International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

# Reconfigurable Finite Field Multiplier For Fir Filter Architecture

Ms. G. Vinothini[1], Ms. K. R. S. Deepa[2], Ms. V. Suganyaa[3], Prof. J. Shafiq Mansoor[4]
[1,2,3] Master of Engineering(VLSI DESIGN) , ECE,
[4] Working as Assistant Professor, ECE,
Karpagam University, Coimbatore, Tamil Nadu, India.

***Abstract* - At present scenario, many multipliers based on the Karatsuba-Ofman algorithm (KOA) polynomial based multiplier was proposed that sacrificed time efficiency for low space complexity. In this paper, a new multiplication formula which is a variant of KOA presented. We also provide a straightforward architecture of a non-pipelined bit-parallel multiplier using the new formula. It is further shown that the systolic structure can be decomposed into two or more parallel systolic branches, where the pair of parallel systolic branches has the same input operand, and they can share the same input operand registers. From the application-specific integrated circuit and field-programmable gate array synthesis results we find that the proposed design provides significantly less area-delay and power-delay complexities over the best of the existing designs. The proposed multiplier has lower space complexity than and comparable time complexity to previous Mastrovito multipliers' for all irreducible trinomials and systolic array structure**

***Index Terms— Karatsuba-Ofman algorithm (KOA), non-pipelined bit-parallel multiplier, finite impulse response (FIR) filters, Mastrovito multipliers***

## I. INTRODUCTION

FINITE impulse response (FIR) filters square measure of nice importance in digital signal process (DSP) systems since their characteristics in linear-phase and feed-forward implementations build them terribly helpful for building stable high-performance filters. The transposed-form FIR filter implementations square measure illustrated in Fig. 1(a) though each architectures have similar quality in hardware, the converse kind is usually most popular

because of its higher performance and power potency.The number block of the digital FIR filter in its converse form [Fig. 1(a)], wherever the multiplication of filter coefficients with the filter input is accomplished, has vital impact on the quality and performance of the look as a result of a large number of constant multiplications square measure needed. This is generally called the multiple constant multiplications (MCM) operation and is additionally a central operation and performance bottleneck in several different DSP systems like

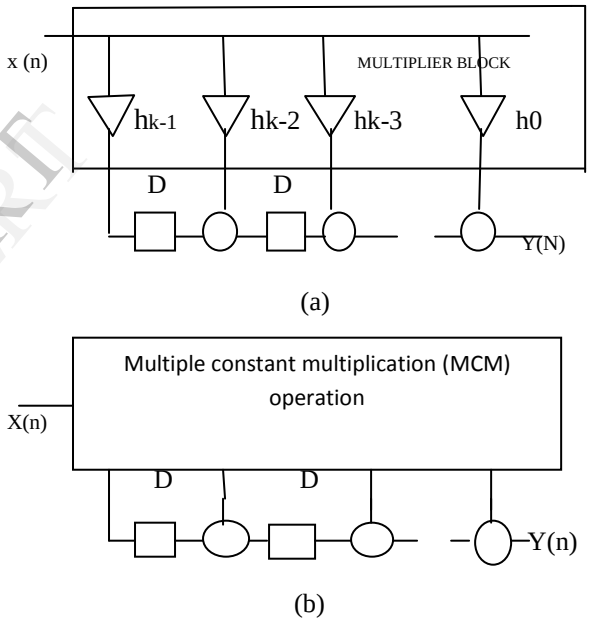


Fig. 1. FIR filter implementations (a) converse kind with generic multipliers. (b) Converse kind with associate degree MCM block.

Fast Fourier transforms, discrete cosine transforms (DCTs), and error-correcting codes. Although area-, delay-, and power-efficient number architectures, such as Wallace and changed Booth multipliers, have been projected, the total flexibility of a number is not necessary for the constant multiplications, since filter coefficients square measure mounted and determined beforehand by the DSP algorithms [1]. Hence, the multiplication of filter coefficients with the input file is usually enforced underneath a shift adds architecture [2], wherever every constant multiplication is realized victimization addition/subtraction associate degreed

shift operations in an MCM operation [Fig. 1(b)].For the shift-adds implementation of constant multiplications , a straightforward methodology, typically called digit based recoding, at the start defines the constants in binary. Then, for every "1" within the binary illustration of the constant, according to its bit position, it shifts the variable and adds up the shifted variables to get the result.

However, the digit-based coding technique doesn't exploit the sharing of common partial merchandise, that permits great reductions within the variety of operations and, consequently in space and power dissipation of the MCM style at the gate level. Hence, the basic improvement downside, called the MCM downside, is outlined as finding the minimum number of addition and subtraction operations that implement the constant multiplications. Note that, in bit-parallel style of constant multiplications, shifts are often completed victimization solely wires in hardware while not representing any space value. The algorithms designed for the MCM downside are often categorized in 2 classes: common sub expression elimination (CSE) algorithms [3]–[4] and graph-based (GB) techniques [5]–[6]. The Communications Security Establishment algorithms at the start extract all potential sub expressions from the representations of the constants when they are outlined below binary, canonical signed digit (CSD), or borderline signed digit (MSD) [3]. Then, they find the "best" sub expression, usually the foremost common, to be shared among the constant multiplications. The GB ways are not restricted to any specific variety illustration and consider a bigger variety of different implementations of a constant, yielding higher solution than the Communications Security Establishment algorithms, as shown in [5] and [6].

However, of these algorithms assume that the input file x is processed in parallel. On the opposite hand, in digit-serial arithmetic, the info words are divided into digit sets, consisting of d bit , that are processed one at a time. Since digit serial operators occupy less space and are freelance of the data word length, digit-serial architectures provide various low complexity designs when put next to bit-parallel architectures. However, the shifts need the employment of D flip-flops, as opposed to the bit-parallel MCM style wherever they're free in terms of hardware. Hence, the high-level algorithms ought to take into consideration the sharing of shift operations furthermore because the sharing of addition/subtraction operations in digit-serial MCM design. Moreover, finding the minimum variety of operations realizing Associate in Nursing MCM operation doesn't perpetually yield Associate in Nursing MCM style with best space at the gate level . Hence, the high-level algorithms ought to think about the implementation cost of every digit-serial operation at the gate level .In this paper, we tend to at the start confirm the gate-level implementation costs of digit-serial addition, subtraction, and left shift operations utilized in the shift-adds style of digit-serial MCM operations. Then, we tend to introduce the precise Communications Security Establishment formula that formalizes the gate-level space improvement problem as a 0–1 whole number applied mathematics (ILP) downside when constants are outlined below a selected variety representation. We tend to additionally gift a brand new improvement model that reduces the 0–1 ILP downside size considerably and, consequently, the runtime of a generic 0–1 ILP thinker. Since there are still instances that the precise Communications Security Establishment formula cannot handle, we tend to describe the approximate GB formula [7] that iteratively finds the "best" partial product that ends up in the optimal space in digit-serial MCM style at the gate level.

Experimental results on a comprehensive set of instances show that the solutions of algorithms introduced during this paper lead to vital enhancements in space of digit-serial MCM designs compared to those obtained victimization the algorithms designed for the MCM downside. The digit-serial FIR filter designs obtained by SAFIR additionally indicate that the conclusion of the multiplier factor block of a digit-serial FIR filter below the shift adds architecture considerably reduces the realm of digit-serial FIR filters with relevance those designed victimization digit-serial constant multipliers. To boot, it's ascertained that the optimal exchange between space and delay in digit-serial FIR filter styles are often explored by dynamical the digit size d.

## II. APPROXIMATE GB ALGORITHM

This algorithm may be a graph-based style methodology which allows common operations like convolution to be enforced victimization reduced numbers of arithmetic operations. This system tries to represent the outputs of the constant multipliers into the graph and whenever it's potential, the technique uses the common components. The primary half is rule and also the second part may be a heuristic methodology. Within the 1st half, if the set of coefficients is totally synthesized, then minimum adder price is gained. The second half uses a look-up table for every constant. The rule primarily consists of the subsequent steps:

- Reduce all coefficients within the set to odd fundamentals.

- Evaluate all single-coefficient prices by victimization the price operation table.

• Remove all cost-0 fundamentals

•Create the graph illustration of elect fundamentals.

Graph-based algorithms area unit bottom-up strategies that iteratively construct the graph representing the multiplier factor block. The graph construction is target-hunting by a heuristic that determines future graph vertex to feature to the graph. Graph-based algorithms supply additional degrees of freedom by not being restricted to a specific illustration of the coefficients, or a predefined graph topology (as in digit-based algorithms), and usually manufacture solutions with the bottom variety of operations. Samples of graph-based algorithms embrace, RAG-n

This paper proposes a replacement graph-based rule. The improvement of gate-level space downside in digit-serial MCM style is associate degree NP-complete downside thanks to the NP-completeness of the MCM downside. Thus, naturally, there'll be perpetually 0–1 ILP issues generated by the precise international intelligence agency rule that current 0–1 ILP solvers notice tough to handle. Hence, the GB heuristic algorithms, that gets decent answer victimization less procedure resources, area unit indispensable. In our approximate rule known as MINAS-DS, as exhausted algorithms designed for the MCM downside given in Definition one, we discover the fewest variety of intermediate constants specified all the target and intermediate constants area unit synthesized employing a single operation. However, whereas choosing associate degree intermediate constant for the implementation of the not yet synthesized target constants in every iteration, we tend to favor the one the potential intermediate constants which will be synthesized victimization the smallest amount hardware and can change United States to implement the not-yet synthesized target constants in a smaller space with the out there constants.

After the set of target and intermediate constants that realizes the MCM operation is found, each constant is synthesized exploitation Associate in Nursing A-operation that yields the minimum area among the digit-serial MCM vogue. In MINAS-DS, the globe of the digit-serial MCM operation is ready as a result of the entire gate-level implementation value of each digit-serial addition, subtraction, and shift operation beneath the digit size parameter d.

## III. FINITE GF (2M) FIELD SUPPORTED PENTANOMIAL

Finite field multipliers over GF(2m) have wide applications in elliptic curve cryptography (ECC) and error management committal to writing systems[8],[9]. Polynomial basis multipliers area unit popularly used as a result of they're comparatively easy to style, and supply quantifiability for the fields of higher orders. Economical hardware style for polynomial-based multiplication is thus necessary for period applications [10], [11].

The pentanomial-based Evariste Galois field is wide used, since the National Institute of Standards and Technology (NIST) has counseled 3 pentanomials for ECC application [12]. There area unit some pulsation realizations of pentanomials-based number for high-throughput implementation [13]–[14]. In a very recent paper [15], Meher has bestowed Associate in nursing economical pulsation style of number supported irreducible pentanomials. it's found that the pulsation structure for field multiplication in [15] incorporates a latency of m cycles.

During this paper, we've got extended the structure of additional to get a lower latency pulsation structure. Initial of all, Associate in nursing economical Montgomery algorithmic rule for pentanomials is planned where the multiplication is rotten into variety of freelance elements that might be processed in parallel. Moreover, we've got introduced a completely unique "pre-computed addition" (PCA) technique such the latency of a number may be reduced additional. The planned structure achieves considerably less time quality than the corresponding existing structures. The rest of the paper is organized as follows: The planned algorithmic rule and therefore the PCA-technique for finite field multiplication GF (2m over supported irreducible pentanomials area unit bestowed in Section II. In Section III, structure of the planned number is delineated. In Section IV, we've got mentioned the estimation of hardware and time-complexities and compared those with those of the prevailing styles. Based on the planned algorithmic rule, we have a tendency to derive here the planned structure of the number.

We've got taken $f(x)=x^{13}+x^4+x^3+x^2+1$ because the irreducible pentanomial for example the planned low latency sys-tolic structure (for*l=1* ). It will but simply be extended to different pentanomials..

From C+ of, similarly, we can get C as

$C^- = (A^{(1)}b_1 + A^{(3)}b_2 + A^{(5)}b_0)$ third unit
$+ A^{(2)}b_5 + A^{(4)}b_3 + A^{(6)}b_1)$ fourth unit

Where c+ and c- is

$$c^- = \sum_{i=1} xi = (x_1+x_{i+1}+\ldots+x_{pi+1}) + \ldots + (x_r+x_{i+r}+\ldots+x_u) + \ldots + (x_i+x_{2i}+\ldots+x_{pi}) \quad \ldots\ldots\ldots 1$$

$$c^+ = \sum_{i=u} Y_i = (Y_u+Y_{1+u}+\ldots Y_{u+Q1}) + \ldots + (Y_{u+t}+Y_{1+u+t}+\ldots+Y_{m-1}) + \ldots +$$

$$(Y_{u+i-1}+Y_{2i+u-1}+\ldots.+Y_{u+qt-1}) \quad \ldots 2$$

For simplicity of dialogue, we've denied the 2 parallel units. Because the third and fourth units, severally, those area unit totally different. Mistreatment the projected PCA technique, one will derive and from and, that involves a delay of solely. each the forward and inverse blocks accommodates 3 major steps, i.e., the proton magnetic resonance operation the bit-multiplica-tion operation, and therefore the bit-addition operation for sys-tolic implementation of multiplication over, the operations of those steps area unit depicted by the SFG, wherever every section (within the dotted box, solely 2 units area unit presented) corresponds to at least one of the units. The first unit consists of three nodes , three bit-mul-tiplication nodes and a pair of bit-addition nodes AD, whereas the second unit has another node , another node and another node The projected systolic-like structure for field multiplication over supported pentanomial (*forl*=1). It consists of 4 heartbeat arrays, wherever every of the arrays correspond to at least one of the units. The primary heartbeat array consists of five PEs, whereas every of the opposite arrays (second, third, and fourth heartbeat arrays) consists of 4 PEs and a delay cell (the delay cell is needed to satisfy the information dependence requirement). Though one will use asystolic adder array consisting of 4 addition cells (ACs) for the ultimate addition of the four arrays, we have a tendency to use a pipelined adder-tree consisting of 3 ACs for a coffee latency implementation.

The four arrays will perform at the same time, such once 5 cycles, the adder-tree receives its initial input and yields its initial output in 2 cycles. The projected style has been coded in VHDL and synthesized by Synopsys style Compiler mistreatment TSMC 90-nm library for together with the simplest of the present designs.The critical-path (CP), space and power consumption (at one hundred Mc frequencies) therefore obtained area unit listed in Table II. The projected style has nearly Sixteen Personality Factor Questionnaire less area-delay product (ADP), 12.5% lower power-delay product (PDP) and forty sixth shorter latency compared to the existing one.

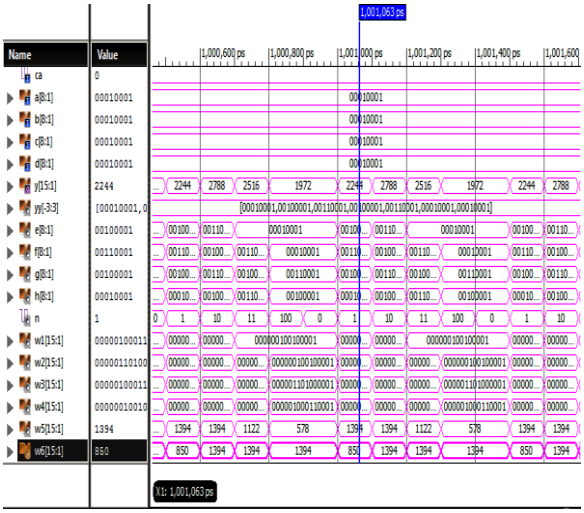

Fig 2 Output waveform for the pentonomial algorithm

From this output waveform the multiplier has less area and less delay because of the same width. So we can reduce the adders and blocks of multipliers. The application of multiplier is error detection and correction

Table-1 gate level results on pentonomials algorithm

| Algorithm | D | 2 | 4 | 8 |
|---|---|---|---|---|
| Graph based Minas-ds | Area($mm^2$) | 86 | 93.4 | 109.2 |
| | Delay(ns) | 4.6 | 5.47 | 7.21 |
| | Power(nw) | 194 | 231 | 312 |
| Irreducible pentanomials | Area($mm^2$) | 72.4 | 81.7 | 98.3 |
| | Delay(ns) | 3.7 | 4.5 | 6.1 |
| | Power(nw) | 190 | 229 | 309 |

## IV. CONCLUSION

The projected style involves considerably less area-delay and power-delay complexities than the fresh according number for irreducible pentanomial, with nearly quartern of the latency of the opposite, for the federal agency suggested pentanomials. Since there are a unit still instances with that the precise CSE algorithmic program cannot cope, we have a tendency to conjointly project AN approximate GB algorithm that finds the simplest partial merchandise in every iteration which yield the optimum gate-level space in digit-serial MCM design. The experimental results indicate that the complexness of digit-serial MCM styles is more reduced mistreatment the high-level optimization algorithms projected during this paper. The application mistreatment of error correction and detection. It is observed that a designer will realize the circuit that matches best in an application by ever-changing the digit size



## REFERENCES

[1] J. McClellan, T. Parks, and L. Rabiner, "A computer program for designing optimum FIR linear phase digital filters," *IEEE Trans. Audio Electroacoust.*, vol. 21, no. 6, pp. 506–526, Dec. 1973.

[2] H. Nguyen and A. Chatterjee, "Number-splitting with shift-and-add decomposition for power and hardware optimization in linear DSP synthesis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 8, no. 4, pp. 419–424, Aug. 2000.

[3] I.-C. Park and H.-J. Kang, "Digital filter synthesis based on minimal signed digit representation," in *Proc. DAC*, 2001, pp. 468–473.

[4] L. Aksoy, E. Costa, P. Flores, and J. Monteiro, "Exact and approximate algorithms for the optimization of area and delay in multiple constant multiplications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 27, no. 6, pp. 1013–1026, Jun. 2008.

[5] Y. Voronenko and M. Püschel, "Multiplierless multiple constant multiplication," *ACM Trans. Algor.*, vol. 3, no. 2, pp. 1–39, May 2007.

[6] L. Aksoy, E. Gunes, and P. Flores, "Search algorithms for the multiple constant multiplications problem: Exact and approximate," *J. Microprocess. Microsyst.*, vol. 34, no. 5, pp. 151–162, Aug. 2010.

[7] L. Aksoy, C. Lazzari, E. Costa, P. Flores, and J. Monteiro, "Efficient shift-adds design of digit-serial multiple constant multiplications," in *Proc. Great Lakes Symp. VLSI*, 2011, pp. 61–66.

[8] *Elliptic Curves in Cryptography*, ser. London Mathematical Society Lecture Note Series. Cambridge, U.K.: Cambridge Univ. Press, 1999

.

[9] "Cryptographic applications of brahmaqupta-bha skara equation,"*IEEE Circuits Syst. I, Reg. Papers*, vol. 53, no. 7, pp. 1565–1571, Jul. 2006

[10] H. Wu, "Bit-parallel polynomial basis multiplier for new classes of finite fields," *IEEE Trans. Comput.*, vol. 57, no. 8, pp. 1023–1031, Aug. 2008.

[11] P. K. Meher, "On efficient implementation of accumulation in finite field over and its applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 4, pp. 541–550, Apr. 2009.

[12] *Digital Signature Standard (DSS)*, FIPS 186–2, National Institute of Standards and Technology, 2000.

[13] T. Zhang and K. K. Parhi, "Systematic design of original and modified mastrovito multipliers for general irreducible polynomials," *IEEE Trans. Comput.*, vol. 50, no. 7, pp. 734–749, Jul. 2001.

[14] C.-Y. Lee, J.-S. Horng, I.-C. Jou, and E.-H. Lu, "A digit-serial multiplier for finite field ," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 4, pp. 476–483, Apr. 2005.

[15] P. K.Meher, "Systolic and non-systolic scalable modular designs of finite field multipliers for reed-solomon codec," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 6, pp. 747–757, Jun. 2009.