Journal of Physics: Conference Series

Four Arithmetic Operations on the Quantum Computer

To cite this article: Yong Zhang 2020 *J. Phys.: Conf. Ser.* **1575** 012037

Four Arithmetic Operations on the Quantum Computer

Yong Zhang

School of Software and Internet-of-Things Engineering, Jiangxi University of Finance and Economics, Nanchang, P.R. China.
Email: zhangyong@jxufe.edu.cn

Abstract. Quantum computer has been proved to be superior to electronic computer in solving some NP problems. Based on the former quantum adder, this paper proposes a new quantum adder and quantum subtracter, and then designs a fixed-point quantum multiplier and a fixed-point quantum divider based on fixed-point number operations. Four arithmetic units are presented using quantum gate circuits. These researches lay a foundation for the quantum implementation of digital filters.

1. Introduction

Since Feynman, more and more scholars believe that the computing power of quantum computer is unmatched by electronic computer [1]. In 1992, Deutsch et al. proposed a quantum computer model, which confirmed that Deutsch problem can be solved faster in quantum computer than in electronic computer [2]. Both Shor quantum factorization algorithm and Grover search algorithm have shown that quantum computers have greater computational advantages than traditional electronic computers in some aspects [3].

Quantum computation and quantum computers have attracted wide attention of scholars [4,5]. Two important applications of quantum computing are quantum cryptography [6,7] and quantum image processing [8]. Since quantum information is non-clonable, quantum entanglement is an important physical guarantee of secure communications [9]. Some chaotic systems realized by quantum gate circuits can be used as pseudo-random sequence generators in image cryptosystems to realize the encryption and decryption of quantum images [10].

On the basis of the previous research on quantum computation and quantum gate circuits, this paper studies in detail the method of realizing basic arithmetic units by means of quantum gate circuits, especially the multiplier and divider of fixed-point number with the quantum gate circuits. The research work paves the way for the realization of fixed-point number operations by means of quantum computer.

2. Quantum Adder

2.1. Existing Quantum Adder

In 1996, Vedral et al. proposed a quantum adder [11]. They designed adders and carry circuits based on quantum circuits such as quantum NOT gate and quantum XOR gate, as shown in figure 1 and figure 2. Then, a quantum adder is implemented using the circuits shown in figure 1 and figure 2, as shown in figure 3.

In figure 1b, the inputs are the carry bit c from the previous stage and two addends a and b from top to bottom, and the outputs are c, a and $a+b$ from top to bottom. In figure 2b, the inputs are successive carry c_0 from the previous stage, two addends a and b, and the carry signal from top to bottom, and the outputs are c_0, a, b and c_1 from top to bottom and the carry signal is stored in c_1.

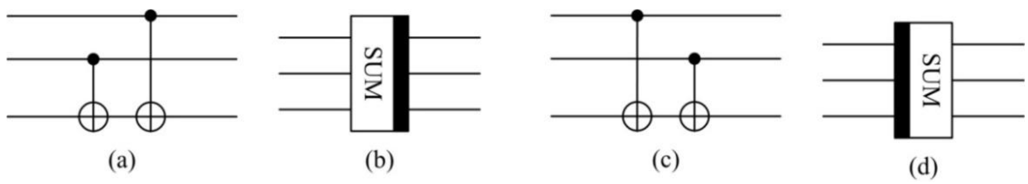

Figure 1. Single qubit adder (a) adder; (b) symbol of adder; (c) subtracter; (d) symbol of subtracter.

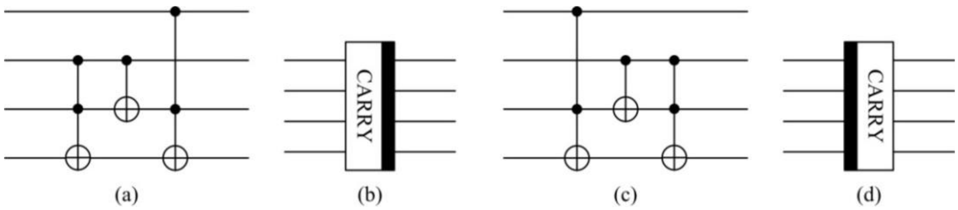

Figure 2. Carry circuit (a) carry circuit; (b) symbol of (a); (c) borrow circuit; (d) symbol of (c).

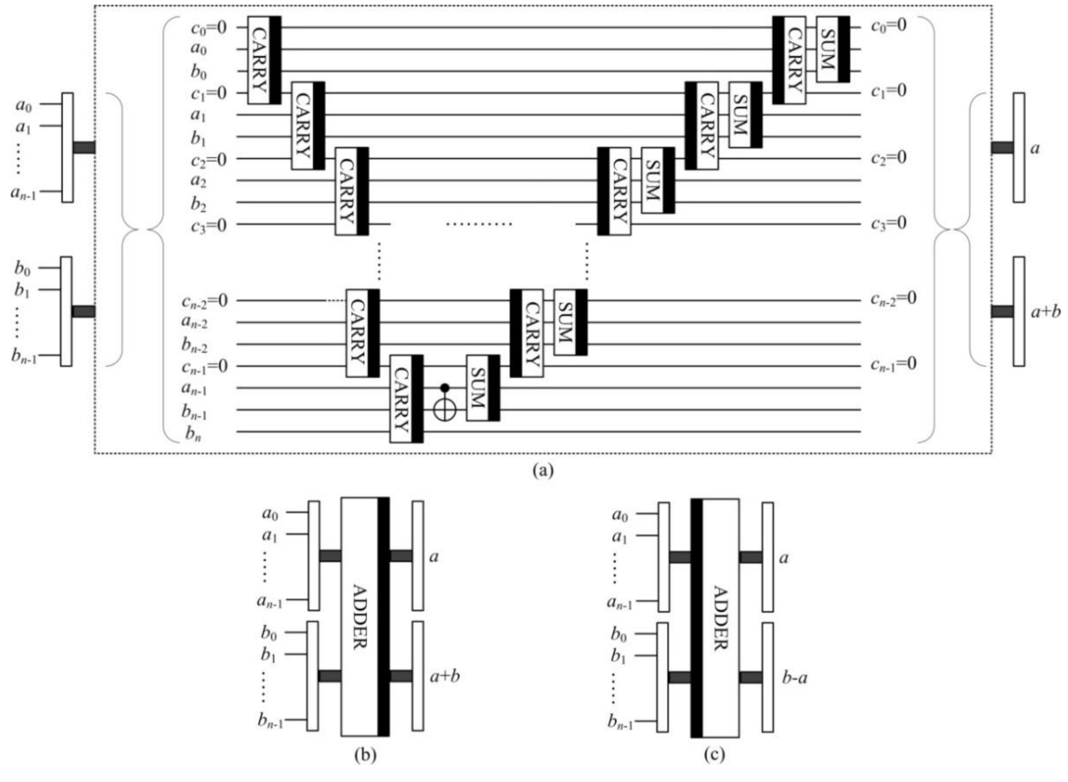

Figure 3. Vedral's quantum adder (a) adder; (b) symbol of (a); (c) symbol of subtracter.

In figure 3, c_0, c_1,..., c_{n-1} are added to save the carry signals, and b_n is added to save the whole carry signal after addition. Figure 3b is the symbol of quantum adder and figure 3c is the symbol of quantum subtracter. That is, figure 3c is the inverse unit of figure 3b.

2.2. Improved Quantum Adder

Based on Vedral's work, three Toffoli gates and two NOT-controlled gates are used to design a quantum full adder, as shown in figure 4. The logical truth table for figure 4a is shown in table 1. In table 1, a_0+b_0+c_0 are assigned to the new b_0. Figure 4c is the reverse circuit of figure 4a to realize subtraction. The adder and subtracter, designed with the help of the quantum circuits shown in figure 4, are shown in figure 5 and figure 6, respectively.

In the electronic computer, there is no subtraction circuit. The electronic computer unifies addition and subtraction into addition operation by means of complement form. In the quantum computer, the addition and subtraction can also be unified into addition operation by means of complement form, just like in the electronic computer. The complement of a positive integer is the same as that of the original, and the complement of a negative integer is the inverse of every bit except the sign bit, followed by 1. The quantum circuit for converting a signed integer to its complement form is shown in figure 7.

In figure 7, if the input is original code of *a*, the output is complement of *a*; if the input is complement of *a*, the output is original code of *a*. In figure 8, the addition and subtraction operations are unified into addition operations with the complement processing unit.

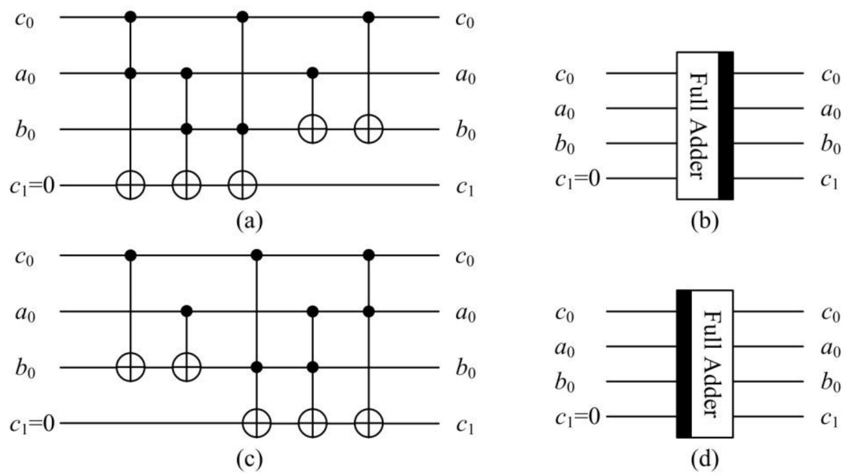

Figure 4. Quantum full adder (a) full adder; (b) symbol of (a); (c) subtracter; (d) symbol of (c).

Table 1. Logic truth table of quantum full adder.

c_0	b_0	a_0	$a_0+b_0+c_0 \rightarrow b_0$	c_1
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

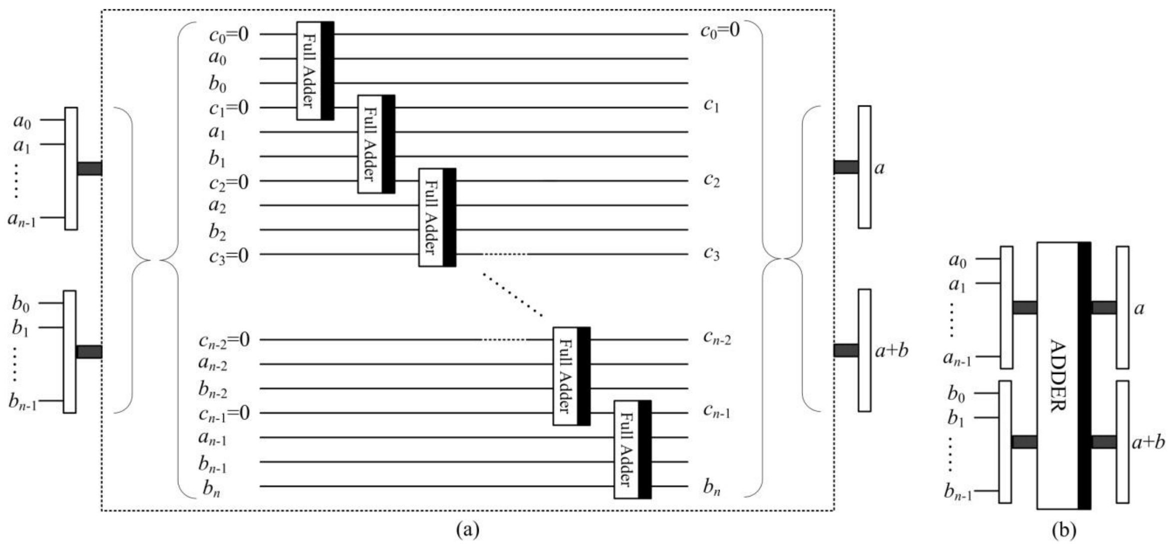

Figure 5. Quantum adder (a) adder; (b) symbol.

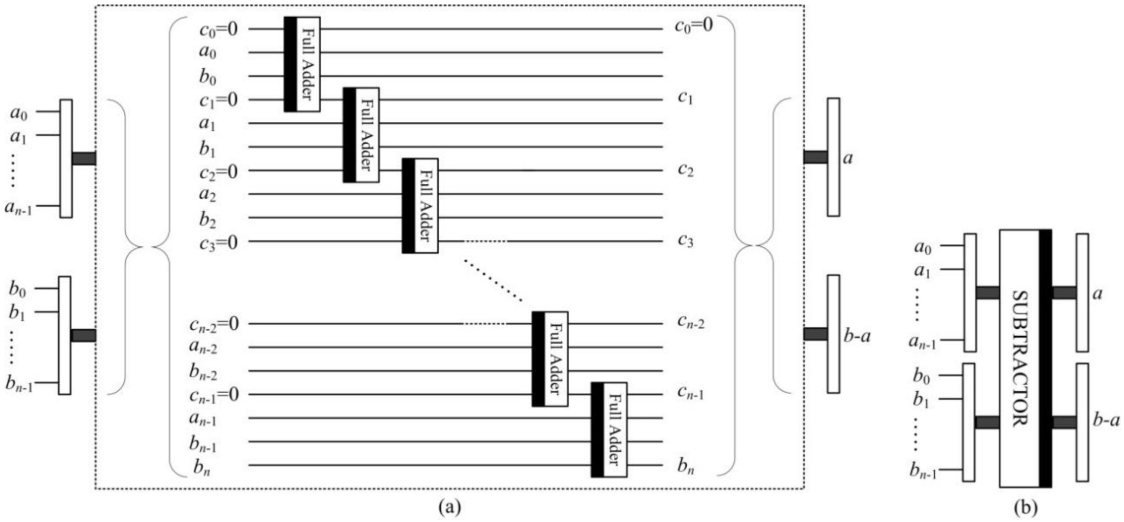

Figure 6. Quantum subtracter (a) subtracter; (b) symbol.

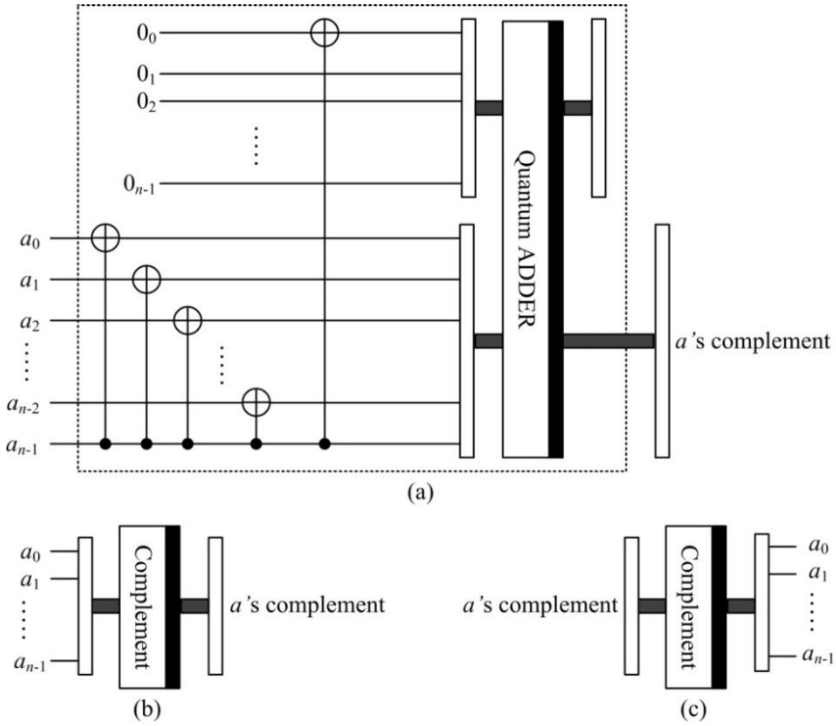

Figure 7. Quantum gate circuits converting a signed integer into its complement form (a) circuit; (b)-(c) symbols.

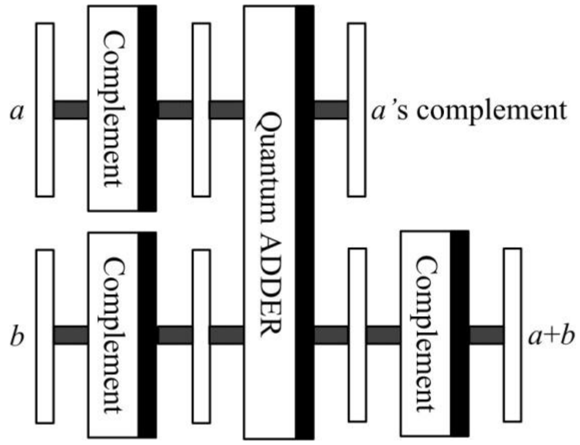

Figure 8. Quantum adder using complement form.

3. Quantum Multiplier of Fixed-point Number

In quantum computer, the multiplication method of fixed-point decimals is to use the calibration method to process the decimals with fixed points. The calibration method is denoted by Q$m.n$, where $m+n+1$ is the word length of the computer. For example, -0.52 uses Q0.15 for calibration to get a fixed-point number 1.851E (in hexadecimal), and 0.68 uses Q0.15 for calibration to get a fixed-point number 0.AE14 (in hexadecimal).

It is well known that the product of two original-code decimals represented by two Q0.(n-1) is the decimal scaled by Q0.(2n-1). This operation process is as follows: Let x and y be two decimals in original-code form represented by Q0.(n-1), where, x=x0.$x_1x_2...x_{n-2}x_{n-1}$, y=$y_0.y_1y_2...y_{n-2}y_{n-1}$. x_0 and y_0 are the sign bits of x and y, respectively. Let $x*y=r$ and $r=r_0.r_1r_2...r_{2n-2}r_{2n-1}$. r_0 is the sign bit of r. Then r_0= $x_0 \oplus y_0$, $r_1r_2...r_{2n-2}r_{2n-1}$= $(x_1x_2...x_{n-2}x_{n-1}) * (y_1y_2...y_{n-2}y_{n-1})*2$.

For example, the product of two original-code decimals represented by Q0.4 is the decimals with Q0.9. The operation process is as follows: Let a and b be the decimals of original-code form represented by Q0.4, where, $a=a_0.a_1a_2a_3a_4$, $b=b_0.b_1b_2b_3b_4$. a_0 and b_0 are the sign bits of a and b, respectively. Let $a*b=r$ and $r=r_0.r_1r_2...r_9$. r_0 is the sign bit of r. And $r_0=a_0 \oplus b_0$, $r_1r_2...r_9=(a_1a_2a_3a_4)*(b_1b_2b_3b_4)*2$. The corresponding quantum circuit is shown in figure 9. In figure 9, zero-controlled gate is used as shown in figure 10.

Journal of Physics: Conference Series **1575** (2020) 012037 doi:10.1088/1742-6596/1575/1/012037

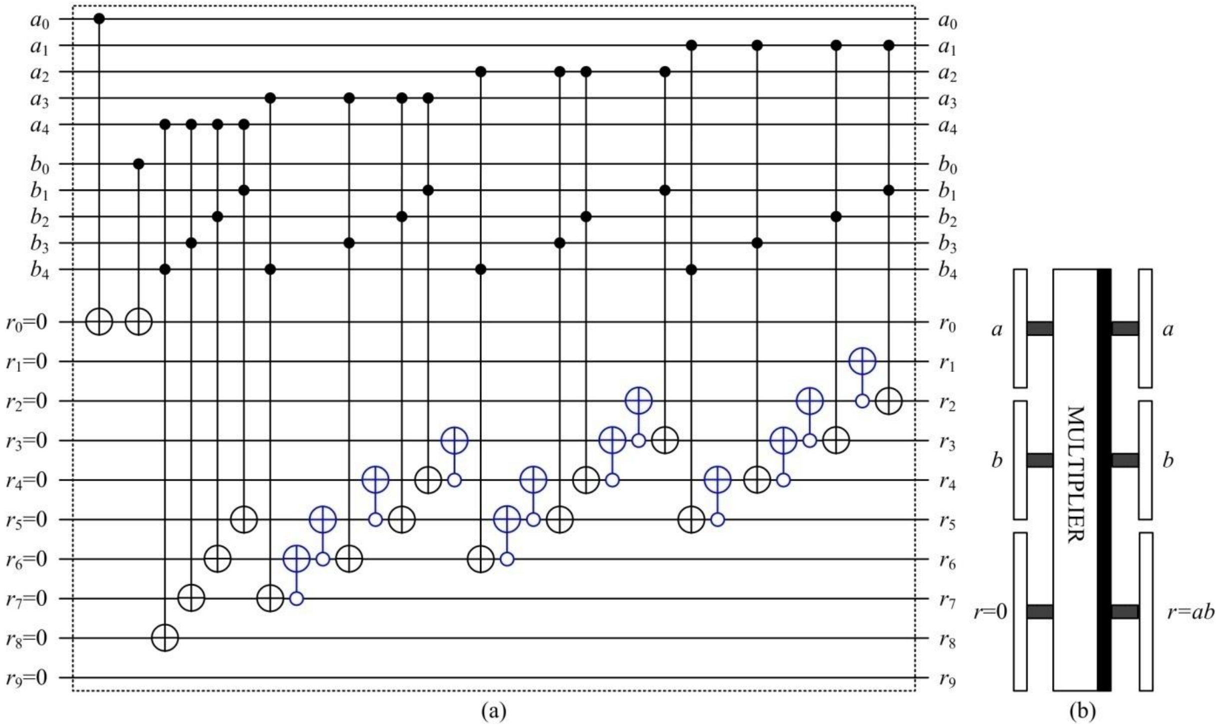

Figure 9. Quantum multiplier of Q0.4 (a) multiplier; (b) symbol.

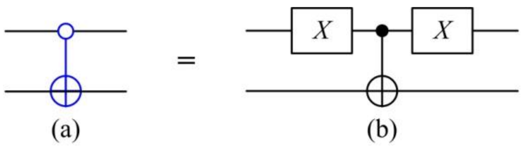

Figure 10. Zero-controlled NOT gate (a) symbol; (b) circuit.

For multiplication of any two Q0.(n-1) decimals, the quantum multiplication circuit is similar to that shown in figure 9 with the expanded part having the property that a zero-controlled NOT gate unit is applied to the upper line every two exclusive-OR operations in the same line.

4. Quantum Divider of Fixed-point Number

The division (b/a) of two fixed-point numbers a and b is considered. Generally, a is formatted as the scaling form Q0.(n-1) or Qm.(n-m-1), and b is formatted as the scaling form Q0.(2n-1) or Qk.(2n-k-1). Thus, $a=a_0a_1a_2...a_{n-1}$(in binary), and a_0 is the sign bit. And $b=b_0b_1b_2...b_{2n-1}$ (in binary) and b_0 is the sign bit. In the quantum computer, the quantum circuit as shown in figure 11 is constructed to divide the fixed-point numbers. The quotient $r=b/a$ and the remainder is saved in b.

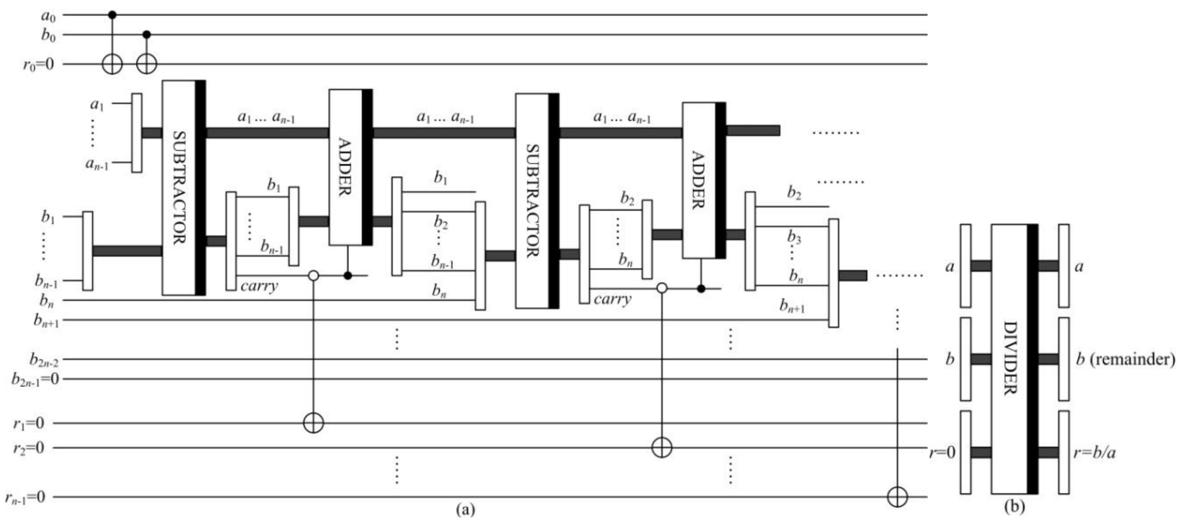

Figure 11. Quantum divider (a) divider; (b) symbol.

In the quantum division unit shown in figure 11, a controlled adder is used. When the i-th borrow signal is 0, the corresponding result r_i is 1. When the i-th borrow symbol is 1, the corresponding output of subtracter needs to add a to restore to the original $b_i b_{i+1} \ldots b_{i+n-2}$.

5. Conclusion

In this paper, four arithmetic operations implemented on quantum computer are studied. At first, the quantum adder and complement quantum adder are designed. Then, the representation and calculation methods of fixed-point numbers are discussed. After that, the general quantum multiplier and divider of fixed-point numbers are constructed. Based on the designed quantum arithmetic units, one can perform high-precision decimal multiplications and divisions. On the basis of this work, we plan to design the quantum versions of floating-point number operations in the future, and realize the quantum processing versions of number system operations used on conventional electronic computers.

6. Acknowledgments

We would like to thank the financial supports from the National Natural Science Foundation of China (No. 61762043), Natural Science Foundation of Jiangxi Province (No. 20192BAB207022), and Scientific Research Foundation of Jiangxi Provincial Education Department (No. GJJ190249).

7. References

[1] Feynman R P 1986 *Found. Phys.* **16** 507
[2] Deutsch D and Jozsa R 1992 *R. Soc. Lond. A* **439** 553
[3] Nielsen M A and Chuang I L 2000 *Quantum computation and quantum information* Cambridge University Press
[4] Makaruk H 2017 *J. Knot Theory Ramif.* **26** 1741006
[5] Kaise U 2017 *J. Knot Theory Ramif.* **26** 1741004
[6] Jiang N and Wang L 2015 *Int. J. Theor. Phys.* **54** 1021
[7] Li D, Yang Y, Bi J, Yuan J and Xu J 2018 *Scientific Reports* **8** 225
[8] Cai Y, Lu X and Jiang N 2018 *Chin. J. Elec.* **27** 718
[9] Kuzyk M G 2019 *Amer. J. Phys.* **87** 325
[10] Jiang N, Dong X, Hu H, Ji Z and Zhang W 2019 *Int. J. Theor. Phys.* **58** 979
[11] Vedral V, Barenco A and Ekert A 1996 *Phy. Rev. A* **54** 147