Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review of 32-bit Floating Point and Galois Field Multipliers using Wave-Pipelining

P. V. Bharambe*, Prof. M. N. Thakare, Prof. G. D. Korde
Department of E & T, RTMNU
Maharashtra, India

Abstract— In this paper, review of Floating point and Galois field multipliers design using Wave pipelining has been described. Wave pipelining is a design of a circuit that allows digital systems to be clocked at rates higher than conventional pipelining techniques in case of synchronous circuits only. Wave pipelining technique is used to improve the throughput of a logic circuit. Multiplication plays a very important role in the application of signal processing, other than this multiplication and shifting operations involves larger computation time. Hence, our aim is to design a multiplier which can operate at higher speed that will increase the performance of signal processing. GFT (Galois Field Theory) performs operation with binary numbers and has the properties of mathematics. Many of the Galois Field operations match those of regular mathematics. Common Galois Field operations are addition multiplication and logarithms, are very useful for checking multiplication results. Galois Field multipliers have been widely used in coding theory and cryptography. Finally, the coding will be done in VHDL (Very High Speed Integrated Circuit Hardware Description Language), synthesis and simulation will be done using Xilinx ISE simulator. Also, the design will be implemented on FPGA (Field Programmable Gate Array) kit.

Keywords— Galois Field Multiplier, Floating Point Multiplier, VHDL, Wave-Pipeling.

I. INTRODUCTION

Nowadays, with the arrival of technology, high speed digital systems are on the rise and the multiplier is an omnipresent unit in almost every digital system. If we compare other operations in an arithmetic logic unit, its main module called as multiplier requires more time and power. Therefore, researchers are always trying to design multipliers which can be a combination in terms delay, speed, power and area. Floating point describes a method for representing real numbers which support a wide range of values. Floating point units have many applications in a dynamic range of engineering and technology applications. The development of faster floating point arithmetic circuits is a necessary choice [3]. For representing floating point numbers into fixed numbers, we use IEEE 754 single or double precision format. This format consists of a sign bit, exponent bits and mantissa / significand bits.

Floating point multiplication is carried out as follows; in the first part, the sign field is determined by taking product of performing xor operation on the sign bits of the two given operands. In the second part, the exponent bits of the operands are given to the adder circuit and a bias of 127 is subtracted from the obtained output. The addition and bias subtraction operations are both implemented using adder circuits. overflow and underflow conditions can be obtained by setting the respective flags. In the third stage, we find the product of the mantissa bits. Finally, combination of these three fields is the floating point multiplication of the two numbers.

Galois Field Theory (GFT) deals with numbers that are binary in nature, have the properties of a mathematical "field," and are finite in scope. Although some Galois computations don't exist in ordinary mathematics, many Galois operations match those of regular math. Addition (Ex-Or) and multiplication are common Galois operations, and logarithms, particularly, are handy for checking multiplication results. For over 40 years, Galois Field multipliers have been used both for coding theory and for cryptography. Both areas are complex, with similar needs, and both deal with fixed symbolic alphabets that neatly fit the extended Galois Field model. Galois field theory is also known as Finite field theory which is generally applied in Elliptic Curve Cryptography, error correction codes, digital signal processing, etc. Hence, specific implementation of hardware based on Galois field arithmetic comes in picture. There are different types of methods provided by galois for addition, multiplication, etc of polynomial equations. In Galois field multiplication two k-bit inputs A, B are multiplied using modulo logic and gives polynomial P(x) over the finite field F_2^k. Incorrect multiplication will give full leakage of the secret key in cryptosystems. Therefore, it is most important to verify the correct hardware to be implemented of finite field multipliers used in such types of system [2].

Wave-Pipelining is one of the techniques, which is currently being used in VLSI circuit designs. Wave pipelining provides a method for reducing clock cycles and area, power, delay, latency of any synchronous circuit. Nowadays, peoples are using this technique because it gives design, analysis, synthesis as well as implementation across a variety of levels viz. process, route, layout, circuit, logic, timing, and architecture which are the main parameters of VLSI design. The idea of wave-pipelining was originally invented by Cotten, who then changed name to maximum rate pipelining. Wave Pipelining is a circuit Design that allows digital systems to be clocked at higher rates than, that can be achieved

with conventional pipelining. Cotten observed that the rate at which logic can propagate through the circuit depends not on the longest path delay but also on the difference between the longest and the shortest path delays. Hence, several computation "waves", i.e., logic signals which are related to different clock cycles, can propagate through the logic simultaneously. Wave-pipelining can also be view as a virtual pipelining, in which each gate acts as a virtual storage element [6].

The method for the proposed design of floating point and Galois field multiplier using wave-pipelining is shown in figures 1. Figure 1 shows the basic diagram of 4 bit Galois field multiplier. The main elements in Galois field multiplier are multiplier section and multiplicand section. The multiplier section consist of D-flip flops, each flip flop stores a single bit. On the other hand, multiplicand section consist of 4 D-flip flops for B value, 4 D-flip flops for R value and 4 D-flip flops for P value (polynomial multiplication result). It also consist of AND gate, EX-OR gate with MUX unit to perform operations.

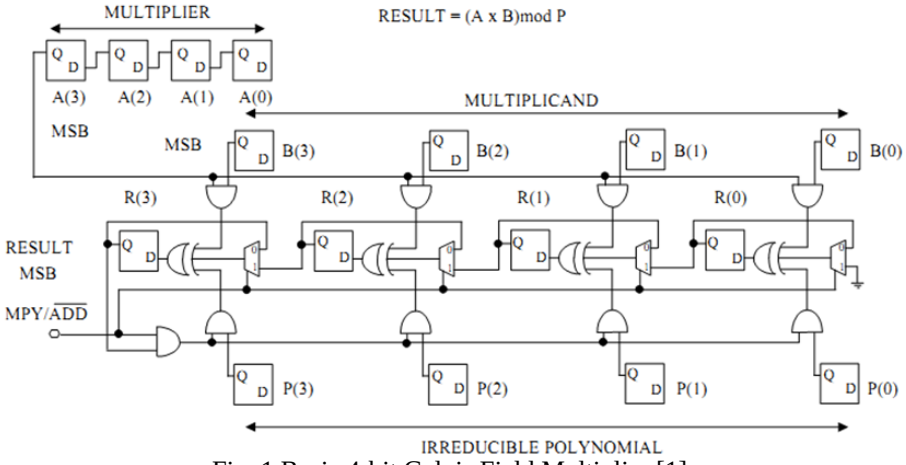

Fig. 1 Basic 4-bit Galois Field Multiplier [1]

II. LITERATURE REVIEW

M. Anbuselvi et.al. [1] in paper entitled "Design and analysis of Floating point and Galois field multipliers using Wave-pipelining" presents a design and analysis of Floating point and Galois field multipliers using a pipelining technique called "Wave pipelining". Wave pipelining is a circuit design technique that allows digital synchronous systems to be clocked at rates higher than conventional pipelining techniques. Wave pipelining can improve the throughput of a logic circuit while avoiding some of the overheads of traditional pipelining. Multiplication plays a very important role in the signal processing application in signal processing, multiplication and shifting operations involves larger computation time. Hence making the multiplier to operate at higher speed will increase the performance of signal processing. Galois Field Theory (GFT) deals with binary numbers, has the properties of a mathematical "field," and are finite in scope. Many Galois operations match those of regular math. Addition and multiplication are the common Galois operations, and logarithms, particularly, are handy for checking multiplication results. Galois Field multipliers have been widely used in coding theory and cryptography. Finally the synthesis reports of different pipelining stages of both the multipliers have been tabulated by implementing the algorithm in Xilinx Spartan 3E FPGA board. In this paper, they analyze the performance of floating point, 8-bit and 23-bit Galois field multipliers with the effect of wave-pipelining. They have found from the tables, Device Utilization Summary of floating point, 8-bit and 23-bit multipliers shows that the number gate count increases with the increase in number of pipeline stages and gets reduced for the wave-pipelining. Hence wave-pipelining is found to be more superior in terms of area when compared with other pipelining stages. The same architectures can be designed with other wave-pipelining technique such as logic reconstruction and node collapsing [1].

Jinpeng Lv et. al. [2] in paper entitled "Formal Verification Of Galois Field Multiplier Using Computer algebra Techniques" presents a formal verification of galois field multipliers using computer algebra techniques. Finite (Galois) field arithmetic finds applications in cryptography, error correction codes, signal processing etc. Multiplication usually lies at the core of all Galois field computations and is a high-complexity operation. In this paper, they addresses the problem of formal verification of hardware implementations of modulo-multipliers over Galois fields of the type F_2^k, using a computer-algebra/algebraic geometry based approach. The multiplier circuit is modeled as a polynomial system in F_2^k [x1, x2, ⋯, xd] and the verification test is formulated as a Null stellensatz proof over the finite field. A Gobner basis engine is used as the underlying computational framework. The efficiency of Gobner basis computations depends heavily upon the variable ordering used to represent and manipulate the polynomials. They present a variable ordering heuristic that significantly improves the efficiency of Gobner basis engines. Using their approach, they verified the correctness of up to 96-bit multipliers, whereas contemporary BDDs/SAT/SMT-solver based methods are infeasible. They also presented a formal approach to model and verify multiplier circuits over Galois fields F_2^k using a computer-algebra based approach. They also model the verification test as a Null stellensatz proof over F_2^k using a Gobner basis engine. They analyze the verification constraints and derive a term order for efficient Gobner basis computation. Using this approach, they were able to verify the correctness of upto 96-bit multipliers over F_{296}, whereas conventional techniques based on SAT/SMT/BDD solvers are infeasible [2].

Anna Jain et. al. [3] in paper entitled "FPGA Design of a Fast 32-bit Floating Point Multiplier Unit" proposed architecture for a fast 32-bit floating point multiplier compliant with the single precision IEEE 754-2008 standard. This design intends to make the multiplier faster by reducing the delay caused by the propagation of the carry by implementing adders having the least power delay constant. The implementation of the multiplier module has been done in a top down approach. The sub-modules have been written in Verilog HDL and then synthesized and simulated using the Xilinx ISE 12.1 targeted on the Spartan 3E FPGA. We have designed architecture for a fast floating point multiplier based on the IEEE-754 single precision format. The modules are written in Verilog HDL to optimize implementation on any FPGA. The design is done in such a way that the floating point unit can be effectively interfaced with any processor of 32-bit. The main idea is to increase the speed on the multiplier by reducing delay at every stage using the optimal adder design. They plan to extend this work to design a fast floating point arithmetic logic unit [3].

Ramy Raafat et. al. [4] in paper entitled "A Decimal Fully Parallel and Pipelined Floating Point Multiplier" presents a design of Fully Parallel and Pipelined Floating Point Multiplier based on Decimal numbers. Decimal arithmetic is important in several commercial applications including financial analysis, banking, tax calculation, currency conversion, insurance, and accounting. This paper presents a fully parallel Decimal 64 floating point (FP) multiplier compliant to IEEE Std 754-2008 for floating point arithmetic. The proposed multiplier possesses novel methods to target low latency. The proposed design is based on a previously published fixed point multiplier that uses a novel BCD–4221 recoding for decimal digits to improve the area and latency of the partial product generation and the partial product reduction tree. Several enhancements are introduced to the design; the final carry propagation adder is implemented using a fully parallel decimal adder with a Kogge-Stone prefix tree, the sticky bit is generated in parallel to the shifter to reduce the critical path delay. The design is extendable to support Decimal128 floating point multiplication. The multiplier is hardware verified for functionality on an FPGA. Several enhancements are used to improve the latency such as the use of a parallel fixed point multiplier, the generation of the sticky bit in parallel and the use of a fast decimal carry propagation adder. The multiplier has been synthesized 0.18 μm technology and pipelined for different numbers of stages. The multiplier shows very good performance with respect to delay and area. The multiplier has been hardware verified through Altera Cyclone II FPGA testing [4].

Many of the literature reviewed presents a design methodology of a floating point multiplier, Galois field multiplier and theory based on wave pipelining. A design and analysis of Floating point and Galois field multipliers using a pipelining technique called "Wave pipelining" [1], includes designing of floating point multiplier and Galois field multiplier based on wave-pipelining. Formal verification of Galois field multipliers using computer algebra techniques has been done to address the problem of formal verification of hardware implementations of modulo-multipliers over Galois fields of the type F_2^k, using a computer-algebra/algebraic geometry based approach [2]. Architecture for a fast 32-bit floating point multiplier compliant with the single precision IEEE 754-2008 standard to make multiplication faster, the main idea is to increase the speed on the multiplier by reducing delay at every stage using the optimal adder design. They plan to extend this work to design a fast floating point arithmetic logic unit [3]. Fully Parallel and Pipelined Floating Point Multiplier based on Decimal numbers is design for fast speed. The multiplier has been synthesized 0.18 μm technology and pipelined for different numbers of stages. The multiplier shows very good performance with respect to delay and area [4].

III. PROPOSED WORK

Figure 2 shows the block diagram of proposed single precision floating point multiplier. It shows the process of floating point multiplication using IEEE 754 single precision format. The process is carried out as follows; sign bit of both the numbers are added using EX-OR gate. Exponent of both the numbers are added using adders with the logic biased and unbiased. Finally, mantissa bits of both the numbers are multiplied using the multiplier block then the result is normalize, then rounding process will be done. At the last, all the respective results are put into the respective field to achieved final 32-bit floating point multiplication.

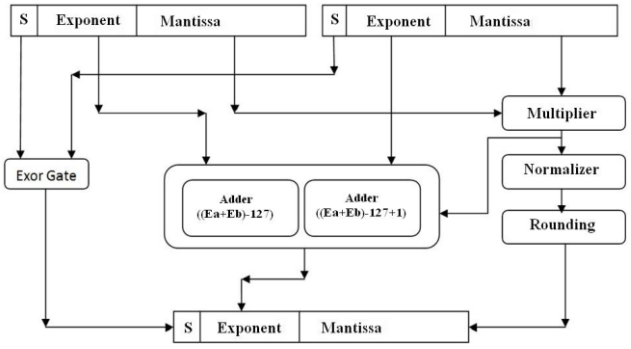

Fig. 2 Block Diagram of Proposed Single Precision Floating Point Multiplier

Figure 3 shows the block diagram of proposed single precision floating point multiplier using wave-pipelining. In this method, there is a buffer circuit between every two stage to increase the driving capacity of the circuit and delay is provided after each and every operation. Using buffer circuit the circuit becomes more efficient in terms of speed, power and delay. The wave pipelining in the Galois field multiplier will be carried by the same approach as floating point multiplier.

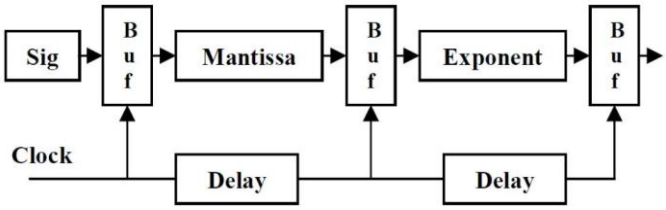

Fig. 3 Block Diagram of Proposed single precision Floating Point Multiplier using Wave-Pipelining [1]

IV. CONCLUSION AND FUTURE SCOPE

In this work, we will use top-down design method in which we will design Floating Point Multiplier and Galois Field Multiplier using Wave-Pipelining and further will be implemented on FPGA kit. VHDL language will be used to describe the system. Wave-Pipelining will be achieved with less clock cycles per operation. Through pipelining, the maximum throughput of operation will be achieved as per design.

The use of VHDL for modelling is especially appealing since it provides a formal description of the system and allows the use of specific description styles to cover the different abstraction levels. The proposed design has been selected by its area, less complicated, less power as well as faster speed. The design can be further implemented for 64-bit i.e. double precision. Hence, a 32-bit Floating Point and Galois Field Multiplier with high speed will be probable outcome of this research work.

REFERENCES

[1] M. Anbuselvi, S. Salivahanan, P. Saravanan, *Design and analysis of Floating point and Galois field multipliers using Wave-pipelining*, 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, 978-0-7695-3915-7/09 $26.00 © 2009 IEEE.

[2] Jinpeng Lv, Priyank Kalla, *FORMAL VERIFICATION OF GALOIS FIELD MULTIPLIERS USING COMPUTER ALGEBRA TECHNIQUES*, 2012 25th International Conference on VLSI Design, 1063-9667/12 $26.00 © 2012 IEEE.

[3] Anna Jain, Baisakhy Dash, Ajit Kumar Panda, Member, IEEE, Muchharla Suresh, Member IEEE, *FPGA Design of a Fast 32-bit Floating Point Multiplier Unit*, 2012 IEEE.

[4] Ramy Raafat, Amira M. Abdel-Majeed, Rodina Samy, *A Decimal Fully Parallel and Pipelined Floating Point Multiplier*, 978-1-4244-2941-7/08/$25.00 ©2008 IEEE.

[5] Donald A. Joy and Maciej J. Ciesielski, *Clock Period Minimization With Wave Pipelining*, IEEE Transaction On Computer Aided Design of Integrated Circuits and Systems, vol.12, No.14 April 1993.

[6] Fabian Klass, Maciji Ciesielski, Wayne P. Burleson and Wental Liu, *Wave –Pipelining: A Tutorial and Research Survey*, IEEE Transactions on Very Large Scale Integration (VLSI) Systems.vol.6, No.3, September 1998.

[7] G.Lakshminarayanan and B.Venkataramanai, *Optimization Techniques for FPGA-Based Wave-pipelined DSP Blocks*, IEEE Transactions on Very Large Scale Integration (VLSI) Systems.vol.13, No.7, July 2005.

[8] Jesus Garcia and Michael J. Schulte, *A COMBINED 16-BIT BINARY AND DUAL GALOIS FIELD MULTIPLIER*, 0-7803-7587-4/02/$17.00 02002 IEEE.

[9] Brian Hickmann, Andrew Krioukov, and Michael Schulte, Mark Erle, *A Parallel IEEE P754 Decimal Floating-Point Multiplier*, 1-4244-1258-7/07/$25.00 ©2007 IEEE.

[10] Eduardo I. Boemo, Sergio L´opez-Buedo, and Juan M. Meneses, *Some Experiments About Wave Pipelining on FPGA's*, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 6, NO. 2, JUNE 1998, 1063–8210/98$10.00 © 1998 IEEE.

[11] Wayne P. Burleson, Member, IEEE, Maciej Ciesielski, Senior Member, IEEE, Fabian Klass, Associate Member, IEEE, and Wentai Liu, Senior Member, IEEE, *Wave-Pipelining: A Tutorial and Research Survey*, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 6, NO. 3, SEPTEMBER 1998, 1063–8210/98$10.00 © 1998 IEEE.

