A NOVEL DESIGN OF SYNDROME CALCULATOR FOR CYCLIC CODE USING REVERSIBLE LOGIC GATES

[1]Shashank Kumar Singh, [2]Supravat Mondal, [3]Bijoy Kumar Mandal
[1,2,3]Assistant Professor
[1]ECE Department, [2,3] CSE Department
[1]University College of Engineering and Technology (UCET), V.B.U., Hazaribag, India.
[2,3] NSHM Knowledge Campus, Durgapur, India.

Abstract- In present scenario, the reversible logic synthesis technique is most important part of the long-term future of computing due to its low power dissipating characteristic. In recent years, reversible logic circuits have attracted considerable attention in improving some fields like nanotechnology, quantum computing, cryptography, optical computing and low power design of circuits due to its low power dissipating characteristic. In this paper we proposed the design of Syndrome Calculator for cyclic code which uses reversible gates and derived quantum cost, constant inputs, garbage output and number of gates to implement it.

Key words: Reversible logic gate, Syndrome Calculator, Constant input, Garbage output, Delay.

I. INTRODUCTION

According to Landauer's research, the loss of one bit of information dissipates KTln2 joules of energy, where (joule/kelvin) is the Boltzmann constant and T is the absolute temperature at which the operation is to be performed [1]. At room temperature the heat dissipation due to loss of one bit of information is very small but it is not negligible. This computation procedure is irreversible. Further Bennett, showed that one can avoid this KTln2 joule of energy dissipation from the circuit if input can be extracted from output and it would be possible if and only if reversible gates are used [2]. Reversible logic supports the process of running the system both forward and backward. This means that reversible computations can generate inputs from outputs and can stop and go back to any point in the computation history. Research is going on in the field of reversible logic and a good amount of research work has been carried out in the area of reversible combinational logic. However, there is not much work in the area of cyclic code encoder, syndrome calculator and decoder. A syndrome calculator is very similar to the encoder for (n,k) [10]. When a code word X is transmitted over a noisy channel, errors are likely to get introduced into it. Thus the received code word Y is different from X. For a linear block code, the first step in decoding is to calculate the syndrome for the received code word. This paper proposes a novel design of 3-bit Gray Code counter using reversible logic gates.

II. BASIC CONCEPTS

This section explains some basic concepts of reversible gates and quantum circuits which are as follows:

A. Reversible logic Function

It is an n-input n-output logic function in which there is a one-to-one correspondence between the inputs and the outputs, i.e. not only the outputs can be uniquely determined from the inputs, but also the inputs can be recovered from the outputs.[6] This prevents the loss of information which is the root cause of power dissipation in irreversible logic circuits. Energy dissipation can be reduced or even eliminated if computation becomes Information-lossless. The reversible logic circuits must be constructed under two main constraints. They are:

- Fan-out is not permitted.
- Loops or feedbacks are not permitted

Quantum logic gates have some properties as shown in "(1.1)."

$$\left.\begin{array}{l} V \times V = NOT \\ V \times V^{+} = V^{+} \times V = I \\ V^{+} \times V^{+} = NOT \end{array}\right\} \quad (1.1)$$

Any reversible logic gate (circuit) is realized by using mentioned gates above, NOT and FG gates. The properties above show that when two V gates are in series they will behave as a NOT gate. Similarly, two V^{+} gates in series also function as a NOT gate. A V gate in series with V^{+} gate, and vice versa, is an identity.

B. Garbage output

This refers to the number of unused outputs present in a reversible logic. A garbage output is an output that is needed to change an irreversible gate to a reversible one and are not used to the input to the other gates

C. Quantum gate

Quantum gates are reversible and based on quantum computing. For realizing 1×1 and 2×2 quantum gates we can use quantum technique. Since bigger quantum gates like 3×3, 4x4 etc. cannot be realized by quantum technique directly, 1×1 and 2×2 quantum gates are used for realizing this bigger quantum gates.

D. Quantum Cost

This refers to the cost of the circuit in terms of the cost of a primitive gate. The quantum cost of a reversible gate is the number of 1x1 and 2x2 reversible gates or quantum gates required in its design. The quantum costs of all reversible 1x1 and 2x2 gates are taken as unity. Since every reversible gate is a combination of 1 x 1 or 2 x 2 quantum gate, so the quantum cost of a reversible gate can be calculated by counting the numbers of NOT, Controlled-V, Controlled-V^{+} and CNOT gates used.[3],[14]

E. Reversible gate

A gate with equal number of input and output in which input and output have one –to-one mapping. This helps to determine the outputs from the inputs and also the inputs can be uniquely recovered from the outputs. If the input vector of a reversible gate is denoted by I_V= (I_1,I_2,I_3,…,I_K), the output vector can be represented as O_V= (O_1,O_2,O_3,…,O_K). A reversible gate can be represented as K×K in which the number of input and output is K.

F. Feynman gate (cnot gate)

The Feynman gate (FG) or the Controlled-NOT gate (CNOT) is a 2-input 2- output reversible gate having the mapping (A, B) to (P = A, Q = A⊕B) where A, B are the inputs and P, Q are the outputs, respectively.[5]. Since it is a 2×2 gate, it has a quantum cost of 1. "Fig. 1" and "Fig. 2" shows the block diagram and quantum representation of the Feynman gate. "Fig. 3" and "Fig. 4" shows the block diagram and quantum representation of Double Feynman Gate respectively. Quantum cost of DFG is 2 as it needs two CNOT gate to implement it.

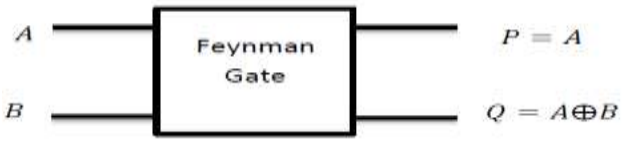


Fig. 1. 2X2 Feynman

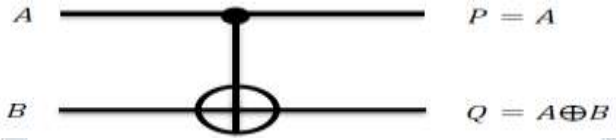


Fig. 2. Quantum representation of Feynman

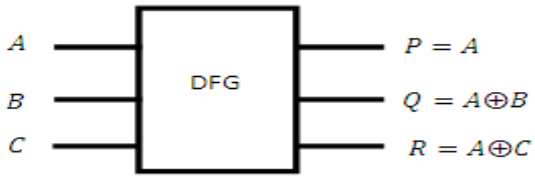


Fig. 3. Double Feynman Gate

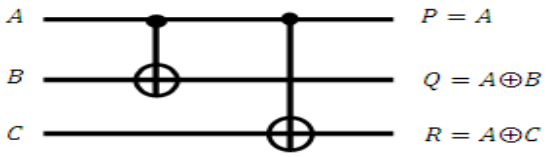


Fig. 4. Quantum Representation of DFG

G. SAM Gate

Input vector I_v and Output vector O_v are represented as I_v=(A,B,C) and O_v= $P = \bar{A}, Q = \bar{A}B \oplus A\bar{C}, R = \bar{A}C \oplus AB$ and respectively. The block diagram of 3x3 SAM gate is shown in "Fig. 5" and its quantum representation is shown in "Fig. 6". The quantum cost of SAM gate is 4. [4],[9]

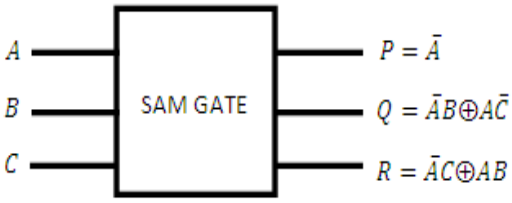


Fig. 5 Block diagram of 3x3 SAM Gate

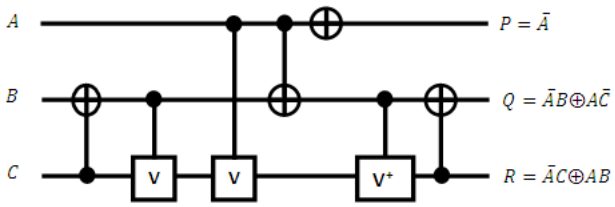


Fig. 6 Quantum representation of SAM gate.

If we give 0 to 3rd input then we get NOT of 1st input in 1st output, OR of 1st and 2nd inputs in 2nd output and AND of 1st and 2nd inputs in 3rd output. This operation is shown in "Fig. 7". So this gate can be used as two input universal gate.

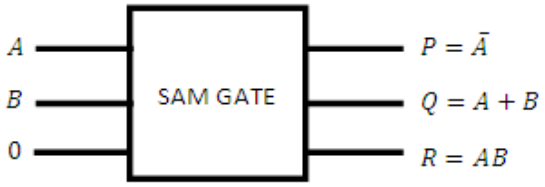


Fig. 7. SAM as NOT, OR and AND.

The Characteristic equation of D Flip-Flop is $Q = \overline{CLK}.Q + CLK.D$ "Fig. 8" shows the D flip-flop implementation by using SAM and DFG gate. Quantum cost of this D Flip-Flop implementation is 6.[7]-[8][11]-[13]

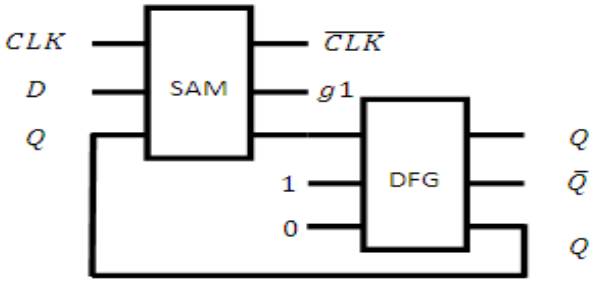


Fig. 8. D Flip-Flop

H. Syndrome calculator for the systematic Cyclic Codes

First we have to calculate syndrome for received code word. If the syndrome is zero, then there are no transmission errors in the received code word. But, if the syndrome is non-zero, then the received code word contains transmission errors which require corrections. Let the received code word be a polynomial of degree (n-1) or less. Let it be given by,

$$y(p) = y_0 + y_1 p + \ldots\ldots + y_{n-1} p^{n-1}$$

Now, we divide y(p) by the generator polynomial G(p). Let Q(p) represents the quotient polynomial and R(p) represents the remainder polynomial. Therefore,

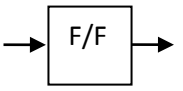
$$\frac{y(p)}{G(p)} = Q(p) + \frac{R(p)}{G(p)}$$

$$y(p) = Q(p).G(p) + R(p)$$

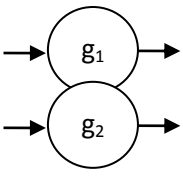
The remainder R(p) is a polynomial with degree (n-k-1) or less. It is called as the syndrome polynomial. "Fig. 10" shows the syndrome calculator, the difference between encoder [10] and this syndrome calculator is that; here the received bits are fed into the (n-k) stages of the feedback shift register from the left.

Working operation of Syndrome Calculator:

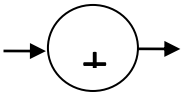
Initially, the output switch is connected to position 1 and all flip-flops are in their reset mode. As soon, as all the received bits are shifted into the shift register, its content will define the desired syndrome S. Once we know the syndrome S, we can determine the corresponding error pattern E and then make the appropriate corrections. After shifting all the incoming bits of received code word Y, the output switch is shifted to position 2 and the clock pulses are applied to the shift register to out the syndrome. The symbols used in the block diagram of syndrome calculator are as shown in "Fig. 9".



: Flip-Flop used for construction of shift-register.



: g_1 and g_2 are multiplying coefficients. The values of coefficients are either 0 or 1.



: Modulo 2-adders.

Fig. 9. Symbols used in the block diagram of syndrome calculator

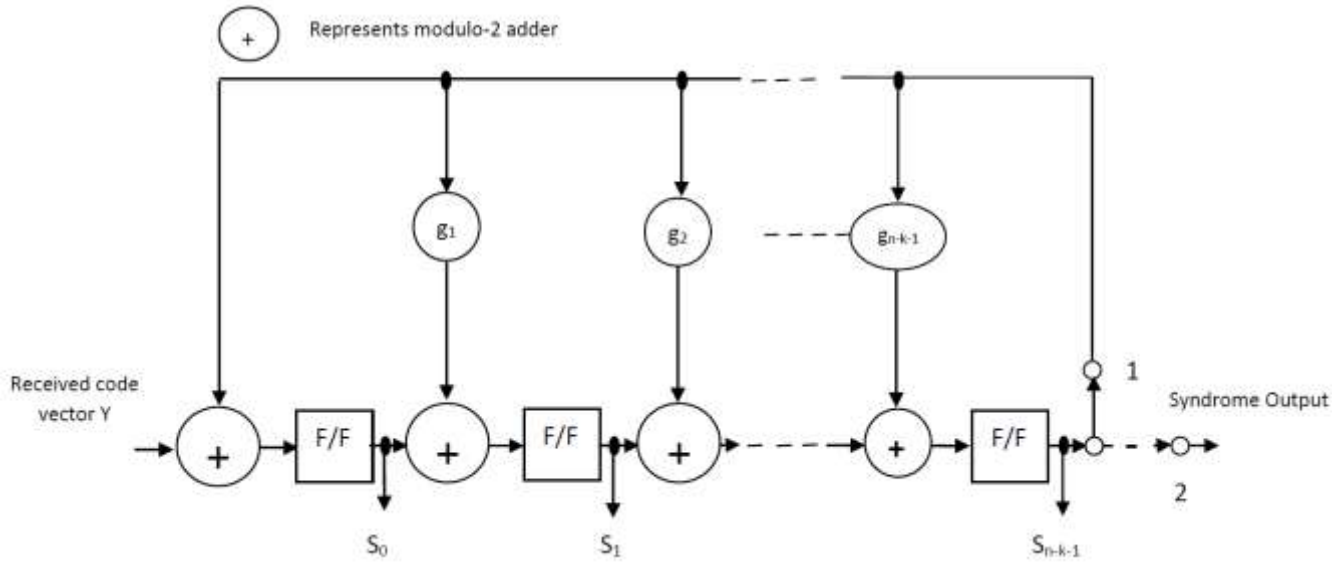


Fig. 10. Block diagram of Syndrome Calculator.

III. PROPOSED WORK

In this paper we propose the design of the syndrome calculator for a (7, 4) cyclic hamming code generated by the generator polynomial, G (p) = $1+p+p^3$. If the transmitted and received code words are given as:
Transmitted code word: X= (0 1 1 1 0 0 1)
Received code word: Y= (0 1 1 0 0 0 1)
Here error is in b_3 bit. So given generator polynomial is

$$G(p) = p^3 + 0.p^2 + p + 1 \quad (3.1)$$

The general form of generator polynomial is as given below:

$$G(p) = p^3 + g_2.p^2 + g_1.p + 1 \quad (3.2)$$

On compairing equation 3.1 and 3.2 we obtain $g_1 = 0$ and $g_2 = 1$. Therefore the required syndrome calulator using reversible logic gates are as shown in "Fig.11"

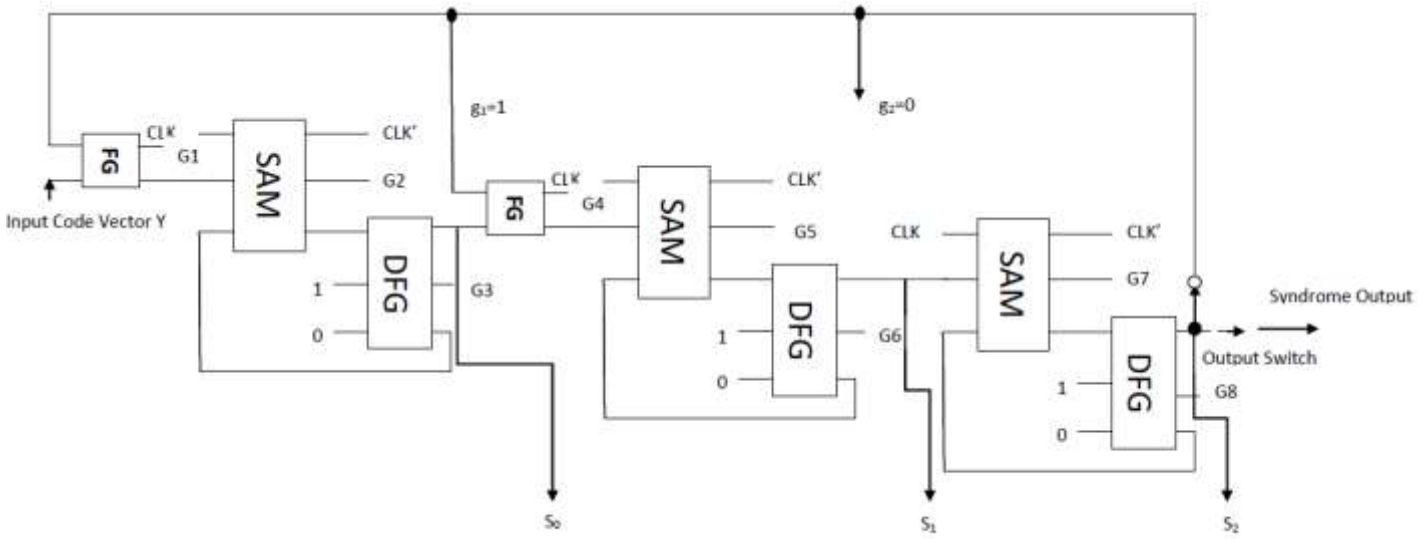


Fig. 11. Proposed Design of 3-bit Gray Code Counter.

IV. RESULTS AND DISCUSSION

In the implementation of the syndrome calculator for a (7, 4) cyclic hamming code generated by the generator polynomial, G (p) = $1+p+p^3$ we use three SAM gate having Quantum cost (QC) of 4 and three DFG gate having Quantum cost of 2 and Two FG having QC of 1. Number of gates, constant inputs, garbage output and quantum cost are shown in Table-I.

TABLE I.

No of Gates	No. of constant input	No. of garbage output	Quantum cost
8	6	8	20

V. CONCLUSION

We have presented the basic concepts of multipurpose binary reversible logic gates and provide basic idea of implementing reversible sequential elements such as flip-flops. Such gates can be used in regular circuits realizing Boolean functions. This paper proposes design of

the syndrome calculator for a (7, 4) cyclic hamming code generated by the generator polynomial, G (p) = $1+p+p^3$. In this paper, we implement the syndrome calculator design directly from reversible gates. Minimization of Quantum cost, garbage output and number of gate is a challenging one. Here in this paper the proposed designs are better in terms of quantum cost and garbage outputs. The proposed design can have great impact in quantum computing and coding theory. The proposed syndrome calculator designs have the applications in building Decoder for Cyclic code, Coding theory, nanotechnology, low power circuit design, cryptography, optical computing etc.

REFERENCES

[1] Landauer, R., "Irreversibility and heat generation in the computing process", IBM J. Research and Development, vol. 5, pp. 183-191, 1961.

[2] C.H. Bennett, "Logical Reversibility of Computation", IBM J.Research and Development, vol. 17, pp. 525-532, November 1973.

[3] J.E Rice, "A New Look at Reversible Memory Elements", Proceedings International Symposium on Circuits and Systems (ISCAS) 2006, Kos, Greece, May 21-24 ,2006, pp. 243-246.

[4] Md. SelimAl Mamun and Syed Monowar Hossain. "Design of Reversible Random Access Memory." International Journal of Computer Applications 56.15 (2012): 18-23.

[5] R. Feynman, "Quantum Mechanical Computers," Optics News, Vol.11, pp. 11–20, 1985.

[6] Perkowski, M., A.Al-Rabadi, P. Kerntopf, A. Buller, M. Chrzanowska-Jeske, A. Mishchenko, M. Azad Khan, A. Coppola, S. Yanushkevich,V. Shmerko and L. Jozwiak, "A general decomposition for reversible logic", Proc. RM'2001, Starkville, pp: 119-138, 2001

[7] M.-L.Chuang and C.-Y. Wang, "Synthesis of reversible sequential elements," ACM journal of Engineering Technologies in Computing Systems (JETC). Vol. 3, No.4, 1–19, 2008.

[8] Lafifa Jamal, Farah Sharmin, Md. Abdul Mottalib and Hafiz Md. Hasan Babu, Design and Minimization of Reversible Circuits for a Data Acquisition and Storage System, International Journal of Engineering and Technology Volume 2 No. 1, January, 2012.

[9] Md. Selim Al Mamun and David Menville, Quantum Cost Optimization for Reversible Sequential Circuit, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 12, 2013.

[10] Shashank Kumar Singh, B.K. Mandal and Supravat Mondal, "A Novel Design of Encoder for Cyclic code Using Reversible Logic Gates", International Journal of Advanced Information Science and Technology, Vol.6, No.10, October 2017.

[11] H. Thapliyal and A. P. Vinod, "Design of reversible sequential elements with feasibility of transistor implementation" In Proc. the 2007 IEEE Intl. Symp. On Cir.and Sys., pages 625–628, 2007.

[12] J. E. Rice, An introduction to reversible latches. The Computer journal,Vol. 51, No.6, 700–709. 2008.

[13] M.S.A.Mamun and B. K. Karmaker," Design of Reversible Counter" International Journal of Advanced Computer Science and Applications (IJACSA),Vol. 5, No. 1, 2014

[14] Himanshu Thapliyal and Nagarajan Ranganathan, Design of Reversible Sequential Circuits Optimizing Quantum Cost, Delay, and Garbage Outputs, ACMJournal onEmerging Technologies inComputer Systems,Vol. 6,No. 4,Article 14, 2010.

[15] Shashank K. Singh, H. Maity and A. Dey,"A novel design of MOD-8 synchronous UP/DOWN counter using Reversible gate", International Journal of Sceintific Research And Education, Vol. 2, Issue 9, pp. 1968-1976, sept. 2014.