Advances in Computer, Signals and Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2022.060501
ISSN 2371-8838 Vol. 6 Num. 5

Can We Build a Quantum Computer?

Weilun Yuan

High School Affiliated to Remin University of China, Beijing, China
yuanweilun2022@163.com

Keywords: quantum computer, hardware, algorithm, application

Abstract: This paper presented and evaluated obstacles and solutions for these problems in building quantum computers. From the perspective of hardware, problems such as processing and controlling qubits, the loss of qubits, the noisy environment, and precision are discussed. From the perspective of algorithms, this paper evaluates quantum algorithms for P&NP problems, Simon's problems, and noisy environments (this problem is discussed in both the aspect of hardware and the aspect of the algorithm). Finally, some future applications of quantum computers and their limitations are appraised. Even though many challenges hinder the construction of quantum computers, it's still able to build quantum computers which have great potential.

1. Introduction

Though they have not been commonly used, quantum computers are theoretically better than classical computers at solving a range of issues [1]. One reason for this might be the different units for computation. Classical computers use bits to calculate: a bit can be either zero or one. Different arrangements of zero and one represent different information. Corresponding to bits used in traditional computers, quantum computers use "quantum bit", the so-called "qubit", to calculate. Qubit reacts to quantum computers' superior computing capabilities compared to conventional computers. Due to the fact that every qubit can be zero and one before observation, n qubits of entanglement can form 2^n arrangements at a time. With 2^n arrangements at a time, it's possible to do parallel computation. In a traditional computer, a computer goes through every route one by one. But in a quantum computer, a computer goes through every route at the same time.

At present, there are three possible ways to build a quantum computer: a photon quantum computer, a superconducting quantum computer, or a neutral atom quantum computer [2,3,4]. Even though different quantum computers have different processing ways, their basic theory is the same: they utilized the entangled state of qubits. A photon quantum computer uses photons to form qubits, a superconducting quantum computer uses superconductors to form qubits, and a neutral atom quantum computer uses neutral atoms as qubits. There are three characteristics of photons in quantum states: spin, polarization, and path. For superconductors, the three characteristics are charge, phase, and magnetic flux. Since characteristics that make up entanglement aren't the central topic of this paper, other papers are recommended for readers who are interested [3]. Take photon computers as an example, when photon A is entangled with photon B, a state is confirmed if one photon is detected.

That is if a pair of photons has the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|VH\rangle + |HV\rangle)$ and photon A's polarization is detected, photon B's polarization is also detected ("H" means that the polarization of the photon is horizontal; "V" stands for the photon that polarized in the vertical direction). With equipment, characteristics from different photons can be entangled [5]. Therefore, entangled photons can be used in operation.

This paper is arranged as follows: In section 2, breakthroughs and problems from the perspective of hardware are discussed. In section 3, puzzles and their solutions in quantum algorithms are evaluated. At last, in section 4, future applications of quantum computers are presented.

2. Hardware

From the perspective of hardware, the problems of making qubits, keeping qubits, and blocking noises that hinder the development of quantum computers and their solutions are discussed. Each topic and its solution will focus on one kind of quantum computer.

The first problem is in producing qubits. In neutral atom quantum computers, neutral atoms are qubits used. These atoms are hard to trap and control. To change the atoms into a state able to calculate, atoms are excited into a state with a high mesoscopic radius [6]. These so-called Rydberg atoms can interact in micrometers, which requires harsh operating conditions. On account of particles in mesoscopic reserve features both microscopic and macroscopic, the interactions of electrons would have an impact on these particles. The author in [7] stated that the ideal environment, leaving room for equipment to control the qubit, needs a 10mK deep trap inside a refrigerator. By contrast, the high optical power in an optical trap renders a high photon scattering rate, which causes decoherence. For this problem, a system including a numerical aperture lens can trap the atom and make it a qubit by catching the atom at the focal point of the lens [8]. Moreover, optical lattice offers another solution to the problem in neutral quantum computers because it provides a means to move a large number of atoms precisely. The lattice can trap many atoms at a time because it has a lot of space for atoms. In this way, qubits can be controlled through laser cooling and spectroscopic techniques: no need for special techniques to complete the operation [9].

Another trouble in all quantum computers, especially photon quantum computers, is the loss of information due to the loss of qubits. Qubits' loss is usually caused by the inefficiency of the machine, in processing, measurements, and preservation. Qubits in the state clustering are used [10]. With the clustering of photons, the computer can detect whether a photon is present indirectly. In particular, the machine can detect the state of photons near the photon we want to measure. When the photon in the middle was lost, the One approach in clustering qubits produces a cluster of two photons. Using beta-barium borates (BBO), polarization beam splitter (PBS), and other equipment to create the source, photons' polarization, and spatial modes are entangled [11]. The error correction process can also solve the problem of losing photons, and one simple way is dual-rail qubits representation [12,13]. This mode ensures the display of error conditions. When an error occurs, the computer rejects the answer and performs again. This method has been proven to reduce the error rate of computers. A more complicated way requires extra qubits to perform [14]. The principle is to detect the error of qubits without ruining their quantum state by making "counterparts" for qubits. After the detection of an error, qubits will be sent through some quantum gates to revolve to the phase that they should be.

In superconducting quantum computers, noise is a crucial problem for qubits. Unlike the theoretical environment, in reality, low-frequency noises appear [15]. One direct reason for losing qubits is the inevitable interactions between the environment and qubits [16]. These noises result in dephasing and decohere, especially for the noises in some frequency [15]. Particles that lose the state of coherence can't be used in the calculation. These noises mainly come from charge fluctuation,

magnetic-flux fluctuation, and current fluctuation. To solve this problem, a method called Dynamical Decoupling is used [17]. The pulses created in this way reduce the net noises, acting on the environment. And this method has been proven effective on the quantum computer built by IBM and Rigetti. Other than the noise, leakage is also a problem. Leakage occurs when a qubit leaves the computational place it should be, resulting in further faults in other qubits [18]. One common solution for leakage is to control the qubit frequency's flux through gates [19]. With a way called fast-adiabatic trajectory, the interaction between the abnormal qubits and normal qubits is reduced. Moreover, we can detect leakage when it exists [20]. Using a kind of special measurement that detects an operator of qubits repeatedly in error detection, the leakage of one qubit won't spread to another qubit.

In addition, problems in precision limit the development of the quantum computer. In practice, most interactions with qubits cannot reach perfection [21]. Therefore, the precision of equipment renders phase differences in information waves. Even if on the small scale, the phase difference can be easily reduced, at a large scale, the phase difference is magnified. Though this problem can be solved, it's complicated to adjust thousands of routes.

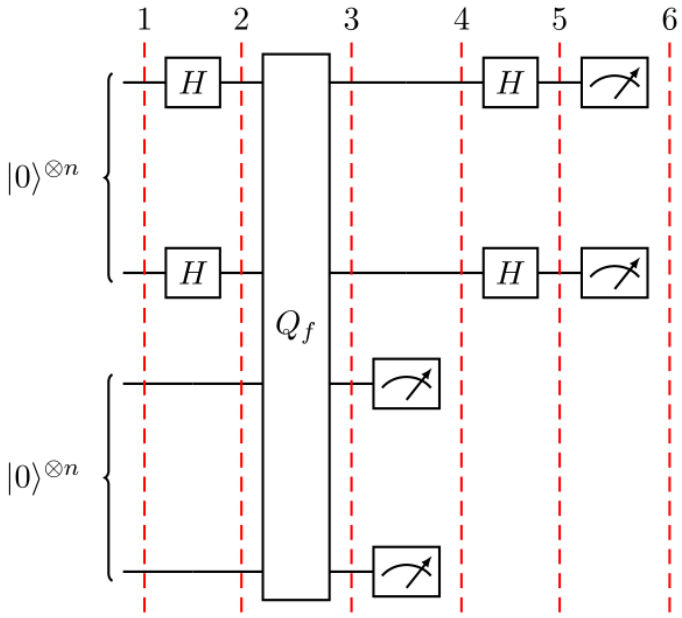
3. Algorithm

The algorithm is also an important part of quantum computers. Quantum algorithms nowadays achieved some breakthroughs, but it still faces a lot of problems [22].

Firstly, quantum algorithms are useful in processing Polynomial problems (P problems), Nondeterministic Polynomial problems (NP problems), and problems out of polynomial time such as factorizing and the discrete log problem. Shor [23] accomplished the algorithm in solving both the discrete log and factorizing problems in 1994. The discrete log problem is finding a group of numbers (x, r, n) that $x^r = n \pmod p$ given a prime number p. Factorizing problem is finding two prime factors other than one given the product of these two factors. The implementation of these algorithms is achieved by a lot of people in different ways; for instance, Vandersypen [24] and other scientists used 7 spin-1/2 nuclei as qubits in 2001. Using nuclear magnetic resonance, these nuclei can be controlled at room temperature. Therefore, a huge refrigerating apparatus required in superconducting quantum computers is not needed. In addition to the algorithm for factorizing the product of two prime numbers, the quantum algorithm that can factorize the product of three prime numbers has also been designed [25]. Nevertheless, even though quantum algorithms can solve NP problems, it hasn't existed a proven efficient algorithm for solving them. Unless an algorithm can find the structure of the problem, an algorithm that can exponentially speed up the solving process won't appear [26].

Secondly, the quantum algorithms for Simon's problem have their advantages and harmful effects. Simon's problem is to find all values in a function. This special 2-to-1 function has two inputs ($X_1 = X$ $X_2 = X + S$)for the same value. For traditional computers, the only way to solve this problem is to treat this problem as a black box (input all possible inputs) to find the rule of the specific cases. But Simon's algorithm, using quantum entanglement, can solve this problem exponentially faster than the traditional way. The first step is to prepare a qubit entangled with either half probability in X and $X + S$ before they were sent into the circuit below [27].

Passing through the circuit in figure 1, a result containing $|x\rangle|f(x)\rangle$ is presented. By measuring the second component of the whole answer ($|f(x)\rangle$), two inputs of the function can be determined. Simon's algorithm is not restricted to theory. Indeed, it's realized in quantum computers. Using a 5-qubit cluster of photons, Tame and other scientists built the route and the gate to make the circuit true. After the implementation of Simon's algorithm, the time cost for every case in Simon's algorithm is also determined by determining the query cost for every case. Even though Simon's algorithm seems not commonly related to cryptography, it can be used for attacking symmetrical encryption [28].



H is a Hadamard gate, it turns $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
Q_f is a function that turns $|x\rangle|a\rangle$ to $|x\rangle|a \oplus f(x)\rangle$
is the gate that can measure the state the of the qubit.

Figure 1: a circuit that implements Simon's algorithm

It's mentioned before that noises affect quantum computers' computational ability by forcing qubits out of their original state. An algorithmic treatment for this solution is to generalize the effect of noise [29]. By the generalization, Franca and Patron were able to deduce the model of noise, which enables them to minimize the influence of noise on quantum computing. A recent application of this simulation is on quantum approximation optimization algorithms (QAOA) done by Filip and other scientists in 2021 [30]. A numerical method is involved to read out the effect of noise. Moreover, algorithms in error corrections can also be useful in dealing with the noise.

4. Future

No matter how far into the future we can produce a quantum computer, we should focus on the potential application problems now

First of all, quantum computers are useful in physic research. Since the physics world is quantized, it's necessary to use a quantum computer to simulate the physical world [31]. But in the physical world simulated by a quantum computer, some presumptions are different from reality. For example, the space in the simulation would be discrete instead of continuous. In the future, the simulation will be able to simulate the dark matter in the universe and other models in nuclear physics, further aiding the research that is difficult to study in normal ways involving general relativity and dark holes [32].

Secondly, quantum computers have both positive and negative effects on cryptography. On one hand, quantum computers destroy a common encryption algorithm used today: large number factorization (RSA) [33]. RSA requires the computer to generate two prime numbers whose product is n digits (the classical value of n is 2048). To find these numbers, the classical computer tries every prime number one by one, which takes a very long time. By contrast, the feature of qubit enables quantum computers to try several numbers at a time. Therefore quantum computers can easily destroy RSA encryption.

On the other hand, quantum computers also promote the development of quantum cryptography. Quantum computers can use quantum to make private keys. This process includes a user sending polarized photons in different bases and different directions to another user. Another user measures these photons on random bases. Then they communicate their bases through the public routes and cross out the data using different bases. The rest of the data forms a private key. If an eavesdropper steals the photon, this eavesdropper cannot send this photon again since his observation alters the photon's state. Moreover, he cannot clone this photon either because perfect quantum cloning is proved unachievable. So, the presence of an eavesdropper increases the error rate when users are exchanging bases they used, and it's possible to determine the eavesdropper's presence when the error rate achieves 11% [34].

Thirdly, in other natural sciences such as chemistry, quantum computers are also a future tool for computation, especially in quantum chemistry. One crucial problem is the properties of electrons. Classically, nuclei are treated as stationary points according to the Born-Oppenheimer approximation (BOA), an assumption in quantum chemistry. But with quantum computers, people can treat this problem without making the approximation, achieving a more universal conclusion. Quantum computers, using quantum algorithms, can better simulate the electronic structure, and they're faster than classical computers [35].

Next, for social science such as finance, quantum computers can promote its development by speeding up calculations like Monte Carlo [36]. Monte Carlo is a sampling way. By choosing the plot randomly in a given area, it's possible to find a possibility that the point is on (under) a function. Therefore, we can find an expectation value (the number of points in the expected area over the total number of points), and it offers a way to simplify a complicated integration or function. The quantum computer's role, in this case, is to speed up the estimation. Nevertheless, quantum finance is limited since functions in finance like Merton-Garman (MG) and Black-Scholes (BS) cannot be solved in the quantum method [37]. When these functions are expressed in field functions, a concept of martingale needs to be added to deal with volatility in a vacuum. But once this concept is added, the symmetry in these functions breaks down, which means that we cannot utilize these functions through quantum physics.

Quantum computers would also aid the development of machine learning of their ability to do parallel computation. So its role is to speed up the process of learning. For example, in the area of unsupervised machine learning, K-mean is a way to do data clustering. K-means requires many tries to find its optimal way: the way that has the lowest total variation. But this process needs the try of different K (the number of clusters) and the different combinations of initial clusters. With quantum computers, this work can be easily done since quantum computers can try many K at a time and try different combinations of initial clusters at a time. In addition, quantum computers enable some new thoughts of neural networks. The neural network includes many points and routes connecting them. The finest state of the network should be an input that results in a stable state for the whole system. And quantum computers may simulate this model by replacing the points with sections containing entangled particles [38].

5. Conclusion

This paper evaluates the problems in building quantum computers from the perspective of hardware, the questions about quantum algorithms, and the future application of quantum computers.

On the side of the hardware, obstacles involving making qubits, preserving qubits, and noises can be overcome. Though there is no convenient way to solve the precision problem, with the development in the manufacturing industry, this problem can be easily solved shortly.

For quantum algorithms, their advantages over classical algorithms are significant while there are some limitations to them. They can resolve P and NP problems much more efficiently than a classical algorithm can. Nonetheless, the speediness of solutions is built on the feature of quantum computers, not on the superiority of the algorithm itself. Simon's problem and the high error rate of computations can also be solved from the perspective of a quantum algorithm while the resolution of Simon's problem results in other problems such as the attack on symmetrical encryption.

The future of quantum computers is promising. Complicated simulations (nuclear models in physic/chemistry, and neural networks in machine learning) and quantum cryptography need to be done by quantum computers because of quantum computers' special features. The high computing ability of quantum computers also enables them to speed up some processes such as factorization and clustering data. The former destroys the RSA encryption while the latter benefits data processing.

References

[1] Wiesner, S. (1996). Simulations of Many-Body Quantum Systems by a Quantum Computer. https:// rxiv.org/pdf/quant-ph/9603028.pdf

[2] Barz, S. (2015). Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments. Journal of Physics B: Atomic, Molecular and Optical Physics, 48(8), 083001. https://doi.org/10.1088/0953-4075/48/8/083001

[3] Huang, H.-L., Wu, D., Fan, D., & Zhu, X. (2020). Superconducting quantum computing: a review. Science China Information Sciences, 63(8). https://doi.org/10.1007/s11432-020-2881-9

[4] Henriet, L., Beguin, L., Signoles, A., Lahaye, T., Browaeys, A., Reymond, G.-O., & Jurczak, C. (2020). Quantum computing with neutral atoms. Quantum, 4, 327. https://doi.org/10.22331/q-2020-09-21-327

[5] Wang, X.-L., Luo, Y.-H., Huang, H.-L., Chen, M.-C., Su, Z.-E., Liu, C., Chen, C., Li, W., Fang, Y.-Q., Jiang, X., Zhang, J., Li, L., Liu, N.-L., Lu, C.-Y., & Pan, J.-W. (2018). 18-Qubit Entanglement with Six Photons' Three Degrees of Freedom. Physical Review Letters, 120(26). https://doi.org/10.1103/physrevlett.120.260502

[6] Naber, J. (2016). Magnetic atom lattices for quantum information. Undefined. https://www.semanticscholar.org/paper/Magnetic-atom-lattices-for-quantum-information-Naber/85a13211ff85a31c77258a0bbb9736fb1edf49ee

[7] Saffman, M. (2016). Quantum computing with atomic qubits and Rydberg interactions: progress and challenges. Journal of Physics B: Atomic, Molecular and Optical Physics, 49(20), 202001. https://doi.org/10.1088/0953-4075/49/20/202001

[8] Jones, M. P. A., Beugnon, J., Gaëtan, A., Zhang, J., Messin, G., Browaeys, A., & Grangier, P. (2007). Fast quantum state control of a single trapped neutral atom. Physical Review A, 75(4). https://doi.org/10.1103/physreva.75.040301

[9] Deutsch, I. H., Brennen, G. K., & Jessen, P. S. (2000). Quantum Computing with Neutral Atoms in an Optical Lattice. Fortschritte Der Physik, 48(9-11), 925–943. https://arxiv.org/ftp/quant-ph/papers/0003/0003022.pdf

[10] Kok, P., Munro, W., Nemoto, K., Ralph, T., Dowling, J., & Milburn, G. (2006). Linear optical quantum computing. https://arxiv.org/pdf/quant-ph/0512071.pdf

[11] Chen, K., Li, C.-M., Zhang, Q., Chen, Y.-A., Goebel, A., Chen, S., Mair, A., & Pan, J.-W. (2007). Experimental Realization of One-Way Quantum Computing with Two-Photon Four-Qubit Cluster States. Physical Review Letters, 99(12). https://doi.org/10.1103/physrevlett.99.120503

[12] Ladd, T., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'brien, J. (2009). Quantum Computing. https://arxiv.org/pdf/1009.2267.pdf

[13] Chuang, I. L., & Yamamoto, Y. (1995). Simple quantum computer. Physical Review A, 52(5), 3489

[14] Streif, M., Leib, M., Wudarski, F., Rieffel, E., & Wang, Z. (2021). Quantum algorithms with local particle-number conservation: Noise effects and error correction. Physical Review A, 103(4). https://doi.org/10.1103/physreva.103.042412

[15] Clarke, J., & Wilhelm, F. K. (2008). Superconducting quantum bits. Nature, 453(7198), 1031–1042. https://doi.org/10.1038/nature07128

[16] West, J. (2000). The Quantum Computer. https://www.xootic.org/wp/wp-content/uploads/2009/02/west.pdf

[17] Jurcevic, P., Javadi-Abhari, A., Bishop, L. S., Lauer, I., Bogorin, D. F., Brink, M., ... & Gambetta, J. M. (2021). Demonstration of quantum volume 64 on a superconducting quantum computing system. Quantum Science and Technology, 6(2), 025020.

[18] Brown, N. C., Cross, A., & Brown, K. R. (2020, October 1). Critical faults of leakage errors on the surface code. IEEE Xplore. https://doi.org/10.1109/QCE49297.2020.00043

[19] Strikis, A., Datta, A., & Knee, G. C. (2019). Quantum leakage detection using a model-independent dimension

witness. Physical Review A, 99(3). https://doi.org/10.1103/physreva.99.032328
[20] Ghosh, J., Fowler, A. G., Martinis, J. M., & Geller, M. R. (2013). Understanding the effects of leakage in superconducting quantum-error-detection circuits. Physical Review A, 88(6). https://doi.org/10.1103/physreva.88.062329
[21] Reilly, D.J. (2019). Challenges in Scaling-up the Control Interface of a Quantum Computer. 2019 IEEE International Electron Devices Meeting (IEDM), 31.7.1-31.7.6.
[22] Lloyd, S., De Palma, G., Gokler, C., Kiani, B., Liu, Z.-W., Marvian, M., Tennie, F., & Palmer, T. (2020). Quantum algorithm for nonlinear differential equations. https://arxiv.org/pdf/2011.06571.pdf
[23] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. https://doi.org/10.1109/sfcs.1994.365700
[24] Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414(6866), 883–887. https://doi.org/10.1038/414883a
[25] Dash, A., Sarmah, D., Behera, B., & Panigrahi, P. (2018). Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. https://arxiv.org/pdf/1805.10478.pdf
[26] Scott Aaronson, S. (2008). the limits of quantum. https://www.ime.usp.br/~pf/clippings/quantum/quantum-computing-200803.pdf
[27] https://qiskit.org/textbook/ch-algorithms/simon.html#algorithm
[28] Santoli, T., & Schaffner, C. (2017). Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information and Computation, 17(1&2), 65–78. https://doi.org/10.26421/qic17.1-2-4
[29] Stilck França, D., & García-Patrón, R. (2021). Limitations of optimization algorithms on noisy quantum devices. Nature Physics, 17(11), 1221–1227. https://doi.org/10.1038/s41567-021-01356-3
[30] Maciejewski, F. B., Baccari, F., Zimborás, Z., & Oszmaniec, M. (2021). Modeling and mitigation of cross-talk effects in readout noise with applications to the Quantum Approximate Optimization Algorithm. Quantum, 5, 464. https://doi.org/10.22331/q-2021-06-01-464
[31] Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6-7), 467–488. https://doi.org/10.1007/bf02650179
[32] Fedorov, A., Gisin, N., Beloussov, S., & Lvovsky, A. (2022). Quantum computing at the quantum advantage threshold: a down-to-business review. https://arxiv.org/pdf/2203.17181.pdf
[33] Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/ijacsa.2018.090354
[34] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2008). Quantum cryptography. https://arxiv.org/pdf/quant-ph/0101098.pdf
[35] Cao, Y., Romero, J., Olson, J., Degroote, M., Johnson, P., Kieferová, M., Kivlichan, I., Menke, T., Peropadre, B., Sawaya, N., Sim, S., Veis, L., & Aspuru-Guzik, A. (2018). Quantum Chemistry in the Age of Quantum Computing. https://arxiv.org/pdf/1812.09976.pdf
[36] Bouland, A., Van Dam, W., Joorati, H., Kerenidis, I., & Prakash, A. (2020). Prospects and challenges of quantum finance. https://arxiv.org/pdf/2011.06492.pdf
[37] Arraut, I., Au, A., & Ching-biu Tse, A. (2020). Spontaneous symmetry breaking in quantum finance. EPL (Europhysics Letters), 131(6), 68003. https://doi.org/10.1209/0295-5075/131/68003
[38] Schuld, M., Sinayskiy, I., & Petruccione, F. (2014). An introduction to quantum machine learning. Contemporary Physics, 56(2), 172–185. https://doi.org/10.1080/00107514.2014.964942