Design of Grover’s Algorithm over 2, 3 and 4-Qubit Systems in Quantum Programming Studio

Diana Jingle, Shylu Sam, Mano Paul, Ananth Jude, and Daniel Selvaraj

Abstract—In this paper, we design and analyse the Circuit for Grover’s Quantum Search Algorithm on 2, 3 and 4-qubit systems, in terms of number of gates, representation of state vectors and measurement probability for the state vectors. We designed, examined and simulated the quantum circuit on IBM Q platform using Quantum Programming Studio. We present the theoretical implementation of the search algorithm on different qubit systems. We observe that our circuit design for 2 and 4-qubit systems are precise and do not introduce any error while experiencing a small error to our design of 3-qubit quantum system.

Keywords—quantum search; Oracle; Qubit; Hadamard transform; phase shift

I. INTRODUCTION

Quantum Search [9], [10] is a technique that can be used to speed up many classical search algorithms. It performs a generic search for a potential solution to a very wide range of problems. For example, given a large integer of size $N$, the problem is to determine whether an numeral $p$ is a non-trivial factor of $N$ with no prior knowledge about the structure of the information. A simple strategy for finding the non-trivial factors is to search through the set until found. Classically, this problem requires approximately $N$ operations, but a Grover’s search algorithm requires approximately $\sqrt{N}$ operations with probability $> 1/2$.

Grover’s Algorithm can be used to searching an actual database but no research has been published on this area. Researchers consider Oracle as Virtual Database to perform searching. The searching time on the database depends upon the size of the database and the quantum hardware. Therefore it is necessary to provide an analysis on designing the quantum circuit using simulation tools. In this paper, we used quantum programming studio for precisely designing the quantum circuit for Grover’s search algorithm on 2, 3 and 4-qubit system so as to reduce the errors in the design. We have also presented the step-wise procedure of Grover’s algorithm theoretically for better knowledge on the algorithm.

The paper is organized as follows: Section 1 presents the significance of Quantum Search Algorithm and its applications. Section 2 provides analysis of existing approaches and their observations on Grover’s search algorithm. Section 3 presents a brief overview on the working principle of Grover’s algorithm. Section 4 presents the implementation and performance results of Grover’s Algorithm for 2, 3, and 4-qubit systems and finally we conclude in Section 5.

II. LITERATURE SURVEY

In [2], a 4-qubit quantum algorithm was implemented on ibmqx5 architecture which was largely published and currently possible and the performance accuracy of their implementation results were compared with simulation results. Their implementation performance requires more hardware support as they faced a complexity in circuit design. In [4], a classical-quantum search algorithm was proposed to find the shortest path of a given graph. Grover’s algorithm cannot be applied to search an item in an actual database. In [5], the theoretical operation of quantum error correction process was demonstrated using QCAD simulator with possible results. Grover’s algorithm can be used to search a single object in an unsorted database. In [6], a generalized Grover’s Algorithm was framed to support multi-object search in a large and unsorted database and they have provided consistent results with Grover’s algorithm for single-object search. The authors in [8] implemented Grover’s algorithm on a real ibmqx4 5-qubit quantum computer. A 4-qubit implementation of Grover’s Search Algorithm was proposed in [11] with test results in which it was observed that quantum computers can accurately solve only simple problems with small amounts of data. In [14], a two-transmon-qubit interaction was designed in a circuit QED to improve the implementation time of Grover’s search algorithm in nanosecond-scale. The Grover’s algorithm was implemented using two trapped atomic ion qubits in order to improve the searching speed. In [15], the Grover’s algorithm was tried in a scalable system to improve the success probability of the search item. Implementation of 2-Qubit quantum algorithm was performed in [12] using a linear optical chip and a 3-qubit quantum circuit was designed and implemented in [13].

III. GROVER’S QUANTUM SEARCH ALGORITHM

Lov Grover in 1996 [1] invented the Grover Search algorithm to perform the fastest possible quantum search for an unsorted database which takes $O(\sqrt{N})$ time and $O(\log N)$ storage space. This mean that, for a list of 108 elements, the number of iterations required to search a desired item is order of 10000 and the obtained result will be accurate with a probability close to 1. Although Grover's algorithm provides only a quadratic speedup, it is considerable when the size of $N$ is large. TABLE 1 shows the Grover’s algorithm and Fig. 1 shows its circuit representation.
The step-wise explanation of the Grover’s algorithm is described as follows: The algorithm begins in the state $|0\rangle^\otimes n$. Now apply Hadamard transform $H^\otimes n$ on the first $n$ qubits and Pauli X transform and Hadamard transform (HX) to the last qubit to obtain equal superposition state; the operation is described as,

$$ H^\otimes n|0\rangle^\otimes n = |\psi\rangle = \frac{1}{\sqrt{2^N}}\sum_{x=0}^{2^N-1} |x\rangle $$

(2)

$$ HX|1\rangle = \left[|0\rangle - |1\rangle\right] $$

(3)

where $|\psi\rangle = \frac{1}{\sqrt{2^N}}\sum_{x=0}^{2^N-1} |x\rangle$ is the superposition of all basis states. Now apply the Grover’s operator. The quantum circuit of Grover iteration is broken up into four steps namely, i) Oracle function, ii) Hadamard transform, iii) Conditional phase shift operation on every computational basis state except $|0\rangle$ receiving a phase shift of $-1$ and iv) Hadamard transform. The oracle is a unitary operator, $O$, which performs the following operation:

$$ |x\rangle|q\rangle \rightarrow |x\rangle|q\oplus f(x)\rangle $$

(4)

where $|x\rangle$ is the input register that stores the index of all elements from 0 to $N-1$, $\oplus$ denotes addition modulo 2, $|q\rangle$ is the oracle qubit which is flipped if $f(x) = 1$, and is unchanged otherwise. The term ancilla or ancillary qubit can be used to refer the oracle qubit $|q\rangle$ as it adds some extra qubits for the algorithm. If $x$ is not found, applying the oracle to the state does not change the state. But if $x$ is found, then the final state is changed to a new state. The oracle used for Grover’s algorithm is very simple. Applying the oracle to inputs $|x\rangle|q\rangle$ will produce output as $|x\rangle|q\oplus f(x)\rangle$. The first two qubits are unmodified (in case when $x = \{0,1\}$). The third qubit is flipped if the first two qubits are 1. Thus we get,

$$ |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow |x\rangle|0\rangle $$

(5)

Equation (5) can be written as,

$$ |x\rangle \rightarrow (-1)^{f(x)}|x\rangle $$

(6)

Steps 2, 3 and 4 can be represented as, $H^\otimes n(2|x\rangle\langle x|)H^\otimes n = 2|\psi\rangle\langle\psi| - 1$ and the Grover’s operator can be denoted as, $G = (2|\psi\rangle\langle\psi|-1)O$. The Grover’s algorithm is regarded as a rotation of $R$ times within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$ and $\theta$ is a real number ranging from 0 to $\pi/2$ and it can be expressed in superposition state as,

$$ |\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{1}{N}}|\beta\rangle $$

(7)

where $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}}\sum_{x=0}^{M-1} |x\rangle$ and $|\beta\rangle \equiv |u\rangle$. The rotation can be expressed as, $R \leq \frac{\pi}{2}\sqrt{\frac{2N}{M}}$ and therefore, $R = O(\sqrt{N/M})$. If $M = 1$, i.e., if the solution is found in one iteration of Grover’s algorithm, then $R = O(\sqrt{N})$.

### IV. IMPLEMENTATION AND PERFORMANCE ANALYSIS

In this section, the system design, implementation and performance results are discussed for 2-qubit, 3-qubit and 4-
qubit system. We implemented the algorithm on Quantum Programming Studio, a web-based IDE and simulator for designing, inspecting and simulating/running quantum algorithms on platforms like IBM Q, Rigetti and Google Cirq. Quantum-circuit is open source simulator implemented in JavaScript. A Quantum-circuit runs 20+ qubit simulations at server (node.js) or in browser. Quantum Circuit can be imported from OpenQASM and Quil. After designing the Quantum circuit in IDE, it can also be exported to OpenQASM, pyQuil, Quil, Qiskit, Cirq, TensorFlowQuantum, QSharp, and QuEST, so it can be used for conversion between quantum programming languages. It is observed that, each quantum gate when applied, creates a small error to the quantum state. This is due to the circuit design and the interaction of each qubit with other qubits and gates.

1) Implementation with 2-Qubits

Assume \( n = 2 \), the possible states are \( N = 2^2 = 4 \) and suppose the solution is found at index 2 i.e., state \(|10⟩\), then we get,

\[
|ψ⟩ → \frac{1}{2}(|00⟩ + |01⟩ - |10⟩ + |11⟩)
\]  

(8)

Thus the action of oracle operator on the state \(|x⟩\), changes the amplitude of that state. Now apply the Hadamard transform \( H^{⊗n} \) on these basis states and the result is shown as,

\[
|ψ⟩ \xrightarrow{H^{⊗n}} \frac{1}{2}(|00⟩ - |01⟩ + |10⟩ + |11⟩)
\]  

(9)

Now perform a conditional phase shift on every computational basis state except \(|0⟩\). Thus we get,

\[
|ψ⟩ \xrightarrow{\text{phase}} \frac{1}{2}(|00⟩ + |01⟩ - |10⟩ - |11⟩)
\]  

(10)

Again apply the Hadamard transform \( H^{⊗n} \) to the obtained superposition states, we get the matched element on an index and for our example it is given as,

\[
|ψ⟩ \rightarrow |10⟩
\]  

(11)

Thus when \( n = 2 \) for the state \(|10⟩\), we got the desired search with just one iteration of the Grover’s algorithm. Figure 2 shows the quantum circuit diagram for 2-qubit system with 22 gates. The circuit of 2-qubit system produces no error and thus it is free from random noise in the system. The vector representation and measurement probability for the 2-qubit state are shown in Figure 3 and Figure 4 respectively.

2) Implementation with 3-Qubits

Figure 5 shows the quantum circuit diagram for 3-qubit system with 39 gates. The circuit of 3-qubit system produces high error rate and thus introduces random noise in the system. The vector representation and measurement probability for the 3-qubit state are shown in Figure 6 and Figure 7 respectively. When \( n = 3 \), the possible states are \( N = 2^3 = 8 \), and suppose the solution is found at index 4 in state \(|10⟩\), then we get,

\[
|ψ⟩ \xrightarrow{H^{⊗n}} \frac{1}{2}(|000⟩ + |001⟩ + |010⟩ + |011⟩ + |100⟩ + |101⟩ + |110⟩ + |111⟩)
\]  

(12)

Thus the action of oracle operator on the \(|x⟩\), changes the amplitude of that state. Now apply the Hadamard transform \( H^{⊗n} \) on these basis states and the result is:

\[
|ψ⟩ \xrightarrow{H^{⊗n}} \frac{1}{2}(|000⟩ + |001⟩ + |010⟩ + |011⟩ - |100⟩ + |101⟩ + |110⟩ + |111⟩)
\]  

(13)

Thus for \( n = 3 \), the desired state is obtained in 2 iterations of the Grover’s algorithm.
80

DIANA JINGLE, SHYLU SAM, MANO PAUL, ANANTH JUDE, DANIEL SELVARAJ

Fig. 5. Quantum Circuit Diagram for the state $|100\rangle$

Fig. 6. Vector Representation of 3-qubit system for the state $|100\rangle$

Fig. 7. Measurement Probability of 3-qubit system for the state $|100\rangle$

3) Implementation with 4-Qubits

Figure 9 shows the quantum circuit diagram for 4-qubit system with 34 gates and it does not produce any noise and error in the design of the system. The vector representation and measurement probability for the 2-qubit state are shown in Figure 10 and Figure 11 respectively. When $n = 4$, the possible states are $N = 2^4 = 16$, assume the solution is found at index 4 i.e., $|0100\rangle$, we get,

$$ |\psi\rangle \rightarrow 1/2(|0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle + |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle)$$

(16)

The state of the system after applying Hadamard transform $H^{n}$ on $|x\rangle$, is shown as:

$$ |\psi\rangle \rightarrow H^{n} |x\rangle$$

(17)

The result after performing a Conditional Phase Shift, on all the basis state except $|0000\rangle$ is shown as,

$$ |\psi\rangle \rightarrow \frac{\epsilon_{\text{phase}}}{2} (|0000\rangle - |0001\rangle - |0010\rangle - |0011\rangle + |0100\rangle - |0101\rangle - |0110\rangle - |0111\rangle + |1000\rangle - |1001\rangle - |1010\rangle - |1011\rangle - |1100\rangle - |1101\rangle - |1110\rangle - |1111\rangle)$$

(18)

$$ |\psi\rangle \rightarrow |0100\rangle$$

(19)

After applying $H^{n}$ to the states, the matching is found. Thus for $n = 4$, the desired state is obtained in 3 iterations of the Grover’s algorithm.

Fig. 8. Measurement Probability of 3-qubit system for the state $|100\rangle$
Fig. 9. Quantum Circuit Diagram for the state $|0100\rangle$

Fig. 10. Vector Representation of 3-qubit system for the state $|0100\rangle$
Quantum Search Algorithms can be potentially applied i) for efficiently counting the number of solutions for a given search problem; ii) speedup the solution of NP-complete problems, iii) finding the shortest path between two cities [7], and iv) searching problems or extracting statistics in unstructured databases [6] more quickly than using classical computing. We have also provided Quantum Programming Studio tool for designing the circuit representation and measurement probability. We used analysis in terms of number of gates used, vector representation and measurement probability. We have also provided theoretical knowledge on the algorithm for 2, 3 and 4-qubit systems and presented our analysis in terms of number of gates used, vector representation and measurement probability. We used Quantum Programming Studio tool for designing the circuit diagram precisely on IBM Q platform. We have also provided theoretical knowledge on the algorithm for 2, 3 and 4-qubit system. In future, we will plan to use the search algorithm for real-time scenario.

ACKNOWLEDGEMENTS

We are very grateful to experts for their appropriate and constructive suggestions to improve this template.

REFERENCES


