Comparison of Quantum and Classical Algorithm in Searching a Number in a Database Case

Zhiyao Wang*

Faculty of Science, University of Waterloo, Waterloo, Canada

*Corresponding author: z2425wan@uwaterloo.ca

Abstract. Contemporarily, quantum computing is one of the hottest research fields. Many quantum algorithms are proposed in order to utilize the power of quantum computers. Grover's searching algorithm is one of them. In this article, by comparing a classical searching algorithm and Grover's algorithm in the problem of finding a number in a finite database, the advantages of the latter are discussed. The actual quantum circuit to solve the problem is built and run on both a simulator and a real quantum computer. According to the analysis, Grover's algorithm provides speedup in a searching task compared to the classical algorithm. However, noises in today's quantum devices make the result of the quantum algorithm unreliable. In searching for multiple numbers, Grover's algorithm has its shortcomings. Nevertheless, noises in quantum computing need to be addressed in order to utilize the potential of quantum computers in solving difficult problems. These results shed light on guiding further exploration of quantum algorithms and quantum computing.

Keywords: Grover's algorithm; classical search algorithm; quantum computing.

1. Introduction

Richard Feynman, in 1982, talked about the idea of a quantum computer in his lecture. He discussed the fundamental disability of using a traditional computer to simulate quantum mechanics. More specifically, the size of the simulator based on a traditional computer needs to grow exponentially if the size of particles increases linearly. He thus proposed a quantum computer, which can possibly simulate physics [1]. Contemporarily, the field of quantum computing was hugely developed. From 1923 to 2020, there were 19778 publications related to quantum computing research [2]. In particular, the developments in algorithms show that quantum computers have the potential to solve computationally difficult problems. Hence, it takes a tremendous amount of time to solve for classical computers. Deutsch-Jozsa algorithm, purposed by David Deutsch and Richard Jozsa in 1992, first showed that for a designed problem, quantum computers can solve it exponentially faster than classical computers [3]. It used a toy problem to show the potential of quantum computing. Shor's algorithm is one of the most famous quantum algorithms. In 1999, Peter W. Shor proposed a quantum algorithm that can factor integers in a reasonable time scale [4]. The importance of this algorithm is that one can crack RSA cryptography by factoring a large integer into two prime numbers and RSA cryptography is used in many aspects of today's digital world [5, 6]. Grover's algorithm, which is the main focus of this article, was purposed by Lov Grover in 1996. This algorithm can speed up the searching process of finding desired elements in a database [7]. The details of Grover's algorithm will be discussed in this article.

From the time that quantum computers were purposed, many types of physical implementations of quantum computers based on different technologies were built. One of the quantum computers based on nuclear magnetic resonance is the SpinQ Gemini quantum computer built by SpinQ Technology in 2021. It is a commercial, 2-qubit, desktop quantum computer for educational purposes [8]. Although it only has two qubits, which is simple, students and researchers can use this desktop to study quantum computing more easily compared to large quantum computers in laboratories. The other quantum computer based on ion traps is the quantum computing demonstrator built in 2021. It has 50 qubits and has the same size as two 19-inch racks [9]. This demonstrator demonstrates the application of complicated quantum computers outside laboratories. For the most cutting-edge quantum computers, IBM released its 127-qubit quantum computer Eagle in November 2021 [10].

Researchers can use IBM Quantum Experience platform to build quantum algorithms and run them on this novel quantum computer online. Online access to laboratory-level quantum computers often refers to as cloud quantum computing, is the general way for researchers to use cutting-edge quantum computers.

The purpose of this article is to discuss the potential of quantum computers based on Grover's algorithm by describing the detail of Grover's algorithm, a searching algorithm, and comparing it with a classical algorithm. First, the fundamentals of quantum mechanics and quantum computing are described. Next, the rationale and mathematics of Grover's algorithm are discussed. The case in which Grover's algorithm is applied to the task of finding a particular integer in a database containing integers from 0 to 63 is present to show the quadratic speedup of Grove's algorithm. The corresponding quantum circuits and results based on IBM Quantum Experience platform are shown. Different aspects of Grover's algorithm and the classical algorithm are compared to illustrate the advantages and limitations of Grover's algorithm. Lastly, some future outlooks are present.

2. Fundamentals of Quantum Computing

Similar to classical computers operating upon classical bits, quantum computers operate based on qubits. In general, a qubit is an object with some specific quantum properties. The details of qubits are discussed in the following section.

2.1. Stern-Gerlach Experiment

Stern-Gerlach Experiment is one important experiment in the history of quantum mechanics. It was performed by Stern and Gerlach in 1922 and demonstrated the properties of the quantum world [11]. For a single silver atom, it has a net angular momentum because it has an unpaired electron on its shell. The purpose of Stern-Gerlach Experiment is to measure the z-axis component of this angular momentum. Figure 1 shows the setup of the experiment. The furnace and the selection process create a straight beam of silver atoms. The beam will be reflected along the z-axis because of the net angular momentum of the silver atoms. Classically, the screen will show a continuous distribution. However, the experiment result is two distinct dots, indicating the z component are either $\hbar/2$ or $-\hbar/2$. In this case, quantum mechanics describes the beam before reaching the screen as the superposition of $|\hbar/2\rangle$ and $|-\hbar/2\rangle$. More precisely, if $|\hbar/2\rangle$ represent state $|0\rangle$ and $|-\hbar/2\rangle$ represent state $|1\rangle$, the state of beam can be written as a state vector $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. In general, for any qubit, it can be written as a state vector $|q\rangle = \alpha|0\rangle + \beta|1\rangle$.

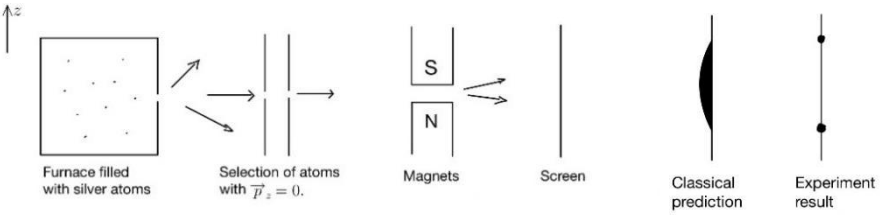


Fig. 1 Stern-Gerlach experiment setup (left panel) as well as predictions and experiment results (right panel).

2.2. Measurement and Matrix Representation

Qubits are usually in superpositions of $|0\rangle$ and $|1\rangle$. To obtain information, measurement is applied to the qubit. The probability of measuring state $|x\rangle$ on an arbitrary qubit $|q\rangle$ is the following:

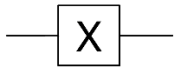
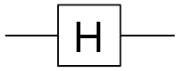
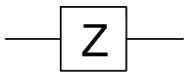
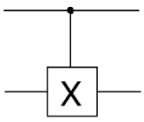
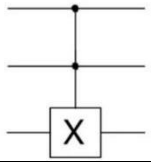
$$p(x) = |\langle x|q\rangle|^2 \tag{1}$$

After the measurement, the qubit collapse to state $|x\rangle$ [12]. For a qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, it can be represented as a 2×1 matrix $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ under a basis of $|0\rangle$ and $|1\rangle$.

2.3. Operators and Quantum Logic Gates

In quantum computers, all manipulations of qubits are achieved by applying operators on one or two qubits. Operators are represented by squared matrices. All of the operators should be unitary. If $UU^{\dagger} = I$ where $U^{\dagger}$ is the Hermitian conjugate of U and I is the identity matrix, then U is unitary. Table. 1 shows some useful operators, also refer to as quantum logic gates [13].

Table. 1 Logic gates, diagrams, matrix representations and examples

Logic Gates	Diagram	Matrix Representation	Example
NOT gate (X gate)		$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\beta\\\alpha\end{pmatrix}$
Hadamard gate (H gate)		$\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$	$H\|0\rangle = \|+\rangle$ $H\|1\rangle = \|-\rangle$
Phase flip gate (Z gate)		$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\alpha\\-\beta\end{pmatrix}$
CNOT gate		$\begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix}$	$CNOT\ \|10\rangle = \|11\rangle$ $CNOT\ \|01\rangle = \|01\rangle$
Toffoli gate (CCX gate)		Omitted since it is too large	$CCX\|110\rangle = \|111\rangle$ $CCX\|111\rangle = \|110\rangle$ $CCX\|010\rangle = \|010\rangle$ $CCX\|100\rangle = \|100\rangle$

It should be noticed that the CNOT gate is a 2-qubit logic gate. This gate applies an X gate on the second qubit if and only if the first qubit is 1. The last gate is the Toffoli gate. It is composited by other 1-qubit gates and 2-qubit gates [13]. The resultant effect on the circuit is similar to CNOT. It applies an X gate on the third qubit only if the first and the second qubit are both 1.

3. Classical Algorithm and Grover's Algorithm

3.1. The Problem

In this article, the classical algorithm and Grover's algorithm will be applied to the following searching problem: find the number x that satisfies the condition $x = \omega = 38$ in a random database containing integers from 0 to 63.

3.2. Classical Algorithm

To solve this problem using the classical algorithm, a classical computer reads the first number in the database and checks whether the condition is satisfied. If not, it repeats the procedure with the next number in the database. Because the database is random, it easy to show that the expected checks are 32, half of 64. In the worst case, the classical computer needs to check the condition for all 64 integers. In general, for a random database with size N, the number of expected steps for a classical algorithm operating on a classical computer is N/2 [12].

3.3. Grover's Algorithms

The idea of Grover's algorithm is that first all the inputs are sent and stored in qubits. The qubits are in the state with the superposition of all inputs. For simplicity, it is called state $|\phi\rangle$. In this state, the probability of measuring each input is the same. Using quantum operators O and Us, the amplitude of the state vector corresponding to the inputs satisfying the conditions is amplified. Repeating this procedure increases the probability of measuring the correct answer. When the probability reaches

the highest, the procedure is stopped and then an actual measurement is made. In the following description, the quantum operators O and Us are discussed in detail.

3.3.1. Oracle O and Us

The quantum oracle O has the following properties:

$$O|x\rangle = \begin{cases} -|\omega\rangle, x = \omega \\ |x\rangle, x \neq \omega \end{cases} \tag{2}$$

For any state vector, it can be written in the sum of the correct input component $|\omega\rangle$ and the component $|\omega_\perp\rangle$.

$$|\phi\rangle = \alpha|\omega_\perp\rangle + \beta|\omega\rangle \tag{3}$$

$$O|\phi\rangle = \alpha|\omega_\perp\rangle - \beta|\omega\rangle \tag{4}$$

After applying the quantum oracle O, the $|\omega\rangle$ component gains a negative phase and the rest of components stay the same. Fig. 2 illustrates the graphic understanding of O. The state vector $|\phi\rangle$ is reflected about the $|\omega_\perp\rangle$ vector. Next, $O|\phi\rangle$ can be written in the following form:

$$O|\phi\rangle = a|\phi\rangle + b|\phi_\perp\rangle \tag{5}$$

$$U_s(O|\phi\rangle) = a|\phi\rangle - b|\phi_\perp\rangle \tag{6}$$

The Us operator reflects the state vector about the $|\phi\rangle$ vector. The final state vector moves close to the correct state $|\omega\rangle$ by 2θ. Us operator can be constructed using the following gates:

$$-U_s = H^{\otimes n}X^{\otimes n}(c^{n-1}Z)X^{\otimes n}H^{\otimes n} \tag{7}$$

Here, H, X gates are the quantum logic gates mentioned above. $c^{n-1}Z$ is the n-1 control Z gate [12]. In the following discussion, G is defined as $G = U_sO$. After applying R times of G operator on the qubits, the probability of measuring the correct number is the highest, where $R = \pi\sqrt{N}/4$ [12].

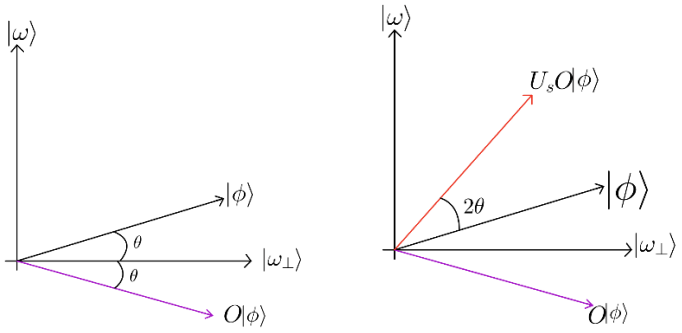


Fig. 2 Graphical understanding of of O (left) and U_s (right)

3.3.2. Building O and Us on IBM Quantum Experience and Results

IBM Quantum Experience provides a platform to construct quantum circuits to solve the problem using quantum computers [14]. In binary, 38 is equal to 100110. The quantum oracle adds a negative phase to the vector component $|100110\rangle$. The following diagram shows the oracle for the problem. Qubit 0 is ancillary. Qubit 1 to qubit 6 are the actual working qubits representing the digits of the number. The convention is that qubit 1 represents the most left digit of the binary number. Us is also built using the equation mentioned above. The realizations based on IBMQ is presented in Fig. 3.

First, Hadamard gates are applied to all 6 working qubits to put the state into the superposition of all inputs. All qubits go through G operators for $R = \pi\sqrt{64}/4 \approx 6$ times and measurements are made. The circuit is executed 4000 times on IBM Quantum simulator. The simulator uses classical computer to simulate the state vectors without consideration of noises. For 3993 times the correct answer is measured. The circuit is also run on ibm_nairobi, one of the quantum computers provided

by IBM Quantum [14]. The result shows no input has a relatively higher probability (seen from Figs. 4 and 5).

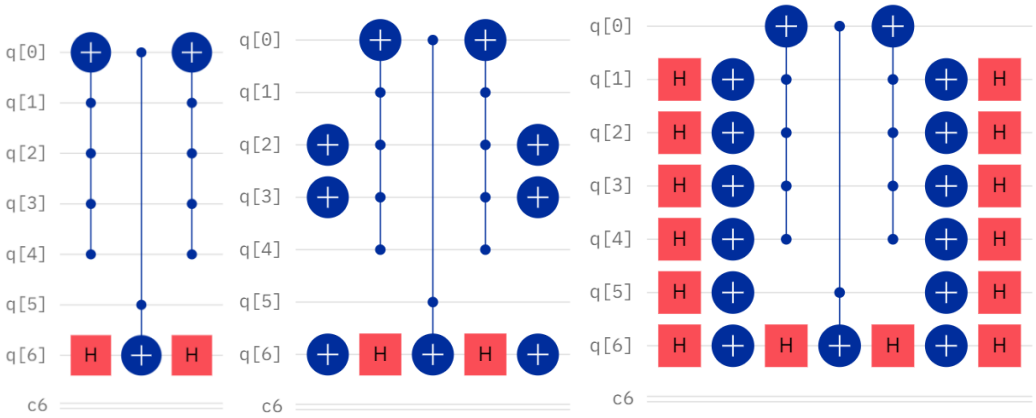


Fig. 3 Control-6 Z gates (left panel), oracle (middle panel), Us(right panel)

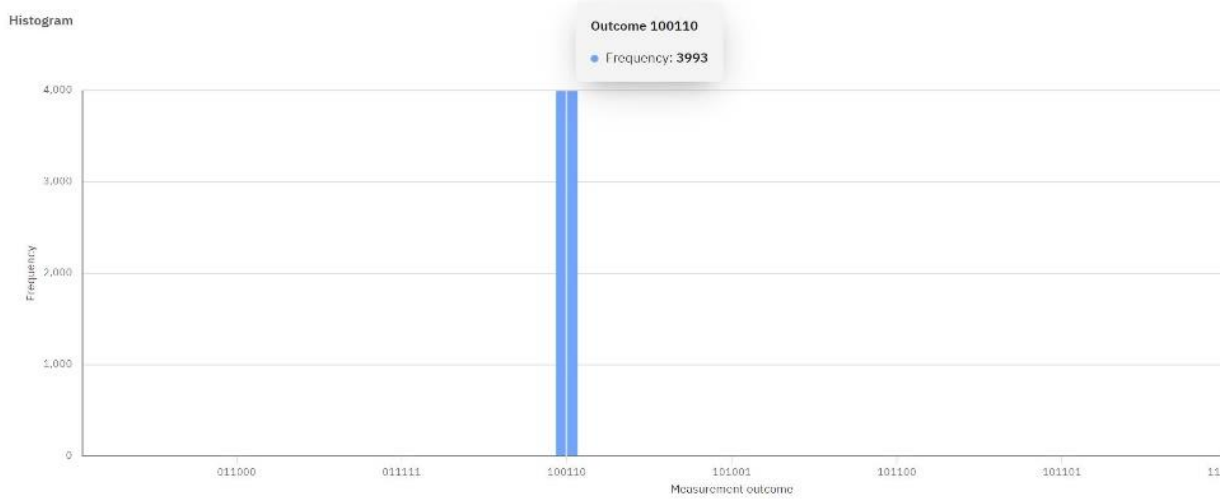


Fig. 4 Results from the simulator

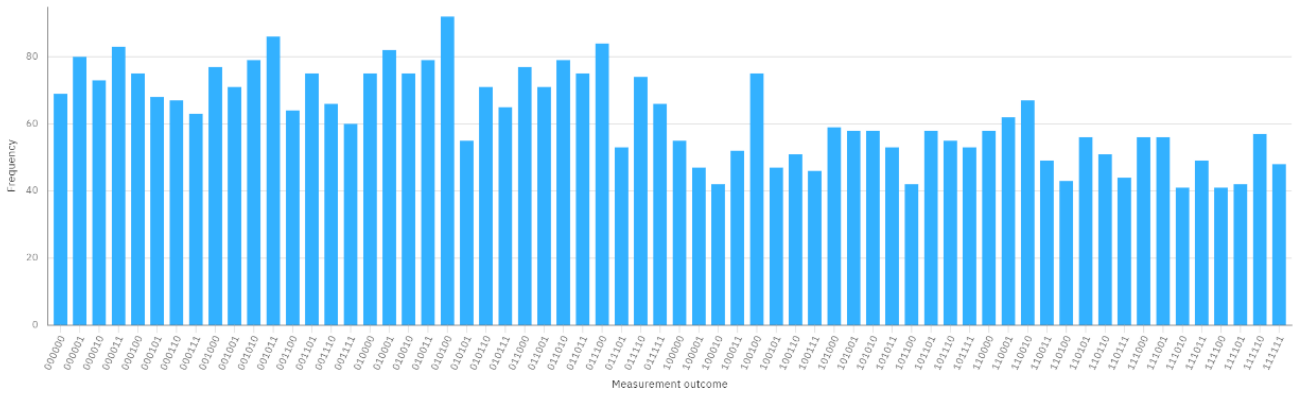


Fig. 5 Results from the ibm_nairobi

4. Discussion

4.1. Speedup

From the perspective of mathematics and algorithms themselves, for a database with size N, to complete the searching task, the classical algorithm takes 16 steps on average while Grover's algorithm takes 6 steps. One step represents one call of the condition checker. It is clear that Grover's

algorithm provides speedup to the searching task. In general, the classical algorithm is in $O(N)$ and Grover's algorithm is in $O(\sqrt{N})$. Although a quantum circuit needs to be executed repeatedly for several of times to ensure that the measurement is the most probable one, the speedup of the quantum algorithm is still powerful when N is considerably large. This is reasonable since the value of quantum computers is to solve those large problems that cannot be solved in a reasonable time by classical computers.

4.2. Fidelity

The classical algorithm for this simple task can be completed on any modern classical computer with very high reliability. Nevertheless, the quantum circuit running on a real quantum device does not produce reliable results. The result from the simulator (seen from Fig. 4) shows that the quantum algorithm itself is no problem. Inevitable noises in real quantum computers are the biggest problem preventing the circuit to obtain the correct answer. Furthermore, according to a study of noise inside IBM's quantum computers, the physical distance between qubits reduces connectivity and prevents two-qubit operators from directly acting on two distant qubits. They need the help of intermediate qubits to complete to operations. It significantly increases the depth of the circuit, the number of gates. Consequently, more noises enter and the results become unreliable [15]. In the task of finding number 38, intensive use of multi-control X gates increases the depth of the circuit and ruins the final result. Therefore, the classical algorithm is more reliable than the quantum one due to the fact that classical computers have higher fidelity in this case.

4.3. Multi-answer Case

Consider the case when $M > 1$ inputs satisfy the conditions. The increase in the number of answers reduces the number of steps in the classical algorithm because the probability of finding the correct inputs increases. However, for Grover's algorithm, the amplitudes of state vectors corresponding to the correct inputs are amplified with no difference. All of them have the highest probabilities. The number of steps is still in the order of $\sqrt{N}$ and one of the answers is measured randomly [12]. One problem with this property is that in the case when M is large and if all answers are to be found, the classical algorithm can complete the task with only a little difference: it just simply goes through all the inputs. In contrast, there is no way to guarantee that all answers are found in Grover's algorithm. The quantum algorithm is more powerful when a relatively small number of answers needs to be found in a relatively large database.

5. Limitations and Future Outlooks

There are certainly several limitations of this study. First, the problem is trivial. The condition in the problem is very easy to check. The quantum oracle is constructed with a little effort. Future research may consider a series of more complex conditions extracted from problems in life and discuss the complexities in designing quantum oracles. In this article, only Grover's algorithm is discussed in detail. Comparisons between Shor's factoring algorithm, other powerful quantum algorithms, and classical factoring algorithms may be carried out in future studies. In addition, the design of the 100110 circuit, the influence of noises in real quantum computers is omitted. The result based on IBM's quantum computer indicates this circuit cannot complete the searching task. Research on reducing the impacts of noises is valuable. Reducing noises in hardware and reducing the depth of circuits in software may be two prospective research fields.

6. Conclusion

In conclusion, this article compares the classical searching algorithm and Grover's quantum algorithm based on a case in which two algorithms are applied to find a number in a database. The comparison shows the quadratic speedup of Grover's algorithm in a searching task. However, the

circuit constructed directly from the algorithm may not complete the job on a real quantum computer because of noises. In a multi-answer case, Grover's algorithm cannot guarantee that all the answers are found. Suggesting that Grover's algorithm is more effective when finding a small number of answers in a very large database. This article ignores the consideration of noises and the problem is relatively simple. The case and the comparison demonstrate the potential of Grover's algorithm in reducing steps in a searching task. It also shows that noises need to be carefully addressed in order to truly apply the algorithm on a real quantum device. In the future, the control of noises in quantum computers may be a very important research field. Constructing new quantum algorithms is a helpful way to develop quantum computing. Overall, these results offer a guideline for quantum computation.

References

[1] Feynman R P. Simulating Physics with Computers. International Journal of Theoretical Physics, 1982, 21(6/7).

[2] Bhat H A, Khanday F A, Kaushik B K, et al. Quantum Computing: Fundamentals, Implementations and Applications. IEEE Open Journal of Nanotechnology, 2022, 3: 61-77.

[3] Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 1992, 439(1907): 553-558.

[4] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 1999, 41(2): 303-332.

[5] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126.

[6] Imam R, Areeb Q M, Alturki A, et al. Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. IEEE Access, 2021.

[7] Grover L K. A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996: 212-219.

[8] Hou S Y, Feng G, Wu Z, et al. SpinQ Gemini: a desktop quantum computer for education and research. arXiv preprint arXiv:2101.10017, 2021.

[9] Pogorelov I, Feldker T, Marciniak C D, et al. Compact ion-trap quantum computing demonstrator. PRX Quantum, 2021, 2(2): 020343.

[10] Chow, Jerry, et al. IBM Quantum Breaks the 100-Qubit Processor Barrier. 16 Nov 2021. Retrieved from: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.

[11] Gerlach W, Stern O. Der experimentelle nachweis der richtungsquantelung im magnetfeld. Zeitschrift für Physik, 1922, 9(1): 349-352.

[12] Mermin N D. Quantum computer science: an introduction. Cambridge University Press, 2007.

[13] Nielsen M A, Chuang I L. Quantum computation and quantum information. Phys. Today, 2001, 54(2): 60.

[14] IBM Quantum. Retrieved from: https://quantum-computing.ibm.com/, 2021

[15] Johnstun S, Van Huele J F. Understanding and compensating for noise on IBM quantum computers. American Journal of Physics, 2021, 89(10): 935-942.