The Principles, Algorithms and State-of-Art Applications of Quantum Computing

Hongyu Duan

Department of math, University College London, London, the U.K.

zcahhdu@ucl.ac.uk

Abstract. Contemporarily, quantum computing has become a popular topic, which is a new approach that is different from classic computing. To be specific, it can deal with information by using mathematical modeling that used to represent quantum mechanics, including superposition, interference, and entanglement. In quantum Computing, information is storage in ‘qubit’, whereas classic computer use bit to store information. This article aims to introduce the principles and some algorithms of quantum computing, and then discuss some up-to -date important development. There are two important algorithms are mentioned in this article, Grover’s algorithms and Shor’s algorithms. According to the analysis, Grover’s algorithms is potentially faster than classic algorithms. However, it requires millions of qubits to make it. Besides, Shor’s algorithms have challenged classic encryption (RSA encryption). Two quantum computer Google Sycamore and Jiuzhang are also mentioned here. The interesting thing is, for some specific question, Jiuzhang performed better than classic computers. Finally, it is found out that the quantum computing is generally slower that classic computer now, due to the restriction of qubit numbers. However, quantum computing still has an advantage in some specific question. These results shed light on guiding further exploration of quantum computer designing.

Keywords: Quantum Computers, Applications, Algorithms.

1. Introduction

In early 19th century, Charles Babbage, who is called as the father of the computer, invented Difference Engine and Analytic Engine. In 1941, a German engineer Konrad Zuse complete a device called Z3, this is considered as “the world’s first working electron mechanical programmable. Fully digital computer.” The concept of modern computer was raised by Alan Turing, “father of computer science”, in 1936. With Turing’s work, the modern computer developed rapidly.

Previously, each computer was designed for a specific function. Changing the function of a computer requires changing the structure of that machine. Stored-program computer changed this situation, by inducing a concept named Instruction Set Architecture (programme), that executed by implementation (e.g., CPU). The first stored-program computer, Manchester Baby was released in 1948 at the university of Manchester [1]. Since then, a computer may run different programmes and working on complicated works. There is an observation called Moore’s law to describe the rapid development of classic computer. Moore’s law is an observation law raised by Gordan Moore in 1968, states that the number of transistors in a dense integrated circuit (IC) doubles about every 18 months

Quantum computing, is a more recent concept. The concept of quantum computing is raised by Paul Benioff in 1980. In 1986 Feynman raised the circuit notation that quantum computer may use. Since then, the quantum computer has been developed as times goes by. So far, it is shown that quantum computing is indeed better than classic computer in some specific question. In 2011, Scott Aaronson and Alex Arkhipov suggested that for questions like Gaussian boson sampling (seen the Galton's board case shown in Fig. 1), quantum computer might have a significance advantage compared to classic computers [2].

Moreover, quantum computer made some huge progress these years. In 2019, Google Artificial Intelligence created Sycamore processor, a quantum computer with 53 qubits. It was claimed that Sycamore completes a task that a state-of-the-art supercomputer takes 10,000 years to finished [3]. Jiuzhang is the first photonic quantum computer to attain quantum supremacy, created by University of Science and Technology of China in 2020. For Software part, some algorithms are invited and proved to be useful in some particular area. Grove's algorithm is potentially better that traditional computer algorithm when the number of qubits is huge. Shor's algorithm is a factorization algorithm and it solves problems involving factorization problem in polynomial time and it might challenge the RSA encryption [4-8]. This article aims to overview these works of quantum computing, finding their advantage compared to classic computer. In addition, the state-of-art applications will be discussed and find out the corresponding limitation.

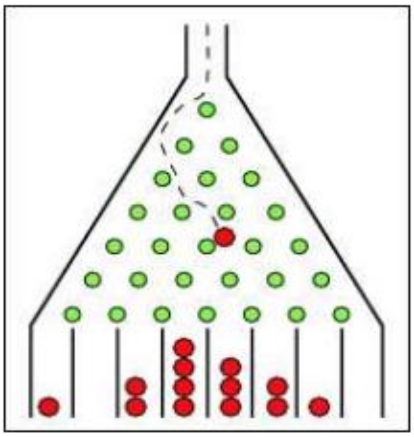

Figure 1. Sketch of Galtons's board.

2. Principle of quantum computing

Different from classic computer, that using bit as a basic unit to store information, the information is stored in qubit in quantum computing. For each bit in classic computer, it could only be "0" or "1". While quantum computing using "qubit" to representing information, a qubit act like the mathematical model of a quantum and it could be a superposition of "0" and "1". Let

$$|0>=\begin{pmatrix}1\\0\end{pmatrix},\quad |1>=\begin{pmatrix}0\\1\end{pmatrix} \tag{1}$$

then for a qubit state $|\psi>$ with superposition of $|0>$ and $|1>$, one could represent it as

$$|\psi>=\ \alpha\,|0>+\beta\,|1>=\begin{pmatrix}\alpha\\\beta\end{pmatrix} \tag{2}$$

where $||\alpha||^2$ is the probability of the qubit in the state of "0", and $||\beta||^2$ represent the probability of being "1". Hence, one has

$$||\alpha||^2+||\beta||^2=1 \tag{3}$$

The entanglement is another important concept is entanglement. One already knows that a qubit could be in the state of superposition of |0> and |1>. If there are two qubits, and they are entangling with each other. It might be in the state of superposition of |00> and |11>. Bell state, e.g., is a state of two qubit that are entangled with each other [6].

Bloch sphere is often used in quantum computing, to visualize the state of qubit as illustrated in Fig. 2. Given an arbitrary qubit state $|\psi >$,let ϕ be the angle away from the x-axis and let θ be the angle away from the z-axis. Then this arbitrary state $|\psi >$ could be written as $|\psi >= \cos\frac{\theta}{2}|0 > +e^{-i\phi}|1 >$, which is just a superposition of state $|0 >$ and $|1 >$, and the angle control the amplitudes (probability).

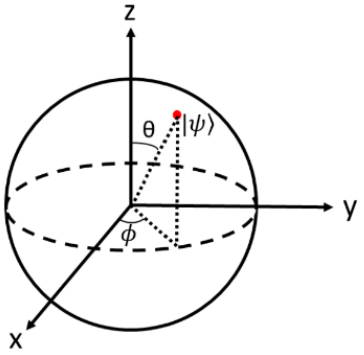

Figure 2. A sketch of Bloch sphere.

So, one knows that each state of a qubit could be represent as a vector in this Bloch sphere. Therefore, it is feasible to use matrix multiplication to control it [5], which is called as 'gates. Pauli gates (X, Y, Z) is created by Pauli, it is a combination of three matrices that acts on a single qubit. For X gate, one has

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{4}$$

This X gate represent the state of qubit rotate around X-axis on Bloch sphere by π radius. For Y gate, one has

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{5}$$

This Y gate represent the state of qubit rotate around Y-axis on Bloch sphere by π radius. For Z gate, one has

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{6}$$

This Z gate represent the state of qubit rotate around Z-axis on Bloch sphere by π radius There are also lots of other quantum gates operating on a qubit. Another power gate is H gate, named by Jacques Hadamard.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{7}$$

This gate maps a qubit basis state to superstition state by $|0 > \mapsto \frac{|0>+|1>}{\sqrt{2}}$, and $|1 > \mapsto \frac{|0>-|1>}{\sqrt{2}}$. With these gates, quantum circuit is formalized (seen an example presented in Fig. 3).

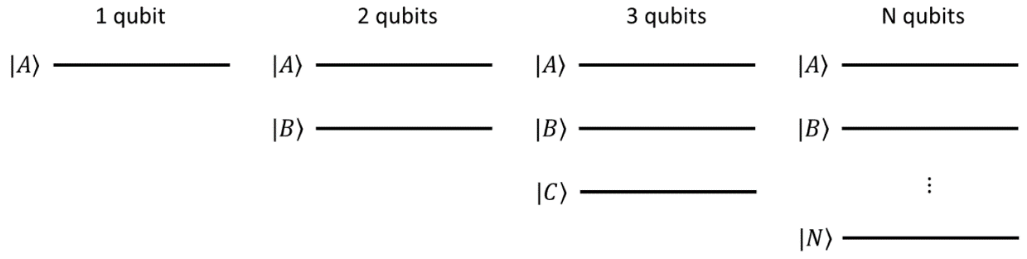

Figure 3. A sketch of different bits.

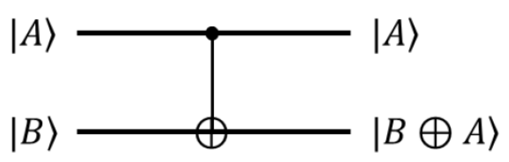

Figure 4. A sketch of CNOT gate.

Here, each qubit is represented by a parallel line. Two qubits may interact with each other. For example, a circuit of two qubit with a CNOT gate is given in Fig. 4, where CNOT gate is a 4×4 matrix of the form

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{8}$$

Here, $|\mathrm{A}>$ is the control qubit and $|\mathrm{B}>$ is the target qubit. With the operation of CNOT gate, $|\mathrm{A}>$ remain unchanged while $|\mathrm{B}>$ turn into $|\mathrm{B} \oplus \mathrm{A}>$. If the control qubit $|\mathrm{A}>$ is '1', then target qubit $|\mathrm{B}>$ flipped from '0' to '1' or from '1' to '0'. Meanwhile, if the control qubit $|\mathrm{A}>$ is '0', then target qubit $|\mathrm{B}>$ remain unchanged [7]. By using the H gate, two qubits are changed into a superstition state that could only represented and operating in quantum computing, and using CNOT gate to connect these two qubits, one obtains a pair of qubits that are entangled. This is how quantum computers work.

3. Quantum computing algorithm

In quantum computation, there are lots of algorithm. For some particular problems, Quantum algorithms might be much faster than classic algorithm. This is because some properties (e.g., quantum entanglement and quantum superstition) are hard to simulated by classic algorithm.

3.1. Grove's algorithm

Grove's algorithm is one of the most important algorithms among quantum computation. It is also known as 'quantum search algorithm'. It is raised by Lov Gover in 1996. This is an efficient algorithm that helps you search for an item in an unorder list. For example, to find out a specific permutation in a binary numeral system of N digits, it takes 2n times to find out the result by using classic computation. However, it takes only 2^n/2 times to find out the result in Grover's result. In this algorithm, the high probability of a particular value will be shown given a black box function with a unique input [6]. The steps of Grove's algorithm are as follows:

- Initialize the target system to the distribution of $(\frac{1}{\sqrt{\mathrm{N}}}, \frac{1}{\sqrt{\mathrm{N}}}, \frac{1}{\sqrt{\mathrm{N}}}, \frac{1}{\sqrt{\mathrm{N}}} \dots \dots \dots, \frac{1}{\sqrt{\mathrm{N}}})$, which is a state of having equal probability of all states.
- Make a "black box": one has a thing called "Black box". It is takes n bits as input and return one bit as output. It is designed to return 1 if the input is in the desired combination, and return 0 in all other cases. This black box can be achieved by the circuit shown in Fig. 5 [7].

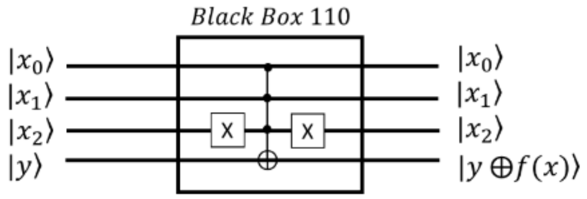

Figure 5. A sketch of realization of black box.

Now, one has a black box and a state of equal probability distribution, highlighting the state of black box by letting its amplitude be negative. Here, let there being a 3 bits system, and one wants the |101> state. Calculate the mean of all amplitudes and then flip the negative amplitudes to the other side of mean value. Then repeat this as iteration for $O(\sqrt{n})$ times, one eventually obtained the requirements. The corresponding circuit is presented in Fig. 6. This is what Grover's algorithm is. It is shown that for problems like finding out a particular state over a unorder list, it is much faster than classic computing, especially when n is very large.

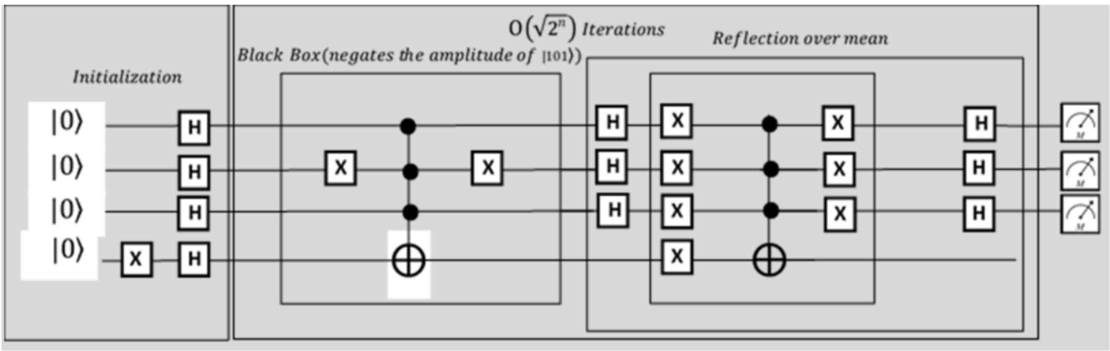

Figure 6. A sketch of circuits for Grover's algorithm.

3.2. Shor's algorithm

Another very important algorithm is Shor's algorithm. It is a prime factorizing algorithm for integer. This algorithm was raised by American mathematician Peter Shor in 1994. Given a 2048-bit number, which is a product of two large prime number, it takes ages that even longer than the universe age to factories it. However, with Shor's algorithm, however, it requires only a few hours given a quantum computer with thousands of qubits.

The steps of Shor's algorithm are as follows [8]. There is a fact that given any two prime number A, B. one has:

$$\boldsymbol{A}^{p} = \boldsymbol{B} \times m + 1, for\ p, m \in\ R \tag{9}$$

Subtract both side with 1, one may obtain:

$$\boldsymbol{A}^{p} - 1 = \boldsymbol{B} \times m \tag{10}$$

$$\left(\boldsymbol{A}^{\frac{p}{2}} - 1\right)\left(\boldsymbol{A}^{\frac{p}{2}} + 1\right) = \boldsymbol{B} \times m \tag{11}$$

and it is shown that it is likely for one of the $(\mathrm{A}^{\frac{\mathrm{p}}{2}} - 1)$ or $(\mathrm{A}^{\frac{\mathrm{p}}{2}} + 1)$ term be a factor of B. Therefore, the remaining question is trying to find number p such that given A, B, A to the power of p is a multiple of B. Subsequently, one may use quantum computer based on designing a quantum circuit to calculate a^{x} mod b given any x. Input co-prime number a and b as given, and input x ranging from 0 to p, once the remainder is 1, ones know that the number x that is needed. In the computational circuit, we input all possible value of x by taking q qubits, and apply H gate to them. Then the input qubits will be in an equal probability of superposition of $|0 >$ to $|\mathrm{Q} - 1 >$ in the form of:

$$|0>|a^0 Mod\ N>+|1>|a^1 Mod\ N>+|2>|a^2 Mod\ N>\ldots\ldots+|Q-1>|a^{Q-1} Mod\ N> \quad (12)$$

It is shown that given any two prime number A, B, and p

$$\boldsymbol{A}^p = \boldsymbol{B} \times m + 1, for\ p, m \in\ R \quad (13)$$

If one has:

$$\boldsymbol{A}^x = \boldsymbol{B} \times y_1 + r, for\ y_1, r \in\ R \quad (14)$$

Then,

$$\boldsymbol{A}^{x+p} = \boldsymbol{B} \times y_2 + r, for\ y_2, r \in\ R \quad (15)$$

This shows the number p, which is what we want, has a periodic property. Next, we apply quantum Fourier transform (QTF) to it. This transform does the following:

a. It removes the offset and gives some probability for state 0
b. It changes the period between the state from r to Q/r

Afterwards, if one measures the qubits, it is feasible to get some multiple of Q/r. Knowing the measure result and Q, we will get some multiple of 1/r. Then one may achieve the periodic that is needed. The circuit of Shor's algorithm for an N=35 factorizing problem is shown in Fig. 7 [9]. This is the way that Shor's algorithm work. It is a really useful and efficient way to factories bit number. As Shor mentioned, Quantum Fourier transform in this algorithm is just like diffraction grating, it makes the periodic obvious to measure.

Shor's algorithm is changeling current encryption. Classic encryption (RSA) encodes a big number composed with two factors. This method is safe because classic computer takes a really long time to factories such a big number, Shor's algorithm, however, make the factories being realistic within a few hours. Therefore, some other encryptions are being developing to prevent Shor's algorithm being abuse in the future, for example, quantum key distribution.

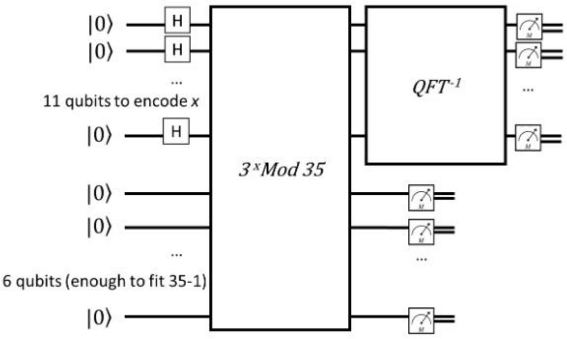

Figure 7. A sketch of circuits for Shor's algorithm.

4. Applications

As quantum computing developed rapidly recent years, more and more applications are being used to solve specific problems. These years, some surprising achievements are reached. Sycamore processor is anquantum processor produced by Google's Artificial Intelligence in 2019 [3]. It was claimed that about 200 seconds was taken for their Sycamore processor to sample one instance of a quantum circuit a million times, where the equivalent task for a latest classical supercomputer would be around 10,000 years. They designed a task of sampling the output of a pseudo-random quantum circuit. Besides, they used a method that comparing if each bitstring is observed experimentally with its ideal probability often via classic computer simulation. They called this method "cross-entropy benchmarking". They conclude that their Quantum processors can perform computations in a Hilbert space of dimension 253, where the circuit is given in Fig. 8.

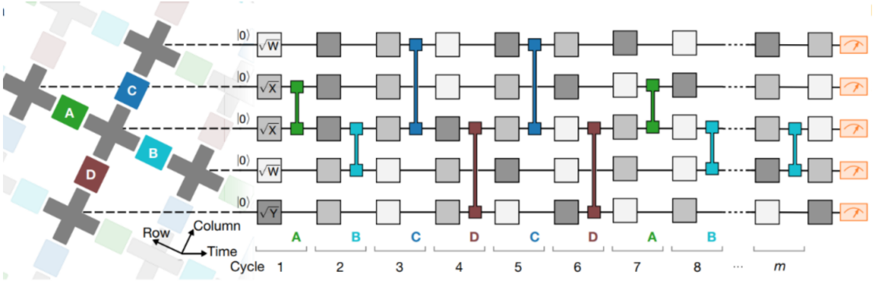

Figure 8. A sketch of circuits for 53 bits.

In 2020, Jiuzhang has been created by University of Science and Technology of China (USTC), led by Pan Jianwei and Lu Chaoyang [10]. This is the first photonic quantum computer to achieve quantum supremacy, with a maximum of 76 detected photons. Jiuzhang 2 was created on 26/10/2021, with 113 photons. In their article, it was mentioned that Gaussian boson sampling was performed in 200 seconds, with 76 detected photons. It was estimated that it would take 2.5 billion years for Sunway Taihulight Supercomputer to preformed same calculation. Jiuzhang can perform calculation of 1030 dimension in Hilbert space.

There are also some other art-of-state applications so far, like in chemistry and quantum key distribution. Quantum key distribution (QKD) is a secure communication method, that used to create and transmit key, with any chosen encryption algorithm. The security is guaranteed without restricting potential eavesdropped [11]. It is the first quantum information task that being in mature level and it has already used for commercial purpose. Nowadays, there are 6 companies offer quantum key distribution commercially around the world. In 2017, Jianwei Pan led team of University of Science and Technology of China measured entangled photons over 1203 km by using satellite [9]. It is shown that around a rate of 20 orders of magnitude is greater than telecommunication fiber under the scale of 1200km as depicted in Fig. 9.

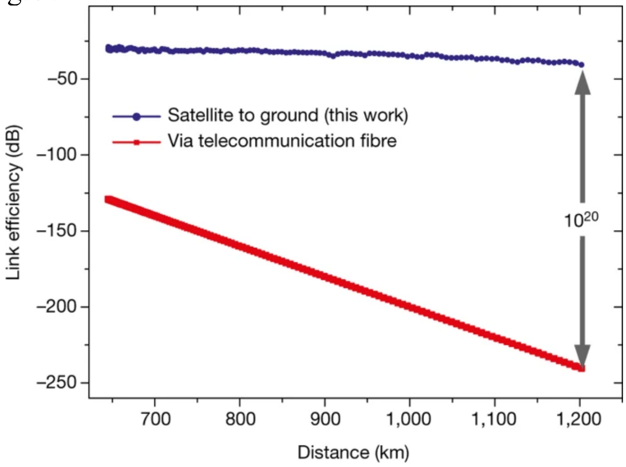

Figure 9. Link efficiency as a function of distance.

5. Limitation and further outlook

Even though quantum computing is shown to be much faster than classic computer in some algorithm and some state-of-art application, and may represent some work that could not be done by classic computer, there are still some limitations of it. Currently, most quantum computer are still in experimental stage. To put quantum computer into real work, it requires thousands of qubits or even millions. So far, there are no enough qubits for Grover's algorithm and Shor's algorithm to solve problem realistically. Using Grover's algorithm, millions of qubits are required to exceed classic computer. it is not realistic to achieve recent years. It might take decades or even longer to produce such a quantum computer. But as we already seen, Quantum computing indeed have significance advantage in solving problems like Gaussian boson sampling, which don't required lots of qubits. Question like this might be the main field that quantum computing devotes into in the following years.

6. Conclusions

In summary, this paper discusses the basic principles and state-of-art applications for the quantum computing. To be specific, two algorithms (i.e., Grover and Shor) are discussed in detail with the corresponding realization circuits and scenarios. Moreover, the state-of-art facilities for realizing quantum bits are demonstrated, including the Google's and China's results. In addition, the current limitations are analyzed accordingly and the prospects are proposed in the meantime. Overall, these results offer a guideline for future designing and development of quantum computing.

References

[1] Burton C P. Replicating the Manchester Baby: Motives, methods, and messages from the past[J]. IEEE Annals of the History of Computing, 2005, 27(3): 44-60.

[2] Aaronson S, Arkhipov A. The computational complexity of linear optics[C]. Proceedings of the forty-third annual ACM symposium on Theory of computing. 2011: 333-342.

[3] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor[J]. Nature, 2019, 574(7779): 505-510.

[4] Information on: https://github.com/microsoft/Reference-Guide-For-Quantum-Computing-A-Microsoft-Garage-Project/blob/main/1-Basic_Quantum_Concepts/2-Gates.ipynb

[5] Feynman R P. Quantum mechanical computers[J]. Optics news, 1985, 11(2): 11-20.

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

[7] Information on: https://github.com/microsoft/Reference-Guide-For-Quantum-Computing-A-Microsoft-Garage-Project/blob/main/2-Quantum_Algorithms/4-Grover_s_Algorithm.ipynbr

[8] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]. Proceedings 35th annual symposium on foundations of computer science. IEEE, 1994: 124-134.

[9] Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution[J]. Nature, 2017, 549(7670): 43-47.

[10] Zhong H S, Wang H, Deng Y H, et al. Quantum computational advantage using photons[J]. Science, 2020, 370(6523): 1460-1463.

[11] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The security of practical quantum key distribution[J]. Reviews of modern physics, 2009, 81(3): 1301.