

A New Universal Quantum Gates and Its Simulation on GPGPU

Huimin Luo^(✉), Jiabin Yuan, and Wenjing Dai

College of Computer Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing, China
{lhm,jbyuan,jing}@nuaa.edu.cn

Abstract. Classic quantum computer simulation will be a hotspot for years until the realistic quantum computers are available. As an essential component of quantum computers, the effects of the basic quantum gate and the equivalent relation are first briefly concluded in this paper. Base on the general-purpose graphics processing units (GPGPU) environment, the novel basic quantum gate simulation platform is achieved, on which any arbitrary quantum algorithm can be simulated. Our platform provides an user-friendly graphical interface for generating quantum circuit and observing the transformation of probability amplitude. Whats more, with the analyse of the combination of the existing universal quantum gates, a new universal quantum gates including Controlled-Z (C-Z), Hadamard (H), T is put forward. The proposed universal gates are considered to be more suitable for GPGPU, and it can be widely used to construct the quantum teleportation circuit and Grover's search algorithm. The new quantum circuit of Grover's search algorithm is conducted in our novel simulation platform. Results of the experiments show that the Grover's search algorithm will acquire quadratic acceleration when solving the search problem, which reflects the validity of the proposed gates.

Keywords: Universal quantum gates · Quantum circuit · GPGPU · Grover's search algorithm

1 Introduction

Quantum computation has attracted much attention in the last three decades [1] for its properties of the nature (superposition and entanglement of quantum states) [2]. A wide range of classical counterpart applications, such as large factor factorization, disordered database search [3] and quantum system simulation, are accelerated with quantum method.

A number of domestic and foreign scholars are devoted themselves to quantum gates realization. Ferrando-Soria et al. introduced two schemes for implementing CNOT and \sqrt{i} SWAP gates with supramolecular assemblies and perform detailed simulations, to demonstrate how the gates would operate [4]. Hu et al. proposed a set of universal quantum gates with topological bases through the developed DDM technique [5]. The companies of Google, Microsoft and

D-WAVE have announced the results of quantum computer research, but realistic quantum computers have not been built yet. Before the utilization of quantum computer, quantum simulation is a significant method to study quantum computing theory. Many different quantum computation simulations, such as Libquantum C, QuBit, jaQuzzi, have been designed till now [6]. Some of them were developed to demonstrate the most known quantum algorithms but not suitable for constructing an arbitrary quantum algorithms [7].

The quantum circuit model is the most widely used quantum computing model, which provides a basic architecture for the physical implementation of quantum computers. In the quantum computing theory of the circuit model, the basic quantum gate library is found first, and then the universal quantum computation is realized with the combination of these gates. The basic gate library, which also called universal quantum gates, that all unitary operations on arbitrarily many bits n can be expressed as compositions of these gates. In recent years, scholars at home and abroad have found common combination of quantum gates as follows: (1) All one-bit quantum gates plus CNOT, due to Barenco [8] (2) Toffoli, Hadamard, and S, due to Kitaev [9] (3) CNOT, Hadamard, and T, due to Boykin [10, 11] (4) Toffoli plus any basis-changing single-qubit real gate; Toffoli, Hadamard; Toffoli and S; CNOT and T; CNOT and S, due to [12] (5) Hadamard, CNOT, S, and T, due to Kliuchnikov [13].

In this study, the novel basic quantum gate simulation platform is achieved under the GPGPU environment, on which any arbitrary quantum algorithm can be simulated. Furtherly, base on the existing universal quantum gates and the equivalently substituted relation, a new strategy for general quantum gates (C-Z, H, T) suitable for GPGPU cluster environment is designed. The search problem is widely used in practice, such as [14, 15]. In order to validate our implementation, quantum teleportation [16] and Grover's search algorithm [17] are implemented on the proposed platform to demonstrate the validity of the proposed quantum gates.

The remainder of the paper is organized as follows. In Sect. 2, we describe the general form of the quantum gates and the form of the quantum circuit briefly. In Sect. 3, the novel basic quantum simulation platform is achieved, and a new universal quantum gates including C-Z, H, T was put forward, and experiments are presented in Sect. 4. Finally, the conclusion is presented in Sect. 5.

2 Background

2.1 Qubit Gates

An elementary unit of quantum information is a quantum bit [2]. The difference between bits and qubits is that a qubit can be in state other than 0, 1. It's also possible to form linear combinations of states, often called superpositions: $\alpha|0\rangle + \beta|1\rangle$, the number α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. The superposition of n qubits is written as $|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, where $|i\rangle$ represents a

specific computational basis state, and α_i means the probability amplitude of the relevant basis state.

The most useful single qubit gates include Hadamard, Pauli X, Pauli Y, Pauli Z, Phase shift, S and T. Multiple qubit gates usually include CNOT, C-Z and Toffoli. This section describes the effects of single quantum bit gates and multi-quantum bit gates.

(1) Single qubit gates

A quantum transformation is operated on the coefficient space of a quantum register [13]. The initial state vector is $|\phi\rangle$, and after unitary matrix operations state vector is $|\phi'\rangle$. More specifically, let us denote

$$\begin{aligned} |\phi\rangle &= a(0\dots 00) |0\dots 00\rangle + a(0\dots 01) |0\dots 01\rangle + \dots + a(1\dots 1) |1\dots 11\rangle \\ |\phi'\rangle &= a'(0\dots 00) |0\dots 00\rangle + a'(0\dots 01) |0\dots 01\rangle + \dots + a'(1\dots 1) |1\dots 11\rangle \end{aligned}$$

In the case of H, for example, when H_j is applied to the state vector $|\varphi\rangle$, transforms the amplitudes according to

$$\begin{aligned} a'(\dots * 0_j * \dots) &= \frac{1}{\sqrt{2}}(a(\dots * 0_j * \dots) + a(\dots * 1_j * \dots)) \\ a'(\dots * 1_j * \dots) &= \frac{1}{\sqrt{2}}(a(\dots * 0_j * \dots) - a(\dots * 1_j * \dots)) \end{aligned}$$

We use the $*$ to indicate that the bits on the corresponding positions are the same. It can be concluded that the H, X, Y, Phase shift gates act on the quantum bits of n require additional space for exchanging amplitudes, and the number of ground probabilities to be updated are 2^n . The gates of S, T, Z do not extra space, the number of amplitudes that need to be updated is 2^{n-1} .

(2) Multiple qubit gates

Multiple qubit gate acting on two qubits is expressed as U_{kj} , where $j < k$. For example, letting C_k^j denote a CNOT with control j and target k , the update of the probability of each basic state will comply with the following formula, all of other states at the input remain unchanged.

$$\begin{aligned} a'(\dots * 0_k * \dots * 0_j * \dots) &= a(\dots * 0_k * \dots * 0_j * \dots) \\ a'(\dots * 0_k * \dots * 1_j * \dots) &= a(\dots * 1_k * \dots * 1_j * \dots) \\ a'(\dots * 1_k * \dots * 0_j * \dots) &= a(\dots * 1_k * \dots * 1_j * \dots) \\ a'(\dots * 1_k * \dots * 1_j * \dots) &= a(\dots * 0_k * \dots * 1_j * \dots) \end{aligned}$$

It can be concluded that the CNOT gate acting on the quantum bits of n requires additional space for exchanging amplitude, and the number of ground probabilities to be updated are 2^{n-1} . The number of ground-state probabilities of the controlled phase gate and Toffoli need to be updated is 2^{n-2} , and no extra space is required.

2.2 Circuit Model for Quantum Computation

In the framework of the quantum circuit model of quantum computation it is assumed that a memory register containing n qubits can be prepared in an arbitrary state. Quantum circuit consists of quantum gates and lines connecting the gates and showing the evolution of qubit states, and it is to be read from left-to-right [7]. In quantum computation, any unitary matrix can be decomposed into a series of gate operations. A number of gates and their arrangement in the circuit determine a quantum algorithm. Note that all quantum gates are usually denoted with some symbols, for example, H is the Hadamard gate, \bullet and symbol \oplus connected with a vertical line represent the control and target qubits in the CNOT.

3 Quantum Circuit Simulation Methods

3.1 The Quantum Simulation Platform Using GPGPU

In view of the fact that the simulation of quantum systems, such as quantum computers, requires computational resources that grow exponentially with the system size. Therefore, time and space overhead are important limited factors for multi-bit quantum computation simulation. GPGPU's efficient parallel computing power is well suitable for quantum simulation techniques to solve time bottlenecks. On the basis of the effects of quantum gate, we achieved a quantum simulation platform, including the basic gates mentioned in Sect. 2, and the quantum fourier transform algorithm. The platform provides an user-friendly graphical interface for generating quantum circuits and the simulation of 29-qubits quantum gates (Fig. 1).

```

yhave realized quantum gate as following:
1 QFT  2 Hadamard  3 CNOT  4 Pauli-X
5 Pauli-Y  6 Pauli-Z  7 S  8 T  9 Toffoli
input: 2
input target bit: 1
There is 4 device beyond 1.0
Threads per block is : 512
( 2.121320 +0.000000i) |0> (|00>)
(-0.707107 +0.000000i) |1> (|01>)
( 4.949748 +0.000000i) |2> (|10>)
(-0.707107 +0.000000i) |3> (|11>)
Do you want to continue?(y/n or Y/N)

```

Fig. 1. Quantum simulation platform

3.2 The Equivalence Relation Between Quantum Gates

(1) The relationship between CNOT and C-Z

$$\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes I \right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes I \right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (1)$$

According to Eq. (1), we can see that CNOT can be generated with C-Z plus H gates, the circuit diagram is as Fig. 2.

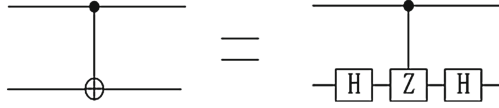


Fig. 2. The relation between CNOT and Ctrled-Z gate

(2) The relationship between S and T

According to the metrical form of S and T can be drawn $S = T^2$, the circuit diagram is as Fig. 3.

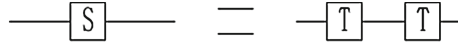


Fig. 3. The relation between S and T gate

We use the GPGPU simulation platform to verify the correctness of Fig. 3. Like show in Fig. 4, the run time of S gate is 54654.55 (ms), and the run time of two T gates is 26677.25 (ms). We can note that T gate is better suitable to run on the GPGPU platform than the S gate. When we construct quantum circuits, two T gates are generally used to replace S gates.

(3) The equivalent relation between other gates

Implementation of the Toffoli gate using H, S, CNOT and T gates as Fig. 5. We also can use the commutation relations between CNOTs to simplify the circuit, as Eqs. 2-5. Letting C_j^i denote a CNOT with control i and target j, Z_i denote a Pauli Z gate acting on the i qubit [18].

$$C_j^i Z_i = Z_i C_j^i \quad (2)$$

$$C_j^i C_j^k = C_j^k C_j^i \quad (3)$$

$$C_k^i C_j^i = C_j^i C_k^i \quad (4)$$

$$C_j^i C_k^j = C_k^j C_k^i C_j^i \quad (5)$$

(a) Implement S gate

(b) Implement T gate

3.3 The Universal Gates

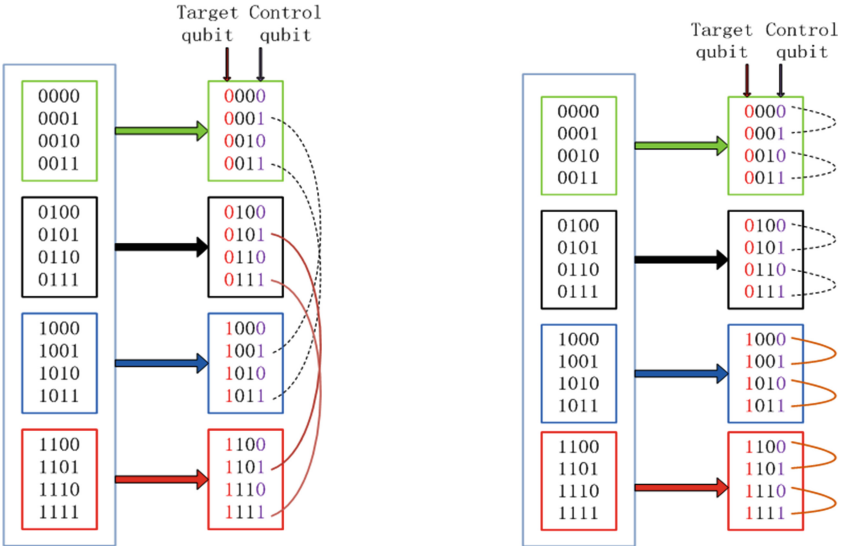
Table 1 shows that there are six kinds of universal quantum gates in currently, basing on the relationship between CNOT and C-Z discussed in Sect. 3.2, we

Index	Item
1	Toffli, H
2	Toffoli, S
3	CNOT, S
4	CNOT, T
5	CNOT, H, T
6	CNOT, H, S

propose a new general quantum gates including H, C-Z and T. The new universal quantum operators, can emulate any other operation.

Proof: First, it has defined that the H and T can approximate each single qubit operation. This is in fact easily provable, since each single qubit operation corresponds to a rotation in 3D [11]. The H operation is a rotation around of 180° around the XZ axis, the T corresponds 45° rotation. According to Ref. [19], an arbitrary unitary matrix on a d-dimensional Hilbert space may be written as a product of single qubit and CNOT gates, since C-Z can replace CNOT, so the universal gates we proposed can approximate any quantum operation.

The advantages of our new universal quantum gate can be outlined in two properties. First, in accordance with the Sect. 3.2, T gate is fit for GPGPU platform than S gate. Second, data distribution methods are discussed in Ref. [20]. An example of the simulation for 4-qubit CNOT in the case of $N=5$, $M=3$ is presented in Fig. 6(a). The size of each batch is 4, and all the coefficients are divided into 4 batches. When the role of CNOT target bit is non-local qubit, there needs data transfer between host and each device. While using C-Z instead of CNOT, it greatly reducing the cost of communication on account of no data transfer during kernel execution like Fig. 6(b).



(a) The data dependency graph of CNOT

(b) The data dependency graph C-Z

Fig. 6. The data dependency graph

4 Experiments and Evaluation

4.1 Implementation of Quantum Teleportation Algorithm

To demonstrate usage of the universal gates proposed in Sect. 3.3, let us consider the quantum circuit shown in Fig. 7 that is used in quantum teleportation. Quantum teleportation is a process by which we can transfer the state of a system and can create replica of a state to another system. Quantum teleportation is the transfer of an unknown quantum state from a sender to a receiver by means of a shared bipartite entangled state and appropriate classical communication [16]. A program is simulated with successful simulation which give successful transfer of random qubit to output and which governs perfect communication between sender and receiver. The problem is to transmit an arbitrary state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ of the top qubit to the bottom qubit.

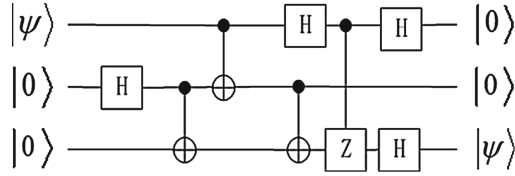


Fig. 7. Circuit implementing quantum teleportation

Input: $\{\alpha, 0, 0, 0, \beta, 0, 0, 0\}^T$ $(\alpha|0\rangle + \beta|1\rangle)|00\rangle = \alpha|000\rangle + \beta|100\rangle$

We can easily see that the final state obtained is exactly the state shown in the right-hand side of Fig. 8.

Output: $\{\alpha, \beta, 0, 0, 0, 0, 0, 0\}^T$ $\alpha|000\rangle + \beta|001\rangle = |00\rangle(\alpha|0\rangle + \beta|1\rangle)$

Base on the Sect. 3.3, we use the new universal quantum gates to construct the circuit of quantum teleportation as Fig. 8. Implementing different circuits in GPGPU simulation platform, we verified that the effect of the two circuit is the same, and we propose a new quantum teleportation circuit only need two types of gates can be achieved.

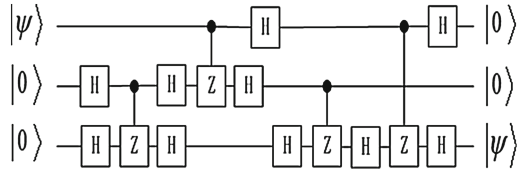


Fig. 8. New circuit implementing quantum teleportation

4.2 Implementation of Grover's Search Algorithm

Grover's search algorithm can achieve quadratic acceleration on search applications over unstructured data. There have been a wide range of generalization and applications of the algorithm, solving problems like pattern classifications and weight decision problem [21,22]. Let us simply remind the reader of the process of Grover's search algorithm. This algorithm employs pure states of n qubits which is initialized to the superposition of all computational basis state $|\psi\rangle = 1/\sqrt{2^n} \times \sum_{i=0}^{2^n-1} |i\rangle$. Then the Grover iteration can be divided into four stages which labeled as Oracle W1, R, W2, and the quantum circuit are illustrated in Fig.9(a). Finally the measurement of the external system is followed.

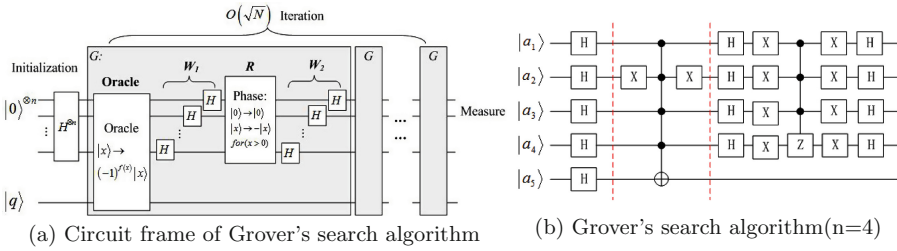


Fig. 9. Quantum circuit implementing Grover's search algorithm

Like Fig.9(b), we consider the case of 4-qubits circuit and let, for instance, $k=11$ be a hidden number, quantum memory register contain five qubits with $|a_5\rangle$ is ancillary qubit [23]. Taking into account the binary expansion (1011) of the number 11, we can check that the function $f(a)$ outputs 1 only if its input $|a\rangle_4$ is equal to the hidden integer $|a\rangle_4 = 1011 = |11\rangle_4$ and 0 otherwise.

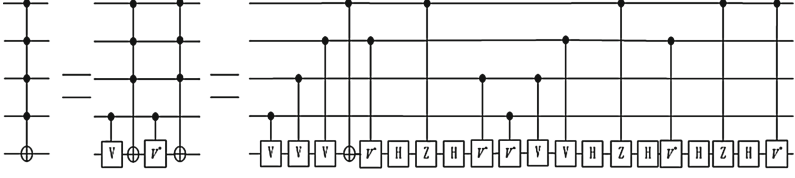
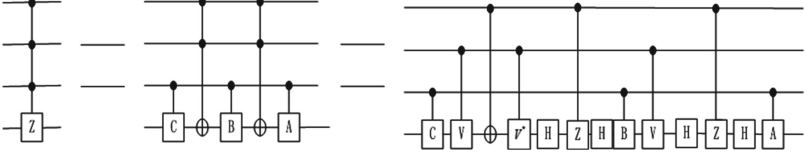
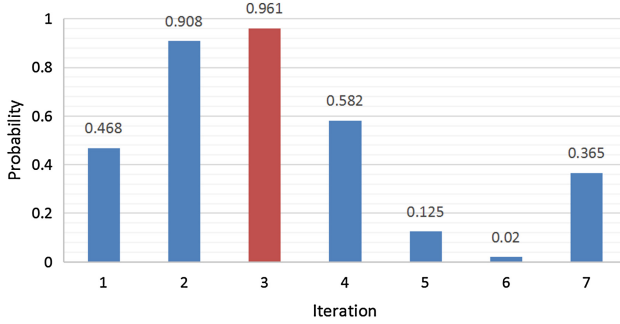
To implement Grover's algorithm, the multi-bit control gate and the multi-bit control phase shift gate in Fig.9(b) need to be decomposed into one-qubit and two-qubit quantum gates. We adopt a version of Feynman's notation to denote $\wedge_4(\sigma_x)$ gate.

Theorem: For a unitary 2×2 matrix W , $W = R_z(\alpha)R_y(\theta)R_z(\beta)$, there exist matrices A , B , and C such that $ABC=I$ and $A\sigma_x B\sigma_x C = W$ [8]. When $W = \sigma_x$, let $A = V$, $B = V^+$, $C=I$. Quantum circuit of $\wedge_4(\sigma_x)$ can be described as Fig.10, where V is shown in Eq. (6). The gates of V and V^+ can be constructed by T^2HT^2 .

$$V = \frac{1}{1+i} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \quad (6)$$

The construction of the 4-bit gate $\wedge_3(Z)$ as Fig.11, where $ABC=I$, and $A\sigma_x B\sigma_x C = Z$. A is shown in Eq. (7), $B = A^+$, $C=I$. The gates of A and B can be constructed by T^2HT^2Z .

$$A = \frac{1}{1+i} \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix} \quad (7)$$

**Fig. 10.** Quantum circuit $\Lambda_4(\sigma_x)$ **Fig. 11.** Quantum circuit $\Lambda_3(Z)$ **Fig. 12.** Probability distribution after Grover's iterations

Base on quantum circuits described in Figs.9(b), 10 and 11, we apply Grover's search algorithm using the new universal quantum gates on the proposed platform. Figure 12 shows that after an iterations a probability to get a correct number $k = 11$ is equal to 46.8%, while after the third Grover's iteration with probability 96.1%. However, at the six iteration, the probability decrease to 2%. The best iteration times is nearest integer to $\pi/(4 \arcsin(1/\sqrt{N}))$, where $N = 2^n$. For larger values of N this number is $O(\sqrt{N})$. Grover's algorithm provides a quadratic speed-up in solving the search problem in comparison with a classical computer which requires $O(N)$.

5 Conclusion and Future Work

In this work, we constructed an original basic quantum gate simulation platform, which can simulate any arbitrary quantum algorithm. Further, a new universal

quantum gates including C-Z, H, T is put forward. To our knowledge, the proposed universal quantum gates is the first idea that uses the concept of C-Z to construct universal quantum gates. Experimental results on quantum teleportation and Grover's search algorithm circuits illustrate that the proposed universal quantum gates more suitable for GPGPU. Moreover, as an example we detailed description the Grover's search algorithm and show that it gives a quadratic speed-up in solving the search problem. In the future work, this work can be used in the simulation of more quantum algorithms.

Acknowledgments. This work was supported by Funding of National Natural Science Foundation of China (Grant No. 61571226), Natural Science Foundation of Jiangsu Province, China (Grant No. BK20140823).

References

1. Feynman, R.P.: Simulating physics with computers. *Int. J. Theor. Phys.* **21**(6), 467–488 (1982)
2. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information: 10th anniversary edition. **21**(1), 1–59 (2010)
3. Tian, Q., Chen, S.: Cross-heterogeneous-database age estimation through correlation representation learning. *Neurocomputing* **238**, 286–295 (2017)
4. Ferrando-Soria, J., Pineda, E.M., Chiesa, A., Fernandez, A., et al.: A modular design of molecular qubits to implement universal quantum gate. *Nat. Commun.* **7** (2016)
5. Hu, Y., Zhao, Y.X., Xue, Z.-Y., Wang, Z.D.: Realizing universal quantum gates with topological bases in quantum-simulated superconducting chains. *NPJ Quantum Inf.* **3**, 1 (2017)
6. Raychev, N., Racheva, E.: Interactive environment for implementation and simulation of quantum algorithms. In: *Proceedings of the 16th International Conference on Computer Systems and Technologies*, pp. 54–60. ACM (2015)
7. Prokopenya, A.N.: Mathematica package “QuantumCircuit” for simulation of quantum computation. In: *International Mathematica Symposium* (2015)
8. Barenco, A., Bennett, C.H.: Elementary gates for quantum computation. *Phy. Rev. A* **52**(5), 3457 (1995)
9. Kitaev, A.Y.: Quantum computations: algorithms and error correction. *Russ. Math. Surv.* **52**(6), 53–112 (1997)
10. Boykin, P.O., Mor, T., Pulver, M., Roychowdhury, V., Vatan, F.: A new universal and fault-tolerant quantum basis. *Inf. Process Lett.* **75**(3), 101–107 (2000)
11. Raychev, N.: Universal quantum operators. *Int. J. Sci. Eng. Res. (IJSR)* **6**(6), 1369–1371 (2015)
12. Shi, Y.: Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Inf. Comput.* **3**(1), 84–92 (2002)
13. Kliuchnikov, V., Maslov, D., Mosca, M.: Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. *Comput. Sci.* **13**(7–8), 607–630 (2012)
14. Qu, Z., Keeney, J., Robitzsch, S., Zaman, F., Wang, X.: Multilevel pattern mining architecture for automatic network monitoring in heterogeneous wireless communication networks. *China Commun.* **13**(7), 108–116 (2016)

15. Fu, Z., Ren, K., Shu, J., Sun, X., Huang, F.: Enabling personalized search over encrypted outsourced data with efficiency improvement. *IEEE Trans. Neural Netw. Learn.* **27**(9), 2546–2559 (2016)
16. Sharma, M.S., De, A., Kulkarni, S.N., De, A.: Quantum teleportation circuit using Matlab and Mathematica. *Int. J. Comput. Sci. Eng. (IJCSET)* **2**(5), 1597–1600 (2010)
17. Xue, Y., Jiang, J., Zhao, B., Ma, T.: A self-adaptive artificial bee colony algorithm based on global best for global optimization. *Soft Comput.* 1–18 (2017)
18. Welch, J., Greenbaum, D., Mostame, S., Aspurguzik, A.: Efficient quantum circuits for diagonal unitaries without ancillas. *New J. Phys.* **16**(3) (2013)
19. De Vos, A., De Baerdemacker, S.: The block-ZXZ synthesis of an arbitrary quantum circuit. *Physics* **94**(5) (2016)
20. Zhang, P., Yuan, J., Lu, X.: Quantum computer simulation on multi-GPU incorporating data locality. In: Wang, G., Zomaya, A., Perez, G.M., Li, K. (eds.) *ICA3PP 2015*. LNCS, vol. 9528, pp. 241–256. Springer, Cham (2015). doi:[10.1007/978-3-319-27119-4_17](https://doi.org/10.1007/978-3-319-27119-4_17)
21. Gu, B., Sheng, V.S.: A robust regularization path algorithm for ν -support vector classification. *IEEE Trans. Neural. Netw. Learn.* **PP**(99), 1–8 (2016)
22. Gu, B., Sun, X., Sheng, V.S.: Structural minimax probability machine. *IEEE Trans. Neural Netw. Learn.* **PP**(99), 1–11 (2016)
23. Gerdts, V.P., Kragler, R., Prokopenya, A.N.: A mathematica package for simulation of quantum computation. In: Gerdts, V.P., Mayr, E.W., Vorozhtsov, E.V. (eds.) *CASC 2009*. LNCS, vol. 5743, pp. 106–117. Springer, Heidelberg (2009). doi:[10.1007/978-3-642-04103-7_11](https://doi.org/10.1007/978-3-642-04103-7_11)

Cloud Computing and Security

Third International Conference, ICCCS 2017, Nanjing,
China, June 16-18, 2017, Revised Selected Papers, Part

I

Sun, X.; Chao, H.-C.; You, X.; Bertino, E. (Eds.)

2017, XXI, 565 p. 236 illus., Softcover

ISBN: 978-3-319-68504-5