wenqiang Yi, Zhiguo Ding, Xiao Liu, Octavia A Dobre, and Naofal Al-Dhahir. Developing noma to next generation multiple access: Future vision and research opportunities. *IEEE Wireless Communications*, 29(6):120–127, 2022.
- [MD21] Harshita Mathur and T Deepa. A survey on advanced multiple access techniques for 5g and beyond wireless communications. *Wireless Personal Communications*, 118(2):1775–1792, 2021.
- [Mit20] Chris J Mitchell. The impact of quantum computing on real-world security: A 5g case study. *Computers & Security*, 93:101825, 2020.
- [MZK24] Swaraj Mondal, Nazmun Nahar Zarin, and Mohammad Ismat Kadir. Grover’s quantum search for the signal detection of ofdma downlink and sc-fdma uplink. In *2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEE-ICT)*, pages 1234–1239. IEEE, 2024.
- [NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
- [RPGE17] Lidia Ruiz-Perez and Juan Carlos Garcia-Escartin. Quantum arithmetic with the quantum fourier transform. *Quantum Information Processing*, 16:1–14, 2017.
- [RS21] Mohammad Rezai and Jawad A Salehi. Quantum cdma communication systems. *IEEE Transactions on Information Theory*, 67(8):5526–5547, 2021.
- [SAI24] Abdulbasit MA Sabaawi, Mohammed R Almasaoodi, and Sándor Imre. Exploiting ofdm method for quantum communication. *Quantum Information Processing*, 23(7):256, 2024.
- [SQB⁺21] Pir Meher Ali Shah, Shahryar Shafique Qureshi, Rizwan Aslam Butt, Sevia Mahdaliza Idrus, and Jawad Mirza. Design and analysis of 5g network architecture with orthogonal frequency division multiple access based passive optical network. *Optical Fiber Technology*, 67:102678, 2021.
- [SR22] Mummadi Swathi and Bhawana Rudra. Novel encoding method for quantum error correction. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1001–1005. IEEE, 2022.
- [WLZL08] Yi Wang, Lihua Li, Ping Zhang, and Zemin Liu. Dft-based channel estimation with symmetric extension for ofdma systems. *EURASIP Journal on Wireless Communications and Networking*, 2009:1–8, 2008.
- [WR22] Chonggang Wang and Akbar Rahman. Quantum-enabled 6g wireless networks: Opportunities and challenges. *IEEE Wireless Communications*, 29(1):58–69, 2022.
- [YHN⁺23] Xin Yuan, Shuyan Hu, Wei Ni, Ren Ping Liu, and Xin Wang. Joint user, channel, modulation-coding selection, and ris configuration for jamming resistance in multiuser ofdma systems. *IEEE Transactions on Communications*, 71(3):1631–1645, 2023.
- [Zur03] Wojciech Hubert Zurek. Decoherence, einselection, and the quantum origins of the classical. *Reviews of modern physics*, 75(3):715, 2003.
- [ZWR⁺24] Wei Zhao, Tangjie Weng, Yue Ruan, Zhi Liu, Xuanguo Wu, Xiao Zheng, and Nei Kato. Quantum computing in wireless communications and networking: A tutorial-cum-survey. *IEEE Communications Surveys & Tutorials*, 2024.
- [ZZDS21] Shuhao Zeng, Hongliang Zhang, Boya Di, and Lingyang Song. Trajectory optimization and resource allocation for ofdma uav relay networks. *IEEE Transactions on Wireless Communications*, 20(10):6634–6647, 2021.

Quantum Signal-Induced Heap Transform Based Realization of Multi-Qubit Operations

Artyom Grigoryan^[0000-0001-6683-0064]

Department of ECE
The University of Texas at San Antonio
Texas 78249, USA
artyom.grigoryan@utsa.edu

Alex Gomez^[0009-0003-0592-8553]

and Isaac Espinoza
Dept. of ECE
The University of Texas at San Antonio, Texas 78249, USA
alex.gomez@utsa.edu,
isaac.romeroespinoza@my.utsa.edu

Sos Agaian^[0000-0003-4601-4507]

Computer Science Department
College of Staten Island, CUNY
Staten Island, NY 10314, USA
sos.agaian@csi.cuny.edu

ABSTRACT

The article presents a new approach to the decomposition of unitary operations by controlled rotations. A new method of quantum signal-induced heap transform based QR decomposition is described. This transform is an analogue of the discrete transform which is generated by a given signal and uses different paths of processing the data. It is shown that among such paths we can find paths that allow constructing efficient quantum circuits for implementing multi-qubit unitary gates. The case of real unitary matrices is considered. The proposed approach is described in detail in examples and quantum circuits are presented for 2-qubit operations. The general case of r -qubit unitary operations, when $r \geq 2$, is considered similarly.

Keywords

Quantum QR decomposition, quantum heap transform, quantum cosine transform.

1. INTRODUCTION

Many methods of QR-decomposition of real matrices are known. We mention the Givens rotations - [DLHL12], Gramm-Schmidt process and the method of Householder transformations [Hou58]. We stand on the method of QR decomposition. The main goal is to efficiently decompose a given operation into a set of simple gates, for example the controlled rotation gates, phase shift gates, and CNOTs.

In this work, a general method of QR decomposition is described, by using the quantum signal-induced heap transform [AM06],[AG14]. We provide a new view of the QR-decomposition of unitary matrices. The resulting codes allow us to simplify the quantum circuits for the quantum operations, including Hartley and cosine transforms.

2. THE CONCEPT OF DsiHT

The N -point DsiHT is the transform that is generated by a given signal x of length N [AM06]. The main characteristic of the DsiHT is the path, that is, the order in which it is assembled from the basic 2-point

rotations of the generator elements. As example, Fig. 1 shows two diagrams of composing the 4-point DsiHT. Each unitary transform T_k , $k = 1, 2, 3$, is the Givens rotation, which is generally described as

$$T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \pm \sqrt{x^2 + y^2} \\ 0 \end{bmatrix}. \quad (1)$$

Here, the angle is defined by the inputs as $\vartheta = -\arctan(y/x)$, and $\vartheta = \pm\pi/2$ if $x = 0$. The path of the transform, which is shown in part (a), is the traditional path and this transform is called the DsiHT with the weak carriage-wheel (see [AG14] for detail). Two rotations are on the adjacent BPs, that is, 0 and 1, 0 and 2. The last rotation operates on BPs 0 and 3 which are not adjacent. The transform of the generator is equal to $Tx = (\pm\sqrt{x_0^2 + x_1^2 + x_2^2 + x_3^2}, 0, 0, 0)$.

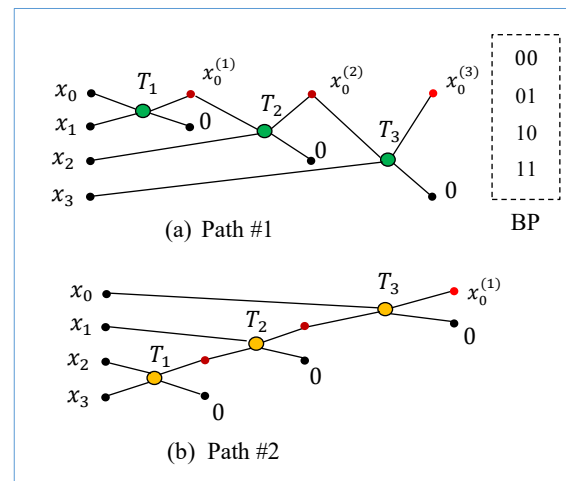


Fig. 1. Two diagrams for the 4-point DsiHTs.

The second path in part (b) also shows that one of rotations operates on the non-adjacent BPs. These BPs are 1 (01) and 2 (10). Figure 2 in part (a) shows path #3 for the 4-point DsiHT. All three rotations in this transform operate on the adjacent BPs. These BPs are 0 and 2, 1 and 3, and then 0 and 1. This path is considered good for building the circuit of the corresponding 2-qubit QsiHT, as shown in part (b).

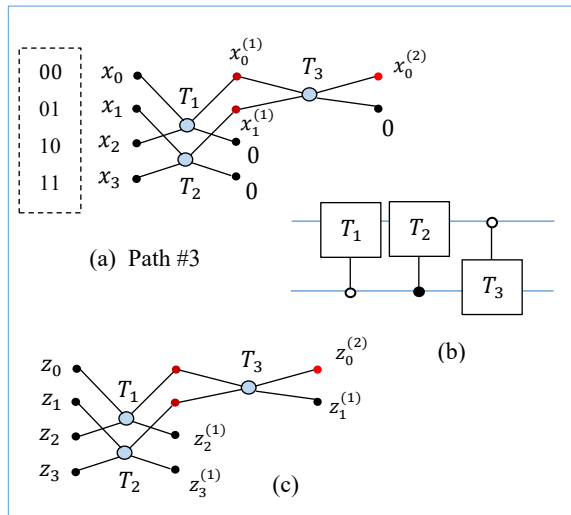


Fig. 2 The diagram and circuit for the 2-qubit QsiHT.

The above three 4-point DsiHTs, H_4 , use different set of angles $A_x = \{\vartheta_1, \vartheta_2, \vartheta_3\}$ which are calculated from the same generator $\mathbf{x} = (x_0, x_1, x_2, x_3)$. The results of the calculations are the same (up to the sign), $H_4(\mathbf{x}) = (x_0^{(k)}, 0, 0, 0) = (\pm\sqrt{x_0^2 + x_1^2 + x_2^2 + x_3^2}, 0, 0, 0)$, $k = 3, 1, 2$. The generated transform operates on an input $\mathbf{z} = (z_0, z_1, z_2, z_3)$ using the same path, as shown in part (c), $H_4(\mathbf{z}) = (z_0^{(2)}, z_1^{(1)}, z_2^{(1)}, z_3^{(1)})$. Such effective paths exist for the N -point DsiHTs, when $N > 2$, and larger this number N , the more such paths can be found. We call them fast paths.

3. DsiHT-BASED DECOMPOSITION

In this section, we describe the QR decomposition of a square matrix A of size $2^r \times 2^r$, $r > 1$, by the Givens rotations. The unitary matrix A is considered with real coefficients. In the QR decomposition of the matrix A , $(2^r - 1)$ DsiHTs are used. This decomposition is illustrated below for a 4×4 unitary matrix,

$$A = \begin{bmatrix} \circ & \circ & \circ & \circ \\ \circ & \circ & \circ & \circ \\ \circ & \circ & \circ & \circ \\ \circ & \circ & \circ & \circ \end{bmatrix} \xrightarrow{\circ: \text{DsiHT}} A_1 = \begin{bmatrix} \star & 0 & 0 & 0 \\ 0 & \star & \star & \star \\ 0 & \star & \star & \star \\ 0 & \star & \star & \star \end{bmatrix} \xrightarrow{\star: \text{DsiHT}} A_2 = \begin{bmatrix} \star & 0 & 0 & 0 \\ 0 & \diamond & 0 & 0 \\ 0 & 0 & \diamond & \diamond \\ 0 & 0 & \diamond & \diamond \end{bmatrix} \xrightarrow{\diamond: \text{DsiHT}} R = \begin{bmatrix} \star & 0 & 0 & 0 \\ 0 & \diamond & 0 & 0 \\ 0 & 0 & \ast & 0 \\ 0 & 0 & 0 & \ast \end{bmatrix}$$

The first DsiHT, H_{0-3} , is generated by the first column of the matrix A and then transforms each of its columns. Six zero coefficients will be obtained in the new matrix A_1 , as shown above. The second 3-point DsiHT, H_{1-3} , is generated by the three components of the second column of the matrix A_1 . This transform is applied to the 3×3 sub-matrix and another four zero coefficients will be obtained in the new matrix A_2 . The last 2-points DsiHT, H_{2-3} , is generated by the last two

coefficients of the third column of A_2 and is applied to its 2×2 sub-matrix. The matrix diagonalization is complete. The matrix R is diagonal with the coefficients ± 1 .

4. TWO-QUBIT OPERATIONS

Triangularization of the square matrix 4×4 in the QR decomposition by three DsiHTs can be written as

$$T: A \rightarrow R = H_{2-3}H_{1-3}H_{0-3}A. \quad (3)$$

Here, the matrix R is a diagonal matrix with the coefficients ± 1 on the diagonal. The diagram of realization of the matrix A is given in Fig. 3.

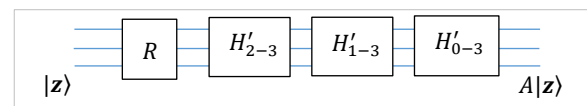


Fig. 3 Block-diagram for a 3-qubit unitary operation.

The operation A can be calculated by the inverse transform as $A = T^{-1}(R) = H'_{0-3}H'_{1-3}H'_{2-3}R$.

The case $N = 4$ (Transform H_{0-3}) The block-diagram and the quantum circuit for the 2-qubit QsiHT are given in Fig. 4.

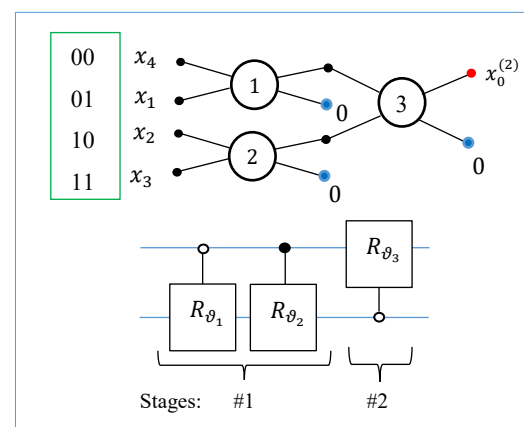


Fig. 4 The block-diagram and circuit of the 2-qubit QsiHT, H_{0-3} , on bit-planes 0-3.

The case $N = 3$ (Transform H_{1-3}) The input is the 2-qubit superposition in the form of $\mathbf{x}_1 = (a, x_1, x_2, x_3)$ and only the last three amplitudes are transformed (see Fig. 5). The rotation on bit-planes 2 (10) and 3 (11) is defined as $R_{\vartheta_1}: (x_2, x_3) \rightarrow (0, \pm\sqrt{x_2^2 + x_3^2})$, with $\vartheta_1 = \text{atan}(x_2/x_3)$.

In the matrix form, the first circuit is described as

$$H_{1-3} = \begin{bmatrix} 1 & \cos \vartheta_2 & -\sin \vartheta_2 \\ & 1 & \\ \sin \vartheta_2 & & \cos \vartheta_2 \end{bmatrix} (I_2 \oplus R_{\vartheta_1}).$$

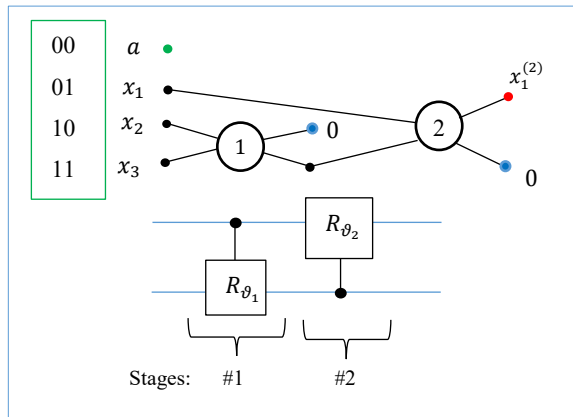


Fig. 5 The block-diagram and the circuit for the 2-qubit QsiHT, H_{1-3} , on bit-planes 1-3.

The case $N = 2$ (Transform H_{2-3}) The input is the 3-qubit superposition in the form of $x_1 = (a, b, x_2, x_3)$ and the transform process only the last two amplitudes. The block-diagram of this 2-qubit QsiHT and the corresponding gate are shown in Fig. 7.

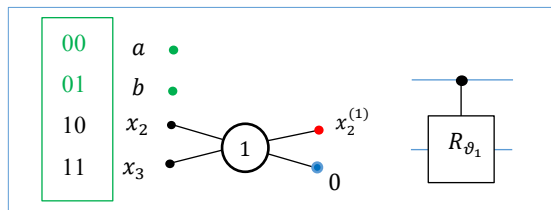


Fig. 6 The block-diagram and the circuit element for the 2-qubit QsiHT, H_{2-3} , on bit-planes 2 and 3.

All these three QsiHTs can be used in the QR decomposition of the 4×4 -matrix, $T(A) = R$. The matrix R is diagonal and the number of controlled rotation gates is equal to $\mu(r) = 3 + 2 + 1 = 6$. The circuits for realization a 2-qubit unitary operation A is given in Fig. 7. Here, $R'_{\vartheta_k} = R_{-\vartheta_k}$, for $k = 1, 2$.

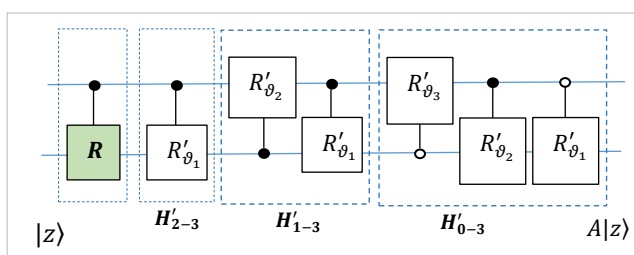


Fig. 7 The quantum circuits for 2-qubit operator.

This circuit is universal. Given a diagonal matrix R and any six angles in Table 1 can be used to generate a 2-qubit operation by the above circuit.

	ϑ_1	ϑ_2	ϑ_3
H_{0-3}	*	*	*
H_{1-3}	*	*	
H_{2-3}	*		

Table 1. 2-qubit operation angles.

If some angles are zero or 90, 180, and 270 degrees, the quantum circuit can be simplified by reducing the number of rotation gates. For comparison, the method described in [FD19] uses $4^2 = 16$ gates.

5. QUANTUM HARTLEY AND COSINE TRANSFORMS

In this section, we apply the described method for computing the quantum Hartley transform (QHyT) and quantum cosine transform (QCT) of type II.

Example 1 (The 2-qubit QCT-II) The N -point DCT-II, X_p , of a signal x_n , is calculated by [RB86]

$$X_p = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x_n \cos\left(\frac{\pi}{N}(n+0.5)p\right),$$

$$p = 0: (N-1),$$

and $X_0 = X_0/\sqrt{2}$. In the $N = 4$ case, the matrix of the transform can be written as

$$A = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1.3066 & 0.5412 & -0.5412 & -1.3066 \\ 1 & -1 & -1 & 1 \\ 0.5412 & -1.3066 & 1.3066 & -0.5412 \end{bmatrix}$$

$\det A = 1$. For example, if the input vector is $z = (1, -3, 2, 3)'/\sqrt{23}$, then the DCT of this vector is equal to $y = Az = (0.3128, -0.5546, 0.5213, 0.5682)'$. The QR decomposition by the DsiHTs with the fast path is accomplished by the rotations with the angles given in Table 2. The matrix R in this decomposition is $R = \text{diag}\{1, 1, 1, 1\} = I_4$, i.e., the identical matrix.

	ϑ_1	ϑ_2	ϑ_3
H_{0-3}	-52.5708°	-28.4221°	-34.6476°
H_{1-3}	249.7543°	256.5505°	
H_{2-3}	-35.2644°		

Table 2. Angles of rotations in the circuit of Fig. 7.

The circuit for the 2-qubit QCT-II includes six controlled rotation gates and is shown in Fig. 8.

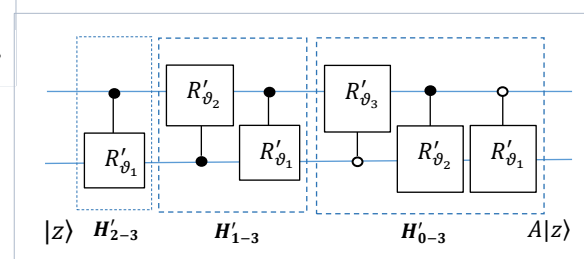


Fig. 8 The quantum circuits for 2-qubit QCT-II.

Example 2 (2-qubit quantum Hartley transform)

The matrix of the N -point transform discrete Hartley transform (DHyT) is equal to

$$A = \frac{1}{\sqrt{N}} \left[\cos\left(\frac{\pi}{N} np\right) + \sin\left(\frac{\pi}{N} np\right) \right]_{n,p=0:(N-1)}.$$

The 4-point transform has the unitary matrix

$$A = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \det A = -1. \quad (12)$$

The QR decomposition of this matrix by the DsiHTs with fast path is accomplished by the rotations with angles given in Table 3. The diagonal matrix is equal to $R = \text{diag}\{1, 1, 1, -1\} = I_2 \oplus Z$.

	ϑ_1	ϑ_2	ϑ_3
H_{0-3}	-45°	-45°	-45°
H_{1-3}	$270^\circ (-90^\circ)$	-90°	
H_{2-3}	225°		

Table 3. Angles of the rotation for 2-qubit QHyT.

Because of angles of 45° , the circuits of the 2-qubit QHyT can be simplified as shown in Fig. 9. It includes four controlled rotation gates and one local rotation.

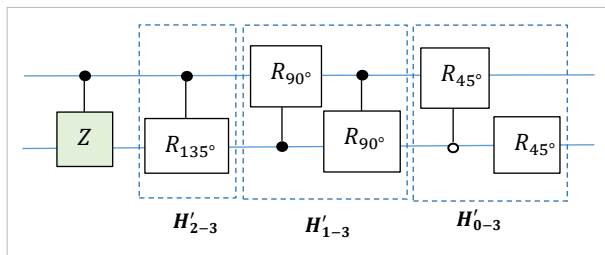


Fig. 13 The quantum circuits of the 2-qubit QHyT.

A. Results of Qiskit Simulation

To validate the proposed quantum signal-induced heap transform (QsiHT)-based QR decomposition, the quantum algorithms were implemented and simulated using IBM's Qiskit framework. In the following tables, the QCT-II and QHyT simulation results are recorded. For each simulation, the circuit was executed for different numbers of shots (1,000, 10,000, and 100,000) to analyze the convergence of results compared to the theoretical expectation. The measurement results were analyzed using the Mean Relative Squared Error (MRSE) metric.

	Ideal	1,000 shots	10,000 shots	100,000 shots
$ 00\rangle$	0.3127	0.2932	0.3122	0.3116
$ 01\rangle$	0.5545	0.5718	0.5494	0.5560
$ 10\rangle$	0.5212	0.5310	0.5189	0.5201
$ 11\rangle$	0.5682	0.5523	0.5757	0.5684
MRSE	0.0000	8.0230e-03	2.3438e-03	5.7055e-04

Table 4: Qiskit results of the 2-qubit QCT-II shown in Example 1.

	Ideal	1,000 shots	10,000 shots	100,000 shots
$ 00\rangle$	0.3127	0.3224	0.3153	0.3120
$ 01\rangle$	0.7298	0.7197	0.7328	0.7310
$ 10\rangle$	0.3127	0.3127	0.3173	0.3116
$ 11\rangle$	0.5212	0.5282	0.5126	0.5211
MRSE	0.0000	3.9322e-03	2.6370e-03	5.3517e-04

Table 5: Qiskit results 2-qubit of the quantum Hartley transform shown in Example 2 with $z = (1, -3, 2, 3)/\sqrt{23}$ as input.

6. CONCLUSION

In this work, we describe the method of QsiHT-based QR decomposition for unitary operations. The quantum circuits for implementing unitary operations on two-qubit superpositions are presented. The corresponding quantum circuit for unitary operations on 2 qubits are presented. Examples with the Hartley and cosine transformations are also considered. The presented method can also be used to construct quantum circuits for m -qubit operations, when $m \geq 2$, since the fast paths with splitting for m -qubit DsiHT can be also found [AG25]. For 3-qubit operations, our quantum circuit uses a maximum of 28 rotations.

7. REFERENCES

- [DLHL12] J. Demmel, L. Grigori, M. Hoemmen, J. Langou, *Communication-optimal parallel and sequential QR and LU factorizations*, SIAM J. Sci. Comp., 34 (1), (2012) 206-239.
- [Hou58] Householder, A.S. "Unitary triangulation of a nonsymmetric matrix," *Journal ACM*, 5 (4), (1958) 339-342
- [AM06] Grigoryan, A.M. Grigoryan, M.M. (2006), "Nonlinear approach of construction of fast unitary transforms," *2006 40th Annual Conference on Information Sciences and Systems*, Princeton, NJ, USA, 1073-1078.
- [AG14] Grigoryan, A.M. (2014), New method of Givens rotations for triangularization of square matrices,' *Journal of Advances in Linear Algebra & Matrix Theory (ALAMT)*, 4 (2), 65-78
- [FD19] Fedoriaka, D. (2019), Decomposition of unitary matrix into quantum gates. <https://arxiv.org/html/2501.07786v1>
- [AG25] Grigoryan, A.M. Gomez, A.; Espinoza, I.; Agaian, S.S. (2025), "Signal-induced heap transform-based QR-decomposition and quantum circuit for implementing 3-qubit operations," *Information*, 16, 466. <https://www.mdpi.com/2078-2489/16/6/466>
- [RB86] Bracewell, R.N. (1986) *The Hartley transform*, Oxford Univ. Press, New York.

Studying how changes on the transpilation and the number of shots can be used to optimize quantum circuits

Elena Desdentado
Institute of Technology
and Information
Systems, University of
Castilla-La Mancha
Camino Moledores
13005, Ciudad Real,
Spain
elena.dfernandez@uclm.es

Macario Polo
Institute of Technology
and Information
Systems, University of
Castilla-La Mancha
Camino Moledores
13005, Ciudad Real,
Spain
macario.polo@uclm.es

Coral Calero
Institute of Technology
and Information
Systems, University of
Castilla-La Mancha
Camino Moledores
13005, Ciudad Real,
Spain
coral.calero@uclm.es

M. Angeles Moraga
Institute of Technology
and Information
Systems, University of
Castilla-La Mancha
Camino Moledores
13005, Ciudad Real,
Spain
mariaangeles.moraga@uclm.es

ABSTRACT

Context: Quantum computing is an emerging technology with the potential to address problems that are unsolvable for classical systems. However, adapting quantum software to current hardware constraints remains a significant challenge, particularly when aiming for efficient and sustainable executions.

Objective: This study explores how two strategies applied during the preparation and execution stages of quantum software development can affect the results and energy consumption of the executions of a simple quantum circuit.

Method: We analyse the impact of (1) the explicit selection of physical qubits within a quantum device, and (2) the number of individual executions per measurement. For each strategy, 12 executions are performed. From each execution, the outcomes of the measurements (to calculate the success rate of each case), and the execution times are collected.

Results: Our analysis shows that the selection of physical qubits has a significant effect, showing a 20% drop in success rate and an increase in execution time (and therefore energy consumption) between a suboptimal qubit allocation versus a better allocation. Furthermore, the number of shots influences the quality of the outcomes, the results suggest that there might be an optimal number of shots for each circuit.

Conclusions: The strategies disclosed in this study seem to affect the final outcomes and runtime required to execute our simple circuit. These strategies should be analysed for more complex circuits, and we should also check how their combination might affect the final results.

Keywords

Quantum computing, Quantum software, Quantum technology, Energy efficiency, Energy consumption

1 INTRODUCTION

The promise of quantum computing lies in its ability to address problems that are unsolvable for classical systems. Although theoretical advances continue, the practical deployment of quantum algorithms remains constrained by the limitations of current hardware. Moreover, quantum devices must be kept at temperatures close to absolute zero to function properly, which requires energy-intensive cooling systems.

Although quantum computing is often evaluated in terms of metrics such as performance, execution time, fidelity, or quantum speedup, energy consumption is not considered one of them ([Des25b]), despite the significant operational demands of these systems, as outlined above. In a previous study, [Des24], we observed that quantum computing can consume up to 150,000 times more energy than its classical counterpart when solving equivalent simple problems, indicating the urgent need to incorporate

energy efficiency into the evaluation criteria for this technology.

In this context, optimization strategies become essential to adapt computations to the actual hardware while improving execution efficiency. Beyond functional correctness, these strategies are increasingly driven by sustainability concerns. As quantum systems scale up, reducing the energy consumption of these computations becomes a priority. We could distinguish two moments of intervention for these strategies [Des25a], during *circuit design and development*, and during *circuit preparation and execution*. This article explores how two strategies applicable during *circuit preparation and execution* can contribute to more sustainable quantum computing.

2 OPTIMIZATION STRATEGIES: EXPERIMENTAL INSIGHTS

In this work, two possible optimization strategies applied to quantum gate-based computation are explored.

These two strategies involve: (1) the selection of the qubits employed from a quantum computer, and (2) the number of individual executions (shots) of a circuit. The objective is to determine whether changes on these two aspects can affect the outcomes obtained and the execution time, and therefore, the energy consumption required to execute a quantum circuit. Let us recall that quantum computers have a constant power consumption, which corresponds to the energy required to maintain the temperature necessary for their operation. Therefore, the energy consumption of a circuit can be directly determined by the time it takes to execute.

Transpilation and physical layout

In digital computation, the development of circuits, firmware, or low-level software must consider the processor's architecture to take advantage of all its characteristics. For this purpose, in quantum computing, the process of transpilation consists on translating the program or circuit written by the developer into a physical circuit adapted to the actual architecture and set of gates of the target QPU [IBM25a]. In general, transpilation is transparently performed by a classical program offered by the quantum computing provider, which generates the tailored code before sending it to execute on the actual computer.

Thus, transpilation takes into account the set of gates available on the target QPU and the physical layout of its physical qubits, with the aim of transforming the original circuit into an equivalent one that can run efficiently on real quantum hardware.

The physical layout of a quantum computer determines how the qubits within this computer are organized and connected, which lets us know where the qubits are and how they can interact with each other. Considering the layout of the quantum computer selected to execute our algorithms is very important, as not all qubits can communicate with each other. The graphical representation of this layout is called coupling map. Figure 1 shows the coupling map of the “*ibm_brisbane*” QPU. Then, the physical layout: refers to the connections between qubits inside the quantum computer; it depends on the design of the computer; and cannot be modified.

Besides the physical layout, there is also a virtual layout. The virtual layout of a quantum computer is a logical representation that is employed while developing a quantum circuit, and it does not represent the real connection between qubits (modified during transpilation to make a better fit for the computer). Thus, the virtual layout serves as an abstraction that simplifies programming.

Consider the “2 taxis, 3 people problem”, consisting of the allocation of three people in two taxis, the only restriction is that passenger one does not stand the others and must travel alone. To solve it we need 3 qubits,

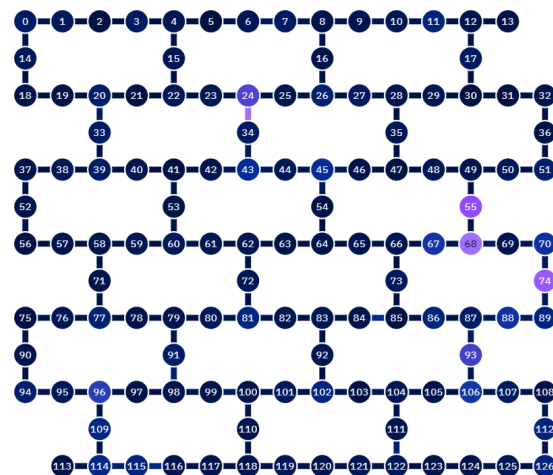


Figure 1: Coupling map of the IBM Quantum's computer “*ibm_brisbane*”.

each representing the final allocation of the person in a taxi. Figure 2 shows a graphical representation of the two possible valid outcomes for this algorithm: “011” and “100”, depending on the assigned taxi.

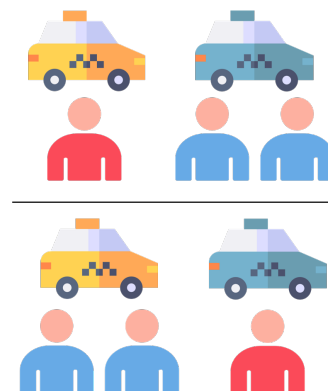


Figure 2: Representation of the possible solutions of the “2 taxis, 3 people problem”.

With this simple problem, we want to check the effect of modifying the transpilation process, by explicitly indicating the physical qubits we want to employ, on: (1) the success rate obtained, and (2) the energy consumption of the executions. In Figure 4 (top) we can see the logic circuit which solves the “2 taxis, 3 people problem”, and, as it can be observed, the three qubits needed are connected 1-2 and 2-3.

Experimentation

To analyse how the physical qubits allocation affects the success and energy consumption, we have executed the algorithm on IBM's computer “*ibm_brisbane*”, in three different ways:

1. As is: i.e., letting the system assign physical to logical qubits. For transpiling, the target computer offers four optimization levels, 0 (no optimization) to

- 3 (high optimization), being level 2 the default setting.
2. HQS (*High Qubit Separation*): during transpilation, IBM's system allows the quantum developer to select the physical qubits to place the logical ones. For this execution configuration, we have selected qubits 0, 63 and 126: as noted in Figure 3, they are placed as far as possible.
3. BQS (*Best Qubit Selection*): for this execution configuration, we have selected qubits 75, 76 and 90. In this case, we checked the coupling map to select qubits with a lower error individually and a better connection (less connection error) than the ones selected by default in the "as is" version.

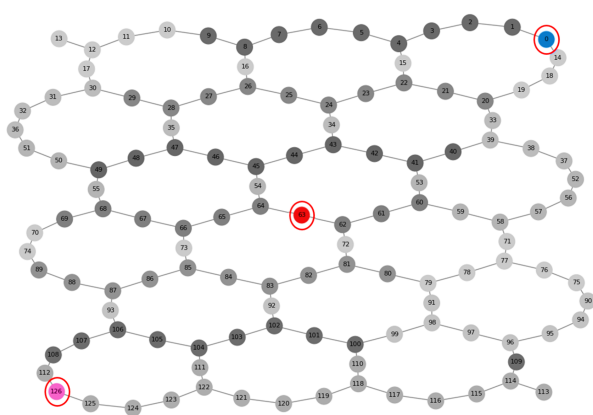


Figure 3: Qubit selection for the HQS version of the "2 taxis, 3 people problem".

To put the differences between these three versions into perspective, we will use two metrics: size and depth. Size refers to the total number of quantum operations applied, including logic gates and measurements. Depth represents the minimum number of sequential steps needed to execute the circuit, considering which operations can be applied in parallel.

The "as is" and the BQS versions present a size of 8 and a depth of 6, while the HQS version reaches a size of 487 and a depth of 194. Therefore, by separating the physical qubits as much as possible, the transpiler needs to add 471 logic gates (size) and 186 execution layers (depth) to execute the HQS version in a real quantum computer.

Figure 4 includes the logic circuit which solves the "2 taxis, 3 people problem" (top), the transpiled circuit of the "as is" version (middle), and the transpiled circuit of the BQS version (bottom). Note that the image of the transpiled circuit of the HQS configuration is not included due to its excessive size, which prevents it from being represented as an image.

All versions were executed twelve times on IBM Quantum's quantum computer "ibm_brisbane". For each execution, we used the default number of shots (1024) and

optimization level (2) defined by the platform. Once the execution finished, we recorded the Qiskit runtime usage and the results obtained. We then filtered the results obtained to take into account only the two possible good results ("011" and "100") with the aim of calculating the success rate percentage. Figure 5 presents the average success rates of all versions. As we can see, the physical distribution of qubits selected matters. In this case, if we compare the optimized (BQS) and the suboptimal selection of qubits, we can see that there is a 19% drop in success rate.

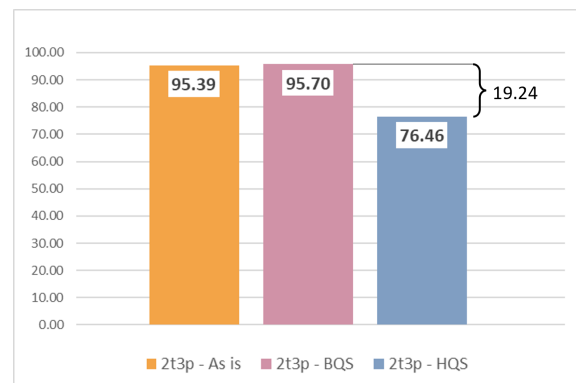


Figure 5: Success rates (%) obtained for all versions of the "2 taxis, 3 people problem" circuit.

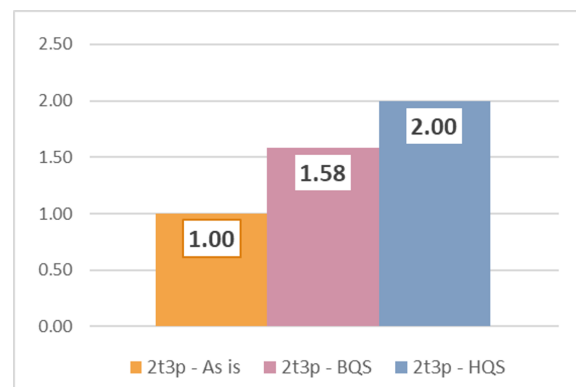


Figure 6: Average execution times (s) obtained for both versions of the "2 taxis, 3 people problem".

Moreover, Figure 6 compares the average execution times (in seconds) of the executions performed. The High Qubit Separation (HQS) version requires twice as much execution time as the "as is" version, and therefore also consumes twice as much energy. The BQS configuration requires 0.58 seconds more time to execute than the "as is" version. It is worth noting that the time values provided by the platform are rounded figures. This implies that the exact execution time is unknown, and that the actual value may differ from the reported one. Nevertheless, these are the only time measurements available, and even if they are not precise, they are sufficient to determine which execution

is longer and, therefore which one consumes the most energy. In the case of the BQS version, the time value is obtained calculating the mean time of the 12 executions. As in some cases the execution time was 1 second, and in other cases 2 seconds, the average of all of them 1.58 seconds.

The differences observed between all versions measured reinforce our initial idea: optimizing the layout can improve the success rate, although this can come at the cost of a slightly increased execution time. We could observe that the suboptimal version (HQS) performs the worst in both dimensions, achieving a success rate 19% lower and requiring twice the execution time compared to the “as is” version. Therefore, finding an optimized selection of qubits can help us to achieve a better balance between success rate and execution time, as our goal is not always to minimize energy consumption, but rather find said balance.

Impact of the number of shots

The quantum computers we can currently use are prone to errors due to quantum noise (small deviations when manipulating subatomic particles) and decoherence (the system cannot completely isolate itself from its environment), which lead to inaccuracies and errors in the results provided by the quantum computer.

To address this, the most common solution is to run the quantum algorithm several times per measurement,

known as number of *shots*. This section focuses on observing if the selected number of shots influences on the success rate and the energy consumption required to execute a circuit.

Experimentation

In theory, and in general belief, the more shots taken, the closer the obtained probability distribution is to the actual solution. We have executed the “2 taxis, 3 people problem” circuit twelve times on IBM Quantum’s quantum computer “*ibm_brisbane*”, with 50; 1,024 (default); 4,500; 10,000; and 24,500 shots. For each execution, we used the default optimization level (2) defined by the platform.

Figure 7 shows a different reality even for such this simple problem: in fact, the success rate (i.e., the percentage of right solutions) tends to grow as the number of shots increases, but starts to decrease when the number of shots seems “too high”.

Employing more shots, as we can see, is not always the best option, likely because as the more shots you run, the more times the circuit is exposed to the noisy environment of quantum computers.

It seems that there could be an optimum number of shots to be employed, a value that could change depending on the characteristics of the quantum circuit to be executed.

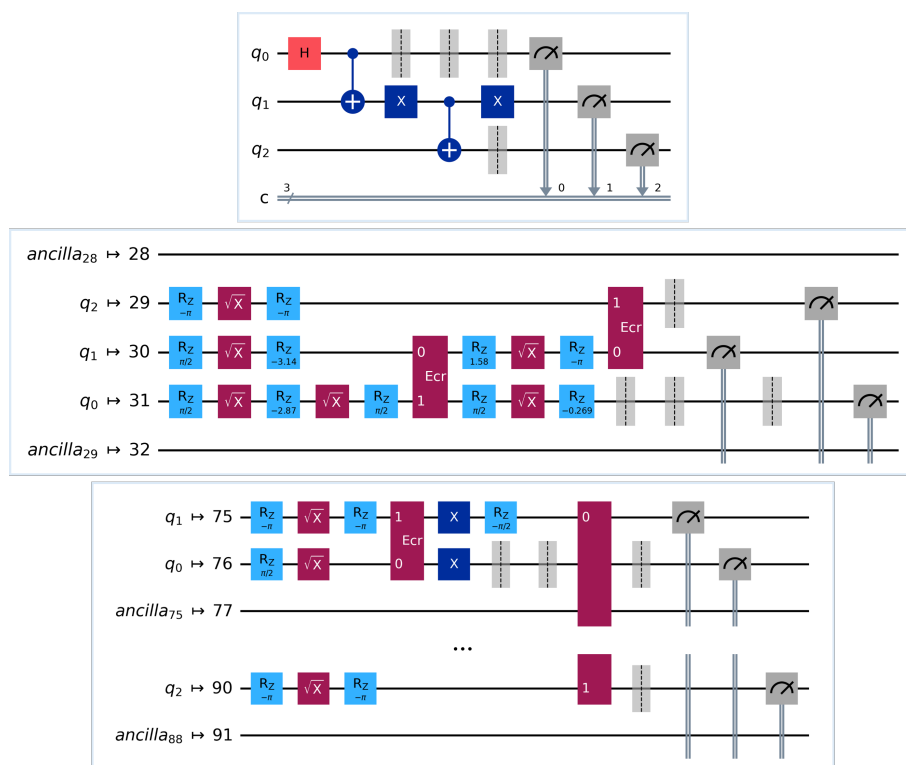


Figure 4: Logical circuit for the “2 taxis, 3 people problem” (top); transpiled “as is” version circuit with 2 as optimization level (middle); and transpiled BQS version with 2 as optimization level (bottom).

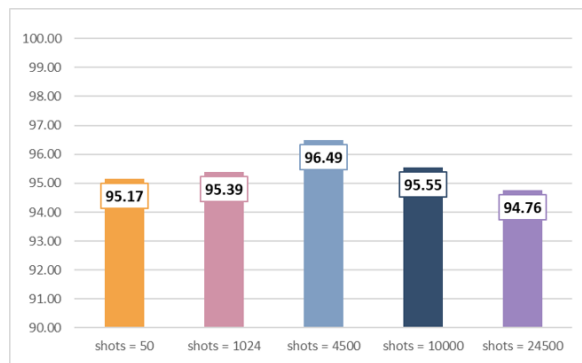


Figure 7: Success rates (%) obtained for 50, 1,024, 4,500, 10,000, and 24,500 shots.

It is also interesting to analyse the relationship between the execution times with respect to the number of shots employed (Figure 8): it is clear that the more shots employed in the execution, the more execution time and therefore the more energy consumption is needed for the quantum computer to run it. In line with our recommendation to look for a balance between time (and therefore energy consumption) and success rate, in this case, it appears that choosing 1,024 shots over 50 is preferable, as both require the same execution time but 1,024 yields a higher success rate. Nevertheless, the best option might be 4,500 shots, since although it takes more than twice the time compared to 1,024 shots, it results in an increase of over one percentage point in the success rate.

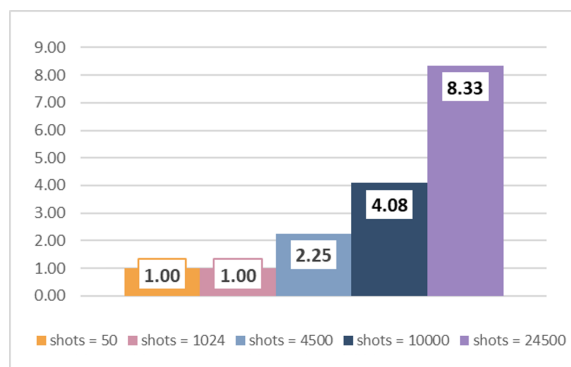


Figure 8: Execution times (s) obtained for 50, 1,024, 4,500, 10,000, and 24,500 shots.

3 CONCLUSIONS AND FUTURE WORK

The analysis of the two strategies presented in this paper, applied to the *preparation and execution* stage of quantum software development, reflects firstly that the physical qubits selected to perform the execution of a quantum circuit can be crucial. As we could see comparing the “*as is*” version, the BQS (Best Qubit Selection) version, and the HQS (High Qubit Separation) version executions, a suboptimal allocation of resources, in this case of qubits, greatly affects the re-

sults. Largely impacting the success rate percentages obtained, and also the time needed and energy consumption to perform the execution itself. And that a better allocation of qubits can obtain a better success rate percentage, with a slight increase of execution time, suggesting the need to find a balance between both dimensions.

And, secondly, that the number of shots employed is also crucial, with results suggesting that there might be an optimal number of shots to be used, that might change from one circuit to another.

In the future we would like to expand this study, employing these two strategies with more complex circuits, experiment with other strategies identified, such as the simplification of circuits, the replacement of error-prone gates, or shortening the search space tree for algorithms that produce specific probability distributions (i.e. Grover’s algorithm [Gro96]). We also plan to evaluate the combined use of these strategies. As each technique focuses on one aspect of quantum circuit design, development and execution processes, the combination of two or more strategies could lead us to more robust, adaptable, and scalable quantum solutions.

4 ACKNOWLEDGMENTS

This work is part of, and has received financial support from, the following projects:

- OASSIS: PID2021-122554OB-C31/AEI/10.13039/501100011033/FEDER, UE.
- PLAGEMIS: Grant TED2021-129245B-C22 funded by MCIN/AEI/ 10.13039/501100011033 and European Union NextGenerationEU/PRTR.
- EMMA: Project SBPLY/21/180501/000115, funded by CECD (JCCM) and FEDER funds. Financial support for the execution of applied research projects, within the framework of the UCLM Own Research Plan, co-financed at 85% by the European Regional Development Fund (FEDER) UNION (2022-GRIN-34110)

In addition, the first author has a pre-doctoral FPI (Research Staff Training) contract at the University of Castilla-La Mancha, Spain, for which funding has been received from the European Union through the European Social Fund Plus (ESF+).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

5 REFERENCES

- [Des25a] Calero C., Polo M., Desdentado E., and Moraga M.A. Consider the energy consumption of your quantum circuits *Nature Reviews Physics* 7, 352-353, June 2025. <https://doi.org/10.1038/s42254-025-00846-0>
- [Des25b] Desdentado E., Calero C., Moraga M.A., and Garcia F. Quantum computing software solutions, technologies, evaluation and limitations: a systematic mapping study. *Computing*, 107(5):110, April 2025. <https://doi.org/10.1007/s00607-025-01459-2>
- [Des24] Desdentado E., Calero C., Moraga M.A., Serano M., and Garcia F. Exploring the trade-off between computational power and energy efficiency: An analysis of the evolution of quantum computing and its relation to classical computing. *Journal of Systems and Software*, 217:112165, July 2024. <https://doi.org/>
- [IBM25a] IBM. Introduction to transpilation. IBM Quantum Documentation, 2025. <https://docs.quantum.ibm.com/guides/transpile>
- [IBM25b] IBM. Set transpiler optimization level. IBM Quantum Documentation, 2025. <https://docs.quantum.ibm.com/guides/set-optimization>
- [Gro96] Grover, L.K. A fast quantum mechanical algorithm for database search, in Proc. 28th Annual ACM Symposium on Theory of Computing, Philadelphia, Pennsylvania, USA, ACM Press, pp. 212-219, 1996.

Theta Function Framework for Quantum Systems with Magnetic Flux

Pavlos Evangelides
Alexander College, Artas 2, 7102 Larnaca, Cyprus
p.evangelides@alexander.ac.cy

ABSTRACT

We develop an analytic framework for quantum systems defined on a circle threaded by magnetic flux, generalizing the Bargmann representation via Theta functions. By introducing flux-dependent coherent states and displacement operators, we construct entire analytic wavefunctions and derive a reproducing kernel with quasi-periodic boundary conditions. This approach captures topological effects such as the Aharonov–Bohm phase and provides tools relevant for mesoscopic rings and topological quantum computation.

Compared to flux-free analytic approaches, the present framework directly encodes quasi-periodic boundary conditions, making it suitable for simulating observables such as persistent currents and phase shifts. Future work includes numerical implementations of the Theta function framework for flux qubits, extensions to multi-particle systems, and exploration of connections to non-Abelian topological phases.

1 INTRODUCTION

Quantum systems on compact topologies, such as circles, offer deep insights into both theoretical and applied physics. Threading such systems with magnetic flux introduces topological changes in boundary conditions, leading to observable quantum effects central to mesoscopic devices, superconducting circuitry, and emerging topological quantum computing paradigms.

A foundational quantum phenomenon illustrating this is the Aharonov–Bohm (AB) effect: a charged particle encircling a magnetic flux acquires a measurable phase shift, even in regions devoid of magnetic fields, underscoring the fundamental significance of topology and potentials in quantum mechanics [15]. In recent years, research has extended these insights to mesoscopic thermoelectric devices, where AB-induced coherence enhances quantum interference in quantum-dot heat engines [16].

Persistent currents in mesoscopic rings remain a topic of active interest. Ganguly and Maiti (2025) reported that synthetic fluxes in non-Hermitian Hatano–Nelson rings, especially in the presence of correlated disorder, can amplify both real and imaginary persistent currents [17]. Similarly, Sarkar et al. (2025) demonstrated enhancements in persistent currents under quasiperiodic

non-Hermitian disorder, even with weak interactions [18]. These studies highlight the intricate interplay between topology, disorder, and flux in modern systems.

Moreover, non-Hermitian delocalization phenomena have recently been revealed where an imaginary velocity component can drive delocalization and entanglement under periodic boundary conditions [19]. Such advances underscore the growing importance of analytic tools capable of capturing flux-induced behavior in non-Hermitian contexts.

In parallel, analytic representations - such as the Bargmann formalism provide powerful perspectives by mapping quantum states into entire analytic functions. Jacobi Theta functions naturally extend these frameworks to compact domains, encoding periodic and quasi-periodic boundary behaviors. Foundational mathematical work on Theta functions and modular forms remains crucial [8, 9], as does more recent adaptation to quantum systems on $\mathbb{Z}(d)$ and circles [10, 11, 12].

However, these prior analytic methods typically assumed strict periodicity ($q(x + 2\pi) = q(x)$) and thus failed to incorporate flux-driven quasi-periodicity or flux-dependent observables. Our work bridges this gap by embedding the AB phase into the analytic representation itself. We construct analytic wavefunctions $Q_\phi(z)$ satisfying $q(x + 2\pi) = e^{i\phi} q(x)$, thus integrating flux topology at the representational level. This extension enables analytic computation of physical observables and lays the groundwork for future exploration of interacting systems, higher-genus topologies, non-Hermitian systems, and non-Abelian topological phases [13, 14].

Contributions

- Development of a flux-dependent analytic framework using Jacobi Theta functions.
- Derivation of reproducing kernels and analysis of flux-driven zero dynamics.
- Analytical computation of persistent currents and interference phases.
- Comparison with flux-free analytic methods, highlighting clear advantages.

- Outlook toward numerical implementations, many-body interactions, and topological computation models.

The paper is structured as follows. Section 2 presents the flux-dependent analytic representation. Section 3 constructs the reproducing kernel and explores zero dynamics. Section 4 details applications including persistent currents and flux qubits. Section 5 extends the discussion to non-Hermitian and topological generalizations. Finally, Section 6 concludes with a summary and future research directions.

1.1 Boundary Conditions with Flux

Consider a quantum system described by a wavefunction $q(x)$ defined on the circle of unit radius, with $x \in [0, 2\pi]$. The Hilbert space is $L^2([0, 2\pi])$ with the usual inner product.

In the absence of magnetic flux, states satisfy strict periodicity:

$$q(x + 2\pi) = q(x).$$

This ensures that wavefunctions are single-valued on the circle.

When a magnetic flux Φ threads the circle, the system acquires a topological phase via the Aharonov-Bohm effect. The boundary condition becomes quasi-periodic:

$$q(x + 2\pi) = e^{i\phi} q(x), \quad \phi = \frac{e\Phi}{h}. \quad (1)$$

The parameter ϕ represents the flux-induced phase shift. Equation (1) encodes the fundamental modification of topology by flux.

1.2 Definition of the Analytic Representation

We now construct an analytic representation of states satisfying the quasi-periodic condition. Let Θ_3 denote the third Jacobi theta function:

$$\Theta_3(u, \tau) = \sum_{n \in \mathbb{Z}} e^{i\pi n^2 \tau} e^{2inu}, \quad \Im(\tau) > 0.$$

Theta functions provide kernels that encode periodic and quasi-periodic structures.

We define the flux-dependent analytic representation $Q_\phi(z)$ of a state $q(x)$ as

$$Q_\phi(z) = \int_0^{2\pi} q(x) \Theta_3\left(\frac{x-z}{2}, i\kappa\right) e^{-i\phi x/(2\pi)} dx, \quad (2)$$

where $\kappa > 0$ is a parameter controlling the scale of the analytic domain.

1.3 Properties of the Representation

Entire Analyticity.

Since $\Theta_3(u, i\kappa)$ is an entire function of u , and the integral in (2) is taken over a compact domain, it follows that $Q_\phi(z)$ is entire in z . Thus the analytic representation maps each physical state $q(x)$ to an entire analytic function on \mathbb{C} .

Quasi-Periodicity.

We now prove that $Q_\phi(z)$ satisfies a flux-induced quasi-periodicity condition. Consider:

$$Q_\phi(z + 2\pi) = \int_0^{2\pi} q(x) \Theta_3\left(\frac{x-(z+2\pi)}{2}, i\kappa\right) e^{-i\phi x/(2\pi)} dx.$$

Using the periodicity $\Theta_3(u + \pi, \tau) = \Theta_3(u, \tau)$, we have

$$\Theta_3\left(\frac{x-(z+2\pi)}{2}, i\kappa\right) = \Theta_3\left(\frac{x-z}{2}, i\kappa\right).$$

Thus

$$Q_\phi(z + 2\pi) = e^{-i\phi} \int_0^{2\pi} q(x) \Theta_3\left(\frac{x-z}{2}, i\kappa\right) e^{-i\phi x/(2\pi)} dx,$$

which implies

$$Q_\phi(z + 2\pi) = e^{-i\phi} Q_\phi(z). \quad (3)$$

Equation (3) shows that the analytic representation faithfully encodes the quasi-periodicity induced by flux.

Norm Preservation.

The map $q(x) \mapsto Q_\phi(z)$ preserves Hilbert space structure through an isometry involving the reproducing kernel (derived in Section 3). Thus the analytic representation is not only mathematically consistent but also physically faithful.

1.4 Consistency with the Flux-Free Case

An essential property of any flux-dependent generalization is its reduction to the flux-free case when $\Phi = 0$.

Setting $\phi = 0$ in (2), we obtain:

$$Q_0(z) = \int_0^{2\pi} q(x) \Theta_3\left(\frac{x-z}{2}, i\kappa\right) dx,$$

which is precisely the analytic representation used in earlier work on compact quantum systems without flux [11, 12].

Thus the present framework smoothly interpolates between the flux-free analytic representations of the literature and the flux-dependent case considered here.

1.5 Physical Interpretation

The representation $Q_\phi(z)$ encodes the entire wavefunction $q(x)$ as an analytic function with quasi-periodicity (3). Physically, this means that the AB phase is built directly into the analytic structure, rather than added later as a correction.

This is crucial for applications. For example:

- In mesoscopic rings, $Q_\phi(z)$ naturally encodes the shift of energy levels and persistent currents due to flux.
- In flux qubits, quasi-periodicity enables the analytic representation to capture flux-dependent tunneling amplitudes and interference.
- In more advanced scenarios, such as higher-genus surfaces, the method generalizes to analytic structures incorporating multiple fluxes.

By embedding flux effects at the level of representation, the framework establishes a foundation for analytic calculations of topological quantum phenomena.

2 REPRODUCING KERNEL AND ZERO DYNAMICS

The analytic representation introduced in Section 2 not only provides a mapping from Hilbert space states to entire functions, but also admits a natural reproducing kernel structure. This reproducing property ensures that the analytic representation is complete and that inner products in Hilbert space can be expressed as integrals in the analytic domain. Furthermore, the presence of flux modifies the geometry of zeros of analytic functions, an aspect that reveals deep connections to topological dynamics and Floquet theory.

2.1 Reproducing Kernel Construction

Let $Q_\phi(z)$ denote the flux-dependent analytic representation defined in (2). To establish a reproducing property, we construct the kernel

$$K_\phi(z, w^*) = \int_0^{2\pi} \Theta_3\left(\frac{x-z}{2}, i\kappa\right) \Theta_3\left(\frac{x-w^*}{2}, i\kappa\right) \times e^{-i\phi x/\pi} dx. \quad (4)$$

This kernel depends explicitly on ϕ , reflecting the role of flux. It reduces to the flux-free kernel when $\phi = 0$, in agreement with previous studies [11, 12].

2.2 Reproducing Property

We now prove that the kernel (4) reproduces analytic functions $Q_\phi(z)$. Consider

$$Q_\phi(z) = \int_A K_\phi(z, w^*) Q_\phi(w) dm(w),$$

where $dm(w)$ is the appropriate measure on the analytic domain A .

The proof follows from Fubini's theorem: inserting the definition of $Q_\phi(w)$ into the right-hand side and exchanging the order of integration recovers the original representation (2). Thus K_ϕ indeed acts as a reproducing kernel.

Inner Products.

The Hilbert space inner product can be expressed in the analytic domain as

$$\langle q_1 | q_2 \rangle = \int_A Q_\phi^{(1)}(z) Q_\phi^{(2)}(z)^* dm(z).$$

This shows that the analytic representation is not only faithful but also norm-preserving, establishing it as a genuine isometry between Hilbert space and the space of analytic functions.

2.3 Translation in the Analytic Representation

A key property of the flux-dependent analytic representation is its transformation under translations in the analytic variable z . In particular, we study how $Q_\phi(z)$ behaves when the argument is shifted by a real parameter a .

Starting from the definition (2), one finds that

$$Q_\phi(z-a) = e^{iKa/2} e^{-iKz} Q_\phi(z), \quad (5)$$

where K is related to the Fourier mode of the state.

Equation (5) shows that translations in z are not purely geometric shifts but are accompanied by flux-dependent phase factors. These exponential terms encode the quasi-periodicity introduced by the magnetic flux.

Physical Interpretation.

In the physical system, translation of z corresponds to shifting the angular coordinate of the wavefunction on the circle. The additional phases represent the Aharonov-Bohm contribution from the enclosed flux. Thus, the translation property reflects how flux modifies the analytic structure and distinguishes the quasi-periodic case from the strictly periodic, flux-free setting.

3 APPLICATIONS AND COMPARISONS

The analytic representation introduced in Section 2 and the reproducing kernel developed in Section 3 provide a rich mathematical framework. In this section, we show

how these tools can be used to compute physically relevant observables in mesoscopic physics and quantum information. We focus on three main applications: persistent currents, interference phase shifts, and comparisons with flux-free analytic methods.

3.1 Persistent Currents in Mesoscopic Rings

One of the most celebrated consequences of flux in quantum systems is the emergence of persistent currents. Consider a particle on a ring of circumference 2π , threaded by a magnetic flux Φ . The Hamiltonian is

$$H = \frac{1}{2mR^2} \left(-i\hbar \frac{d}{dx} - \frac{e\Phi}{2\pi} \right)^2,$$

where R is the radius of the ring (here set to 1). The eigenenergies are

$$E_n(\Phi) = \frac{\hbar^2}{2m} \left(n - \frac{\phi}{2\pi} \right)^2, \quad n \in \mathbb{Z},$$

with $\phi = e\Phi/\hbar$.

The persistent current is obtained as

$$I(\Phi) = -\frac{\partial E_n(\Phi)}{\partial \Phi} = -\frac{e\hbar}{m} \left(n - \frac{\phi}{2\pi} \right) \frac{1}{2\pi}. \quad (6)$$

Analytic Representation.

Within our framework, the wavefunction associated with the n -th state is encoded by

$$Q_\phi^{(n)}(z) = \int_0^{2\pi} e^{inx} \Theta_3 \left(\frac{x-z}{2}, i\kappa \right) e^{-i\phi x/(2\pi)} dx.$$

The flux-dependence is explicit in the exponential factor. Differentiating the analytic phase factor with respect to Φ reproduces the persistent current formula (6), confirming the physical validity of the analytic framework.

Physical Interpretation.

Equation (6) demonstrates that persistent currents oscillate with Φ , vanishing when $\phi = 2\pi n$. This periodicity is a direct manifestation of the quasi-periodicity of $Q_\phi(z)$. The analytic representation therefore not only encodes the correct boundary conditions but also provides a calculational tool for observables.

3.2 Phase Shifts in Interference Devices

Another key application is to interference devices such as SQUIDs and flux qubits. In such systems, the AB phase manifests as measurable shifts in interference patterns.

The quasi-periodic property

$$Q_\phi(z + 2\pi) = e^{-i\phi} Q_\phi(z)$$

implies that a translation in the analytic domain introduces a global phase shift. In an interference experiment, the relative phase between two paths enclosing different fluxes becomes

$$\Delta\phi = \frac{e}{\hbar} (\Phi_1 - \Phi_2).$$

This reproduces the experimental signature of the AB effect: oscillations in current or voltage as a function of applied flux.

Application to Flux Qubits.

In flux qubits, logical states are associated with clockwise and counter-clockwise current loops. The analytic representation captures the phase difference between these states as a flux-dependent quasi-periodicity. This provides an alternative analytic perspective on flux qubit dynamics.

3.3 Comparison with Flux-Free Analytic Methods

Flux-free analytic representations, such as those studied in [11, 12], assume strict periodicity of the form $q(x + 2\pi) = q(x)$. While these approaches successfully describe systems without flux, they fail to account for AB phase shifts and flux-controlled observables.

The present framework generalizes these methods by including the exponential factor $e^{-i\phi x/(2\pi)}$ in the representation. The advantages can be summarized as follows:

- **Boundary conditions:** Flux-free methods impose periodicity, while our framework encodes quasi-periodicity induced by flux.
- **Observables:** Persistent currents and AB phase shifts cannot be computed in flux-free analytic methods, but emerge naturally here.
- **Topological effects:** Flux introduces winding numbers and modified zero dynamics, extending beyond flux-free results.
- **Generality:** The flux-dependent framework reduces smoothly to the flux-free case when $\Phi = 0$.

3.4 Comparative Summary

Table 1 summarizes the differences between flux-free and flux-dependent analytic frameworks.

	Flux-Free	Flux-Dependent
Boundary condition	$q(x + 2\pi) = q(x)$	$q(x + 2\pi) = e^{i\phi} q(x)$
Phase shifts	Absent	Encoded by $e^{-i\phi}$
Persistent currents	Not captured	Computable via $Q_\phi(z)$
Translation / dynamics	Closed orbits	Flux-modified quasi-periodicity
Applications	Compact systems	Mesoscopic rings, flux qubits

Table 1: Comparison between flux-free and flux-dependent analytic frameworks.

In conclusion, the analytic framework developed here not only reproduces established results such as persistent currents and AB phase shifts, but also extends analytic representations to new regimes where topology and flux are central. In the next section, we discuss broader implications, including numerical implementations, interacting systems, and connections to non-Abelian phases in topological quantum computing.

4 DISCUSSION: TOWARD TOPOLOGICAL QUANTUM COMPUTING

The analytic framework developed in this paper has implications that extend beyond mesoscopic physics. By encoding flux-induced quasi-periodicity into analytic functions, the representation provides a platform for exploring topological quantum computation, fault-tolerant architectures, and quantum simulation of interacting systems. In this section, we highlight several directions of future research.

4.1 Numerical Implementations

A practical advantage of analytic representations is the possibility of developing efficient numerical algorithms. In conventional approaches, simulating flux qubits or mesoscopic rings often requires diagonalization of large Hamiltonians or time-evolution under flux-dependent operators. Such methods scale poorly with system size.

The Theta-function framework offers a more compact description. Because quasi-periodicity is built directly into $Q_\phi(z)$, simulations can focus on analytic properties such as reproducing kernels and zero dynamics, bypassing brute-force diagonalization. One can envision hybrid numerical-analytic methods where states are represented by truncated series expansions of $Q_\phi(z)$, and observables are extracted using the kernel (4).

This approach could significantly reduce computational cost and may provide advantages in simulating arrays of flux qubits or larger superconducting circuits, particularly when coupled with modern spectral methods.

4.2 Multi-Particle and Interacting Systems

The analytic representation has so far been applied to single-particle wavefunctions on a circle. An important

extension is to multi-particle and interacting systems on compact topologies.

In such cases, the Hilbert space is spanned by states $q(x_1, \dots, x_N)$ defined on N -fold circles. Introducing a flux Φ threading the system modifies the boundary conditions in each variable, leading to a multi-dimensional quasi-periodic structure.

The corresponding analytic representation would involve multivariable Theta functions, generalizing (2) to higher dimensions. Such an extension would allow the study of flux-dependent entanglement, coherence, and correlation effects.

For example, in a two-particle system one may examine how flux controls the exchange statistics of particles on a compact topology. In interacting systems, flux could modulate collective excitations, potentially giving rise to new topological phases.

4.3 Higher-Genus Surfaces and Modular Structure

The circle is the simplest compact topology. More complex surfaces, such as tori or higher-genus Riemann surfaces, are also relevant in condensed matter and topological field theories.

Theta functions naturally generalize to these cases. Analytic representations on higher-genus surfaces would encode multiple fluxes, each associated with a distinct cycle of the surface. The modular properties of Theta functions then acquire direct physical interpretation: modular transformations correspond to different ways of threading flux through the system.

This line of research could unify analytic representations with the study of modular invariance in conformal field theory and with the use of Riemann surfaces in string theory.

4.4 Connections to Non-Abelian Topological Phases

Perhaps the most exciting extension concerns non-Abelian anyons, which are central to fault-tolerant topological quantum computation [13, 14]. Non-Abelian phases arise in systems where exchanging quasiparticles implements unitary transformations

on the ground-state manifold, providing inherent robustness to local errors.

The analytic framework developed here may serve as a stepping stone toward describing such systems. By encoding flux and topology in analytic functions, one may attempt to generalize the representation to non-Abelian settings, where states transform under higher-dimensional representations of the braid group.

In particular, the monodromy of zeros in the flux-dependent analytic representation suggests an analogy with braiding statistics: as flux is varied, zeros trace structured paths, reminiscent of anyonic worldlines. Investigating this analogy more rigorously may provide analytic tools for understanding non-Abelian braiding in quantum Hall states or Kitaev-type models.

4.5 Future Perspectives

The implications of flux-dependent analytic representations extend across several domains:

- In mesoscopic physics, they provide compact tools for computing persistent currents and interference shifts.
- In quantum technology, they offer analytic perspectives on flux qubits and superconducting circuits.
- In mathematical physics, they connect to modular forms, Riemann surfaces, and the theory of Theta functions.
- In topological quantum computing, they open potential pathways toward analytic descriptions of non-Abelian anyons.

Thus the framework presented here not only addresses immediate questions of flux and boundary conditions, but also lays a foundation for broader exploration of topological and analytic structures in quantum theory.

5 CONCLUSION

In this work we have developed a flux-dependent analytic representation for quantum systems on a circle, based on Jacobi Theta functions. By incorporating the Aharonov–Bohm phase directly into the analytic formalism, we constructed entire analytic wavefunctions that satisfy quasi-periodic boundary conditions. This generalizes the classical Bargmann representation and earlier flux-free Theta function approaches to systems where magnetic flux plays a fundamental role.

We showed that the representation admits a reproducing kernel, ensuring mathematical completeness and preserving Hilbert space structure. The presence of flux modifies the kernel and introduces quasi-periodicity in the analytic domain.

Applications of the framework were demonstrated through explicit calculations. We showed how persistent currents in mesoscopic rings arise naturally from the flux-dependent analytic wavefunctions, and how AB phase shifts in interference devices are directly encoded in the quasi-periodicity of the representation. A systematic comparison with flux-free analytic methods highlighted the advantages of our approach: while flux-free methods capture periodic dynamics, the present framework extends them by including topological effects central to mesoscopic physics and flux qubits.

Beyond immediate applications, we discussed broader implications. Analytic representations provide a promising foundation for numerical implementations, potentially enabling efficient simulations of flux qubits without large-scale Hamiltonian diagonalizations. The formalism also generalizes naturally to multi-particle and interacting systems, where flux can control entanglement and correlation effects. Finally, connections to higher-genus surfaces and non-Abelian topological phases suggest that the analytic representation may contribute to the mathematical foundations of fault-tolerant quantum computing.

Future Directions

Several avenues remain open for further exploration:

- **Numerical Algorithms:** Develop spectral and kernel-based methods for simulating flux-dependent dynamics in mesoscopic devices using truncated analytic expansions.
- **Interacting Systems:** Extend the representation to multi-particle systems on compact manifolds, examining flux-dependent entanglement and collective excitations.
- **Topological Generalizations:** Generalize to higher-genus surfaces and explore the modular properties of Theta functions in quantum systems.
- **Non-Abelian Phases:** Investigate connections between zero dynamics and braiding statistics, with applications to topological quantum computation.

In summary, the flux-dependent Theta function framework unifies analytic methods and topological quantum physics. It provides new mathematical tools, yields physically relevant observables, and opens pathways toward future research in mesoscopic systems, quantum information, and topological quantum computing.

6 REFERENCES

- [1] Y. Aharonov and D. Bohm. Significance of electromagnetic potentials in quantum theory. *Phys. Rev.*, 115(3):485–491, 1959.
- [2] N. Byers and C. N. Yang. Theoretical considerations concerning quantized magnetic flux in superconducting cylinders. *Phys. Rev. Lett.*, 7(2):46–49, 1961.
- [3] M. Büttiker. Small normal-metal loop coupled to an electron reservoir. *Phys. Rev. B*, 32(3):1846–1849, 1985.
- [4] H. F. Cheung, Y. Gefen, E. K. Riedel, and W. H. Shih. Persistent currents in small one-dimensional metal rings. *Phys. Rev. B*, 37(10):6050–6062, 1988.
- [5] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-Cooper-pair box. *Nature*, 398:786–788, 1999.
- [6] J. Q. You and F. Nori. Atomic physics and quantum optics with superconducting circuits. *Nature*, 474:589–597, 2011.
- [7] F. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 2019.
- [8] J. D. Fay. *Theta Functions on Riemann Surfaces*. Springer, 1973.
- [9] D. Mumford. *Tata Lectures on Theta I*. Birkhäuser, 1983.
- [10] A. Vourdas. Quantum systems with finite Hilbert space. *J. Phys. A*, 37(40):9335–9361, 2004.
- [11] P. Evangelides, Y. Lei, and A. Vourdas. Analytic representations with Theta functions for systems on $\mathbb{Z}(d)$ and on S . *J. Math. Phys.*, 56(6):062104, 2015.
- [12] H. E. A. Eissa, P. Evangelides, Y. Lei, and A. Vourdas. Paths of zeros of analytic functions describing finite quantum systems. *Phys. Lett. A*, 380(20):1643–1649, 2016.
- [13] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma. Non-Abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80(3):1083–1159, 2008.
- [14] A. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Phys.*, 303(1):2–30, 2003.
- [15] Y. Avishai and Y. B. Band. AharonovâBohm and AharonovâCasher effects in mesoscopic physics: A brief review. *arXiv preprint*, arXiv:2302.06300, 2023.
- [16] S. Bedkihal. Quantum-dot AharonovâBohm interferometric configurations for enhanced thermoelectric transport. *arXiv preprint*, arXiv:2410.01006, 2024.
- [17] S. Ganguly and S. K. Maiti. Persistent current in a non-Hermitian HatanoâNelson ring: Disorder-induced amplification. *Phys. Rev. B*, 111:195418, 2025. :contentReference[oaicite:1]index=1
- [18] S. Sarkar, S. Satpathi, and S. K. Pati. Enhancement of persistent current in a non-Hermitian disordered ring. *Phys. Rev. B*, (in press), 2025. :contentReference[oaicite:2]index=2
- [19] S.-X. Hu, Y. Fu, and Y. Zhang. Non-Hermitian delocalization induced by residue imaginary velocity. *Commun. Phys.*, 8:269, 2025. :contentReference[oaicite:3]index=3

Introducing the hidden subgroup problem in discrete mathematics class

Sehee Kim, Jiwoo Seo, Minju Kim, Yerak Kim, Seohyeon Baek, Seongbin Park*

Korea University, Sungbuk-ku, Anam-ro 145, Seoul, 02841, Korea

{sehee020512, jw3124, mim0924, yerak213, beth0508, hyperspace}@korea.ac.kr

ABSTRACT

Discrete mathematics is a branch of mathematics that deals with discrete structures, where a discrete structure is defined as either a finite nonempty set or a countably infinite set over which various relations, operations are defined. For computer science students, this is a class where fundamental subjects such as logic, number theory, relation, set theory, graph theory, algorithms are introduced in such a way that these subjects can be understood without much mathematics[Sandefur22]. In this poster, we describe our ongoing research that aims to introduce quantum computing to students without technical backgrounds[Jkim23, Slee23, Sjeong24]. More specifically, we argue that the hidden subgroup problem[Hallgren03] is a good subject that can be taught in discrete mathematics class because the problem deals with a simple discrete structure that can be easily explained to the students of discrete mathematics class. In addition, since it is well known that the famous quantum algorithms such as Simon's algorithm and Shor's algorithm solve the instances of the hidden subgroup problem[Nielsen16], we believe that introduction to the hidden subgroup problem can help students gain insights into the structural properties of computational problems in a wide perspective.

Keywords

Discrete mathematics, Hidden subgroup problem, Quantum computing

1 INTRODUCTION

The field of quantum computing has been progressing rapidly recently and it is expected to revolutionize a lot of technologies in the future[Alil22]. As is argued in[Bacon10], we believe that important ideas of quantum computing such as superposition, entanglement, reversibility, etc. can be introduced to students without backgrounds in mathematics and quantum mechanics.

In this poster, we describe our ongoing project that aims to introduce well-known quantum algorithms to the students in discrete mathematics class using the hidden subgroup problem(HSP).

The motivations of our research are as follows.

First, HSP can be defined using the concepts that students in discrete mathematics are already familiar with. For example, to define HSP, we need the concepts of a function, an equivalence class, a closure property, a binary operation, and a set and all of these are explained in discrete mathematics class.

Second, HSP naturally fits with the themes of discrete mathematics because HSP asks to find a certain structure (a subgroup) in a bigger structure (a group) that is discrete while discrete mathematics deals with various examples of discrete structures that we encounter in computing such as algorithms, computational problems, data structures, number theory, etc.

Finally, knowledge about HSP can serve as a window through which students can see a different world (that

is, the world of quantum computing) than the world of classical computing since well-known quantum algorithms such as Simon's algorithm and Shor's algorithm solve instances of HSP more efficiently than classical algorithms.

This poster is structured as follows. In section 2, we explain how HSP can be introduced to the students in discrete mathematics with simple instances of HSP. Then, this poster concludes with research perspectives.

2 INSTANCES OF HSP

To introduce HSP to the students in discrete mathematics, we can start with a definition for HSP. Then, two different instances of HSP are explained so that their structural common denominator can be easily recognized.

HSP is defined as follows. We are given a finite group G and a function f from G to a finite set A such that f has the following property: (1) for all elements in the same coset of a subgroup H of G , the function values are the same, and (2) for elements x, y each of which belongs to a different coset of H , $f(x)$ and $f(y)$ are different. We say that the subgroup H is hidden by the function f and the problem is to find H .

Then, we can explain a simple example with a group G that consists of a set $Z_6 = \{0, 1, 2, 3, 4, 5\}$ with a binary operation that is addition mod 6. For this structure, there is a subgroup H that consists of a set $B = \{0, 3\}$.

Now, there are 3 cosets of H which are $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$.

We can point out that Z_6 is divided into 3 cosets so that when a function is defined, it can be interpreted as assigning 3 different colors to the members of Z_6 depending on the membership against the cosets.

An instance of HSP here is as follows. Assume that we are given a function f that maps Z_6 to $A=\{a, b, c\}$ such that $f(0) = f(3)=a$, $f(1) = f(4)=b$, and $f(2) = f(5)=c$, respectively. What is the hidden subgroup?

Once this example is understood by the students, we can explain the problem that Simon's algorithm addresses.

The problem is defined as follows: We are given a function f from $\{0, 1\}^n$ to $\{0, 1\}^n$ such that for all $x, y \in \{0, 1\}^n$, $f(x)=f(y)$ if and only if $x=y \oplus s$, for some $s \in \{0, 1\}^n$, where \oplus is the bitwise exclusive or operation. The problem is to find s .

The underlying structure of Simon's problem is HSP because if we let the group as the set, $\{0, 1\}^n$ with the binary operation \oplus , then the hidden subgroup is the set $\{0^n, s\}$.

3 CONCLUSION

In this poster, we report our ongoing project that aims to introduce well-known quantum algorithms to the students in discrete mathematics class.

When mathematical structures are taught, it is important that the teacher should know more about structures than can be discussed in class[Taylor65]. We believe that introduction of HSP as a way to open students' eyes about applications of discrete structures is something that achieves this guideline because it connects a structure with a way to exploit it for solving a problem. This is similar to a matroid that can be exploited when an optimization problem possesses it[Edmonds71].

Introduction of HSP as well as an instance of the problem such as Simon's problem may help students get interested in a subtle subject such as what makes quantum computers more powerful than classical computers. In addition, students may ask whether there exists a general theorem that states the existence of a structural property that makes quantum computation more powerful compared to classical computation[Aaronson11].

Currently, we are working on intuitive ways to introduce instances of HSP such as Shor's period finding

problem as well as graph isomorphism problem to students in discrete mathematics class. In addition, we are investigating ways by which visualization tools can be used to introduce quantum algorithms.

4 REFERENCES

- [Sandefur22] E. Hart, G. Greefrath, J. Sandefur, E. Lockwood, Teaching and learning discrete mathematics, ZDM - Mathematics Education, Volume 54, pp. 753-775, 2022.
- [Jkim23] Teaching an Elective Course about Quantum Computing, J. Kim, C. Lee, J. Song, C. Sim, S. Park, Poster, The 16th International Conference on Informatics in Schools, October 2023, HEP Vaud, Lausanne, Switzerland, <https://zenodo.org/records/8431971> (PDF).
- [Slee23] Introduction to Quantum Computing for Middle School Students, S. Lee, J. Kim, Y. Kim, C. Sim, S. Jeong, S. Park, Poster, The 16th International Conference on Informatics in Schools, October 2023, HEP Vaud, Lausanne, Switzerland, <https://zenodo.org/records/8432008> (PDF).
- [Sjeong24] An approach to introduce entanglement to novices, S. Jeong, S. Oh, S. Song, S. Park, Short paper, QC Workshop 2024: GI Quantum Computing Workshop September 24, Germany, 2024, <https://dl.gi.de/server/api/core/bitstreams/77f9cb92-3e70-40d6-92b0-bd4b2882880a/content> (PDF).
- [Hallgren03] A. Russell, A. Ta-shma, S. Hallgren, The hidden subgroup problem and quantum computation using group representations, SIAM Journal on Computing, Volume 32, No 4, pp. 916-934, 2003.
- [Nielsen16] I. L. Chuang, M. A. Nielsen, Quantum computation and quantum information, Cambridge University Press, 2016.
- [Alil22] T. Yue, R. Abreu, S. Ali, When software engineering meets quantum computing, Communications of the ACM, Volume 85, No 4, pp. 84-88, 2022.
- [Bacon10] D. Bacon, W. van Dam, Recent progress in quantum algorithms, Communications of the ACM, Volume 53, No 2, pp. 84-93, 2010.
- [Taylor65] T. L. Wade, H. E. Taylor, On the meaning of structure in mathematics, The mathematics teacher, Volume 58, No 3, pp. 226-231, 1965.
- [Edmonds71] J. Edmonds, Matroids and the greedy algorithm, Mathematical Programming, Volume 1, pp. 127-136, 1971.
- [Aaronson11] A. Ambainis, S. Aaronson, The need for structure in quantum speedups, Proceedings of Innovations in Theoretical Computer Science (ITCS), arXiv:0911.0996, 2011.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.