Implementation Grover's search algorithm on IBM Eagle r3

Luu Thi Thu Hong*, Nguyen Duy Ninh

Institute of Electronic, Academy of Military Science and Technology, 17 Hoang Sam, Cau Giay, Hanoi, Vietnam.

*Corresponding author: thuhong.11@gmail.com

Received: 30 Sep. 2024; Revised 09 Nov. 2024; Accepted 12 Nov. 2024; Published 25 Nov. 2024.

DOI: https://doi.org/10.54939/1859-1043.j.mst.99.2024.119-124

ABSTRACT

Nowadays, quantum computing has emerged as a global technology trend, attracting active research worldwide. One of the most popular quantum algorithms is the quantum search algorithm, commonly known as Grover's algorithm, for unstructured search purposes. This paper presents the implementation of the algorithm with a search space of 3 to 10 qubits using the Python-based Qiskit tool developed by IBM. The implementation results on the IBM QSAM simulator and on the IBM Eagle r3 quantum hardware are analyzed and compared. This paper also provides results with circuits of varying iteration numbers. Finally, the paper discusses the advantages of this quantum search algorithm compared to traditional methods, and the obstacles towards realizing its hardware implementation.

Keywords: Quantum Computing; Grover Algorithm; Qubit; IBM; Oracle.

1. INTRODUCTION

Grover's algorithm was created to solve the problem of searching in an unsorted database, also known as the "needle in the haystack" problem. It allows to reduce the search time from O(N) to $O\left(\sqrt{N}\right)$ which is the optimal search algorithm [1]. This algorithm is applied to solve many practical problems in medicine [2], financial optimization [3], security [4], etc.

Although Grover's search algorithm is a promising technique with a wide range of potential applications, published papers on the algorithm's hardware implementation only feature circuits with 4 qubits at most [6-9] with the highest probability achieved when using NISQ (Noisy Intermediate Scale Quantum computer) being 25%. In [6], higher probabilities were achieved by using an oracle structure without ancilla qubits, combined with error-correcting codes. However, with 5 qubits, the search results were still indistinguishable. On the other hand, in the co the results reported in [7-9] are not useful results, but the circuits were implemented on older quantum hardware with capabilities limited to only 5 or 16 qubits. With the rapid and consistent advancements in quantum hardware over the years, today, IBM offers a wide range of cloud-accessed quantum computers for public use, some with over 100 qubits intergrated. Our goal in this paper is to evaluate the implementation efficiency of Grover's algorithm, and experiment on the IBM Eagle r3, featuring 127 qubits and improved qubit coherence time. The subsequent section of this paper is presented as follows: 2-Overview of Grover's algorithm; 3-Implementation; 4-Results and Discussion and 5-Conclusion.

2. OVERVIEW OF GROVER'S ALGORITHM

To state the problem, consider an unstructured data array $X=\{x_0,x_1,...,x_{N-1}\}$ and some combinatorial function $f : X \rightarrow \{0,1\}$, whose goal is to find an element x that satisfies

$f\left(x\right)=1$. The search problem is expressed as: $f(x)=\begin{cases}0 & ;x\neq\omega\\ 1 & ;x=\omega\end{cases}$ (1)

with ω being the element to be searched. The problem is to find ω one of N possible states of the search space consisting of n qubits.

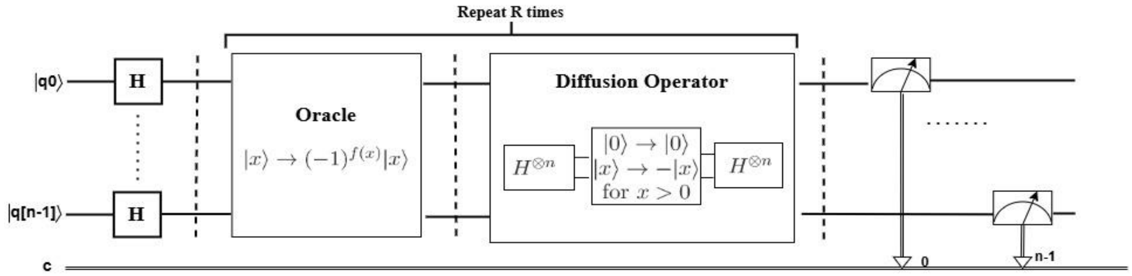

Figure 1. *Grover's algorithm [5].*

As shown in Fig.1, Grover's algorithm is implemented in four stages: initialization, oracle (search state marking), diffusion operator (amplitude amplication) and measurments. Also, the subroutine known as the Grover's Operator (G) which includes the oracle and diffusion stages [5] can be repeated multiple times. The workings of Grover's algorithm can be summarized as follows:

The initialization process prepares the superposition states by passing all qubits through Hadamard gates (H). The desired state is then searched and marked by changing the sign of its amplitude at the oracle. At this stage, although marked, the search state's probability is still indistinguisable from other states. The diffusion operator then amplifies this difference by flipping all state amplitudes by the their average value. This not only recovers the sign of the search state but also amplifies its amplitude, making its probability more significant than others. For larger search spaces with more qubits, the oracle and diffusion steps are required to be repeated R times to ensure clear seperation of the search state. At measurements, the search state with higher amplitude will yield significantly higher probability, and the search is complete.

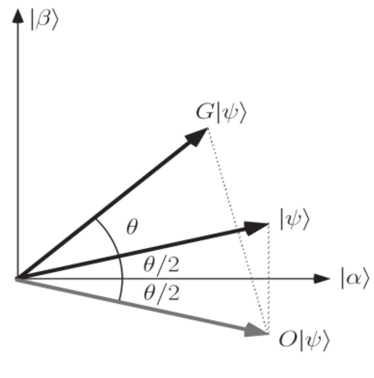

Figure 2. *The action of a single Grover iteration, G [5].*

The effect of single Grover's iteration can be visualized in Fig.2. Grover iterations aim to move $\left|\psi\right\rangle$ closer to vector $\left|\beta\right\rangle$ so that the measured value is $\left|\beta\right\rangle$ with high probability. After step 2, the state of the circuit is at position $O\left|\psi\right\rangle$. After step 3, completing one

Grover iteration, the state of the circuit is at position $G|\psi\rangle$. After each iteration, the state vector of the circuit rotates by angle θ towards $|\beta\rangle$. After R iterations, the angle between the superposition state of the circuit and $|\alpha\rangle$ is $R.\theta+\frac{\theta}{2}$. The optimal number of iterations is such that this angle approaches $\pi/2$ as $R\sim\frac{\pi}{4}\sqrt{2^n}-\frac{1}{2}$. Choose the number of iterations approximately R.

3. IMPLEMENTATION

The algorithm is implemented with the number of qubits n varying from 3 to 10 qubits. The implementation circuit consists of n Hardamard gates (Fig.1) and a Grover iteration circuit. Fig.3 shows an example implementation of a Grover iteration that includes steps 2 and 3 of the algorithm. The oracle is an operator able to recognize the target state and mark it by phase shifting: $|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$. In this paper, we use an oracle circuit with no ancilla qubits proposed in [6]. First, the oracle uses NOT gates, denoted X, on qubits with value $|0\rangle$ in the search state. This will turn the search state and only the search state to the full positive state $|11...1\rangle$. The Z gate inverts the states $|1\rangle$ and does not invert the phase with $|0\rangle$. The CZ (Control Z) gate applies a phase flip (change in the relative phase) to the target qubit only when the control qubit is in the state $|1\rangle$. According to [5], HXH = Z, we can create $C^{n-1}Z$ as the structure in Fig.3. Next, the $C^{n-1}Z$ (Control-Z) gate, with only the last qubit being controlled by the rest of the qubits, transforms the state $|11...1\rangle$ into $-|11...1\rangle$. The following X gates recovers the search state, this time with phase π.

The structure of the diffusion operator is in the form HX+Oracle+XH [5] (Fig.3). Increasing the number of qubits, the schematic of single Grover iteration is repeated R times.

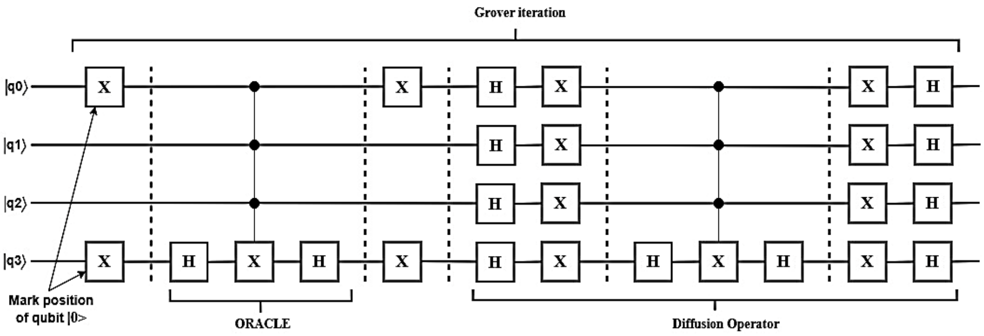

Figure 3. *Schematic of single Grover iteration for 4 qubit search* $|0110\rangle$.

4. RESULTS AND DISCUSSION

4.1. Setup

The circuit designs were implemented on Jupyter notebooks using IBM Qiskit version 1.2. The notebooks and other auxilary files can be found on the Github repository:

https://github.com/NinhVDT/mach_luong_tu_co_ban. The circuits are run in three scenarios: ideal simulation, noisy simulation and actual quantum hardware. In the ideal scenario, the circuit is ran on a digital QASM simulation on a local computer. There is no noise and strictly theoretical results are expected. The second scenario, the noise was modeled after the ibm_sherbrooke quantum computer. In the third experiment scenario the circuits are run on cloud-based quantum hardware, namely ibm_sherbrooke, ibm_kyiv and ibm_kyoto, all using 127-qubit Eagle r3 quantum chips. In each runthrough in these three scenarios, the number of shots is set to be 4096.

4.2. Results and Discussion

Table 1 summarizes the experimental results of this paper. According to table 1, the ideal simulation results show that with only $O\left(\sqrt{N}\right)$ executions, Grover's algorithm gives a probability of finding the target of nearly 100%. However, noise has a very large impact, so the probability when simulating with noise is greatly reduced, especially when the number of qubits increases and the circuit structure is more complicated. From 5 qubits or more, the simulation result with noise is not feasible, it is impossible to distinguish the target state from other states.

As the iterations increase, the more complex the circuit is, and the more interference occurs. For the 3 qubit case, with fewer iterations, the ideal simulation gives a result that is significantly lower than the theoretical one by 17.5%, but the actual run gives a probability 6.2% higher (Fig.4, Fig.5). The results are similar to the 4 qubits case. Thus, in practice, the appropriate number of iterations should be chosen based on the calculated value of the number of loops, the corresponding idealsimulation probability achieved, and the complexity of the circuit.

Comparing with results from similar works (table 2), for the 4 qubit problem, the execution on IBM servers has a higher probability of finding 9.3% compared to [7]-[9] due to the improvement of IBM's current quantum chip and the oracle structure not using ancilla qubits. This and the results from [7-9] are significantly lower than that in [6], which employs an error correcting technique.

Table 1. *Simulation results and hardware experiments.*

n	R	Probability (%)		
		Ideal simulation	Simulation with noise	IBM Eagle r3
3	1	77,81	64,48	50,71
	2	95,21	64,6	44,56
4	2	90,04	49,17	9,3
	3	96,68	50,2	6,84
5	3	90,14	14,18	3,15
	4	99,9	9,47	3,13
6	5	96,6	x	x
	6	99,66	x	x
7	8	99,58	x	x
8	12	99,98	x	x
9	17	99,98	x	x
10	25	99,93	x	x

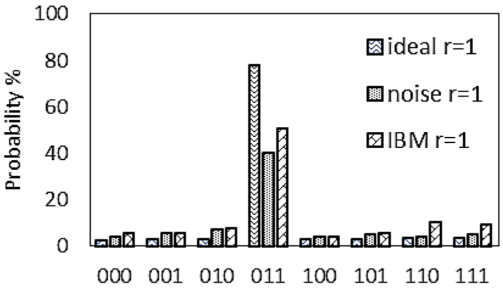

Figure 4. *Experiments with 3 qubit $|011\rangle$, r = 1.*

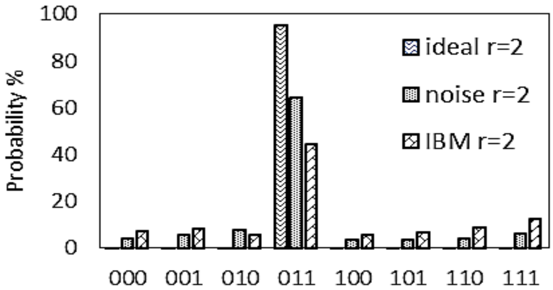

Figure 5. *Experiments with 3 qubit $|011\rangle$, r = 2.*

Table 2. *Experiment with different implementations.*

	This paper	[7]-2021	[8]-2018	[9]-2018	[6]-2023
Quantum hardware	Eagle r3 127 qubit	IBMQ 5 qubit	IBMQX5 16 qubit	IBM Q 5 qubit	NISQ 27 qubit
Probability	9,3%	4,96%	6,62%	6,56%	25%

5. CONCLUSIONS

This paper has implemented the algorithm with cases from 3 qubits to 10 qubits with different iterations according to the Oracle circuit structure without using ancilla qubits. The simulation results are ideally consistent with the theory, showing the advantage of Grover's algorithm over traditional search methods. With 4 qubits, the paper gives a finding probability of 9.3%, which is better than some published results on circuit structures using ancilla qubits and older versions of IBM quantum computers. However, the implementation results on current quantum hardware are still very limited, requiring additional error-correcting codes to improve the results. The next research direction of the paper is to combine error-correcting codes to improve the results with cases with more qubits.

REFERENCES

[1]. C. Zalka, "*Grover's quantum searching algorithm is optimal*," Physical Review A, *(*1999).
[2]. Ma, P., Chen, Y., Lu, H., & Zhong, W. *"Bisection Grover's Search Algorithm and Its Application in Analyzing CITE-seq Data"*. Journal of the American Statistical Association, 1–20, (2024). https://doi.org/10.1080/01621459.2024.2404259.
[3]. Orús, R., Mugel, S., & Lizaso, E. "*Quantum computing for finance: Overview and prospects."* Reviews in Physics, 4, 100028, (2019). https://doi.org/10.1016/j.revip.2019.100028.
[4]. Vu, M. T., Nguyen, V. N., Le, Q. D., & Do, Q. T. *"Demonstration of Grover's algorithm for retrieving secret keys in a basic SPN block cipher". CTU Journal of Innovation and Sustainable Development*, *16* (Special issue: ISDS), 8-16, (2024). https://doi.org/10.22144/ctujoisd.2024.317
[5]. I. L. C. Michael A. Nielsen, "*Quantum Computation and Quantum Information*", Cambridge University Press, (2011).
[6]. Y. El Kaderi, A. Honecker and I. Andriyanova, "*Performance of Uncoded Implementation of Grover's Algorithm on Today's Quantum Processors*" 2023 IEEE Information Theory Workshop (ITW), Saint-Malo, France, pp. 209-214, (2023), doi: 10.1109/ITW55543.2023.10160239.
[7]. Saasha Joshi, Deepti Gupta, "*Grover's Algorithm in a 4-Qubit Search Space*", Journal of Quantum Computing, Vol.3, No.4, (2021). Doi: 10.32604/jqc.2021.018114.

[8]. P. S. Vera Blomkvist Karlsson, "*4-qubit Grover's algorithm implemented for the ibmqx5 architecture*," (2018). [Online]. Available: https://www.diva-portal.org/smash/get/diva2:.
[9]. A. Mandviwalla, K. Ohshiro and B. Ji, "*Implementing Grover's Algorithm on the IBM Quantum Computers*" 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, pp. 2531-2537, (2018), doi: 10.1109/BigData.2018.8622457.

TÓM TẮT

Thực thi thuật toán tìm kiếm Grover trên IBM Eagle r3

Hiện nay, máy tính lượng tử đang là một xu hướng công nghệ được đẩy mạnh nghiên cứu trên thế giới. Một trong các thuật toán lượng tử phổ biến nhất là thuật toán tìm kiếm lượng tử, thường được biết đến với tên thuật toán Grover, cho các mục đích tìm kiếm không cấu trúc. Bài báo này trình bày thực thi thuật toán với không gian tìm kiếm từ 3 qubit tới 10 qubit sử dụng công cụ Qiskit dựa trên ngôn ngữ lập trình Python do IBM phát triển. Kết quả thực thi trên mô phỏng QSAM IBM và trên phần cứng lượng tử IBM Eagle r3 được phân tích và so sánh. Bài toán cũng cung cấp các kết quả với các trường hợp số lần lặp khác nhau. Nhìn chung, bài báo mô tả những ưu điểm của thuật toán tìm kiếm lượng tử so với phương pháp truyền thống, đồng thời các vấn đề cần đối mặt để hiện thực hoá điều đó.

Từ khoá: Máy tính lượng tử; Thuật toán Grover; Qubit; IBM; Oracle.