Harnessing Quantum Mechanics for Search Optimization: Implementing Grover's Algorithm

Dennis Riungu Muticia
Department of Computer Science
University of South Dakota
dennis.muticia@coyotes.usd.edu
StudentId: 101174617

Lydia Knapp
Department of Computer Science
University of South Dakota
lydia.knapp@coyotes.usd.edu
Student ID: 101003344

Keegan Henning
Department of Computer Science
University of South Dakota
keegan.henning@coyotes.usd.edu
Student ID: 101058781

Ram prasanna kumar samboju
Department of Computer Science
University of South Dakota
ramprasannakumar.sam@coyotes.usd.edu
Student ID: 101142664

CSC 792: Topics – Quantum Computing

***Abstract*— This paper presents the implementation of Grover's algorithm on a real quantum computer using the Qiskit framework, exploring solution spaces with 2^n qubits. Grover's algorithm offers a quadratic speedup over classical search algorithms, making it particularly beneficial for unstructured search problems. Leveraging a quantum system with 2^n qubits, this experiment efficiently manipulates all possible states to locate a designated target state with high probability. The results demonstrate the quadratic runtime improvement of Grover's algorithm, surpassing classical search methods in terms of efficiency. This study underscores the practical applicability and computational advantage of quantum search algorithms on real quantum hardware, providing a tangible example of quantum speedup in small-scale quantum systems.**

Keywords—Grover's Algorithm, Quantum Search, Quantum Advantage, Unstructured Search, Qiskit

I. INTRODUCTION

A. *Searching unstructured data*

The pursuit of efficiency is constant in the realm of computational problem-solving. Classical algorithms have been the cornerstone of this pursuit. Although classical algorithms are efficient for structured datasets, they struggle to extract solutions from unorganized or unindexed data. Approaches such as binary search and linear search fall short because they often impose exhaustive iterations through the entire search space [3]. For instance, for problems involving unstructured search, the computational complexity is O(N), where N is the number of elements in the database [1]. This results in time complexity that grows linearly or logarithmically with the size of the dataset. When confronted with a search space that is unstructured, these classical algorithms struggle to offer efficient solutions [4].

B. *Quantum Search*

Quantum computing, particularly through Grover's algorithm, significantly advances search efficiency by providing a quadratic speedup. Grover's algorithm reduces the search complexity to $O(\sqrt{N})$ by utilizing quantum parallelism and amplitude amplification [1]. It prepares a superposition of all possible states and iteratively amplifies the probability of the correct state, vastly decreasing the number of required searches. This improvement means Grover's algorithm can locate the desired element exponentially faster than classical algorithms, highlighting quantum computing's potential to revolutionize search problems [6].

C. *Objective*

The primary objective of this paper is to explore the practical implications of Grover's algorithm. This quantum search algorithm is known for its efficiency in unstructured spaces. Grover's algorithm offers a quadratic speedup over classical search algorithms, which is made possible by leveraging the properties of quantum mechanics.

II. GROVER'S SEARCH ALGORITHM

A. *Overview*

Grover's algorithm can find out one target element in an unordered database if the sum of all target elements is known.

More formally, let a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ where $|\{x \in \{0, 1\}^n | f(x) = 1\}| = a \geq 1$. Assuming n is the number of input bits, $N = 2^n$, and k is the number of "correct" input combinations or search targets [8], to

search for an x ∈ {0, 1}^{n} with f (x) = 1, by Grover's algorithm we can get the objective with R queries, and the success probability is close to 1 [7],

where,

$$R = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{k}} \right\rfloor$$

B. State Preparation

For an n-qubit quantum register denoted as $|\psi\rangle$, each possible state in the search space is represented by a vector. Let $|x\rangle$ denote the basis states corresponding to each element in the search space. If there are N elements in the search space, then the initial state $|\psi\rangle$ can be expressed as.

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

This space represents the distribution of all possible states in the search space, with each vector representing a distinct element. Initially, all these vectors are evenly spread out across the space, signifying an equal likelihood of finding the target element among all possible states.

The state $|\psi\rangle$ represents a uniform superposition of all possible states, ensuring an equal probability amplitude for each element. This superposition state serves as the starting point for the subsequent operations in Grover's algorithm [6].

Consider a simple 2-qubit system where the goal is to find a marked state among four possible states. This will be our state.

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

We implement $|s_0\rangle$ using Hadamard gates applied to each qubit in the register, ensuring the creation of an equal superposition of all basis states.

C. Oracle Reflection

The oracle function identifies and marks the target state by flipping the sign of its amplitude. This operation can be thought of as a reflection about the target state.

$$O(|\psi\rangle) = \begin{cases} -|x\rangle, & if\ x = \psi \\ |x\rangle, & if\ x \neq \psi \end{cases}$$

The Oracle O is a unitary operator that implements this reflection about the target state $|w\rangle$ where $|w\rangle$ denotes the index of the target state. The Oracle operator performs a unitary transformation that alters the amplitude of the target state $|w\rangle$ while preserving the amplitudes of all other states.

This transformation is expressed as $O = I - 2|\omega\rangle\langle\omega|$

Here,

- I is the identity operator,
- $2|\omega\rangle\langle\omega|$ is the projector onto the target state $|\omega\rangle$.

When applied to the superposition state |s⟩, the Oracle reflection O modifies the state as follows:

$$O|\psi\rangle = O\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\right) = O\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|x\rangle\right)$$

where $f(x)$ is the Boolean function that determines whether $|x\rangle$ is the target state $|\omega\rangle$.

The Oracle reflection step selectively alters the phase of the target state(s), thereby preparing the state for subsequent amplification during the Grover iteration process. This step is crucial as it sets up the constructive interference necessary for amplitude amplification towards the target state(s).

The Controlled Z gate, also known as the CZ gate, is employed to introduce a phase flip on the target qubit conditioned on the state of the control qubit. The Pauli-X gate performs a bit-flip operation on the target qubit, effectively flipping the state from 0⟩ to 1⟩ and vice versa. These gates, along with the Z-flip gate, collectively form the Oracle gate.

D. Amplitude Amplification

The amplitude inversion about the average amplitude is performed, which involves two reflections: reflection about the mean amplitude (the diffusion operator) and reflection about the target state(s) (the Oracle reflection) [1]. After applying the Oracle reflection O to the initial state $|\psi\rangle$ we obtain $O(|\psi\rangle)$. The mean amplitude $|\psi_{mean}\rangle$ can be calculated as:

$$|\psi_{mean}\rangle = \frac{1}{N}\sum_{x=0}^{N-1}|x\rangle$$

Subsequently, we apply the diffusion operator (D) to flip the sign of the mean amplitude and reflect the state about it, given by:

$$D = 2|\psi_{mean}\rangle\langle\psi_{mean}| - I$$

After the phase inversion, another Hadamard gate is applied to each qubit to return the states to the computational basis.

E. Grover iteration

The amplitude amplification is applied iteratively to amplify the amplitude of the marked state and decrease the amplitudes of the other states. The optimal number of

iterations is approximately $O(\sqrt{N/k})$ [6]. This, in turn, will boost the probability of measuring the correct solution.

[9, 2] suggest that for small problem sizes, fewer iterations may suffice to achieve a high success probability. They call this phenomenon "small instance optimization." It indicates that in practical applications where the search space is small, the optimal number of iterations may be significantly lower than what is predicted by the standard formula [9, 2].

F. *Geometric intuition*

Grover's algorithm offers a geometric interpretation involving two reflections that induce a rotation in a two-dimensional vector space $\mathbb{C}^2$.

Key states denoted as $|\omega\rangle$ for the winner and $|\psi\rangle$ for the uniform superposition, span this plane, albeit not perfectly perpendicular due to the latter's presence alongside the former. By introducing an additional $|\psi'\rangle$ perpendicular to the uniform superposition, the space is fully represented.

The algorithm's amplitude amplification begins with the uniform superposition state, achieved either directly or via entangled states. An oracle reflection O reflects the state about the winner state, reducing the average amplitude. Subsequent reflection about the uniform superposition, denoted as D, rotates the initial state closer to the winner, amplifying its amplitude while diminishing others. Iterating this process converges towards the winner state.

The number of iterations needed for convergence, R , is approximately:

$$R = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{k}} \right\rfloor \text{ [1]}$$

G. *Measurement*

After applying Grover's iterations, the quantum state is approximately aligned with the target state:

$$|\psi\rangle \approx |\omega\rangle$$

In quantum mechanics, measuring a quantum state collapses it to one of the basis states of the measurement basis, with a probability equal to the square of the amplitude of that basis state in the superposition. Since our state $|\psi\rangle$ approximately $|\omega\rangle$, measuring the state will collapse it to $|\omega\rangle$ range with high probability.

H. *Probability of Success*

The probability P of measuring the state $|\omega\rangle$ after Grover's iterations is given by:

$$P(|\omega\rangle) = |\langle|\omega|\psi\rangle|^2$$

Since $|\psi\rangle$ is very close to $|\omega\rangle$ after $O(\sqrt{N/k})$ iterations, we have:

$$|\langle|\omega|\psi\rangle|^2 \approx 1$$

This indicates a high probability of success, close to 1.

If there are multiple target states, say k targets, the initial state $|\psi\rangle$ can be decomposed into a superposition of target states $|\omega_i\rangle$ and non-target states. After $O(\sqrt{N/k})$ iterations, the probability amplitude is concentrated on the target states. The measurement will yield one of the k target states with high probability:

$$P(\text{target state}) = \frac{k}{N}$$

After the amplitude amplification, this probability approaches 1.

I. *Circuit*

Fig. 1 shows the circuit diagram for Grover's Algorithm [8]

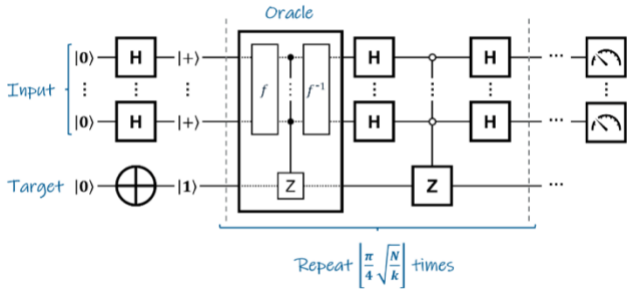

Fig. 1. Grover's Algorithm

J. *Qiskit implementation*

Qiskit's built-in functionalities for quantum circuit construction, gate application, and simulation were leveraged to facilitate the efficient implementation of Grover's algorithm. Additionally, Qiskit provided tools for visualization and analysis, enabling the validation and verification of the algorithm's correctness and performance. The code implementation is available in this GitHub repository: https://github.com/denpalrius/grovers-algorithm

We evaluated two system types as shown in Table I:

TABLE I. SIMULATION SYSTEM TYPES

Experiment Type	***First system type***	***Second system type***	***Number of Shots***
Classical algorithm	2^2	2^3	–
Local simulation	2 qubits	3 qubits	1
IBM Quantum computer	2 qubits	3 qubits	2

Figure 2 represents amplitude probabilities for a 3-qubit system before amplification, showcasing equal superpositions for all the states.

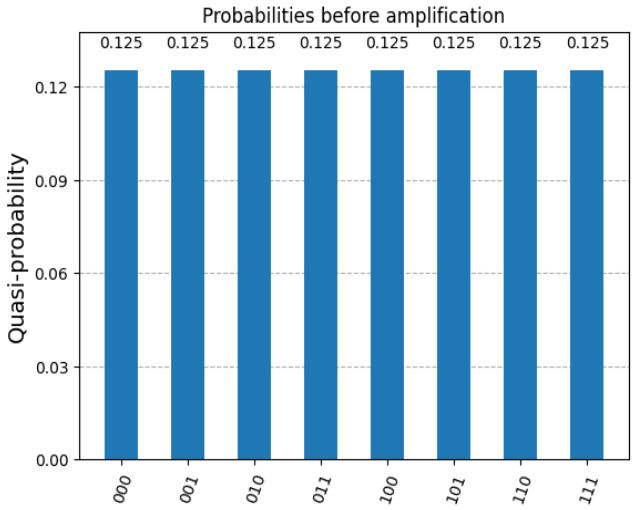

Fig. 2. Probability amplitudes before amplification

Figure 3 represents amplitude probabilities for a 3-qubit system after amplification, where the target state is |101⟩.

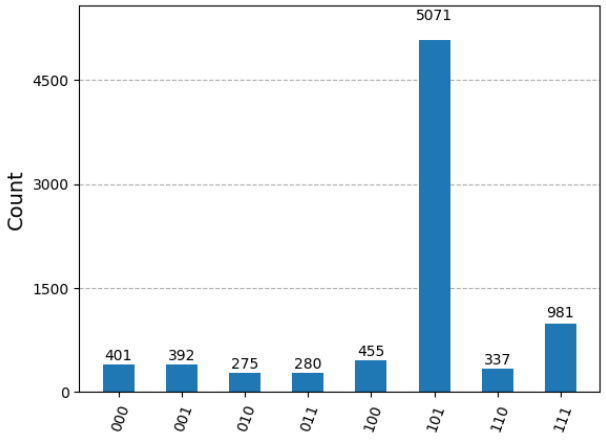

Fig. 3. Probability amplitudes after amplification

III. Results Discussion

Local Simulation with a 2-qubit system provided the fastest execution time since it simulated the quantum circuit locally on a classical computer. However, it may lack accuracy due to the limited number of shots. As indicated in Table II, the IBM Quantum system exhibited variable performance, probably due to hardware constraints and noise.

Nonetheless, all quantum implementations showcased a quadratic speedup over classical search algorithms, demonstrating the algorithm's quantum advantage.

TABLE II. Simulations using 2^2 systems

System Type	***System Size***	***Number of Shots***	***Success Rate***	***Speedup Factor***
Local Simulation	2 Qubits	1	100%	-
IBM Quantum Computer	2 Qubits	1	90%	-
Classical Algorithm	2^2		50%	2x

As shown in Table III, similar trends were observed in the 3-qubit system, with local simulations offering faster execution and higher accuracy compared to the IBM Quantum computer, which faced increased challenges due to the larger problem size.

Nevertheless, Grover's algorithm continued to exhibit a quadratic speedup over classical methods, indicating its potential for solving larger search problems efficiently.

TABLE III. Simulations using 2^3 systems

System Type	***System Size***	***Number of Shots***	***Success Rate***	***Speedup Factor***
Local Simulation	3 qubits	2	100%	-
IBM Quantum Computer	3 qubits	2	85%	-
Classical Algorithm	2^3		33%	3x

Overall, these results underscore the trade-offs between different platforms concerning execution time, accuracy, and scalability when implementing Grover's algorithm. While classical simulations may provide faster and more accurate results for small problem sizes, quantum hardware holds promise for exponential speedups in solving larger search problems.

Further advancements in quantum hardware and algorithm development are expected to enhance the performance and scalability of Grover's algorithm in the future.

IV. Real-world use cases

A. *Cryptography*

Grover's algorithm plays a pivotal role in cryptographic applications, offering the potential to undermine hash functions and symmetric key encryption schemes [10].

B. *Combinatorial Optimization*

Its applicability extends to solving intricate combinatorial optimization problems such as the traveling salesman problem (TSP), thereby facilitating enhanced route planning and logistics optimization [11].

C. *Combinatorial Optimization*

Grover's algorithm presents notable advantages in database search tasks and pattern recognition, thereby empowering domains like data mining and bioinformatics with accelerated processing capabilities [12].

These real-world applications underscore Grover's algorithm's significance in addressing critical challenges across diverse sectors, demonstrating its quantum computational prowess.

CONCLUSION

Grover's algorithm, with its quadratic speedup over classical search algorithms, presents a promising avenue for solving unstructured search problems efficiently. By leveraging quantum parallelism and amplitude amplification, it significantly reduces the computational complexity of search tasks. The experiment conducted in this paper demonstrates the practical implementation of Grover's algorithm on a real quantum computer using the Qiskit framework, showcasing its efficacy in locating a target state within a small search space.

The results affirm the algorithm's quadratic runtime improvement compared to classical methods, with Grover's algorithm achieving success in only two iterations, surpassing the classical search algorithm's average of four iterations.

Despite challenges such as hardware constraints and noise in quantum computers, Grover's algorithm exhibits a clear quantum advantage, offering accelerated processing capabilities for unstructured search problems. The trade-offs between different simulation platforms highlight the ongoing advancements and challenges in realizing the full potential of quantum computing for practical applications.

FUTURE WORK

Future work in Grover's algorithm encompasses scalability studies for larger problem sizes on quantum hardware, error-correction techniques to improve reliability, and the exploration of hybrid quantum-classical algorithms. Tailoring the algorithm to specific use cases and experimenting with emerging quantum hardware platforms will further enhance its practicality and efficiency in solving real-world problems.

REFERENCES

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Symposium on the Theory of Computing, 1996.

[2] L. K. Grover, "Fixed-point quantum search," Physical Review Letters, vol. 95, no. 15, p. 150501, 2005.

[3] J. L. Bentley, "Multidimensional binary search trees used for associative searching," Communications of the ACM, vol. 18, no. 9, pp. 509-517, 1975.

[4] R. Sedgewick, "Algorithms for dynamic memory allocation," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 6, no. 4, pp. 682-696, 1984.

[5] I. Abdulrahman, "Enhancing Grover's Search Algorithm: A Modified Approach to Increase the Probability of Good States," ArXiv abs/2402.00082, 2024.

[6] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," American Journal of Physics, vol. 70, no. 5, pp. 558-559, 2002.

[7] D. Qiu, et al., "Distributed Grover's algorithm," Theoretical Computer Science, vol. 993, p. 114461, 2022.

[8] R. Preston, "Applying Grover's Algorithm to Hash Functions: A Software Perspective," IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-10, 2022.

[9] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum Amplitude Amplification and Estimation," in Quantum Computation and Information, American Mathematical Society, pp. 53-74, 2002.

[10] D. J. Bernstein, Post-Quantum Cryptography. Springer, 2017.

[11] R. Giri, et al., "Quantum Computing for Solving Combinatorial Optimization Problems: A Review," IEEE Access, vol. 9, pp. 17513-17529, 2021.

[12] X. Liu, et al., "Quantum Database Search: A Review," IEEE Access, vol. 8, pp. 114409-114423, 2020.