© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Multi-Valued Logic Concept for Galois Field Arithmetic Logic Unit

T. R. Harinkhede, Pooja R. Thakare, Puja R. Tonde, Snehal B. Patil, Divya R. Savale, Koyal T. Karare, Manisha P. Dongre

Department of Electronics and Telecommunication, Smt. Rajshree Mulak College of Engineering for Women, Nagpur, Maharashtra, India

ABSTRACT

Large bus width increases the problem of interconnections in the modern system on chip (SOC) design. Interconnection increases the delay, area and energy consumption in CMOS digital circuits. For design circuitry in VLSI, multiple-valued logic (MVL) plays a very vital role. MVL is an apparent extension of binary logic where any proposition can have more than two values. Dynamic power requirement can be reduced by using the concept of level transition in multiple-valued logic. MVL is also helps to reduce the number of interconnections. It provides the key benefit of a higher density per integrated circuit area compared to traditional binary logic. In this paper, we are presenting an application of these circuits with response to Galois field operations and also a quaternary converter circuits using Down Literal Circuit (DLC). Arithmetic operations such as addition and multiplication are the two basic operations in Galois field. Tanner has created a software platform that is cost-effective and easy to use.

Keywords : Down Literal Circuit, Galois Field, Multiple-valued logic, Quaternary logic, Standard CMOS Technology, Very Large Scale Integrated Circuit.

I. INTRODUCTION

From the last three-four decades, we have been giving considerable attention to the Multiple-valued Logic. The tremendous increment in the density of very large scale integrated circuit (VLSI) results into the increment in number of ICs. As the number of devices accommodated on VLSI chips increases, many problems also arise. Interconnections are responsible for delay, area and energy consumption in CMOS digital circuit. Interconnections may increases routing problems. Therefore, proper routing does not take place. Inappropriate routing results in a larger chip size and thus cause timing and cross-talk problems.

The partial solution to this problem is to use Multiple-valued Logic (MVL). In the last few decades, multiple-valued logic has been proposed as an alternative to binary logic whereas binary logic is limited to only true and false state. Multi-valued logic replaces these with finitely or infinitely numbers of values. A MVL system is defined as a system which operates on a higher radix than two. Multiple-valued logic offers higher opportunities for implementation of digital processing algorithms than traditional binary logic. In applied problems, MVL reduces the total number of operations, simplifies computational processes, and can be used to find alternative computational methods, more easily formalize and better understand the problem to be solved and finally generate efficient ways to solve the problem. Application of multilevel signals in the design of digital devices (such as multilevel or multiple-valued design modules, arithmetic units etc) opens additional opportunities, namely, reduced number of connections with external devices, which solve the so-called pin out problem; reduces the number of ripple through carrier used in the process of realizations of arithmetic operations; increase the packing density.

Application of multilevel signals in the design of digital devices (such as multilevel or multiple-valued design modules, arithmetic units etc) opens additional opportunities, namely, reduced number of connections with external devices, which solves the so-called pin-out problem; reduces the number of ripple through carrier used in the process of realizations of arithmetic operations; increase the packing density.

If we use multiple-valued logic then it decrease the average power requirement for level transition and reduces the number of required interconnections, hence also reduces the number of interconnections on overall energy consumption. However, in an emblematic binary number system based on VLSI circuit about 70 percent of chip area is occupied by interconnections which occupy a large portion of physical area even when it is not in use. Therefore the interconnections will be more efficient if several levels of logic are injected into the only wire, as in multiple-valued logics. Thus, the direct benefit of such logics is the improved overall information efficiency. This occurs because each r-valued signal can carry more information than a binary signal. As radix r increases, routing area gets compact on a logarithmic scale. As can be seen, the routing area of 4-valued logic design is two times smaller than the corresponding binary logic system. Before performing arithmetic operations, 4-valued signals are converted to 2-valued signals. Result of arithmetic operations are also binary signals. Hence these binary signals are then converted to quaternary signals. In this paper, we are going to design quaternary to binary converter, binary to quaternary converter and the arithmetic logic unit for addition and multiplication operations in such a way to get minimum number of gets and minimum depth of net using CMOS Galois Field.

A. Galois Field

Galois Field is the field which contains finite number of elements. Galois fields are readily implemented with today's MVL technology. Galois field circuits are useful in many applications, from error correcting code encoders to cryptographic protection devices. Binary Galois field circuits have been investigated by many researchers. All fields containing a finite number of elements must have the number of elements equal to the primary number (p) or some power of it. Such fields are known as Galois Fields. In this paper, we are using GF (4).

II. METHODS AND MATERIAL

1. Design Of Proposed Plan Of Work

One key metric to consider for any MVL circuits through is the interface logic to the traditional binary circuits. The edge to and from binary logic to the MVL logic does need to have the level conversion to allow successful integration. Circuits namely "radix converters" helps to address the cross-region interface needs. The radix exchange is relatively easy for radices which are power of two (example, radix-2(binary), radix-4(quaternary) and radix-8, radix-16 etc).

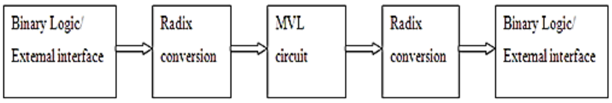

Figure 1: Block diagram of proposed design

The radix conversion process gets complex and more careful handling for other radices like radix-3, radix-5, radix-7, radix-9 etc. So, the area advantages can only be seen in lager circuits. MVL circuit avoids the logic duplication due to binary logic. Also higher radices would allow the increased number of functions that can be implemented, making it easier for large and more complex functions implementation. The main advantage of MVL logic systems and circuits are greater speed of arithmetic operations realization, reduction in interconnections complexity and interconnections area, greater density of memorized information, better usage of transmission paths, decreasing of pin number of integrated circuits and printed boards, reduces depth of net, problems due to interconnection delay, low power dissipation, possibilities of easier testing etc.

2. Down Literal Circuit

Down Literal circuit (DLC) is one of the most useful circuit elements in multi-valued logic. The DLC can divide the multi-valued signal into a binary state at an arbitrary threshold. It consists of variable threshold voltage by way of controlling only two bias voltages.

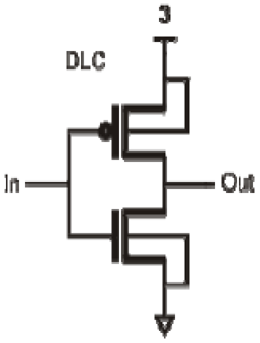

Figure 2 : Circuit diagram of DLC

3. Quaternary Converter Circuit

Quaternary converter circuits are used to minimize number of gates needed. This circuit is also helps to minimize the depth of net. Depth of net is the maximum number of gates in any path from input to output. We are choosing these objectives because during implementation of any VLSI circuit, they will give good properties. The reduced number of gates will condense the chip area and also give opportunity to use highest clock frequency.

A. Quaternary to Binary Converter (Q2B)

A basic quaternary to binary converter uses three down literal circuits DLC1, DLC2, DLC3 (each having diverse threshold voltage) and 2:1 multiplexer. Q is the quaternary input varying as 0, 1, 2 and 3 which is certain to three DLC circuits. The binary outputs thus obtained will be in complemented form and are required to pass through inverters to get actual binary numbers. Down literal circuits are realized from basic CMOS inverter by changing the threshold voltages of PMOS and NMOS transistors.

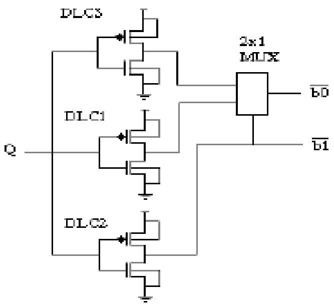

Figure 3 : Quaternary to Binary converter circuit

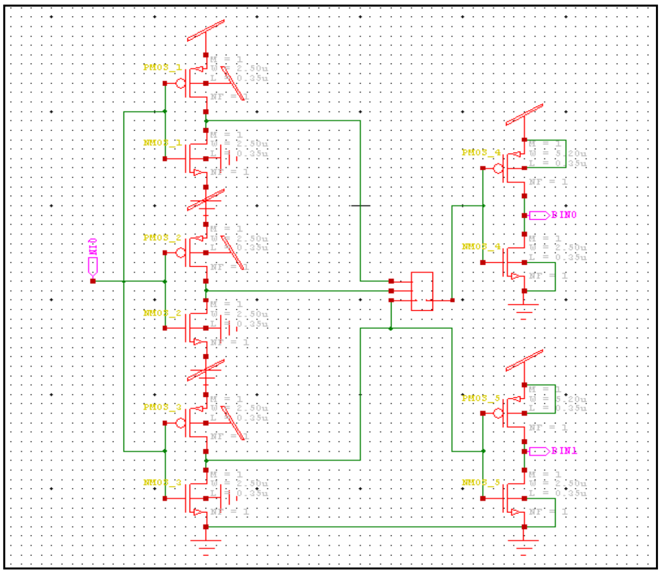

Figure 4 : Schematic for Quaternary to Binary converter Circuit

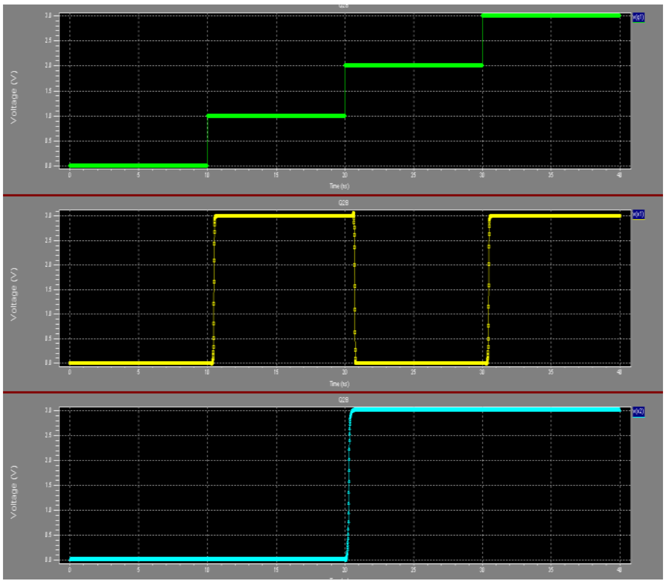

Figure 5 : Simulation result of Quaternary to Binary Converter Circuit

B. Binary to Quaternary Converter (B2Q)

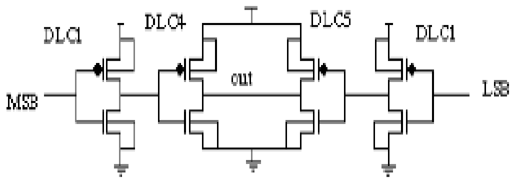

Figure 6: Binary to Quaternary converter circuit

Binary to Quaternary converter circuit is shown in figure 6. LSB and MSB of a two bit binary number are given to DLC1.

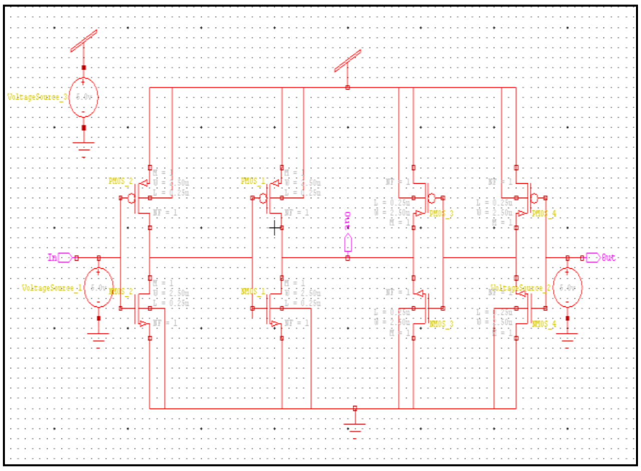

Figure 7 : Schematic for Binary to Quaternary Converter Circuit

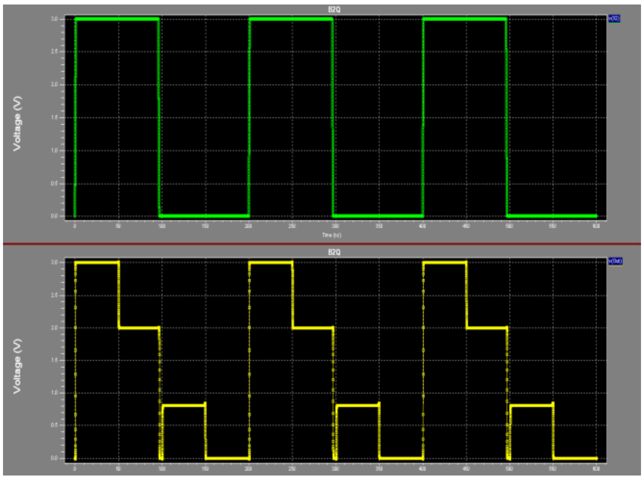

Figure 8: Simulation result of Binary to Quaternary Converter Circuit

4. Galois Field Adder

Addition can be performed in many ways in quaternary logic. Number of quaternary logic can be directly added or numbers in quaternary logic can be converte to binary logic and addition can be performed in binary logic. Result of addition is in binary logic and can be displayed in quaternary logic after conversion. Hence Q2B converter is used in the beginning and B2Q converter is used to display the result.

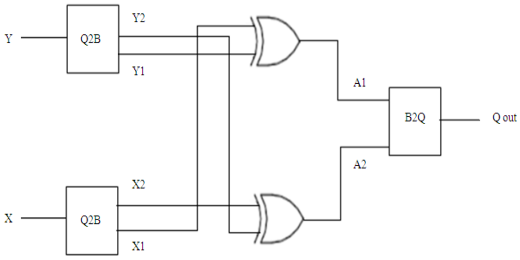

Figure 9 : Logic diagram for GF (4) adder

Figure 9 shows two XOR gates. Input to these XOR gates are X1, X2 and Y1, Y2 which is binary representation of quaternary numbers. The two bit result of addition between X1X2 and Y1Y2 shown by A1 and A2 square measure.

X1X2

Y1Y2

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Table 1: Addition for GF (4)

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Table 2: General table for GF (4) Adder

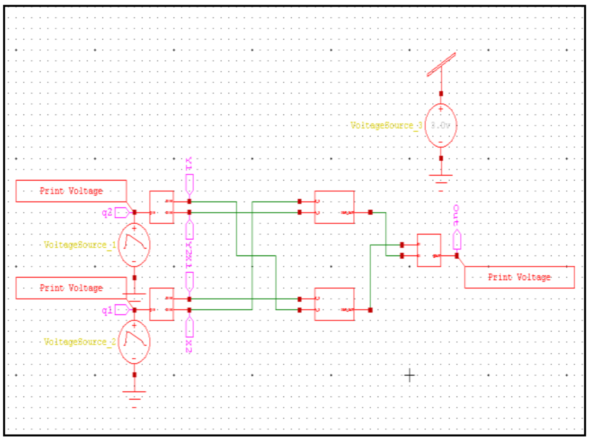

Figure 10: Schematic for GF (4) Adder

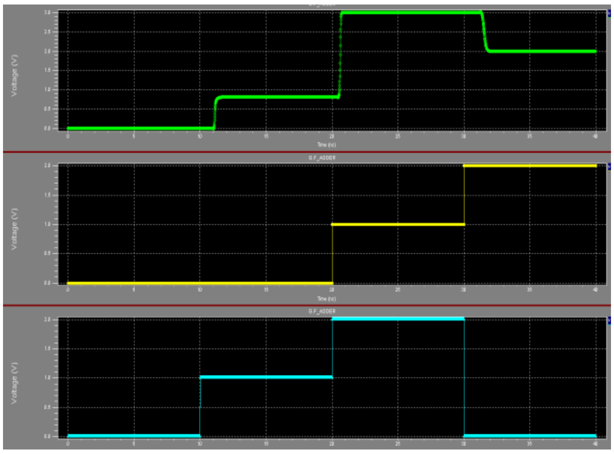

Figure 11: Simulation result of GF (4) Adder

5. Galois Field Multiplier

Multiplication operations in the galois field have many applications in communication systems. Some examples are their utilization for error detection and/or correction in cryptography.

Figure 12 shows the Galois field multiplier factor circuit. During circuit, no would like of quaternary to binary and binary to quaternary conversion. Here, this circuit is that the combination of three 4:1 multiplexers.

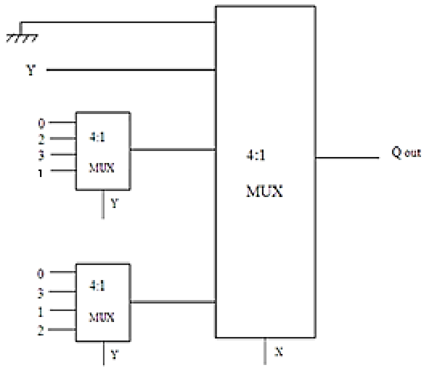

Figure 12: Logic diagram for GF (4) multiplier

X

	*	0	1	2	3
	0	0	0	0	0
Y	1	0	1	2	3
	2	0	2	3	1
	3	0	3	1	2

Table 3: Multiplication for GF (4)

*	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Table 4: General table for GF (4) Multiplier

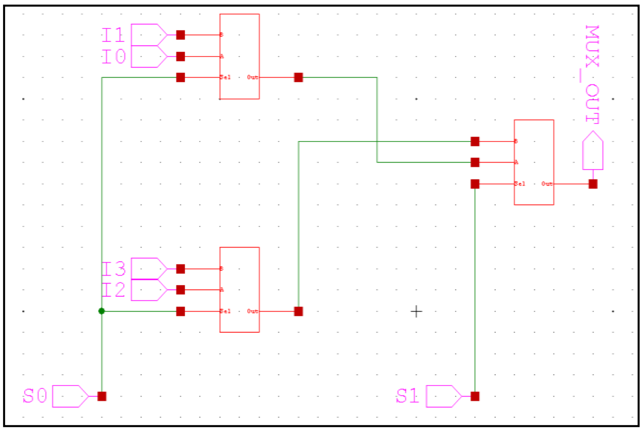

Figure 13: Schematic for GF (4) multiplier

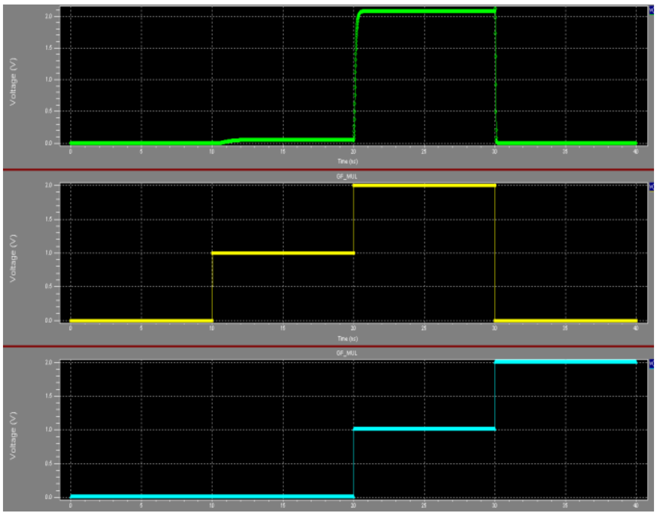

Figure 14: Simulation result of GF (4) multiplier

III. RESULTS

Thus, schematic and simulation results for quaternary converter circuit i.e. quaternary to binary conversion and binary to quaternary conversion, Galois field adder and multiplier are shown in above figures.

IV. CONCLUSION

With the help of quaternary logic levels, we have reduced the interconnections. We have also used less number of gates. Thus proposed circuits of Galois Field adder and multiplier require fewer gates, so that complexity of circuit is get reduced. Proposed circuits are suitable for implementing in VLSI with less number of interconnections and less area.

V. REFERENCES

[1] Diogo Brito, Jorge fernandes, Paulo Flores, Jose Monteiro, Taimur Rabuske, Senior member IEEE "Quaternary Logic Look Up Table in standard CMOS" 2014 IEEE transaction on very large scale integrated system.

[2] Diogo Brito, Jorge fernandes, Paulo Flores, Jose Monteiro, "Design and Characterization of a QLUT in a standard CMOS Process", 2012 IEEE.

[3] Nagamani A. N., Nischai S., PES Institute of Tecnology, Karnataka, "Quaternary High Performance Arithmetic Logic Unit Design" 2011 Euromica Conference.

[4] Vasundara Patel K. S., K. S. Gurumurthy, "Arithmetic Operation in Multi-valued Logic" International Journal of VLSI design & Communication System (VLSICS), March 2010.

[5] Ankita N. Sahkare, M. L. Keote, "Applications of Galois Field in VLSI using Multi-Valued Logic" International Journal of Engineering Science and Innovative Technology, January 2013.

[6] Gauri Poshattiwar, Prof. Seema S. Wasnic, "Design of CMOS Galois Field arithmetic logic unit using 120nm BSIM-4 model" International Research Journal of Engineering and Technology (IRJET), June 2015.

[7] Prashant Y. Shende, Dr. R.V. Kshirsagar, "Quaternary Multiplier using VHDL" 2013 International Journal Paper.

[8] Marcus Ritt, Carlos Arthur lang Lisboa, Luigi Carro, Cristiano Lizzari, "A cost effective Technique for mapping BLUTs to QLUTs in FPGAs" 2010 IEEE conference.