Quantum Query Complexity
for Svetlichny-Like Functions

Project Proposal

AUTHORS

Syed Danial Haseeb	12429
Ashnah Khalid Khan	22889
Muhammad Rasib Nadeem	22976

ADVISOR

Dr Jibran Rashid

ABSTRACT

This project aims to advance the understanding of quantum algorithms by focusing on quantum query complexity. Building upon Simon's use of parity functions, the project seeks to identify different classes of functions and bases for which there may exist a quantum advantage, such as quantum boolean functions and Svetlichny functions, for algorithmic development. Utilising the promise problem framework, the study will experiment with various classes of functions, such as Svetlichny to determine their quantum query complexity. A key tool in the study is expected to be the quantum generalisation of the Gram-Schmidt procedure.

School of Mathematics & Computer Science

Contents

1 Overview

TITLE Quantum Query Complexity for Svetlichny-Like Functions

ACRONYM QQC

TAGLINE The curious case of quantum query complexity

START DATE September 1^{st}, 2023

END DATE May 21^{st}, 2024

1.1 Project Brief

Quantum computing promises unprecedented computational capabilities, which has led to a surge in research to understand how quantum algorithms can outperform classical algorithms. Quantum query complexity is a pivotal concept that form the cornerstone of quantum computing research. This project aims to explore this area further by considering quantum boolean functions and Svetlichny functions. Additionally, we aim to experiment with different types of function *promises* in order to assess their on quantum query complexity.

2 Problem Statement

2.1 Identifying the Problem

In the rapidly evolving field of quantum computing, progress in both hardware and software is crucial for unlocking the technology's full potential. While strides have been made in hardware, especially in qubit stability, the need for innovative quantum software remains pressing.

Early groundbreaking work by researchers like Simon, Vazirani, and Shor provided a theoretical foundation for quantum algorithms, highlighting their transformative potential across various domains, from cryptography to new computational paradigms.

Building on this, there is a growing need for a future where quantum hardware improvements go hand-in-hand with algorithmic advancements, enabling solutions to problems previously considered intractable in classical computing.

Target Audience

Understanding the key stakeholders in theoretical quantum computing is essential for tailoring effective solutions and communications. The main audience groups are:

1. Theoretical Quantum Computing Researchers: Primarily scholars and researchers, they delve into the theoretical aspects of quantum algorithms and mechanics. Affiliated mostly with academic and research institutions, they push the boundaries of the field.
2. Quantum Algorithm Developers: Tasked with translating theory into practical algorithms, this group plays a pivotal role in connecting theoretical insights with real-world applications.
3. Quantum Hardware Engineers: Focused on the hardware aspects of quantum computing, their work is nonetheless influenced by theoretical advancements, especially in areas like qubit stability and coherence.

2.2 Quantifying the Problem

Socioeconomic Significance

Theoretical quantum computing holds broad implications that affect multiple sectors, from healthcare and finance to national security. Here's a brief overview of its transformative potential:

1. Healthcare: Quantum algorithms could accelerate drug discovery and improve diagnostics, impacting public health positively.
2. Finance and Economics: The technology has the potential to optimise financial systems, affecting trading strategies and fraud detection.
3. Energy Sector: Quantum optimisation algorithms could lead to more efficient energy use and contribute to climate change mitigation.
4. National Security: Quantum computing poses both risks and rewards for encryption and data security.
5. Education: Advances in the field will inevitably impact educational curricula, enhancing scientific literacy.

Target Audience Size

Understanding the size and scope of our target audience is crucial for the successful dissemination and impact of our research findings. It is challenging to quantify this group's size. However, considering the heavy investments in quantum hardware development, from both governmental and private sectors, it is safe to assume that at least a few thousand engineers and scientists are engaged in quantum research and development globally.

These numbers are by no means exhaustive but provide a good starting point for understanding the scale of our target audience. The continuous growth in each of these sectors emphasizes the urgent need for innovative research in quantum algorithms.

3 Literature Review

The Connection Between early Quantum Algorithm and Shor's Algorithm

John Watrous's quantum lecture [1] notes provide valuable insights into the historical development and connection between Shor's algorithm and earlier quantum algorithms like Simon's and Deutsch-Jozsa. Simon's algorithm, introduced by Daniel Simon in 1994, was a pioneering quantum algorithm designed to solve a specific problem in exponential speedup compared to classical counterparts. It was the precursor to Shor's algorithm, which made further strides in demonstrating the quantum advantage. Simon's algorithm was primarily focused on solving a black-box problem, where the algorithm aims to find a hidden pattern in a function using quantum superposition and interference. Simon's algorithm's significance lies in its revelation that quantum computers could potentially outperform classical ones in certain cases. Building upon the ideas of Simon's algorithm, Peter Shor developed his groundbreaking quantum algorithm in 1994, which fundamentally altered the landscape of quantum computing. Shor's algorithm solved the long-standing problem of efficiently factoring large numbers, a task deemed classically infeasible and crucial for modern cryptography. Shor's innovation was to combine the principles of quantum superposition and interference, similar to Simon's algorithm, with modular arithmetic to factor numbers exponentially faster than classical algorithms. We studied this example of the quantum algorithm ideation phase to gain insight on how we can try to find a different quantum algorithm, following a similar vein of thought.

There are a multitude of directions we could explore for our research, but based on hints from our supervisor, we have narrowed them down to three gateway articles that we have looked at to initiate our research.

1. Quantum Gram-Schimidt [2]
2. Quantum Boolean Function [3] [4] [5]
3. Svetlichny functions - Periodic Fourier Representation [6]

Quantum Boolean Functions

References [3] and [5] introduce the concept of quantum Boolean functions, which are unitary operators that, when squared, yield the identity operator. These functions constitute a fundamental element of our research, as we explore diverse function types with the potential to replace those employed in Simon's algorithm.

Simon initially employed functions in the form of $f(x) = s \cdot x$. Within the scope of our research, we aim to investigate whether functions meeting the condition $f^2 = I$ can provide fresh insights or confer advantages in quantum algorithm development.

Quantum Gram–Schmidt

The paper titled "Quantum Gram-Schmidt Processes and Their Application to Efficient State Read-out for Quantum Algorithms" [2] represents a significant breakthrough in the field of quantum computing, offering an efficient protocol for generating orthogonal bases. Previous research efforts, as evidenced by references [52–55] in the aforementioned paper, have explored various methodologies for constructing orthogonal states. However, these methods often deviate from the conventional Gram-Schmidt process and exhibit limited versatility in their applications. In contrast, the Quantum Gram-Schmidt Process (QGSP) protocol distinguishes itself through its efficiency and adaptability. It provides a robust framework for creating orthonormal bases, thereby expanding the potential applications within the realm of quantum computing. This advancement opens doors to innovative quantum algorithm development. For our purposes, this paper holds particular significance as it provides insights into a promising tool that allows us to obtain orthonormal bases in polynomial time, which could prove useful for for instance extending Simon's algorithm since it does not always return an orthonormal basis.

Svetlichny functions - Periodic Fourier Representation

The paper titled "Periodic Fourier Representation of Boolean Functions" [6] introduces a new representation of Boolean functions known as the "periodic Fourier representation" or Svetlichny functions. The researchers investigate the relationship between the "periodic Fourier sparsity," which quantifies the number of non-zero coefficients in this representation, and the required qubit count for exact computation.

The research mainly demonstrates that Boolean functions related to certain mathematical structures exhibit small periodic Fourier sparsities. And that such functions can be efficiently computed.

4 Details

4.1 Proposed Solution

Our project aims to create a new understanding in the field of quantum query complexity by focusing on its applications in Svetlichny-like functions. We aim to dissect and extend the foundations set by Simon's algorithm and explore new functional bases, such as quantum boolean functions and Svetlichny functions. The aim is to replace the function types employed in Simon's algorithm with quantum boolean functions and assess their potential for application in quantum query algorithms.

Unique Selling Points (USPs)

- Innovation in Quantum Query Complexity: Our work could potentially introduce new paradigms in quantum query algorithms, opening the door for exponential speedup in solving certain computational problems.
- Experimental Element: In addition to theoretical analysis, we intend to conduct quantum simulations, providing a comprehensive analysis that includes both theoretical and empirical evidence.
- Educational Outreach: We will develop engaging and informative educational materials and resources for students. Utilizing newly developed visualization libraries, we aim to clarify seemingly complex concepts and make them more intuitive for students to grasp. This educational component adds a broader impact dimension to our project.

4.2 Project Objectives

The overarching goal of this project is to contribute to the field of quantum computing...

1. Theoretical Exploration: Investigate the theoretical underpinnings...
2. Functional Basis Extension: To extend the functional bases...
3. Algorithmic Development: Develop new quantum query algorithms...
4. Quantum Simulations: Conduct quantum simulations...
5. Educational Outreach: Create a suite of educational content...

Educational Outreach Objectives

- Educational Tutorials: Produce step-by-step guides...
- Interactive Lessons: Develop interactive online modules...
- Explanatory Videos: Create short, accessible videos...
- Public Outreach: Engage with educational institutions...

4.3 Methodology

Theoretical Exploration

We will begin with a comprehensive review of the current state of the field, focusing on quantum query complexity, Svetlichny functions, and quantum Boolean functions. Mathematical models will be developed to simulate the behavior of different quantum query algorithms.

Functional Basis Extension

Our next step is to extend the functional bases used in quantum algorithms. We will start by replacing Simon's parity functions with quantum Boolean functions and Svetlichny functions to assess their impact on quantum query complexity.

Algorithmic Development

Once a new functional basis is chosen, we will develop new quantum query algorithms around it. We will compare their performance against classical algorithms in a range of scenarios.

Quantum Simulations

We will employ popular quantum computing frameworks such as Qiskit to run simulations of our algorithms. These simulations will provide insights into the practicality and effectiveness of our newly developed algorithms.

Educational Outreach

Simultaneously, we will develop educational content to demystify the concepts behind our research and make them accessible to a broader audience. This will include interactive tutorials, explanatory videos, and possibly webinars.

5 Work Division

The nature of our project does not warrant specific roles to be assigned to group members. Instead, each student will independently explore research material, collect and present their insights individually to our Advisor. Subsequently, a peer-review process will be undertaken, enabling critical evaluation and scrutiny of one another's contributions. The collective findings will then be condensed into their final analyses.

The project will dynamically adapt to ongoing research developments. Further material to be researched will also be assigned to the group on a weekly basis based on their findings and work so far.

The project does entail a technical aspect where different algorithmic models will be developed, tested and analysed, and these will be done collectively by the group as well.

Basic Elements of Algorithm Development and Research:

1. Conduct an extensive literature review to gather insights from relevant research papers.
2. Focus on the exploration of quantum boolean functions and their potential applications in quantum query complexity; explore the potential to replace quantum boolean functions employed in Simon's algorithm.
3. Lead efforts in developing quantum algorithm prototypes and conducting simulations to assess their performance.
4. Design and execute quantum simulations using quantum computing platforms or simulators.
5. Analyze experimental results and provide critical insights into algorithm performance.

References

[1] J. Watrous. "Quantum computation lecture notes." Latest update: April 11, 2006. (2006), [Online]. Available: https://cs.uwaterloo.ca/~watrous/QC-notes/ (visited on 09/08/2023).

[2] K. Zhang, M. H. Hsieh, L. Liu, and D. Tao, "Quantum gram-schmidt processes and their application to efficient state readout for quantum algorithms," *Physical Review Research*, vol. 3, no. 4, p. 043 095, Nov. 2021. DOI: 10.1103/PhysRevResearch.3.043095.

[3] A. Montanaro and T. J. Osborne, "Quantum boolean functions," *arXiv preprint arXiv:0810.2435*, 2008, Last revised: 2010-08-24 (v5). arXiv: 0810.2435. [Online]. Available: https://arxiv.org/abs/0810.2435.

[4] R. O'Donnell. "15-859bb: Quantum computation and quantum information 2018." (2018), [Online]. Available: https://www.cs.cmu.edu/~odonnell/quantum18/ (visited on 08/17/2023).

[5] R. O'Donnell, *Analysis of Boolean Functions*. Cambridge University Press, Jun. 5, 2014.

[6] R. Mori, "Periodic fourier representation of boolean functions," *arXiv preprint arXiv:1803.09947*, 2018. arXiv: 1803.09947. [Online]. Available: https://arxiv.org/abs/1803.09947.