Grover's Algorithm – Implementations and Implications

Chenxi Guo

Moscow State University, Moscow 119234, Russia

guochenxi912@gmail.com

Abstract. Ever since the realisation of the potential computational power of quantum-natured circuits, multiple quantum algorithms have been proposed, exploiting quantum superposition or quantum entanglement features to simulate quantum systems that classical computers cannot efficiently probe. The most notable among these strategies is Shor's algorithm, which takes advantage of the quantum Fourier transform and has been shown capable of solving integer factorisation problems within polynomial time. This article's focus is on one type of quantum algorithm based on amplitude amplification, namely Grover's algorithm. This algorithm's working principle is explained, and a discussion of its recent developments and possible direction of future reach is provided. In addition, implementations of Grover's algorithm have been performed using the IBM Quantum Lab, followed by a reference to its connection to life sciences.

Keywords: quantum computation; quantum simulation; quantum algorithm; Grover's algorithm; IBM quantum; quantum algorithm implementations.

1. Grover's Algorithm – Implementations and Implications

In 1981, Richard Feynman envisioned the possibility of quantum computation, observing that accurate and efficient simulation of quantum mechanical systems would be an unfeasible task for classical computers. However, a new kind of machine, a computer itself "built of quantum mechanical elements which obey quantum mechanical law" [1], might eventually realise effective quantum simulations of quantum systems. The total amount of data required to describe a quantum system grows exponentially with the increase in degrees of freedom, consequently, classical computers encounter overwhelming time and space complexity when solving problems of this sort. At the extremely basic level, even the most advanced modern supercomputers ultimately depend on the binary state of millions of physical transistors that can be set to either 0 or 1 at any given moment [2]. By comparison, the computational power of a quantum-natured computer grows exponentially with the number of its qubits, thanks to the possibility of the coexistence of multiple entangled states. Harnessing the power of quantum mechanical phenomena, quantum computing is a rapidly-emerging technology that attracts intensive research and investment. A more comprehensive account of the history of quantum computing technologies can be found in an article by Carude [2][3]. In addition, a beginner-friendly yet thorough introduction to the realm of quantum computing can be found in the work by Michael Nielson and Isaac Chuang[4].

Not long after the proposal of the concept of quantum computation, Peter Shor's 1997 publication, *A Quantum Algorithm for Performing Prime* Factorisation *of Integers in Essentially Polynomial Time* [5] ,became the best-known development in quantum computation. Further evidence of the power of quantum computers came with the advent of a plethora of other monumental algorithms, including Grover's algorithm, Deutsch-Jozsa algorithm etc. The extensive applicability of Grover's algorithm on search-based problems has sparked considerable interest in its research. Below is an in-depth discussion on Grover's algorithm.

1.1 Grover's Algorithm

In his hallmark work, "A fast quantum mechanical algorithm for database search", published in the *Annual ACM Symposium on Theory of Computing* in 1996 [6], L. K. Grover illustrates his discovery of a highly effective algorithm for unstructured information retrieval in the context of quantum simulation. The Grover quantum search algorithm is a significant application of quantum computing, featuring an accredited increase in speed over classical searches of an unsorted data library. The problem to be solved was to identify a single target item with specific properties from an unsorted data library of size N. Conventionally, similar problems would necessitate $O(N)$ binary search for any Boolean algorithm. The Grover search algorithm, noticeably, provides a potent method to perform such tasks – the one-time probability of sorting out the correct answer is boosted to near-unity through repetitive performance of the amplifying procedures $O(N^{1/2})$ times.

1.2 The Amplitude Amplification Procedure

Amplitude amplification is a technical procedure of quantum computing which generalises the concept behind the Grover's search algorithm and generates a family of quantum algorithms , including quantum counting. This strategy allows the amplification of the probability amplitude of a chosen subspace of a quantum state, which usually leads to quadratic speedups compared to the corresponding classical algorithms. Below is a detailed illustration on how this procedure unfolds for Grover's algorithm.

In this example, there is a large list of N items, among which one is sought for a unique property. The item is traditionally called the winner, w. In the Dirac notation, for example, if there are $n = 3$ qubits, the list will be the states |000>, |001>…|111>. In addition, the winner in this example is the target state |w>=|101>. The process begins by taking the state of uniform superposition |s>. At this point, any measurement will lead to the collapse of the superposition wave function to one of the basis states, with equal probability of $\frac{1}{N}=\frac{1}{2^n}$. The chance of measuring the correct state w is therefore 1 in 2^n. The amplitude amplification procedure introduces significant enhancement to this probability and shrinks the other items' amplitudes, thus yielding the desired result with near certainty.

Geometrically, the procedure can be interpreted in terms of two reflections in a space spanned by the states |w> and |s>(Fig.1). It can be noticed that these two states are not orthonormal, and an auxiliary state |s'> that is perpendicular to |w> can be introduced, being obtained from state |s> by removing the component of |w> and renormalising. The angle θ between states |s> and |s'> is therefore arcsin($\frac{1}{\sqrt{n}}$).

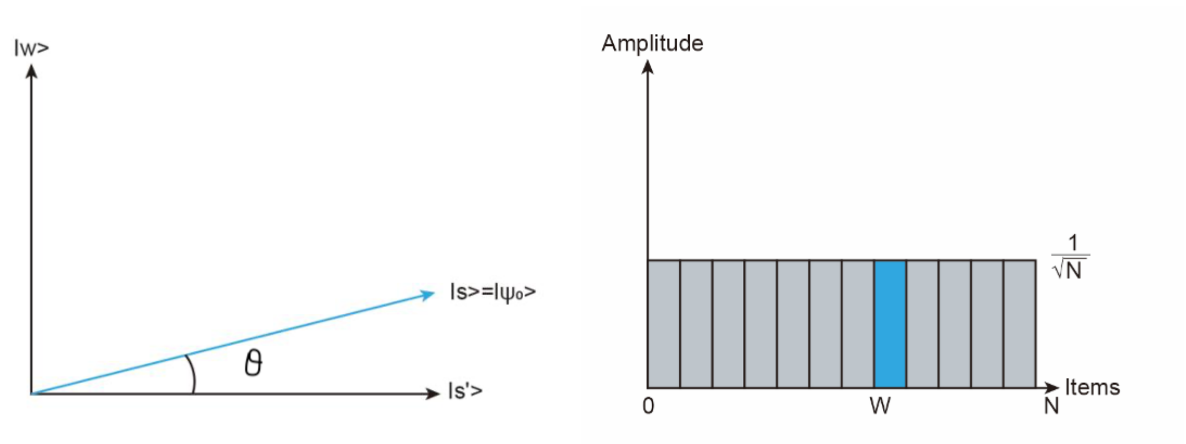

Figure 1 Geometrical representation of states

Next, the reflection operator U_f is applied to the state |s>, flipping it around the |s'> state and reducing the average amplitude (indicated by a dashed line).

The first flipping operator U_f can be typically represented by an oracle, which is a diagonal matrix in which the entry that corresponds to the marked item has an additional negative phase (Fig.2). In this example with three qubits and a target state of |w>=|101>, the oracle takes the matrix form:

$$\text{Equation 1 Oracle matrix} U_f = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

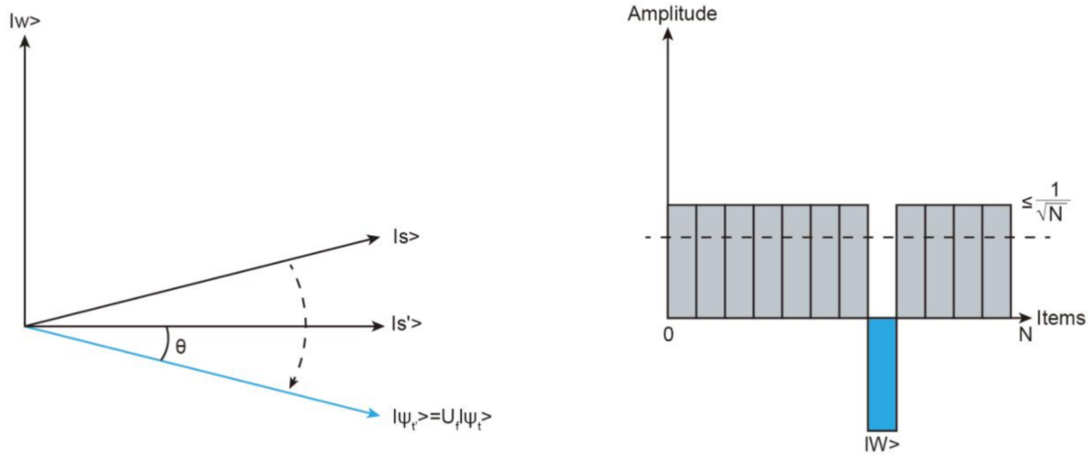

Figure 2 First reflection

The last step is to apply an additional reflection Us around the initial |s> state: Us = 2|s><s| - 𝕀. The resulting transformation maps the state to $U_S U_f$|s>. The probability amplitude of the winner state is then greatly enhanced (Fig.3).

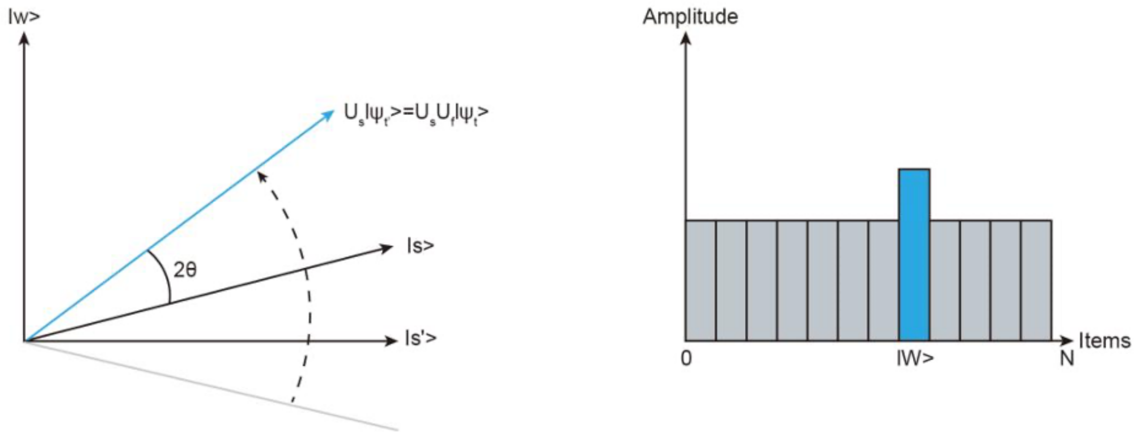

Figure 3Second reflection

These two steps are then repeated multiple times, with the winner state gaining increased probability amplitude each time while the other amplitudes decrease.

1.3 Grover's Algorithm in the Language of the Hamiltonian

Grover's algorithm can be intuitively interpreted as the evolution of a quantum state [7].

Following the Dirac notation, the first projection operator P_f = |w><w| represents the potential energy. Likewise, the isotropic kinetic energy term can be described as the second projection operator

P_s = |s><s|. Therefore, the two reflection operators discussed above can be simply written as $R_f = \mathbb{I} - 2P_f$ and $R_s = \mathbb{I} - 2P_s$. Grover's algorithm can be then expressed as the discrete Trotter formula:

$$|w\rangle = (-R_s R_f)^t \ |s\rangle,$$

which solves the problem with t queries.

As mentioned above, an auxiliary state is needed, residing in the same subspace spanned by |s> and |w> and perpendicular to |w>. These states can be expressed as vectors:

$$|w\rangle = \binom{1}{0}, \ |s'\rangle = \binom{0}{1}, |s\rangle = \binom{sin\vartheta}{cos\vartheta}$$

Grover's algorithm then reiterates the evolution operator:

$$U_G = (-R_s R_f) = \begin{pmatrix} 1 - 2sin^2\vartheta & cos2\vartheta \\ -cos2\vartheta & 2cos^2\vartheta - 1 \end{pmatrix} = \cos(2\vartheta)\ \mathbb{I} + i\cos(2\vartheta)\sigma_2,$$

which leads to state rotation by the angle 2θ in the two-dimensional Hilbert space. The corresponding Hamiltonian evolution is :

$$U_G = \exp(-iH_G\tau), \text{ where } H_G\tau = 2\theta\sigma_2 .$$

After a total of t rounds of reflections, the resulting state will form an angle θ_t = (2t + 1) θ with the initial averaged |s'> state.

1.4 Recent Developments Related to Grover's Algorithm

Grover's algorithm has been successfully implemented on several physical platforms. Two-qubit algorithms have already been executed on superconducting quantum processors [9], trapped atomic ions , and neutral atoms , as well as platforms using nuclear magnetic resonance . Multi-qubit implementation schemes have recently been carried out on the scalable system of trapped atomic ions . Trapped neutral atoms, likewise, have been used to increase the system's scalability with the featured Rydberg blockade gate mechanism .

More noticeably, it has been revealed that classical waves likewise search a database. An experimental setup that exploited classical Fourier optics has been demonstrated to possess the computational power equivalent to approximately 20 qubits, opening experimental access to problems that are yet outside the scope of the computational power of existing prototypes of quantum computers16].

Furthermore, the connection between Grover's search and some biological systems has been explored recently. Some works have already revealed the presence of the trace of Grover's algorithm in the structure of genetic languages . A second biological occurrence relevant to Grover's algorithm is energy flow during photosynthesis, from the chlorophyll pigment molecules that absorb photons to the site of glucose synthesis .

1.5 Implementation of Grover's Algorithm on IBM Quantum Computers

IBM is one of the influential organisations that are investing large amounts of capital to support the development of quantum simulation and computation [8]. Two of its major contributions are the IBM Quantum Composer and the IBM Quantum Lab, featuring convenient public access to the cloud-based quantum computing services offered by IBM Quantum. Situated in the in-dilution refrigerators at the IBM research headquarters, IBM's quantum processors are made of superconducting qubits. At the time of this writing, IBM currently maintains over twenty devices as their extensive software resources, six of which are readily available to the public. In the rest of this section, the implementation of Grover's algorithm for 2 qubits and 3 qubits in the IBM Quantum Lab is discussed.

1.6 Experiment Description

Three experiments were conducted using the *simulator_statevector* system , which consists of 32 qubits. A detailed discussion of the experiments conducted on IBM's quantum devices is presented below. For each experiment, a bar chart is included to demonstrate the results. There is also a brief discussion regarding accuracies and implications.

Experiment 1: Simple Demonstration of Grover's Algorithm for a 2-Qubit System

The circuit below illustrates the simplest 2-qubit Grover's algorithm to find the marked state |11>. To find the marked state |11>, the oracle is simply the controlled-Z gate. In order to complete the circuit, an additional reflection Us = 2|s><s| – 𝕀 is required. The initialisation step, oracle, and diffuser are shown in the circuit.

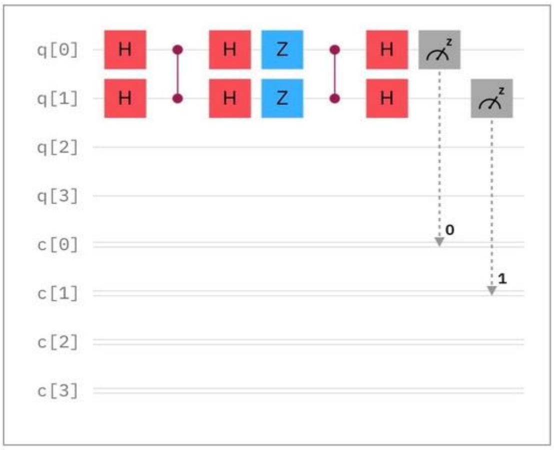

Figure 4 experiment 1, circuits

For a 4-item database, Grover's algorithm can be implemented with very high accuracy with one reflection. The initial θ equals π/6; hence, after one flipping round, the resulting angle equals π/2, which indicates the overlap of resulting state |s> and the marked state |w>.

The measurement outcome agrees perfectly with the mathematical prediction. From a total of 1024 attempts, all experimental results yielded the desired state.

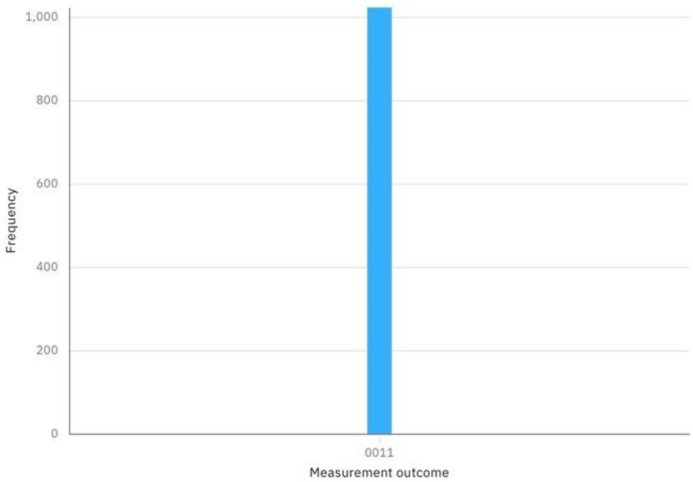

Figure 5 experiment 1, results

Experiment 2: Grover's Algorithm for a 3-Qubit System With One Grover's Iteration

In this experiment, one iteration was used to increase the probability of finding the state |111>. Below is the circuit for the algorithm and the result histogram. The probability of correct measurement was 59.4%.

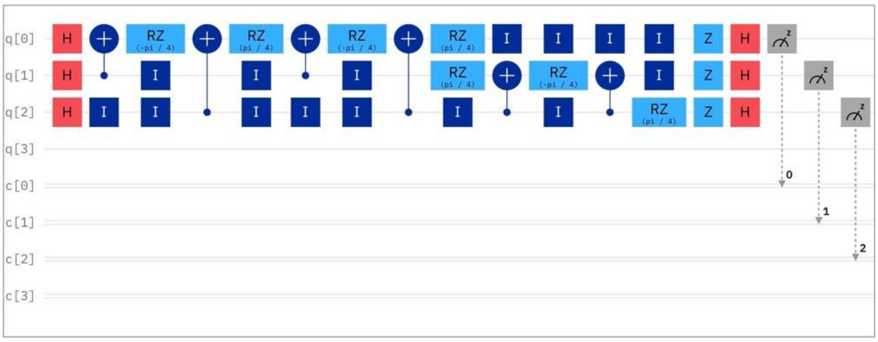

Figure 6 Experiment 2, circuits

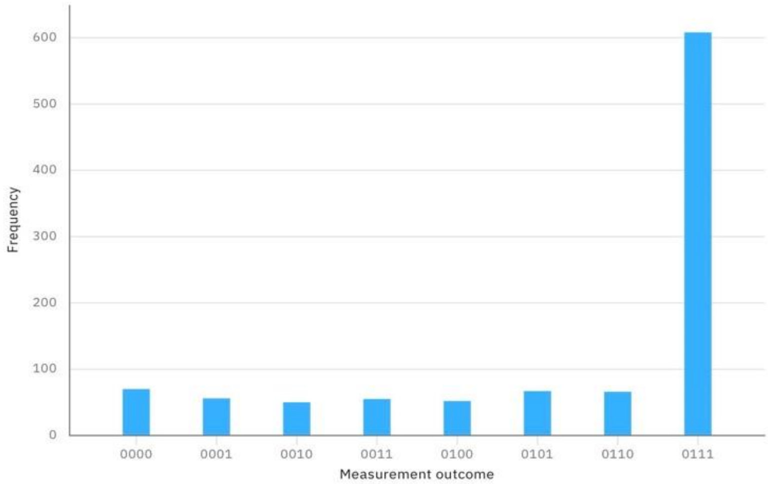

Figure 7 Experiment 2, results

Experiment 3: Grover's Algorithm for a 3-Qubit System With Two Grover's Iterations

In this experiment, the same basic algorithm from experiment 2 was used with two Grover's iterations to further enhance the probability of correct measurement. A total gate number of 33 was required. The histogram for results is shown below. The probability of correct measurement was 77.6%.

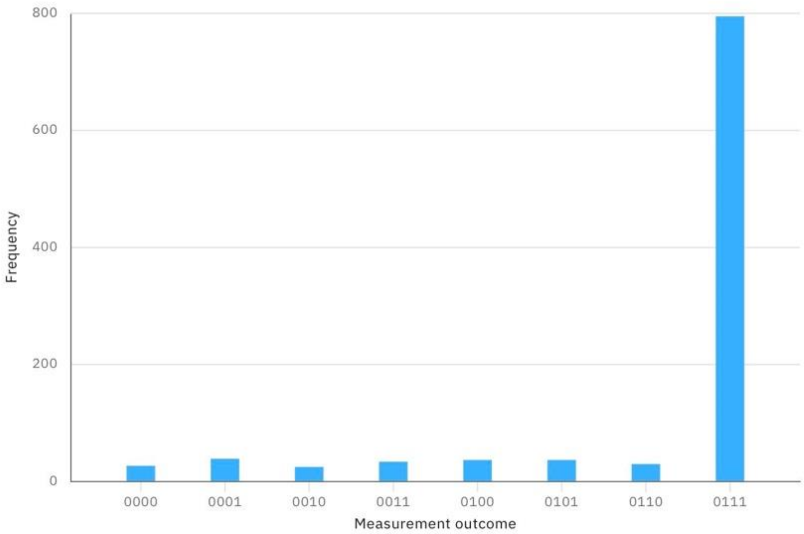

Figure 8 Experiment 3, results

2. Results and Discussion

As can be seen from experiment 1, for a two-qubit system, current technology allows nearly perfect accuracy for finding a desired state. Experiment 2 has demonstrated the procedure of using Grover's algorithm for three-qubit system via the simplest possible circuit route, with acceptable accuracy that implies the viability of performing this algorithm for even larger systems. Experiment 3 aimed to prove one of the most noticeable features of Grover's algorithm, namely that accuracy increases along with the number of Grover's iterations. Even with two rotations, the probability of successful measurement grew roughly by 30% compared to experiment 2.

However, as can be seen from the circuit diagram for experiments 2 and 3, the number of required gates can exponentially increase with more qubits under consideration. This increase is one of the difficult issues in many-body problems; the complexity grows exponentially in larger systems. This difficulty represents a significant challenge in the realisation of large-scale quantum simulators. Nevertheless, the simplification of combined gates may be a solution. More specifically, it is advisable to create a publicly accessible library of gates, which can be expanded and strengthened through the combined efforts from the scientific community as well as the public.

3. Conclusion

We have provided here a detailed description of Grover's algorithm and have demonstrated its viability on IBM cloud-based quantum simulators. As one of the most well-known quantum algorithms, Grover's algorithm is likely to play a pivotal role in preparing the world for the arrival of a quantum computer, which is still at its early stage of development. Despite the critical voice on its widely celebrated search power and cost efficiency , this algorithm has been frequently discussed for its ingenuity and simplicity. Moreover, the emerging evidence that quantum searches are an intrinsically ordinary feature of electron behaviour may relate the fundamentals of living organisms to quantum algorithms. For example, researchers from Université de Toulon have recently claimed that free electrons naturally implement Grover's search algorithm when moving across the surface of certain crystals . This finding might further advance understanding of the genetic code and the origin of life. For these reasons, this powerful algorithm may deserve more attention for its potentially profound implications.

References

[1] R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, no. 6/7, pp. 467–488, 1982.

[2] Aamir Mandviwalla, Keita Ohshiro and Bo Ji, "Implementing Grover's Algorithm on the IBM quantum computers, http://dx.doi.org/10.1109/BigData.2018.8622457, 2018.

[3] C. S. Calude and E. Calude, "The road to quantum computational supremacy," arXiv preprint arXiv:1712.01356, 2017.

[4] Michael A . Nielsen and Isaac L. Chuang, "Quantum Computation and Quantum Information," 10th Anniversary Edition, https://doi.org/10.1017/CBO9780511976667, 2010.

[5] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, no. 5, p. 1484.

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 1996, pp. 212–219.

[7] Apoorva D. Patel, "Grover's Algorithm in Natural settings'', arXiv:2001.00214 [quant-ph],2021.

[8] I. Murphy, "Ibm ups the stakes for quantum computing," https://www.enterprisetimes.co.uk/2017/11/13/ibm-ups-stakes-quantum-computing,

[9] 2017, accessed: 2018-10-06.

[10] L. Dicarlo et al., “Demonstration of Two-Qubit Algorithms with a Superconducting Quantum processor, arXiv:0903.2030v2 [cond-mat.mes-hall], 2009.

[11] K.-A.Brickman et al., “Implementation of Grover’s Quantum Search Algorithm in a Scalable System”, arXiv:quant-ph/0510066v2, 2005

[12] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, Science 287,463, 2000.

[13] M. S. Anwar, et al., Chem. Phys. Lett. 400, 94 ,2004.

[14] M. Riebe, et al., Nature 429, 734, 2005.

[15] J. Chiaverini, et al., Science 308, 997, 2005.

[16] Klaus Molmer, et al., “Efficient Grover search with Rydberg blockade”, arXiv: 1102.3573v2[quant-ph], 2011.

[17] N. Bhattacharya, et al., “Implementation of quantum search algorithm using classical Fourier optics”, 2002.

[18] A. Patel, “Quantum algorithms and the genetic code”, Pramana, 56, pp. 367-381, 2001.

[19] A. D. Patel, “Towards understanding the origin of genetic languages”, in “Quantum Aspects of Life”, Eds. D. Abbott, P. C. W. Davies and A. K. Pati, Imperial College Press, pp. 187-219, 2008.

[20] Y.-C. Cheng, G. R. Fleming, “Dynamics of light harvesting in photosynthesis, Annu. Rev. Phys.Chem.,60, pp. 241-262, 2009.

[21] Scott Fluhrer, “Reassessing Grover’s Algorithm”, https://ia.cr/2017/811, 2017.

[22] Y. Claveau, “Electron Transport in Ultra-Thin Films and Ballistic Electron Emission Microscopy”, https://hal-univ-rennes1.archives-ouvertes.fr/hal-01484634, 2017.

[23] Alberto Galindo, et al., “A Family of Grover’s Quantum Searching Algorithms”, arXiv:quant-ph/0009086, 2000.

[24] https://quantum-computing.ibm.com/lab/docs/iqx/guide/grovers-algorithm

[25] https://qiskit.org/documentation/stubs/qiskit_aer.StatevectorSimulator.html