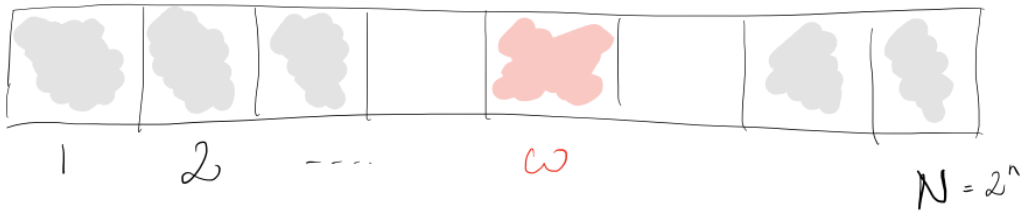
Computational Complexity of a 4-Qubit Grover's Search Algorithm

Saasha Joshi
UE173085
BE CSE (7th Semester)

Abstract

Grover's Algorithm is a Quantum Algorithm which conducts a search on an unsorted dataset with N entries in O(√N) time and O(logN) storage space [1]. Classically, performing a linear search on an unsorted dataset takes O(N) time in the worst-case scenario. Whereas, Grover's Algorithm implemented on a Quantum Computer provides a quadratic speed up to the same problem.

Suppose we are given a large list of N items. Among these items there is one item that we wish to locate; we will call this one the winner (w). Let us say all items in the list are gray except the winner (w), which is pink.



To find the pink box -- the marked item -- using classical computation, we would have to check on average N/2 of these boxes, and in the worst case, all N of them. On a quantum computer, however, we can find the marked item in roughly √N steps with Grover's amplitude amplification trick. A quadratic speedup is indeed a substantial time-saver for finding marked items in long lists [2].

Purpose

The purpose of this project is to implement Grover's algorithm in a search space of 4 qubits. The project would start by discussing the basic concepts of qubits in a Quantum Computer and lead to an analysis of Grover's Search Algorithm on a real Quantum

Computer (IBM). In addition to the implementation of the quantum algorithm, the project would discuss the computational complexity of Grover’s Algorithm and would conclude by comparing the theoretical and real-life execution results of the algorithm [3, 4].

Topics to Discuss in the Project: Quantum Computers, Qubits, Grover’s Algorithm, Computational Complexity, Oracle, Amplitude, Theoretical Results, Execution Results.

Execution Timeline

- **September 2020 -** Study Grover’s Algorithm
- **October 2020 -** Implement Grover’s Algorithm with Qiskit SDK
- **November 2020 -** Analysis of the results obtained
- **December 2020 -** Compilation of the results and insights

Further Research

The Grover’s Algorithm can be further implemented on the following cryptanalysis schemes:

1. Grover Oracles for Advanced Encryption Standard (AES) [5]
2. Grover Algorithm on Simon Cipher [6]

(If possible to extend the Minor Project by a few months, one of the above tasks can also be completed)

References

1. Grover LK. A fast quantum mechanical algorithm for database search. InProceedings of the twenty-eighth annual ACM symposium on Theory of computing 1996 Jul 1 (pp. 212-219).
2. https://qiskit.org/textbook/ch-algorithms/grover.html
3. Figgatt C, Maslov D, Landsman KA, Linke NM, Debnath S, Monroe C. Complete 3-Qubit Grover search on a programmable quantum computer. Nature communications. 2017 Dec 4;8(1):1-9.
4. Strömberg P, Blomkvist Karlsson V. 4-qubit Grover's algorithm implemented for the ibmqx5 architecture.
5. Jaques S, Naehrig M, Roetteler M, Virdia F. Implementing Grover oracles for quantum key search on AES and LowMC. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2020 May 10 (pp. 280-310). Springer, Cham.
6. Anand R, Maitra A, Mukhopadhyay S. Grover on SIMON. arXiv preprint arXiv:2004.10686. 2020 Apr 22.