ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Application of Galois Field in VLSI Using Multi-Valued Logic

Ankita.N.Sakhare[1], M.L.Keote[2]
[1]Dept of Electronics and Telecommunication, Y.C.C.E, Wanadongri, Nagpur, India
[2]Dept of Electronics and Telecommunication, Y.C.C.E, Wanadongri, Nagpur, India

Abstract- ***Multi-valued logic is an apparent extension of binary logic where any proposition can have more than 2 values. Interconnections play a crucial role in deep sub-micron designs because they dominate the power and area. Design of the binary logic circuits is limited by the requirement of the interconnections. In modern SOC design, the interconnection is becoming a major problem because of the bus width. This problem can be solved by using Multiple-valued logic inter-connection. The benefits of multivalued logic is such as reduced area due to signal routing reduction along with the important advantage of being able to easily interface with traditional binary logic circuits. Galois field plays an important role in communications including error correcting codes, cryptography, switching and digital signal processing. Here, in this paper Quaternary converter circuits are designed by using down literal circuits. Arithmetic operations like addition, multiplication and subtraction in Modulo-4 arithmetic and addition in Galois field are performed by using multi-valued logic (MVL). And multiple-valued half adder circuit is also designed. Logic design of each operation is achieved by reducing the terms using Karnaugh diagrams, keeping minimum number of gates and depth of net in to consideration. The proposed circuit is Galois multiplication which requires fewer gates and also going to propose implementation of a voltage-mode Multiple-Valued (MV) maximum or minimum function. Simulation result of each operation is shown separately using Tspice.***

Keywords **- Down Literal Circuit, Multiple-Valued Logic, Quaternary Logic, Modulo-N Addition and Multiplication, Quarter-Nary Half Adder.**

I. INTRODUCTION

Multiple-valued logic has in the last few decades been proposed as a possible alternative to binary logic. Whereas binary logic is limited to only two states, ”true” and ”false”, multiple-valued logic (MVL) replaces these with finitely or infinitely numbers of values. A MVL system is defined as a system operating on a higher radix than two. Multiple-valued logic offers wider opportunities for implementation of digital processing algorithms than traditional binary logic. In applied problems, MVL substantially simplifies computational processes, reduces the total number of operations, and can be used to find alternative computational methods, more easily formalize and better understand the problem to be solved, and, finally, discover more efficient ways for solving the problem. Application of multilevel signals in the design of digital devices (such as multilevel or multiple-valued memory modules, arithmetic units etc) opens additional opportunities, namely, (i) substantially reduces the number of connections with external devices, which solves the so-called pin-out problem; (ii) reduces the number of ripple-through carriers used in the process of realization of arithmetic operations (normal binary addition or subtraction); and (iii) increases the packing density. Quaternary signals are converted to binary signals before performing arithmetic operations. Results of arithmetic operations are also binary signals. Hence these binary signals are to be converted to quaternary signals. In this paper, quaternary to binary and binary to quaternary converter are designed, and also Modulo-4 arithmetic operations are performed in such a way to get minimum number of gates and minimum depth of net. Novel quaternary half adder, full adder, and a carry-look ahead adder are introduced by M Thoidis. In his paper, the proposed circuits are static and operate in voltage mode. There is no current flow in steady states and thus no static power dissipation [7]. A 32 X 32 bit Multiplier using Multiple-valued Current Mode Circuit has been fabricated in 2 –um CMOS technology. The implemented 32x32 bit multiplier based on the radix-4 signed digit number system is superior to the fastest CMOS binary multiplier reported [8]. DOWN LITERAL CIRCUIT (DLC): Down literal circuit (DLC) is one of the most useful circuit element in multi-valued logic. The DLC can divide the multi-valued signal into a binary state at an arbitrary threshold. It has a variable threshold voltage by way of controlling only two bias voltages.

A. Modular Arithmetic Modular arithmetic sometimes called clock arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the modulus. Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations of the ring of integers: addition, subtraction, and multiplication. Modular arithmetic is referenced in number theory, group theory, ring theory, knot theory, abstract algebra, cryptography,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

computer science, chemistry and the visual and musical arts. In computer science, modular arithmetic is often applied in bitwise operations and other operations involving fixed-width, cyclic data structures. The modulo operation, as implemented in many programming languages and calculators, is an application of modular arithmetic.

B. Galois Field Field with finite number of elements is called Galois field. There are alternative to Boolean algebras for representing Boolean functions, e.g. Galois Field (GF(2)).Some functions have much shorter expression in GF(2) as compared to SOP expression in Boolean algebra. A field is an algebraic structure in which operations of addition, subtraction, multiplication, and division (except by zero) can be performed, and satisfy the usual rules. Field with finite number of elements is called Galois field. GF (2) is binary field and it can be extended to GF (2^K). These two fields are most widely used in digital data transmission and storage system [9]. GF (2^K) plays an important role in communications. The use of multiple-valued logic (MVL) approach to minimize the systolic architecture of AB^2 algorithm over binary Galois fields. The design is composed of four basic cells connected in a pipelined fashion [6]. A new algorithm based on a pattern matching technique for computing multiplication and division of two elements in *GF* (2*m*) is developed by Kovac, M. Ranganathan and N.Varanasi [10].

II. QUATERNARY CONVERTER CIRCUITS

Quaternary converter circuits are used to minimize number of gates needed and also to minimize depth of net. Depth of net is the largest number of gates in any path from input to output. The reason for choosing these two objectives is that they will give very good properties when implemented in VLSI. Minimizing number of gates will reduce the chip area, and minimizing depth will give opportunity to use highest clock frequency. As shown in figure 1, there is a simple DLC circuit which is realized from basic CMOS inverter by changing the threshold voltages of pmos and nmos transistors. A basic Quaternary to binary converter uses three down literal circuits DLC1, DLC2, DLC3 and 2:1 multiplexer as shown in figure 2. Q is the quaternary input varying as 0, 1, 2 and 3 which is given to three DLC circuits. The binary out puts thus obtained will be in complemented form and are required to pass through inverters to get actual binary numbers. Binary to quaternary converter circuit is shown in figure 3.There are three DLC circuit DLC1, DLC4, DLC5 each having different threshold voltage. LSB and MSB of a two bit binary number are given to DLC 1 as shown in the figure 3.As shown in table 1, there are five DLC circuits each having different threshold voltage. These threshold voltages are found by varying threshold voltage by way of controlling only two bias voltages. Threshold voltages of

DLC1: Vtp = -2.2V and Vtn = 0.2V, DLC2: Vtp = -1.2V and Vtn = 1.2V, DLC3: Vtp = 0.2V and Vtn = 2.2V,
DLC4: Vtp = -0.6V and Vtn = 0.6V, DLC5: Vtp = -1.2V and Vtn = 0.6V given in the reference paper [1].

In this paper, we have achieved the same Threshold voltages for different DLC's by using Threshold voltage Formula. This is the alternative method to find the same threshold voltages as mentioned above. Threshold voltage formula is shown in Equation (1).Substituting the parameters of LEVEL 3 in the threshold voltage formula and by varying the value of PHI, different threshold voltages are found out. Here 350nm LEVEL 3 technology file is used. Each LEVEL having different threshold voltage formula.

Threshold Voltage Vth:

$$Vth = Vbi - ((8.14e^{-22}.ETA) \div (COX.L^3_{eff})).V_{ds} + GAMMA.f_s.(PHI + V_{sb})^{1/2} + f_n.(PHI + V_{sb}) \quad (1)$$

Where

The f_s term expresses the effect of the short channel:

$$f_s = 1 - (XJ_{scaled} \div Leff).\theta\{((LD_{scaled} + W_c) \div (XJ_{scaled})).[1 - ((W_p) \div (XJ_{scaled} + Wp))^2]^{1/2} - (LD_{scaled} \div XJ_{scaled})\}$$

The f_n parameter specifies the narrow width effect:

$$f_n = (DELTA \div W_{eff}).(1 \div 4).(2\pi.E_{si} \div COX)$$

$$V_{bi} = V_{fb} + PHI \text{ or } V_{bi} = VTO - GAMMA.\theta.PHI^{1/2}$$

The function of DLC $D_{j(x)}$ is given in Equation (2) .It outputs R-1 if x is equal or less to the threshold j, else the output is zero.

$$D_{j(x)} = \begin{cases} R-1 & (x \le j) \\ 0 & (x \ge j+1) \end{cases} \quad (2)$$

Where xϵ {0,1,2……R-1} and jϵ {0,1,2…..R-2} and R is the Radix of the signal.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Table 1: Truth Table Of Down Literal Circuit

In	Out				
	DLC1	DLC2	DLC3	DLC4	DLC5
0	3	3	3	3	3
1	0	3	3	0	0
2	0	0	3	0	0
3	0	0	0	0	0

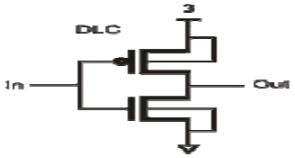


Fig 1: Circuit diagram for DLC Circuit Diagram of DLC Result

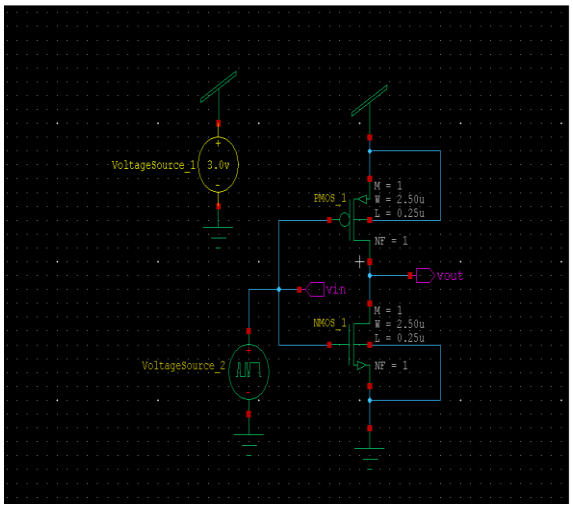


Fig 2: Quaternary to Binary Converter Circuit

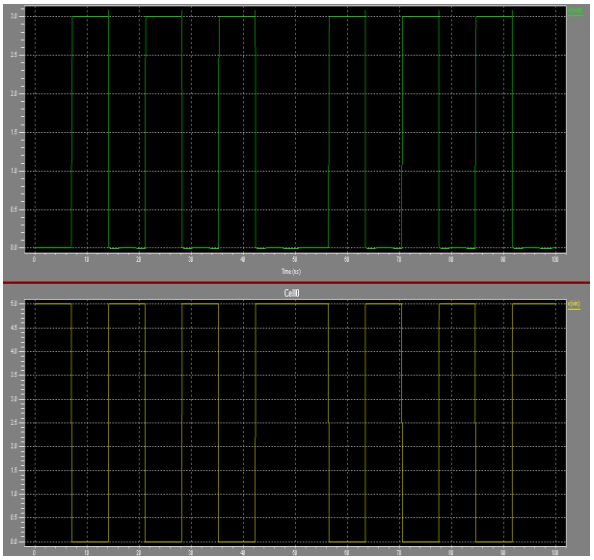
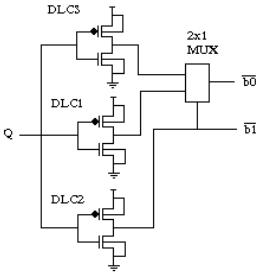
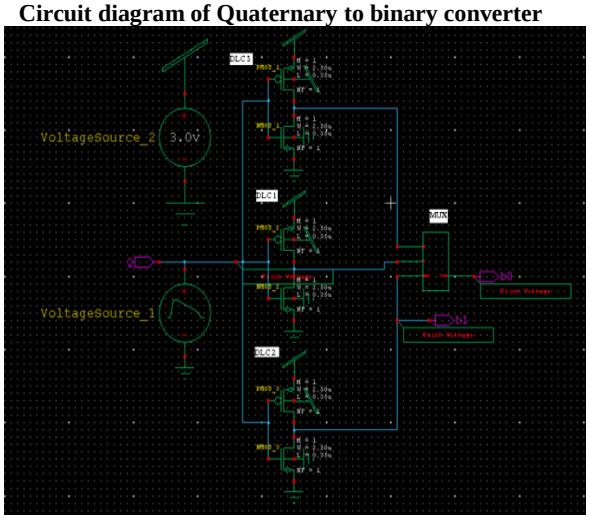
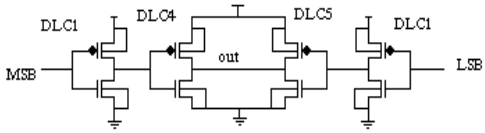


Fig 3: Binary to Quaternary Converter Circuit

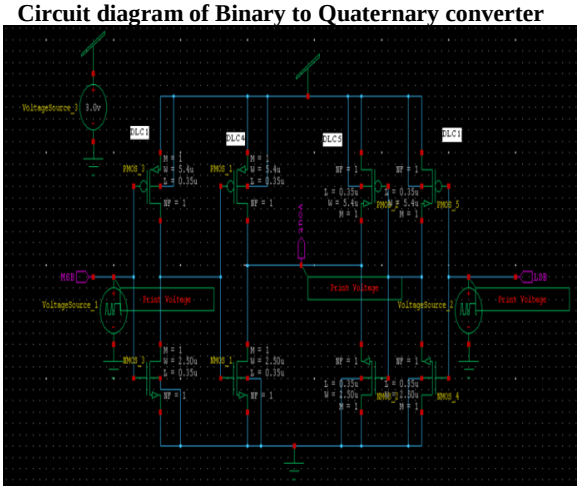


Circuit diagram of Quaternary to binary converter



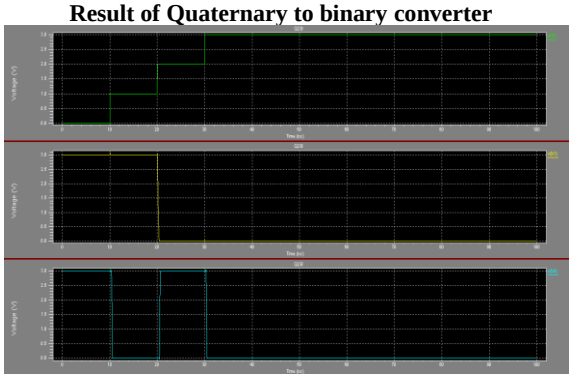


Circuit diagram of Binary to Quaternary converter

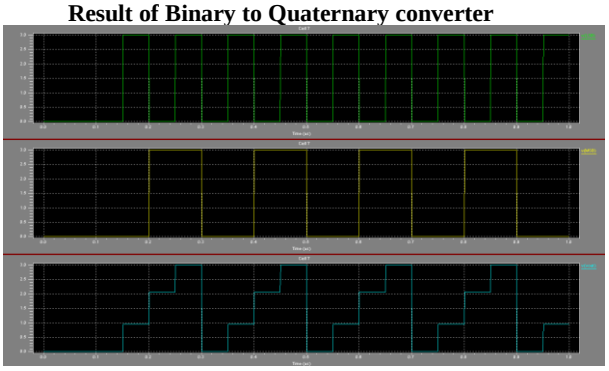


ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Result of Quaternary to binary converter



Result of Binary to Quaternary converter



III. MODULO-4 ARITHMETIC OPERATIONS

A. Modulo-4 Addition: Modulo-4 addition circuit is shown in figure 4. In this Circuit, To get input and output in quaternary form, quaternary to binary circuit is connected to the input of the modulo-4 addition circuit and binary to quaternary circuit is connected to the output of the modulo-4 addition circuit. Here in this figure giving input in quaternary form and getting output in quaternary form. This output satisfies the modulo-4 addition table as shown in table (2). Minimal functions have been obtained from the Karnaugh diagrams for the addition table shown in table 2 and then simplified as much as possible using all possible gate types. Minimal functions obtained from the minimal polynomials extracted from the Karnaugh diagrams are shown below. Let x1 x2 and y1 y2 be the binary representation of quaternary numbers which has to be added.

For addition:

$a_1 = (x_1 \oplus y_1) \oplus (x_2\ y_2)$ (3)

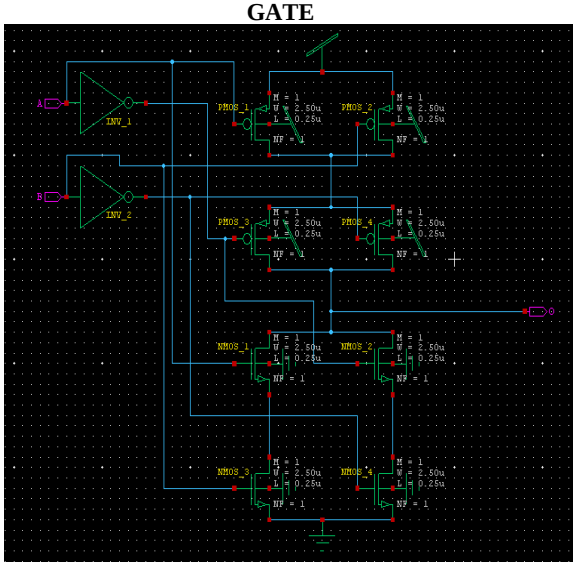
$a_2 = (x_2 \oplus y_2)$ (4)

Table 2: Table for modulo-4 addition

y_1y_2 \ x_1x_2	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Modulo-4 addition

Circuit Diagram of X-NOR GATE



Circuit Diagram of AND GATE

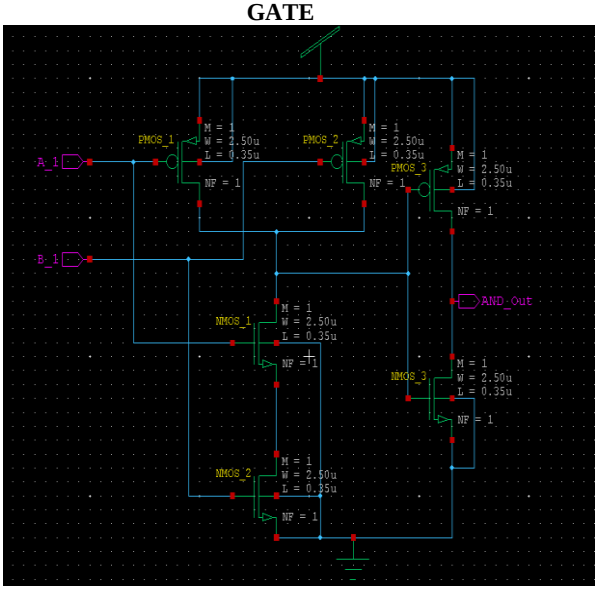
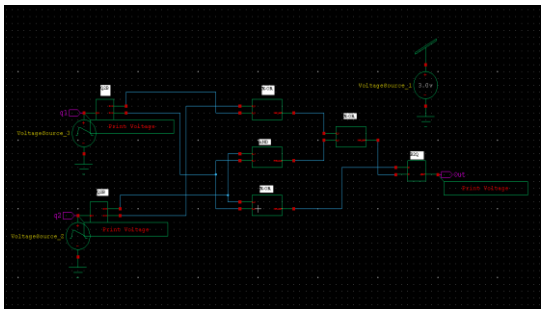
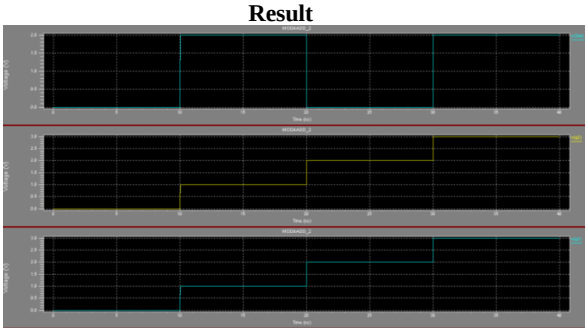


Fig 4:- Circuit Diagram for Modulo-4 Addition Giving Quaternary input and getting Quaternary output

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013



Result



B.Modulo-4 Multiplication: Modulo-4 multiplication circuit is shown in figure 5. In this circuit, to get input and output in quaternary form, quaternary to binary circuit is connected to the input of the modulo-4 multiplication circuit and binary to quaternary circuit is connected to the output of the modulo-4 multiplication circuit. Here in this figure giving input in quaternary form and getting output in quaternary form. This output satisfies the modulo-4 multiplication table as shown in table (3). Minimal functions have been obtained from the Karnaugh diagrams for the multiplication table shown in table 3 and then simplified as much as possible using all possible gate types. Minimal functions obtained from the minimal polynomials extracted from the Karnaugh diagrams are shown below. Let x1 x2 and y1 y2 be the binary representation of quaternary numbers which has to be multiplied.

For multiplication:

$$m_1 = x_1y_1'y_2 + x_1x_2'y_2 + x_1'x_2y_1 + x_2y_1y_2' = (x_1\, y_2) \oplus (x_2\, y_1) \qquad (5)$$

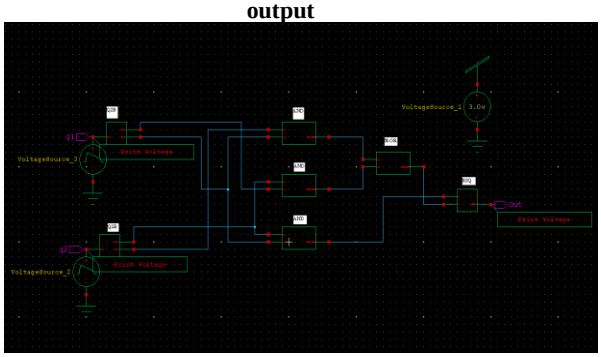
$$m_2 = x_2\, y_2 \qquad (6)$$

Table 3: Modulo-4 multiplication

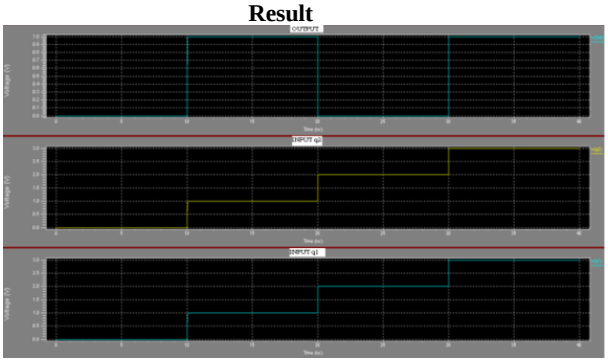
y_1y_2 \ x_1x_2	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fig 5:-Circuit Diagram for Modulo-4 multiplication:

Giving Quaternary input and getting Quaternary output



Result



C. Modulo-4 subtraction

Modulo-N addition and multiplication are commutative in nature, whereas Modulo-N Sub-traction is not commutative. Hence we are subtracting y1 y2 from x1 x2. If X is the quarter-nary value of x1 x2 and Y is the quaternary value of y1 y2, then S = (X + 4) – Y, if X <Y. For example if X = 2 and Y = 3 then 2 + 4 = 6 - 3 = 3, table 4 shows subtraction of y1 y2 from x1 x2. Modulo-4 subtraction circuit is shown in figure 6.In figure 6(a), circuit diagram of Modulo-4 subtraction is designed, in this figure, giving input in binary form and getting output in binary form. In figure 6(b), to get input and output in quaternary form, quaternary to binary circuit is connected to the input of the modulo-4 subtraction circuit and binary to quaternary circuit is connected to the output of the modulo-4 subtraction circuit. Here in this figure giving input in quaternary form and getting output in quaternary form. This output satisfies the modulo-4 subtraction table as shown in table (4). Minimal functions have been obtained from the Karnaugh diagrams for the subtraction table shown in table 2 and then simplified as much as possible using all possible gate types. Minimal functions obtained from the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

minimal polynomials extracted from the Karnaugh diagrams are shown below. Let x1 x2 and y1 y2 be the binary representation of quaternary numbers which has to be subtracted.

For subtraction:

$s_1 = (x_1 \oplus y_1) \oplus (x_2' y_2)$ (7)

$s_2 = x_2 y_2' + x_2' y_2 = (x_2 \oplus y_2)$ (8)

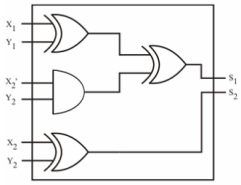


Table 4: Modulo-4 subtraction

x_1 x_2	y_1y_2 0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Fig 6: Modulo-4 subtraction

Circuit Diagrams for Modulo-4 subtraction:

Fig 6(a):-Giving Binary input and getting Binary output Result

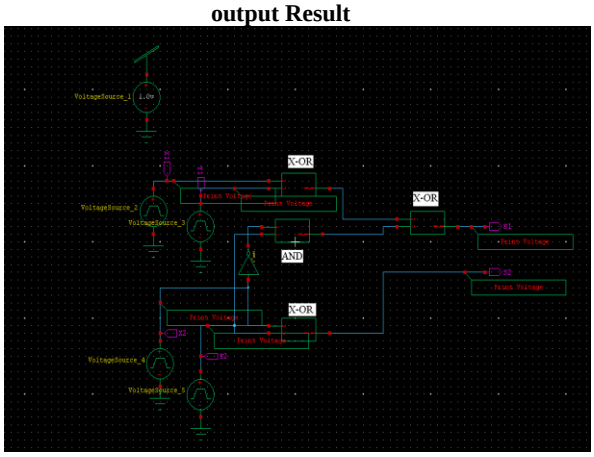
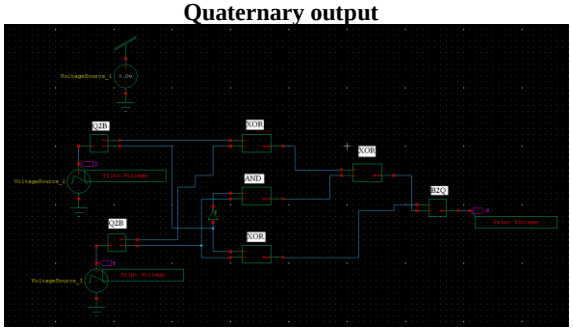
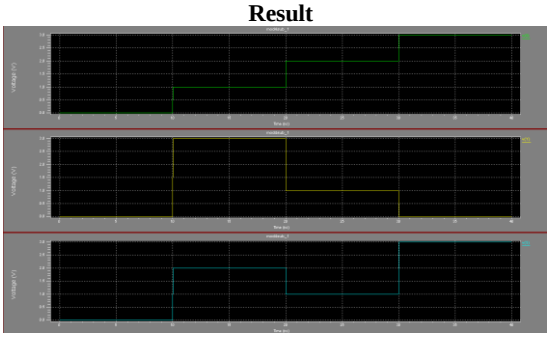


Fig 6(b):-Giving Quaternary input and getting Quaternary output



Result



IV. GALOIS ADDITION

Galois addition table in Figure 7 is used in Karnaugh diagrams to obtain minimum function. Minimal functions obtained from the minimal polynomials extracted from the Karnaugh diagrams for GF (4) addition is shown below. Let x1 x2 and y1 y2 be the binary representation of two quarternary numbers which have to be added. a 1 and a 2 are the two bit result of addition between x1 x2 and y1 y2 .

Equation 9 & 10 shows that addition in GF (4) requires only two gates and depth of net is reduced to one. This is a very good design among four circuits. Logical implementation of the circuit is shown in figure 7.

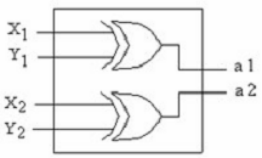
For Galois Addition

$a_1 = (x_1 \oplus y_1)$ (9)

$a_2 = (x_2 \oplus y_2)$ (10)

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

Fig 7: Galois Addition



X1X2

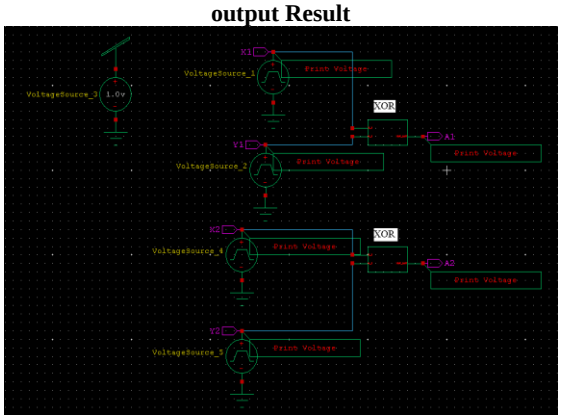
+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Y1Y2

Table 5: Galois Addition

Circuit Diagrams for Galois Addition:

Fig 7(a):-Giving Binary input and getting Binary output Result



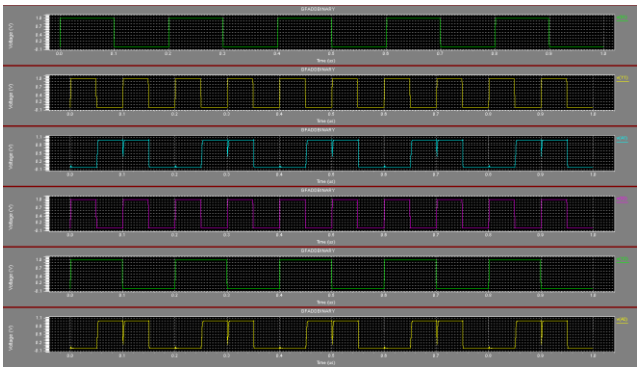
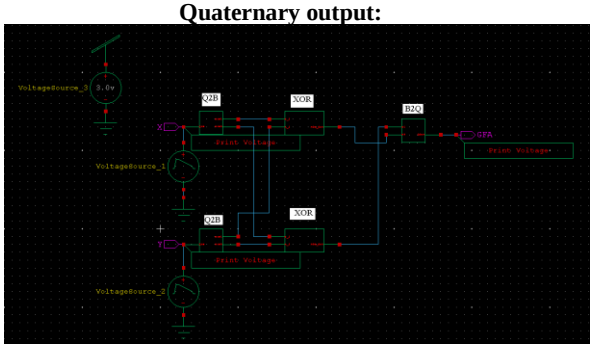
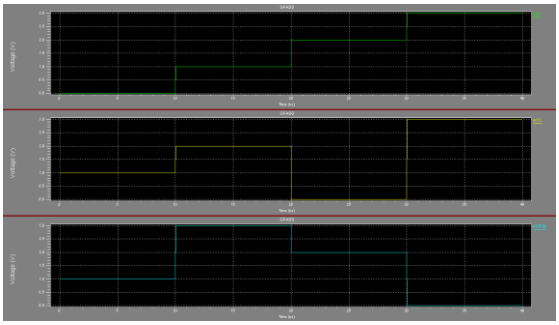


Fig 7(b):-Giving Quaternary input and getting Quaternary output:



Result



V. IMPLEMENTATION OF QUATERNARY HALF ADDER

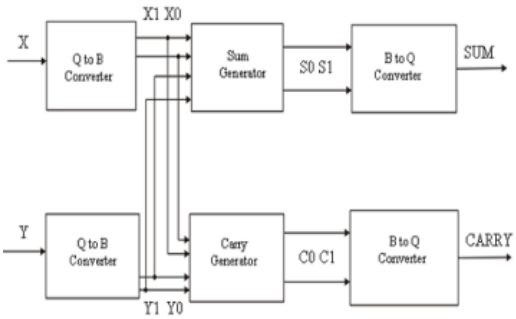
In quaternary logic, addition can be performed in many ways. Numbers in quaternary logic can be directly added or numbers in quaternary logic can be converted to binary logic and addition can be performed in binary logic. Binary results of addition can be displayed in quaternary logic after conversion. Hence quaternary to binary converter is required in the beginning. Binary to quaternary converter is used to display the result in quaternary logic. Two bit natural representation of binary logic is used for each quaternary number and addition is performed in binary itself with only 4 gates. Figure 8 explains the block diagram of quaternary half adder. As shown in table 6, X and Y are quaternary numbers which are converted to 2 bit binary numbers using quaternary to binary converter [1]. X0, X1 are the two bit binary representation of X, where as Y0 and Y1 are the two bit representation of quaternary number Y. In table 6, S1 and S0 are the result of addition in binary and S is in quaternary because binary to quaternary converter is used for conversion. C1 and C0 are in binary. In table 6, carry is nothing but C0 and actually conversion is not required. Sum generator block shown in figure 8 has 4 binary logic gates as explained in figure 9. Carry generator block is explained in figure 10.

Table 6: Truth Table of Quaternary Half Adder

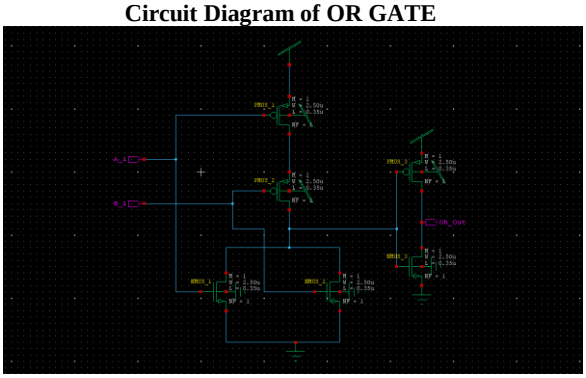
ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

X	Y	X_1	X_0	Y_1	Y_0	S_1	S_0	C_1	C_0	S	C
0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	1	0	0	1	0
0	2	0	0	1	0	1	0	0	0	2	0
0	3	0	0	1	1	1	1	0	0	3	0
1	0	0	1	0	0	0	1	0	0	1	0
1	1	0	1	0	1	1	0	0	0	2	0
1	2	0	1	1	0	1	1	0	0	3	0
1	3	0	1	1	1	0	0	0	1	0	1
2	0	1	0	0	0	1	0	0	0	2	0
2	1	1	0	0	1	1	1	0	0	3	0
2	2	1	0	1	0	0	0	0	1	0	1
2	3	1	0	1	1	0	1	0	1	1	1
3	0	1	1	0	0	1	1	0	0	3	0
3	1	1	1	0	1	0	0	0	1	0	1
3	2	1	1	1	0	0	1	0	1	1	1
3	3	1	1	1	1	1	0	0	1	2	1

Fig 8: Block Diagram of Quaternary Half Adder Circuit



Circuit Diagram of OR GATE



A) Sum Generator Block: Sum generator circuit is shown figure 9. X0, X1 are the binary representation of the quaternary number X, and Y0 and Y1 are the two bit representation of quaternary number Y. S0S1 are the outputs of sum generator block which is in binary. Minimal functions have been obtained from the Karnaugh diagrams for the tables shown in table 6 and then simplified as much as possible using all possible gate types. Minimal functions obtained from the minimal polynomials extracted from the Karnaugh diagrams are shown below. Sum generator in figure 9 is designed using these two expressions. This circuit uses 3 binary XOR gates and one binary AND gate. Depth of net is maximum of two gates. Depth of net is nothing but the number of gates between input and the output.

$S0 = x0y0' + x0'y0 = (x0 \oplus y0)$ (11)

$S1 = (x1 \oplus y1) \oplus (x0y0)$ (12)

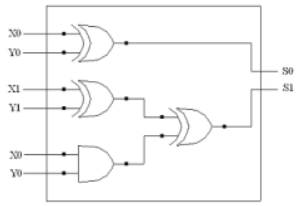
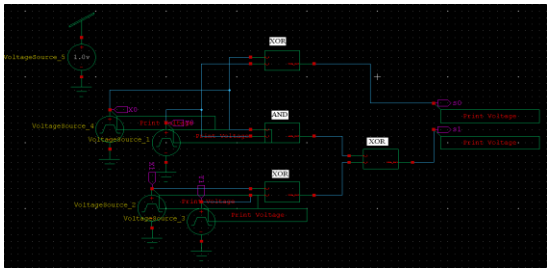
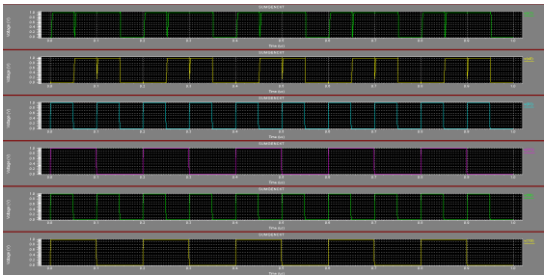


Fig 9: Sum Generator Circuit

Circuit Diagram for Sum Generator Circuit



Result



B) Carry Generator Block: Carry generator circuit is shown figure 10. X0, X1 and Y0 Y1 are the input to the block. Co C1 are the outputs of the block. This circuit is designed by the expression obtained from the Karnaugh

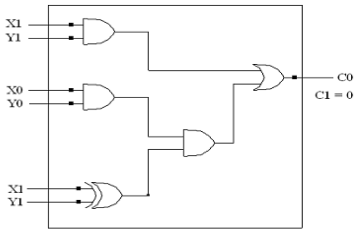
ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

diagrams for the tables shown in table 6 and then simplified as much as possible using all possible gate types. The circuit contains two binary OR gates and three binary AND gates. Depth of the net is three. Simulation result shown in figure 11 verifies the table 6.

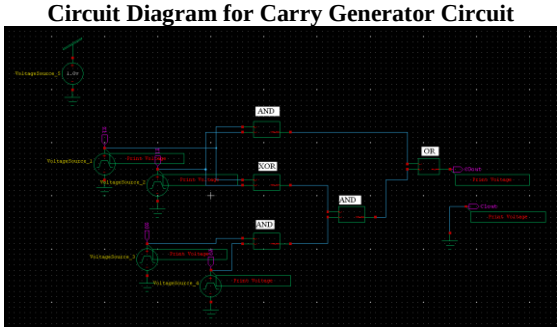
$C_0 = x_1 y_1 + x_0 y_0 (x_1 + y_1)$ (13)

$C_1 = 0$ (14)

Fig 10: Carry generator circuit



Circuit Diagram for Carry Generator Circuit



Result

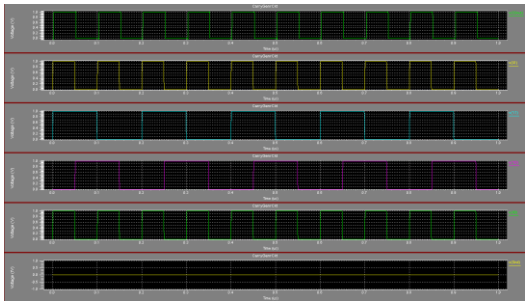
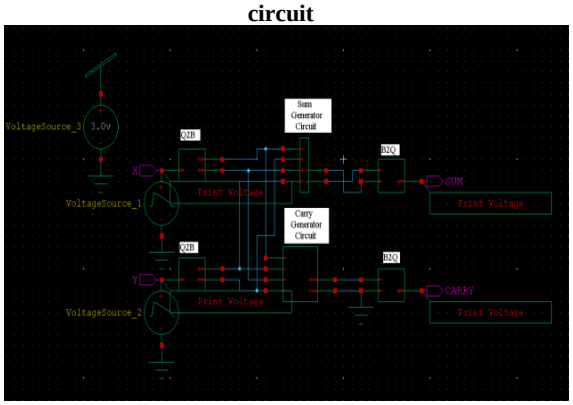
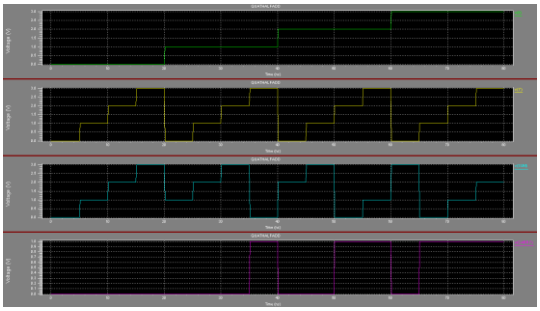


Fig 11: Circuit Diagram for quaternary half adder circuit



Result



A basic Quaternary to binary converter uses three down literal circuits DLC1, DLC2, DLC3 and 2:1 multiplexer. Q is the quaternary input varying as 0, 1, 2 and 3 which is given to three DLC circuits. The binary out puts thus obtained will be in complemented form and are required to pass through inverters to get actual binary numbers. A basic binary to quaternary circuit consists of two PMOS and two NMOS transistors which form two inverters and two DLC 1 circuits. LSB and MSB of 2 bit binary numbers are given to two DLC1 circuits and output of two inverters will provide quaternary number.

VI. RESULTS

TSPICE transient analysis simulation is done to verify the functionality of the circuits. 350nm technology files are used for simulations. Simulation result of quaternary to binary and binary to quaternary are shown in figure 2 and figure 3 respectively. Simulation results of Modulo-4 addition, Modulo-4 multiplication, Modulo-4 subtraction and Galois Field addition are shown above. There result of polynomials shown in equations obtained by K map reduction. Modulo-4 addition requires 40 transistors (4 gates), Modulo-4 multiplication requires 24 transistors (4 gates). Modulo-4 subtraction requires 42 transistors (5 gates), Galois addition requires 24

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 1, January 2013

transistors (2 gates). Simulation result of quaternary half adder is also shown. Quaternary half adder requires only 76 transistors. These circuits consume less number of transistors and shows high performances.

VII. CONCLUSION

Thus binary to quaternary and quaternary to binary converters are designed using down literal circuits. A circuit for Modulo-4 addition and Modulo-4 multiplication requires only 4 gates and Modulo-4 subtraction circuit requires only 5 gates. With the help of quaternary logic levels, we have reduced the interconnections. We have also used less number of gates and hence less area for modulo-4 arithmetic operations. The proposed circuit is Galois multiplication which requires fewer gates and also going to propose implementation of a voltage-mode Multiple-Valued (MV) maximum or minimum function. Proposed circuits are suitable for implementing in VLSI with less number of interconnections and less area.

REFERENCES

[1] Vasundara Patel k s1, k s gurumurthy2 “arithmetic operations in multi-valued logic”, International journal of VLSI Design and communication system (VLSICS) Vol.1, No.1, March 2010.

[2] Vasundara Patel K S, K S Gurumurthy” Design of High Performance Quaternary Adders”, International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010.

[3] Vasundara Patel K S, K S Gurumurthy, Vinay Sheshadri and Sivaram Krishnan R “Static random access memory using quaternary D latch ”, International Journal of Engineering Science and Technology Vol. 2(11), 2010, 6371-6379.

[4] Hirokatsu Shirahama and Takahiro Hanyu, “Design of High-Performance Quaternary Adders Based on Output-Generator Sharing”, Proceedings of the 38th International Symposium on Multiple Valued Logic P: 8-13, 2008.

[5] Ricardo Cunha, “quaternary lookup tables using voltage mode CMOS logic design”, ISMVL 2007. 37th International Symposium on Multiple-Valued Logic, pp.56-56, 2007, 13-16 May, 2007.

[6] Nabil Abu-Khader, Pepe Siy, “Multiple-Valued Logic Approach for a Systolic^2 AB Circuit in Galois Field”. 35th International Symposium on Multiple-Valued Logic (ISMVL'05), May 19-May 21, 2005.

[7] M. Thoidis, D. Soudris , J.-M. Fernandez, and A. Thanailakis, "The circuit design of multiple-valued logic voltage-mode adders ", Proceedings of the 2001 IEEE International Symposium on Circuits and Systems (ISCAS 2001), May 6-9, 2001, Sydney, Australia, vol. IV, pp.162-165.

[8] Kawahito, S. Kameyama, “A 32 X 32 bit Multiplier using Multiple-valued MOS Current Mode Circuit”, Journal of Solid-State Circuits, IEEE, Vol.1, pp. 124 - 132 Feb.1988.

[9] Shulin, Daniel J, Costello, “Error control coding”, Pearson Prentice Hall, second edition.

[10] Kovac, M. Ranganathan, N. Varanasi, “ M SIGMA: a VLSI systolic array implementation of a Galois field GF(2 m) based multiplication and division algorithm”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol.1, pp. 22-30, March 1993.