Baltic J. Modern Computing, Vol. 7 (2019), No. 1, pp. 99–111 https://doi.org/10.22364/bjmc.2019.7.1.08

A Faster Half Subtractor Circuit Using Reversible Quantum Gates

Francisco ORTS¹, Gloria ORTEGA², Ester Martín GARZÓN¹

¹ Dpt. of Informatics, Univ. of Almería, ceiA3, Almería, Spain
² Computer Architecture Department, Campus Teatinos, Univ. of Málaga, Spain

francisco.ortsQual.es, gloriaortegaQuma.es, gmartinQual.es

Abstract. Quantum computers base their operations on optimized circuit designs. These quantum circuits, unlike classic circuits, follow the set of rules determined by quantum mechanics. Currently, one of the main problems to solve in Quantum Computation is Shor's algorithm, which consists in factoring large numbers. It is based on arithmetic operations, therefore to optimize such operations is hence relevant. In this work, a novel half subtractor circuit is presented; it is referred to as FGE^* and it has demonstrated to be a 25% faster than the state-of-the-arts reversible circuits. It is based on reversible quantum gates and it does not have any garbage output. Moreover, a robust metric is considered for comparing, in terms of resources and speed, the proposed circuit with other circuits in the literature.

Keywords: Quantum subtractor circuit, Quantum half subtractor circuit, Reversible half subtractor, Reversible circuits

1 Introduction

Quantum Computation and quantum information are the study of the information processing tasks that can be accomplished using quantum mechanical systems. One of the goals of them is to develop tools which improve our intuition about quantum mechanics, and make its prediction more transparent to our minds. It is well-known that quantum mechanics, which is a mechanical framework for the construction of physical theories, is counterintuitive in spite of the fact that its rules are simple (Nielsen et al., 2017). Nevertheless, it gives some improvements that classical computation cannot offer (Heilmann et al., 2015).

The Church-Turing thesis says that any algorithmic process can be simulated efficiently using a Turing machine (Goldin et al., 2005). However, randomized algorithms and other problems cannot be efficiently solved on a deterministic Turing machine (Papadimitriou et al., 2003). Inspired by this idea, David Deutch was able to define a class

Orts et al.

of computing machines that was capable of efficiently simulating an arbitrary physical system. These machines are the quantum generalization of the Turing machines (Deutsch, 1985). So, the idea is that there are several problems which can be efficiently solved on these quantum computers, but not in classical computers. Quantum Computation is used in a wide variety of situations such as optical computation (Nielsen et al., 2004), coloring images using encryption/ decryption methods (Yang et al., 2014) and machine learning (Lloyd et al., 2017). Currently, the best examples on which Quantum Computation supplies a more powerful model for computation than classical computers are Shor's algorithm for integer factorization (Shor et al., 1999) and Grover's algorithms for searching an unsorted database with N entries (Grover, 1996).

Following the idea that quantum computers are more efficient than classical ones solving several problems, their applicability in supercomputing is of great interest. Quantum computers take advantage of the quantum mechanics in order to get features like parallel superposition, which gives the possibility of efficiently computing parallel and distributed programs (Back et al., 1992). With the superposition of n qubits, the quantum version of a bit, 2^n possibilities can be represented and computed at the same time, making possible new ways for solving problems. Nowadays, it is not clear what classes of problems can be efficiently solved using quantum computers. Nevertheless, the problems studied in (Shor et al., 1999, Grover, 1996) have shown to obtain better performance -in terms of runtime- on them (Nielsen et al., 2017).

Quantum computers work with a special kind of circuits: quantum circuits. Quantum circuits are based on basic operations with quantum gates, and they are in consonance with the quantum features like the superposition. Even complex operations are based on a set of basic operations (Möttönen et al., 2004), such as additions and subtractions. Therefore, the use of optimized basic operations is important to design circuits which have a suitable exploitation of the available resources (Orts et al., 2018). In the literature, there are several papers about quantum addition and quantum subtraction of two positive integers (Gidney, 2018, Murali et al., 2002, Takahashi et al., 2008, Takahashi et al., 2017, Thapliyal, 2016, Thapliyal et al., 2009), which are the most important basic operations. All these works are focused on getting faster circuits to be used as part of greater circuits, such as a module in Shor's algorithm. Since Shor's discovery, lots of works have investigated ways of building quantum circuits for this algorithm (Beauregard, 2002, Fowler et al., 2004, Proos et al., 2003, Takahashi et al., 2006, Vedral et al., 1996, Zalka et al., 1998). It is noteworthy that these basic operations are optimized to implement efficient algorithms. For instance, the subtraction is a basic operation for constructing quantum circuits for Shor's algorithm. Thus, to develop an efficient subtraction circuit will also benefit a high-performance Shor's algorithm. A half subtractor circuit computes the subtraction of two digits, and there are several works which address it in terms of Quantum Computation (Murali et al., 2002, Thapliyal et al., 2009, Montaser et al., 2017, Theresal et al., 2015, Das et al., 2017, Sarma et al., 2018, Thapliyal, 2016).

The main contribution of this work is the description of a novel and optimized quantum half subtractor circuit of integers, which improves the delay of the other state-ofthe-arts half subtractor circuits, being faster than them. The half subtractor circuit is based on reversible gates, and it does not have any garbage output. Moreover, it has been analyzed and compared with other state-of-the-art approaches using a fair metric.

The rest of this work is presented as follows: Section 2 contains a description of quantum circuits and the quantum gates involved in the half subtractor circuits. Section 3 speaks about the state-of-the-art reversible half subtractor circuits. Section 4 presents the proposed circuit. Finally, Section 5 summarizes the main conclusions.

2 Concepts of quantum circuits

A quantum circuit works similarly to a classical one. However, it uses its own gates which have to follow several quantum rules. One of them is that all gates must be reversible. That means that knowing the output of a gate (which is a quantum state), must be possible to obtain the previous quantum state. Such a situation is different in classical computers, which have irreversible behavior like the XOR gate. Irreversibility is not possible on quantum computers as the superposition needs to be maintained among the circuit. Quantum circuits could have extra costs in several classical operations if they had to transform non-reversible procedures into reversible ones (Shor, 1999).

Another important issue is the fact that quantum circuits do not allow loops. Feedback from one part of the quantum circuit to another is not possible, so new ways of working should be found in order to solve some classical problems. By the other hand, classical circuits allow joining wires, resulting in a single wire which has the bitwise of the inputs wires. However, this operation is not reversible so it cannot be done on quantum circuits. Moreover, a qubit cannot be duplicated, so copies of a quantum state are not allowed (Nielsen et al., 2017). The value can be copied in several cases. For instance, if a qubit is set to 1, another can be set to 1, but this concept is different from to copy a quantum state.

2.1 Quantum gates

Quantum gates are specifically designed to be used in quantum computers. There are quantum gates which perform the same operations than any classical gates, but there are also quantum gates which do not have an equivalent gate in classical circuits. These gates can be seen as reversible matrices, which operate on a qubit or a set of qubits, transforming their initial states into others. This section briefly describes the gates used in this work.

2.1.1 The Pauli-X gate For single qubits, there are three gates, called Pauli gates, which are especially useful and widely used (Williams, 2010). In this work, one of them is used, the Pauli-X gate (shown in Fig. 1). Such gate consists of a 2×2 (2 inputs and 2 outputs) matrix which permutes the computational basis states of a qubit. The Pauli-X gate is the equivalent in quantum terms of the classical NOT gate. Negating a qubit state is more complicated than to negate a bit. However, in this work only the standard bases are used, so it can be seen in a similar way than a classical negation.

 $A \xrightarrow{\qquad } \bar{A} \xrightarrow{\qquad } \bar{A} \xrightarrow{\qquad } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Orts et al.

Fig. 1: Symbol used to denote the Pauli-X gate and its matrix form.

2.1.2 The controlled-NOT gate The controlled-NOT (CNOT) gate performs an operation with two qubits, a control qubit and a target qubit. Its effect is similar to the Pauli-X on the target qubit, with the difference that if the control qubit takes the value 0 then the target qubit is unaltered (Deutsch et al., 2000). That is, the operation is only performed if the control qubit is set to 1. Controlled gates in quantum circuits are built attaching an identity matrix to the top-left corner of the matrix of the original gate. The gate representation and its matrix form are shown in Fig. 2. The CNOT gate is similar to a generalization of the XOR classical gate (Nielsen et al., 2017).



Fig. 2: Symbol used to denote the CNOT gate and its matrix form.

2.1.3 The *V* and *V*⁺ gates The *V* gates were developed in (Hung et al., 2006). The *V* gate is a 1×1 gate which applies the operation $V = \frac{1+i}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$ to the input value. On the other hand, the *V*⁺ gate (which is also a 1×1 gate) applies the operation $V^+ = \frac{1-i}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$. Representations and matrix forms are shown in Fig. 3.

A V V V(A)
$$V = \frac{1+i}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

A V V V V A) $V^+ = \frac{1-i}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$

Fig. 3: Symbol used to denote the V and V^+ gates and their matrix forms.

Only the standard bases 0 and 1 are used in this work, so there are four possibilities: $V(0), V(1), V^+(0)$ and $V^+(1)$. The results of each possibility are shown below:

$$V(0) = \frac{1+i}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1+i}{2} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$
(1)

A Faster Half Subtractor Circuit Using Reversible Quantum Gates

$$V(1) = \frac{1+i}{2} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1+i}{2} \begin{pmatrix} -i \\ 1 \end{pmatrix}$$
(2)

$$V^{+}(0) = \frac{1-i}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1-i}{2} \begin{pmatrix} 1 \\ i \end{pmatrix}$$
(3)

$$V^{+}(1) = \frac{1-i}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1-i}{2} \begin{pmatrix} i \\ 1 \end{pmatrix}$$
(4)

Taking into account such possibilities, there are three very important properties that can be derived from the V and V⁺ gates: (1) $V(A) \times V(A) = \overline{A}$; (2) $V^+(A) \times V^+(A) = \overline{A}$; and (3) $V(A) \times V^+(A) = V^+(A) \times V(A) = A$. These properties are widely used in several works in order to simplify and reduce quantum circuits (Thapliyal, 2016, Thapliyal et al., 2009, Maslov et al., 2003).

2.1.4 The Controlled-V and Controlled-V⁺ gates These gates are similar to the previous V and V⁺ gates, but adding a controller qubit as it has been explained in the *CNOT* gate (Hung et al., 2006). So, such gates are 2×2 gates. They maintain the properties of the V and V⁺ gates, but they can be activated or deactivated using the control qubit conveniently. Their symbol and matrix forms are shown in Fig. 4.



Fig. 4: Symbol used to denote the Controlled-V and Controlled- V^+ gates and their matrix forms.

2.1.5 The Toffoli gate The Toffoli gate (Toffoli, 1980) is similar to the CNOT gate. However, it has two control qubits. So, the gate only operates on the target qubit if the other 2 qubits are set to 1. If only the standard (orthonormal) basis $|0\rangle$ and $|1\rangle$ are considered, the Toffoli gate can be used to simulate the classical NAND gate (Fig. 6a) and also to do FANOUT (Fig. 6b) (Nielsen et al., 2017). Taking into account that this work is about integer subtraction, such consideration is always true. However, in any other situation on which $|\alpha\rangle = \beta |0\rangle + \gamma |1\rangle$ with $\beta \neq 0$ and $\gamma \neq 0$ that is not true due to negate a quantum state is not as simple as to negate a bit. The truth table for the standard basis of the Toffoli gate is shown in Table 1. Nowadays, the design presented in (Thapliyal, 2016) is the most optimized: it uses 2 Controlled-V gates, 1 Controlled-V⁺ gate and 2 CNOT gates. Its symbol and matrix form are shown in Fig. 5.

Orts et al.

Table 1: Truth table of the Toffoli gate. i_1/o_1 and i_2/o_2 are the control qubits, and i_3/o_3 is the target qubit.



Fig. 5: Symbol used to denote the Toffoli gate and its matrix form.

On the other hand, to build a Multiple-Controlled Toffoli (MCT) gate (that is, a Toffoli gate with more than 2 control qubits) is not trivial. In (Miller et al., 2011) a MCT gate was presented, which was smaller to others built in the past, and also had fewer ancilla qubits. In this work, such a gate is not used, so it is not necessary to explain in detail the MCT.

2.2 Measures in a quantum circuit

It is necessary to take into account several important factors to analyze a quantum circuit. One of them is the number of involved qubits. One of the most important issues



Fig. 6: (a) A NAND gate using a Toffoli gate. (b) FANOUT using a Toffoli gate.

quantum computers must face nowadays is the lack of resources. Qubits are scarce, so it is important to reduce the number of involved qubits. Firstly, the inputs of a problem and also the auxiliary qubits should be reduced to make possible to compute it in a current quantum computer/ simulator. Secondly, the circuit should not have any garbage outputs (that is, qubits which cannot be used at the end of the circuit as it is impossible to know their value), so it is necessary to reverse the outputs which are not useful. Unless these garbage outputs are reversibly removed (uncomputed), such outputs (qubits) cannot be used later, which would result in a waste of resources. If they are entangled with inputs of other circuits, they will produce uncertain results (Nielsen et al., 2017).

In terms of efficiency, the most important parameter is the delay (Thapliyal, 2016). Delay represents the speed of a circuit. Several metrics can be used. One of the most popular metrics is to consider any gate has a unit delay $(1\triangle)$ (Biswas et al., 2008). Following this metric, a Toffoli gate (which involves five 2×2 gates) has the same delay that a 1×1 Pauli-X gate. In (Mohammadi et al., 2009), a more realistic metric is proposed, where each gate is relatively weighed depending on the size. Such a metric considers the delay of all 1×1 and 2×2 gates to be $1\triangle$. Moreover, the delay of a $N\times N$ gate can be calculated as its depth when is designed using 1×1 and 2×2 gates. For example, the Toffoli gate has a delay of $5\triangle$ as it is conformed by 2 Controlled-V gates, 1 Controlled- V^+ gate and 2 CNOT gates, and none of them can be computed in parallel with another (Thapliyal, 2016). Furthermore, it defines the concept of Quantum Cost of a circuit as the number of gates with delay $1\triangle$ which it includes. The Quantum Cost of the Toffoli gate is also 5.

This work considers the metric presented in (Mohammadi et al., 2009).

3 A half subtractor as a quantum circuit

As it was aforementioned, a half subtractor is a circuit used to compute the subtraction of two digits. In the quantum case, it performs the subtraction of two digits A (the minuend) and B (the subtrahend) using qubits, which are set into the states $|0\rangle$ or $|1\rangle$, so their values can be considered as a normal bits. There are two outputs: the difference $D = A \oplus B$, and the borrow $B_{out} = \overline{AB}$. The truth table is shown in Table 2.

Table 2: Truth table of a half subtraction circuit. A is the minuend, B the subtrahend, D the difference and B_{out} the borrow.

Inputs	Outputs		
A B	$D B_{out}$		
0 0	0 0		
0 1	1 1		
1 0	1 0		
1 1	0 0		

Several previous works have approached the design of half subtractors in terms of quantum circuits. Their contributions were focused on reducing the required resources

Orts et al.

to construct a subtractor circuit and also decreasing the delay of the circuits. As it was mentioned in the previous section, qubits are limited and also the more depth of a circuit is, the more runtime to compute it. Moreover, quantum circuits must be reversible, which can imply that quantum circuits could have extra costs than classical ones to compute some kinds of problems. Due to this limitation, circuits must be optimized in order to avoid waste of resources and to reduce their computation time.

A design of a subtractor was introduced in (Murali et al., 2002). It has a Quantum Cost of 7 and a delay of $7\triangle$. It needs two input qubits and a auxiliary one, and it produces no garbage outputs. The design of the circuit consists of 2 CNOT gates and 1 Toffoli gate. The difference D is calculated using only one CNOT gate, and the remaining gates are used to compute the borrow.

Another reversible half subtractor was introduced in (Thapliyal et al., 2009), which improves the previous one. This circuit has a Quantum Cost of 6 and a delay of $6\triangle$. As the previous one, it uses three qubits as input (A, B and an auxiliary one), and there are not any garbage output. It implements the half subtractor by benefiting from the described principles of the V and V^+ gates.

A new reversible half adder/subtractor using R gate was presented in (Montaser et al., 2017). The authors affirm that the quantum cost of this circuit is 4 as they consider each gate as $1\triangle$. Due to the fact that it consists of 2 CNOT gates, 1 Pauli-X gate and 1 Toffoli gate, its quantum cost would be 8 (delay would be also $8\triangle$) following the metrics of (Mohammadi et al., 2009). Because this half subtractor can be also used as an adder, so this extra cost is justified. In (Theresal et al., 2015) another half adder/subtractor is presented, with a quantum cost of 7, delay of $7\triangle$ and 4 inputs. The extra inputs of (Montaser et al., 2017) and (Theresal et al., 2015) are used to switch between addition and subtraction. A similar proposal is presented in (Sarma et al., 2018) with a quantum cost of 5, delay of $5\triangle$ and 3 inputs.

In (Thapliyal, 2016) was presented the fastest half subtractor currently available. It has a delay of $4\triangle$. Moreover, it reduces the quantum cost to 4, maintaining 3 inputs qubits and no garbage outputs. It is an optimized version of the circuit of (Thapliyal et al., 2009), using the design of a new gate called TR as a reversible half subtractor. Such gate is shown in Fig. 7. After (Thapliyal, 2016), (Das et al., 2017) proposed a reversible half-subtractor using a DG gate (Dehgan et al., 2014) and a Pauli-X gate, as it is shown in Fig. 12 of (Das et al., 2017). DG gate has a quantum cost of 5 and a delay of $4\triangle$. Adding the Pauli-X gate, the half-subtractor has a quantum cost of 6 and a delay of $5\triangle$.



Fig. 7: Quantum implementation of TR gate based on the reversible half subtractor presented in (Thapliyal, 2016).

4 Proposed half subtractor

The TR gate presented in (Thapliyal, 2016) is able to compute the half subtraction with a delay of $4\triangle$. This delay cannot be improved as the operations contained in the gate cannot be computed in parallel. Taking into account that the $A \oplus B$ operation and the first Controlled-V gate cannot be computed in parallel since there are two read operations over the same qubit (simultaneous read operations are not allowed by the rules of quantum mechanics), in this work we have designed a new gate to sort the operations of TR gate, postponing the $A \oplus B$ operation. This will be extremely useful to reduce the delay. This new gate is called FGE, and it is shown in Fig. 8.



Fig. 8: Quantum implementation of a reversible half subtractor based on a FGE gate. FGE gate has a delay of $4\triangle$, the same delay of the TR gate presented in (Thapliyal et al., 2009).

FGE gate has similar Quantum Cost and delay to TR gate. However, it allows to improve the delay if a new auxiliary qubit Q is added. Steps 2 and 3 of the Fig. 8 cannot be computed in parallel for the same reason as it was mentioned in the previous paragraph. Nevertheless, if the value of A is moved into the new auxiliary qubit Q in the first step, the $A \oplus B$ operation can be supplied by $Q \oplus B$, which can be computed in parallel with the Controlled- V^+ of the step 2. Then, the obtained circuit, called FGE^* , has a delay of $3\triangle$. It is necessary to reverse Q avoiding a garbage output, but this can be done in the last step in parallel with the last Controlled-V gate. The circuit of FGE^* is shown in Fig. 9.



Fig. 9: Our proposal FGE^* , which is the optimization of FGE gate. It has a delay of $3\triangle$. It requires an auxiliary qubit to improve the delay in $1\triangle$.

Design proposed in	Delay	Quantum	Auxiliary	Garbage
		Cost	Inputs	Outputs
(Montaser et al., 2017)	8	8	1	0
(Theresal et al., 2015)	7	7	2	0
(Murali et al., 2002)	7	7	1	0
(Thapliyal et al., 2009)	6	6	1	0
(Das et al., 2017)	6	5	1	0
(Sarma et al., 2018)	5	5	1	0
(Thapliyal, 2016)	4	4	1	0
FGE	4	4	1	0
FGE^*	3	6	2	0

Table 3: A comparison of the different designs of half subtractor circuits in terms of delay, quantum cost, auxiliary inputs and garbage outputs.

4.1 Evaluation of half subtractor circuits

A full comparison between the studied half subtractors is shown in Table 3 in terms of delay, quantum cost, auxiliary inputs and garbage outputs. This table shows that the proposal presented in (Thapliyal, 2016) is the most competitive among the half subtractor circuits currently available. Focusing on (Thapliyal, 2016), our proposal has two disadvantages. Firstly, the number of gates. The proposed circuit needs two extra gates: one gate to copy the value of A to the new auxiliary qubit, and another to reverse such a qubit. On the other hand, it needs two auxiliary qubits, whereas the circuit of (Thapliyal, 2016) only needs one. However, our proposed circuit shows better results in terms of delay with respect to the other designs of the table.

	Improvement of FGE^* (in %)			
Design proposed in	Delay	Quantum	Auxiliary	Garbage
		Cost	Inputs	Outputs
(Montaser et al., 2017)	62	25	-50	0
(Theresal et al., 2015)	57	14	0	0
(Murali et al., 2002)	57	14	-50	0
(Thapliyal et al., 2009)	50	0	-50	0
(Das et al., 2017)	50	-14	-50	0
(Sarma et al., 2018)	38	-14	-50	0
(Thapliyal, 2016)	25	-33	-50	0

Table 4: Rate of improvement of FGE^* gate (in %) over the remaining designs, in terms of delay, quantum cost, auxiliary inputs and garbage outputs.

The percentage of improvement of FGE^* gate over the remaining designs in terms of delay, quantum cost, auxiliary inputs and garbage outputs is shown in Table 4. The table shows that FGE^* implies the use of more quantum gates than (Das et al., 2017, Sarma et al., 2018, Thapliyal, 2016). Moreover, FGE^* needs an extra input qubit with respect to (Montaser et al., 2017, Murali et al., 2002, Thapliyal et al., 2009, Das et al., 2017, Sarma et al., 2018, Thapliyal, 2016) to improve the delay. Also, in a similar way to the other approaches, the number of garbage outputs is 0. If we focus our attention in the delay column of Table 4, it can be observed that FGE^* overcomes even the fastest one (Thapliyal, 2016). This means that our proposal can be seen as the fastest half subtractor in the literature, and it is the best option when speed is the most important factor to be considered.

5 Conclusions

In this paper, a quantum half subtractor circuit has been presented, called FGE^* . It is a 25% faster than other state-of-the-arts half subtractor circuits. Its depth is only $3\triangle$, and it does not have any garbage output. The design of the circuit has been explained and studied in detail. Moreover, a robust metric to evaluate the proposed circuit in comparison to the currently available circuits to compute reversible half subtractors has been followed.

Acknowledgements

This work has been supported by the Spanish Science and Technology Commission (CICYT) under contract TIN2015-66680, Junta de Andalucía under contract P12-TIC-301 in part financed by the European Regional Development Fund (ERDF). G. Ortega is a fellow of the Spanish 'Juan de la Cierva Incorporación' program. The authors wish to thank N.C. Cruz for his valuable support.

References

- Back, R., Sere, K. (1992). Superposition refinement of parallel algorithms. In: Formal Description Techniques, IV, Elsevier, 475–493.
- Beauregard, S. (2002). Circuit for Shor's algorithm using 2N + 3 qubits. arXiv preprint quantph/0205095.
- Biswas, A. K., Hasan, M. M., Chowdhury, A. R., Babu, H. M. H. (2008). Efficient approaches for designing reversible binary coded decimal adders. Microelectronics journal, 39(12), 1693– 1703.
- Das, J. C., De, D. (2017). Reversible binary subtractor design using quantum dot-cellular automata. Frontiers of Information Technology & Electronic Engineering, 18(9), 1416–1429.
- Dehghan, B., Roozbeh, A., Zare, J. (2014). Design of low power comparator using *DG* gate. Circuits and Systems, 5(01), 7.
- Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. A, 400(1818), 97–117.

- Deutsch, D., Hayden, P. (2000). Information flow in entangled quantum systems. In: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, The Royal Society, (456), 1759–1774.
- Fowler, A. G., Devitt, S. J., Hollenberg, L. C. (2004). Implementation of Shor's algorithm on a linear nearest neighbour qubit array. arXiv preprint quant-ph/0402196.
- Gidney, C. (2018). Halving the cost of quantum addition. Quantum, (2), 74.
- Goldin, D., Wegner, P. (2005). The Church-Turing thesis: Breaking the myth. In: Conference on Computability in Europe, Springer, 152–168.
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, ACM, 212–219.
- Heilmann, R., Gräfe, M., Nolte, S., Szameit A. (2015). A novel integrated quantum circuit for high-order W-state generation and its highly precise characterization. Science bulletin, 60(1), 96–100.
- Hung, W. N., Song, X., Yang, G., Yang, J., Perkowski, M. (2006). Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reachability analysis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 25 (9), 1652–1663.
- Lloyd, S., Mohseni, M., Rebentrost, P. (2017). Quantum algorithms for supervised and unsupervised machine learning. arXiv preprint arXiv:1307.0411.
- Maslov, D., Dueck, G. W. (2003). Improved quantum cost for N-bit toffoli gates. Electronics Letters, 39(25), 1790–1791.
- Miller, D. M., Wille, R., Sasanian, Z. (2011). Elementary quantum gate realizations for multiplecontrol Toffoli gates. In: Multiple-Valued Logic (ISMVL), 2011 41st IEEE International Symposium on, IEEE, 288–293.
- Mohammadi, M., Eshghi, M. (2009). On figures of merit in reversible and quantum logic designs. Quantum Information Processing, 8(4), 297–318.
- Montaser, R., Younes, A., Abdel-Aty, M. (2017). New design of reversible full adder/subtractor using R gate. arXiv preprint arXiv:1708.00306.
- Möttönen, M., Vartiainen, J. J., Bergholm, V., Salomaa, M. M. (2004). Quantum circuits for general multiqubit gates. Physical Review Letters, 93(13), 130502.
- Murali, K., Sinha, N., Mahesh, T., Levitt, M. H., Ramanathan, K., Kumar, A. (2002). Quantuminformation processing by nuclear magnetic resonance: Experimental implementation of half-adder and subtractor operations using an oriented spin-7/2 system. Physical Review A, 66(2), 022313.
- Nielsen, M. A. (2004) Optical quantum computation using cluster states. Physical review letters, 93(4), 040503.
- Nielsen, M. A., Chuang, I. L. (2017). Quantum Computation and Quantum Information 10th edition. Cambridge University Press.
- Orts, F., Ortega, G., Garzón, E. (2018). A quantum circuit for solving divisions using Grover's search algorithm. In: Proc. 18th Int. Conf. Comput. Math. Method. Sci. Eng, 1–6.
- Papadimitriou, C. H. (2003). Computational complexity. John Wiley and Sons Ltd.
- Proos, J., Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv preprint quant-ph/0301141.
- Sarma, R., Jain, R. (2018). Quantum gate implementation of a novel reversible half adder and subtractor circuit. In: 2018 International Conference on Intelligent Circuits and Systems (ICICS), IEEE, 72–76.
- Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303–332.
- Takahashi, Y., Kunihiro, N. (2008). A fast quantum circuit for addition with few qubits. Quantum Information & Computation, 8(6), 636–649.

- Takahashi, Y., Kunihiro, N. (2006). A quantum circuit for Shor's factoring algorithm using 2N+2 qubits. Quantum Information & Computation, 6(2), 184–192.
- Takahashi, Y., Tani, S., Kunihiro, N. (2017). Quantum addition circuits and unbounded fan-out. arXiv preprint arXiv:0910.2530.
- Thapliyal, H. (2016). Mapping of subtractor and adder-subtractor circuits on reversible quantum gates. In: Transactions on Computational Science XXVII, Springer, 10–34.
- Thapliyal, H., Ranganathan, N. (2009). Design of efficient reversible binary subtractors based on a new reversible gate. In: Design of Efficient Reversible Binary Subtractors Based on a New Reversible Gate, IEEE, 1–6.
- Theresal, T., Sathish, K., Aswinkumar, R. (2015). A new design of optical reversible adder and subtractor using MZI. Published at International Journal of Scientific and Research Publications (IJSRP), 5(4).
- Toffoli, T. (1980). Reversible computing. In: International Colloquium on Automata, Languages, and Programming, Springer, 632–644.
- Vedral, V., Barenco, A., Ekert, A. (1996). Quantum networks for elementary arithmetic operations. Physical Review A, 54(1), 147.
- Williams C. P. (2010). Explorations in quantum computing. Springer Science & Business Media.
- Yang, Y. G., Jia, X., Sun, S. J., Pan, Q. X. (2014). Quantum cryptographic algorithm for color images using quantum fourier transform and double random-phase encoding. Information Sciences, 277, 445–457.
- Zalka, C. (1998). Fast versions of Shor's quantum factoring algorithm. arXiv preprint quantph/9806084.

Received January 24, 2019, revised March 4, 2019, accepted March 4, 2019