Dhaka Univ. J. Sci. 58(2): 319-324, 2010 (July)

Design of Shift Register Counters Using Quantum Principle

Nishatul Majid[1], Shuvabrata Saha[2] and S. K. Aditya[1]

[1]*Department of Applied Physics, Electronics & Communication Engineering, Dhaka University, Dhaka-1000, Bangladesh*

[2]*Department of Computer Science & Engineering, Bangladesh University of Engineering & Technology, Dhaka, Bangladesh*

Received on 19.02.2010. Accepted for Publication on 30.03.2010

Abstract

The goal of this paper is to propose a design for shift register counters using quantum principles for classical computations. In this context, two 3-Qubit Quantum gates are designed which are capable of performing directly as 3-bit left shift and right shift registers. Using those gates, quantum circuits for two reversible synchronous counters; a MOD-3 shift register counter (equivalent to Ring counter) and a MOD-6 shift register counter (equivalent to Twisted Ring/ Johnson Counter) , are presented. To increase the MOD number of the counters in this methodology is also proposed. Basically, this work is a theoretical effort to realize an important subsection of transforming the classical computers we have today using the reversible logic of Quantum Mechanics.

I. Introduction

A quantum computer is a device for computation that makes direct use of quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. The basic principle behind quantum computation is that quantum properties can be used to represent data and perform operations on these data. [1] Quantum computing combines quantum mechanics, information theory, and aspects of computer science [Nielsen, M. A. & Chuang, I. L. 2000]. The field is a relatively new one that promises secure data transfer, dramatic computing speed increases, and may take component miniaturization to its fundamental limit.

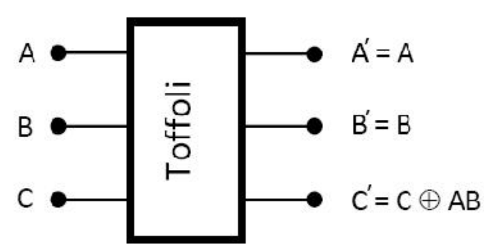
Although quantum computing is still in its infancy, experiments have been carried out in which quantum computational operations were executed on a very small number of Qubits. Both practical and theoretical research continues with interest, and many national government and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis. [2]

The work in this paper is entirely theoretical. The objective of this work is to propose a methodology to obtain shift-register counters (ring counter, twisted ring/ Johnson counter) under the domain of quantum physics. In this purpose, two 3-qubit quantum gates in 8 X 8 unitary matrix formats are introduced. In the following sections, these reversible gates are vividly illustrated, analyzed; and the block diagram of the shift register counters using these gates are presented.

II. Background of the Work

It is possible to simulate a classical logic circuit using a quantum circuit. It would be very surprising if this were not the case, as physicists believe that all aspects of the world around us, including classical logic circuits, can ultimately be explained using quantum mechanics. But, this can't be done directly as because unitary quantum logic gates are inherently reversible, whereas many classical logic gates such as the AND, OR, NAND, NOR gate are irreversible. Moreover there are some properties of a quantum gate which arise difficulties to implement classical operations; such as quantum gates do not support FAN-IN and FAN-OUT, and they are Acyclic. [3, 4, 5]

A very much popular gate especially in this context is **Toffoli** gate introduced by Tommaso Toffoli in 1981. This is a 3-qubit gate in quantum logic; the functional name of this gate is CCNOT (**C**ontrolled **C**ontrolled **NOT** operation) gate. The functional block diagram and matrix representation of this gate is shown in figure 1.



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Fig.1. Block diagram & 8 X 8 Matrix representation of Toffoli gate

Two of the most important features of this gate are, it can be used as a NAND gate and it can simulate fan-out operation shown in figure 2.

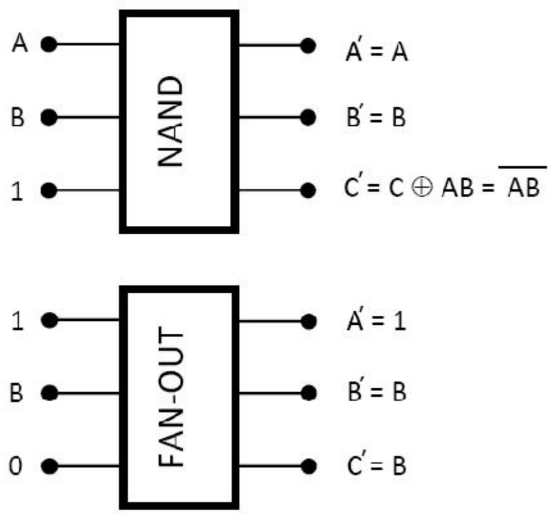


Fig.2. Toffoli gate to simulate (**a**) Classical NAND operation (**b**) FAN-OUT operation

As the NAND gate is a Universal gate in the context of classical computation, together with these two properties, any classical circuit can be simulated by an equivalent reversible circuit. Hence, Toffoli gate is the principle gateway and it ensures that quantum computers are capable of performing any computation which a classical (deterministic) computer may do. But, in most of the cases, the cost of preparing irreversible logic using reversible gate elements has to be paid in reduction of overall efficiency and increase in structural complexity.

Here, in this work, an efficient method of preparing one of the most significant elements in digital circuitry; i.e. the Counter is proposed using reversible quantum logics. Ring counter and Johnson counter are most basic type counters prepared using a number of Flip-flops which are arranged in a way to work as a shift register which is shown in figure 3.

In digital logic and computing, a counter is a device which stores (and sometimes displays) the number of times a particular event or process has occurred, often in relationship to a clock signal. A shift register counter is a type of counter composed of a circular shift register. The output of the last shift register is fed to the input of the first register. There are two types of it.

1. A Straight Ring Counter or Overbeck counter connects the output of the last shift register to the first shift register input and circulates a single '1' (or '0') bit around the ring.

2. A Twisted Ring Counter or Johnson counter connects the complement of the output of the last shift register to its input and circulates a stream of '1's followed by '0's around the ring. [6, 7]

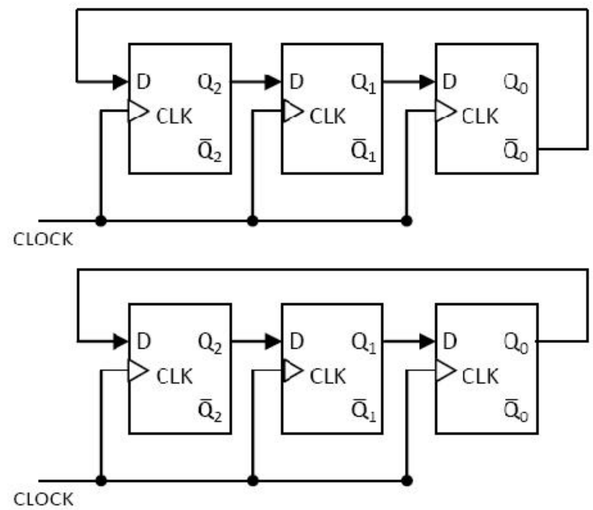


Fig. 3. Classical Shift Register Counters with Flip-flops (a) mod-6 Johnson Counter (b) mod-3 Ring Counter

In this paper, a direct 3-qubit quantum gate is proposed which exhibits the property exactly as a 3-stage shift register (i.e. 3 D-Flip-flops connected in series under a single clock). Afterwards, the design for the counters are shown using that/ those gates in the same way it is done in classical computers. As it has already mentioned that, Quantum gates does not support FAN-OUT or FAN-IN properties, a CNOT gate is used to make a copy of the Qubits in sharp state and the quantum property of entanglement is used for feedback purpose. Ultimately, design block of a MOD-3 ring counter and MOD-6 Johnson counter is presented and to increase the counting sequence, a brief projection of a similar 4-qubit quantum gate for 4-stage shift register is illustrated.

III. Proposed Gates

Unitary Matrix for the Gates

According to the theory of quantum gates, any arbitrary n-bit quantum gate can be represented by a 2^n X 2^n Unitary matrix and the vice versa. In order to represent the 3-stage left and right shift register, two 3-qubit quantum gates are proposed in this format. [3] These gates will shortly called by LSR (Left Shift Register) and RSR (Right Shift Register) in the following sections. The Unitary matrices for these gates are shown in the followings.

$$LSR = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$RSR = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Behavior Analysis of the Gates

The behavior of these gates for input Qubits in sharp states (which is therefore equivalent to bits corresponding to classical computation) can be shown with the following truth table.

Classical Equivalent Truth table for LSR and RSR gate

Input Qubits			LSR Output Qubits			RSR Output Qubits		
A	**B**	**C**	**A′**	**B′**	**C′**	**A′**	**B′**	**C′**
0	0	0	0	0	0	0	0	0
0	0	1	0	1	0	1	0	0
0	1	0	1	0	0	0	0	1
0	1	1	1	1	0	1	0	1
1	0	0	0	0	1	0	1	0
1	0	1	0	1	1	1	1	0
1	1	0	1	0	1	0	1	1
1	1	1	1	1	1	1	1	1

That is, the truth table drawn above is exactly the same as they are for the classical left and right shift registers. Hence, the functional block representation for these gates would be as shown in figure 4.

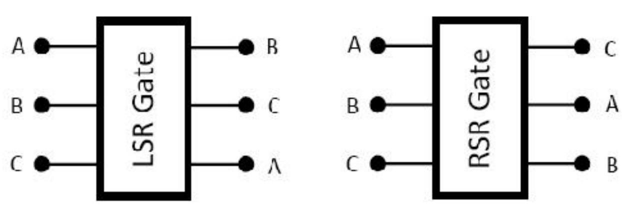


Fig.4. Block representation of LSR and RSR Gate

Now, to analyze the behavior of these gates for an arbitrary quantum state, let's assume |φ⟩ represents an arbitrary 3-qubit input stage as follows

$|\varphi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$

Where, $(\alpha_{KKK})^2$ is the probability of |φ⟩ being in the stage |KKK⟩

So that, $(\alpha_{000})^2 + (\alpha_{001})^2 + (\alpha_{010})^2 + (\alpha_{011})^2 + (\alpha_{100})^2 + (\alpha_{101})^2 + (\alpha_{110})^2 + (\alpha_{111})^2 = 1$

Generally, during operations, the input/ output states are usually represented in KET notation (1 column vector notation) like

$$|\varphi\rangle = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 \end{bmatrix}^T ;$$

where, the subscript 0-7 denotes simply the decimal values of the binary states 000-111.

Now, if |φ'⟩ be the output, then the operations of the LSR and RSR gates can be showed by the following matrix operations.

$$|\phi'\rangle_{LSR} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_4 \\ \alpha_1 \\ \alpha_5 \\ \alpha_2 \\ \alpha_6 \\ \alpha_3 \\ \alpha_7 \end{bmatrix}$$

$$|\phi'\rangle_{RSR} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_2 \\ \alpha_4 \\ \alpha_6 \\ \alpha_1 \\ \alpha_3 \\ \alpha_5 \\ \alpha_7 \end{bmatrix}$$

Correlation between the Gates

The correlation between these gates; which is almost deducible from the functions of these gates; is these are conjugate transpose (also called Hermitian adjoint) of one another. That is,

$$[LSR]^{\dagger} - [RSR] \quad \text{and} \quad [RSR]^{\dagger} - [LSR]$$

That is, these are not two different gates in the sense of physical implementation; rather they are a single gate with reverse direction of action.

Higher Order Similar Gates

In this same methodology it is possible to construct higher order gates. As for example, a 4 - Qubit quantum gate working as a left shift register is shown in the unitary matrix format below.

$$
\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}
$$

And similarly, the right shift operation can be achieved with the quantum gate which can be expressed with,

$$[RSR_4] = [LSR_4]^{\dagger}$$

IV. Building block of the Shift Register Counters

MOD-3 Ring Counter

The architecture for this counter includes a 3-qubit shift register, CNOT gates and Entanglement based Feedback circuitry. The block diagram if this is illustrated in figure 5.

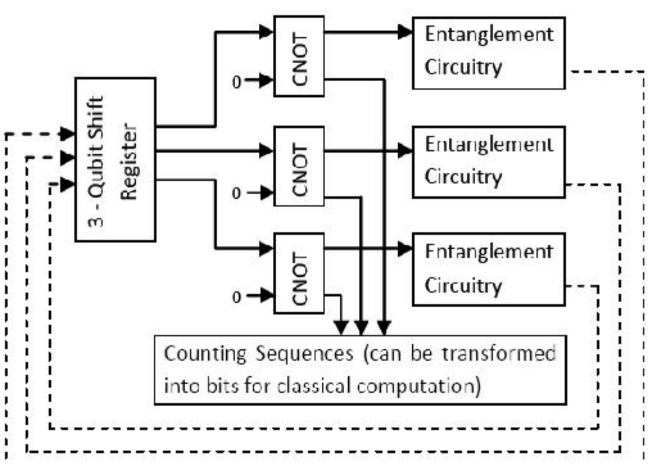


Fig.5. Block Diagram of MOD – 3 Ring Counter (here dotted line indicates Quantum Teleport)

Here, the shift register is the quantum gate which has already proposed; i.e. it can either be LSR or RSR. The variation will only be in the rotation of the state diagram demonstrated in figure 6.

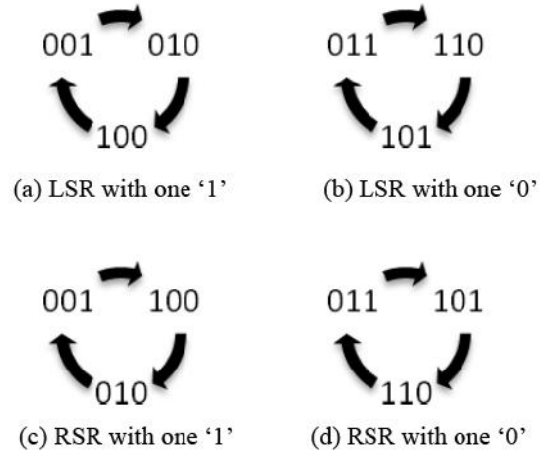


Fig.6. State Diagrams for different situations.

The CNOT gates are used in this circuit as Qubit copying circuits, shown in figure 7. According to the quantum no-cloning theorem, a Qubit can never be copied unless it is in a sharp state (that is either 1 or 0). [3] Here all of the operations are entirely based on the sharp states and these CNOT gates have to be used because quantum gates do not support FAN-OUT.

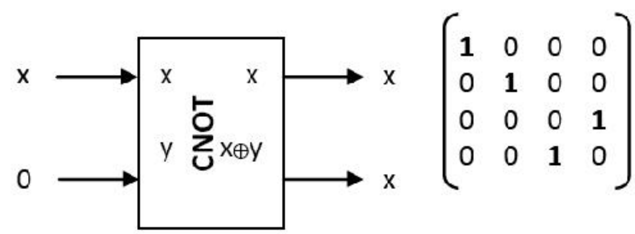


Fig.7. (**a**) CNOT gate as a Qubit copying circuit & (**b**) Its Unitary Matrix

In classical computers, shift register counters are constructed using feedbacks. As this concept of feedback is not allowed in Quantum Circuit, a special phenomenon called 'Quantum teleportation' is used to teleport Qubits to serve the purpose of feedback. The basic circuit for quantum teleportation is illustrated in figure 8.

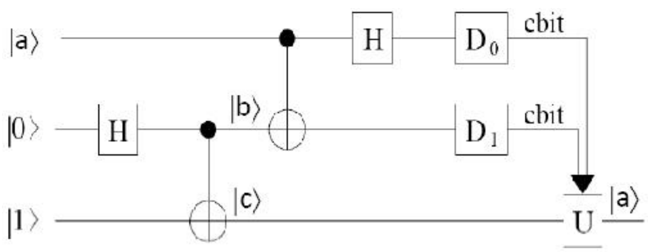


Fig.8. Quantum circuit for teleportation. The first line represents the Qubit to be teleported, the second line a Qubit possessed by the transmitter, and the third a Qubit possessed by the Receiver. Here the 'H' represents Hadamard gate, D_0 and D_1 are detectors. [5]

Quantum entanglement-assisted teleportation is a technique used to transfer quantum information from one quantum system to another. The prerequisites are a conventional communication channel capable of transmitting two classical bits (i.e. one of four states), and an entangled pair (**b, c**) of qubits, with b at the origin and c at the destination. A Hadamard gate followed by a CNOT gate is used here to generate the entangled pair. In simple language, the protocol has three steps: measure **a** (the Qubit to be teleported) and **b** jointly to yield two classical bits; transmit the two bits to the other end of the channel; and use the two bits to select one of four ways of recovering **c**.[8, 5]

MOD-6 Johnson or Twisted Ring Counter

The proposed architecture for this counter is almost same as the one for the Ring counter except that here the last CNOT gate does not operate as a copying circuit; rather it inverts the state of the Qubit from the Shift Register gate towards the entanglement circuitry. The functional block diagram for Johnson counter is as shown in figure 9.

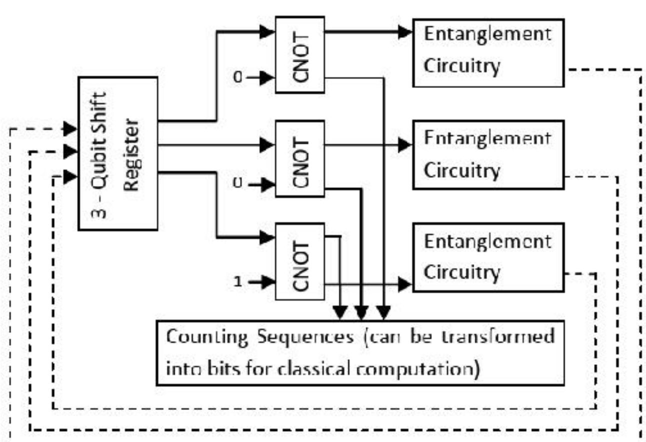


Fig.9. Block Diagram of MOD – 6 Twisted Ring or Johnson Counter

The MOD number of a Johnson counter will always be equal to twice the number of stages in shift register; i.e. the double of the MOD number of a Ring counter with a similar arrangement. The state diagrams of this counter are shown in figure 10.

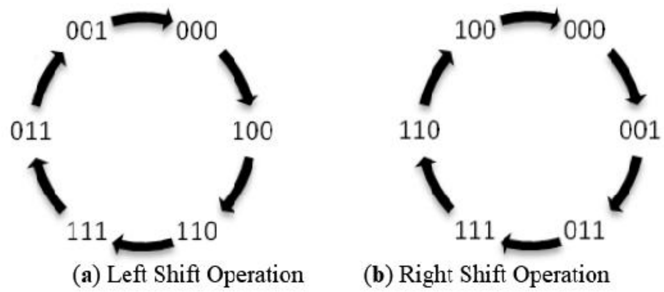


Fig.10. State Diagrams for Johnson Counter

Finally, the MOD number of these counters can be increased simply using higher order Qubit gates in the proposed methodology. While binary logic is the most usual basis for quantum computation, multi-valued logic offers a route to scale up quantum computers by logarithmic reduction in the number of separate quantum systems needed to span the quantum memory. Therefore, day by day ternary and quaternary logic systems are positioning to be interesting alternatives to traditional binary logic base of quantum computation and hence there is a scope for upgrading the proposed systems from binary quantum base to Qutrit and/or Qudit systems.

V. Conclusion

In this paper, it is tried to present the methodology of obtaining a type of classical counters with quantum physics by introducing shift register quantum gates. The gates proposed here do not have any ancillary or garbage outputs and therefore it assures an efficient construction. Therefore, these gates can also be used in the construction of other logical components in a CPU. As already said, similar concept can be transformed for Qutrit/ Qudit based systems. Again, as 'feedback' is not allowed in quantum circuits, a remarkable quantum phenomenon known as 'Quantum entanglement' was used to teleport the Qubits to the shift register inputs. This phenomenon is supported by most of the quantum computer approaches till now except a few; and unfortunately this includes the most advanced one, MRI based quantum computation.

The technology of quantum computer is still in an immature stage and not developed close enough to its full potential. But, hopefully, the days are not very far when Quantum mechanics would merge with classical computation to create quantum computers. When the physical implementation of quantum computer will be in our reach, circuits like shift register and shift register counter would be very handy to reduce the circuit complexities.

1. "*Quantum Computing with Molecules*" article in Scientific American by Gershenfeld, Neil.

2. Wikipedia, the Free Encyclopedia. "*Quantum computer*". Jan 10, 2010. Jan 23, 2010. <http://en.wikipedia.org/wiki/Quantum_computer>

3. Nielsen, Michael A. and Chaung, Isaac L. "*Quantum Computation and Quantum Information*", United Kingdom: Cambridge University Press, 2000.

4. Perry, Riley T. "*The Temple of Quantum Computing*", Version 1.1 – April 29, 2006. <http://www.toqc.com/>

5. Benenti, Giuliano; Casati, Giulio and Strin, Gluliano. "*Principles of Quantum Computation: Basic Concepts - vol.1*", World Scientific.

6. Tocci, Ronald J. and Widmer, Neal S. "*Digital Systems: Principles and Applications*", Prentice Hall, 2002.

7. Wikipedia, the Free Encyclopedia. "*Counter*". December 16, 2009. January 23, 2010. <http://en.wikipedia.org/wiki/Counter>

8. Wikipedia, the Free Encyclopedia. "*Quantum Teleportation*". January 20, 2010. Jan 23, 2010. <http://en.wikipedia.org/wiki/Quantum_teleportation>