Design of Reconfigurable Multipliers Based on High Speed Shannon Adders

Divya Madhuri, Kedhareswarao
Dept. of ECE, Avanthi Institute of Engineering and Technology, Visakhapatnam.

Madhavi Latha
Asst. Prof., Dept. of ECE, GITAM University, Hyderabad.

Bolla Prasad
Asst. Prof., Dept. of EIE, GITAM University, Hyderabad.

Abstract

Multiplication is indeed the most crucial operation in digital signal processing (DSP). Its implementation requires large hardware resources and significantly affects the size, performance, and power consumption of a DSP system. Several DSP algorithms require different types of multiplications, specifically integer or Galois field (GF) multiplication. Since both functions share similarities in their structures, it is better to combine both circuits in a single circuit. In this paper, various types of multipliers for integer and Galois field multiplication will be analyzed and discussed in detail. A comparative study of reference, reconfigurable and proposed high speed Shannon adder based reconfigurable structures is made. Such study shows proposed structures have area savings of up to 11-14% at a marginal reduction in delay and power around 2-3% compare to the conventional adder based reference and reconfigurable structures. From this perspective, function-specific reconfigurable circuits based on high speed Shannon adder can be considered feasible alternatives to standard ASIC solutions.

Keywords: Integer field; Galois field; Reconfigurable multipliers; Shannon adder;

1. Introduction

Extensive digital signal processing (DSP) capabilities are a major characteristic of a large number of System-on-Chip (SoC) designs mainly deployed in embedded systems. DSP applications in SoC's range from audio or video processing to wireless communication. Consequently, various different architecture concepts for their implementation exist ranging from application specific components to embedded reconfigurable [1] hardware or digital signal processors. Each solution represents a specific trade-off between chip area, power consumption, performance, and design effort, currently the most important parameters in SoC design. The focus is on the analysis of multiplier circuits for integer and Galois field arithmetic [2].

Reconfigurability refers to system incorporating some form of hardware programmability that customizes how the hardware is using a number of physical control points. These control points can be changed periodically in order to execute different applications using the same hardware. The technology offers real hardware and software co-design, fast functionality, flexible hardware and high performance.

Integer arithmetic may be essential for instance in filtering algorithms or Fourier transforms, while many algorithms from the communication domain like error correction codes or the widely used Advanced Encryption Standard (AES) [3], Data Encryption Standard (DES) are based on GF arithmetic. Since integer and GF multipliers [4] share numerous similarities in their structures, the potential of efficient methods for integration of both operations in one circuit is provided.

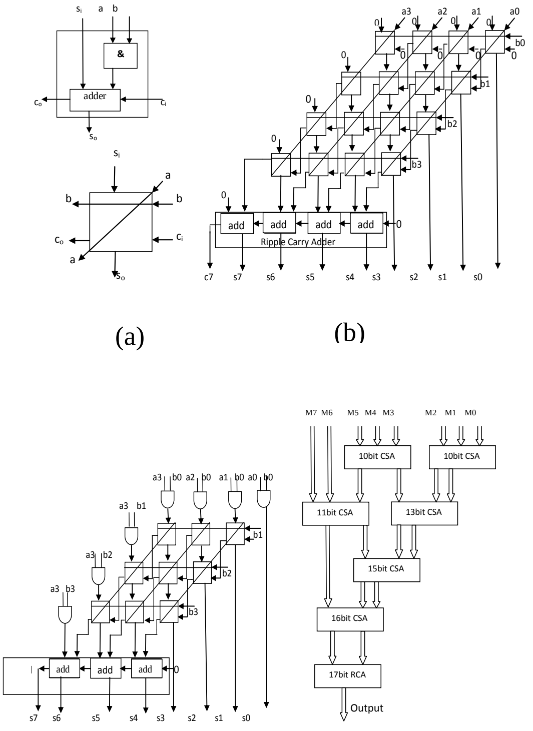
The main involvement of this work is the broad evaluation of design alternatives of parallel integer and GF multipliers, mostly including their combined reference and reconfigurable implementation based on conventional adder and Shannon adder [5], and the complete analysis of their area, delay and power results. The results allow to develop guidelines for designers facing the implementation of high speed circuits for integer and GF multiplication.

The rest of the paper is organized as follows. Section 2 introduces the integer and Galois field multipliers Section 3 specify the combination integer and Galois field multiplies including our proposed model based on high speed Shannon adder. The results from the proposed method and the comparison with the previous versions are given in Section 4. Finally our conclusion is made in Section 5.

2. Integer and Galois field multipliers

2.1. Integer field multipliers

The multiplication of two n-bit numbers will deliver a result of size 2n. An unsigned integer number representation will be used for all integer operations in our operations. They are various types of integer field multipliers are proposed for high speed operations we are considering these three architectures Carry save array (CSA), Braun array (BA) and Wallace tree (WT).



(a) (b)

(c) (d)

Figure 1. (a) Basic cell for integer field multipliers (b) CSA (c) BA (d) WT

The BA architecture is somewhat more optimized modification of the CSA structure. The Wallace tree [8, 9] has a similar structure, but instead of adding the partial products row by row it uses a balanced tree structure to obtain some parallelism and reduce the critical path length. [7]. These structural differences will be important for the later transformation into reconfigurable multipliers.

2.2. Galois binary field (2^m)

As In general, the code with symbols from any Galois field GF(q), where q is prime can be constructed. However, codes with symbols from the binary field GF(2) or its extension GF(2^m) [6] are most widely used in digital data transmission and storage systems because information in these systems is universally coded in binary form for practical reasons. In binary arithmetic, modulo-2 addition and multiplication is used. This arithmetic is actually equivalent to ordinary arithmetic, except that it is considered that 2 to be equal to 0 (i.e., $1 + 1 = 2 = 0$). Note that since $1 + 1 = 0$, $1 = -1$. Hence, in binary arithmetic, subtraction is the same as addition [6].

2.3. Polynomials over finite fields

A primitive polynomial $g(x)$ is used to generate the elements of GF(2^m).
where g_i, $0 \le i \le m$, are the elements of GF(2^m). Addition and multiplication of polynomials follow

$$g\;\; x \;\; = g_0 + g_1x + g_2x^2 + \ldots\ldots.. + g_mx^m$$

standard addition and multiplication rules of ordinary polynomials except that addition and multiplication of the coefficients are done modulo-2. If $g_m = 1$, the polynomial is called monic. If the polynomial of degree m over GF(2^m) cannot be written as the product of two polynomials of lower degrees over the same Galois field, then the polynomial is called irreducible polynomial. For instance, $x^2 + x + 1$ is a irreducible polynomial over GF(2^2) where as x^2+1 is not a irreducible polynomial over GF(2^2) because $x^2 + 1 = (x + 1)^2$. In our analysis a 8-bit Galois field multiplier with irreducible polynomial $x^8 + x^4+x^3+x^2+1=0$ is used.

2.4. Galois field multiplier

Modular Galois field multiplier (MGF) is used in this work. The subsequent GF multipliers are generic in the sense that the generator polynomial p is an extra input, so that the multipliers can be used for any field of the kind GF(2^8). This characteristic is important, since not all DSP algorithms are based on the same Galois fields.

MGF is base on a very natural approach for standard basis multiplication in GF(2^m) is to multiply two elements in the field as polynomial multiplication and modulo reduction with irreducible polynomial as shown in Figure 2.

Let $a(x)$, $b(x)$, $c(x)$ elements in GF(2^m) and $g(x)$ the irreducible polynomial generating GF(2^m). Then the finite field multiplication of $a(x) \times b(x)$ is accomplished by calculating

$$c\;\; x \;\; = \;\; a\;\; x \;\; \times b\;\; x \quad \bmod g\;\; x$$

where × denotes polynomial multiplication. In a first stage the product $a(x) \times b(x)$ is calculated, resulting in a polynomial $q(x)$ of degree at most $2m-2$. In a second stage the modular reduction is performed on $q(x)$, that is $c(x) = q(x) \bmod g(x)$, resulting in the polynomial $c(x)$ of degree at most $m-1$.

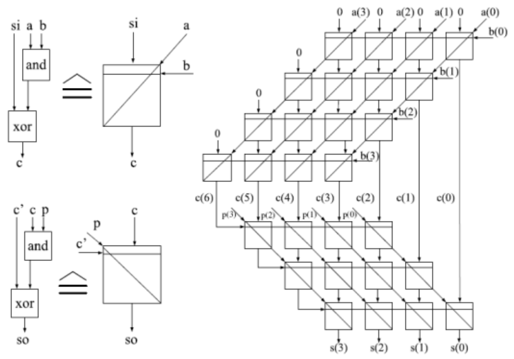


Figure 2. MGF multiplier of 4 × 4 bit

3. Combination of integer and Galois field multipliers

In this paper we are presented three types of design combinations for integer and Galois field (MGF) multipliers including our proposed model. The three different models are described below.

3.1. Reference multipliers

Reference architectures have been constructed as illustrated in Figure 3 by placing a fixed instance of integer and GF multipliers in parallel and selecting the result through a multiplexer. Implementing both multiplication types always introduces a penalty in area, performance and power consumption compared to reference architecture which is a single architecture. Which of these alternatives provides the best efficiency is evaluated in the following Section 4.

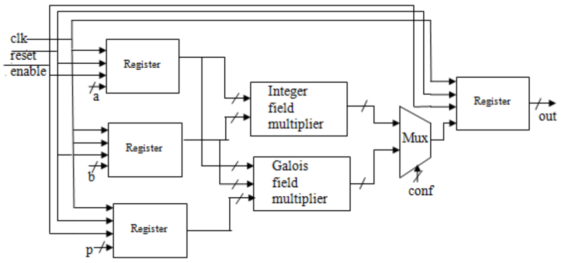
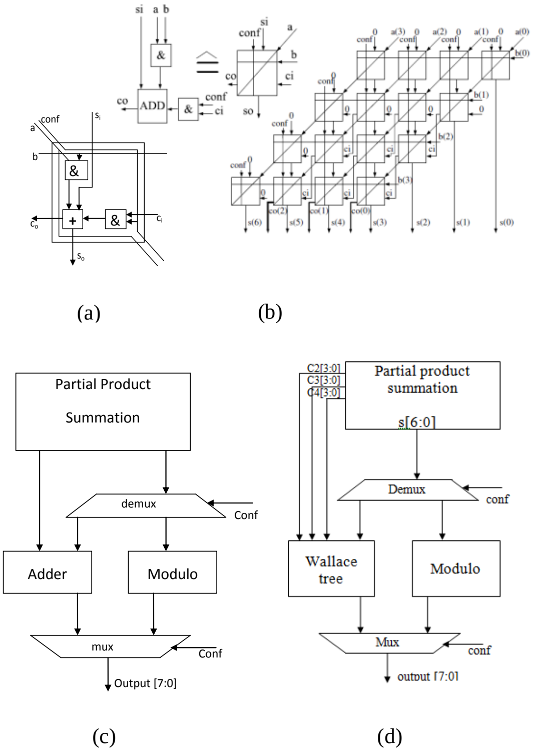


Figure 3. Reference structure

3.2. Reconfigurable multipliers

The design and analysis of three special reconfigurable multiplier architectures that have been constructed based on the integration of MGF multiplier architecture with each of the three integer multiplier architectures. Due to the individual structures of the multipliers, special methods for the combination have been applied, which will be explained in the following.

The technique merges an array structure (CSA and BA) with the MGF architecture. It can be observed that the cells of both the integer and the MGF multipliers share a similar functionality and both contain an AND operation followed by an XOR operation. This is exploited to form a reconfigurable cell usable for both operations, which is depicted in Figure 4. (a) Compared to the original array cell in Figure 1. (a) only one extra gate is necessary. Carry propagation can be disabled for GF multiplication (*conf* = 0) and enabled for integer multiplication (*conf* = 1) by configuring the signal *conf*. The reconfigurable structures are shown in Figure 4.



(a) (b)

(c) (d)

Figure 4. (a) Basic cell (b) Partial product summation (c) CSA&MGF (d) WT&MGF reconfigurable multipliers

3.3. Proposed reconfigurable multipliers based on high speed adders

Reference Multiplication dominates the execution time of most digital signal processing algorithms; therefore, high-speed multiplier is much desired. Adders are the building blocks of the integer multiplication. To reduce the critical path delay in multipliers, it is needed to use high performance adders as building blocks to design reconfigurable multipliers.

Proposed reconfigurable multipliers are designed by high speed Shannon adder and the comparison results with the conventional adder based reconfigurable multipliers will be discussed in Section 4.

3.3.1. Conventional adder

Conventional adder can be implemented by using two half adders and one logic OR gate as shown in the Figure 5 where the sum and carry outputs are generated by

$$Sum = A \oplus B \oplus Cin$$

$$Cout = (A \bullet B) + Cin \bullet (A \oplus B)$$

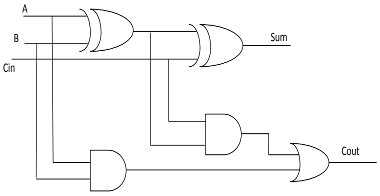


Figure 5. Implementation of full adder using two half adders and one OR gate

3.3.2. High speed Shannon adder

The Shannon theorem states that any logic expression can be expanded into two terms, the first with a particular variable setting a variable to *1*, then multiplying it by the variable and then setting the variable to *0* and multiplying by the inverse. By repeating Shannon theorem for each variable in the expression, the fullest reduction in critical path can be achieved. Shannon theorem, stated in a generalized form, is as follows a function of many variables can be written as the sum of two terms, one with a particular variable (say a_i) set to *0*, and one with it set to *1*.

$$f\ \ a_0,a_1,a_2,\ldots,a_i,\ldots,a_n\ \ =$$

$$\bar{a}_i f\ \ a_0,a_1,a_2,\ldots,0,\ldots,a_n\ \ + a_i f\ \ a_0,a_1,a_2,\ldots,1,\ldots,a_n$$

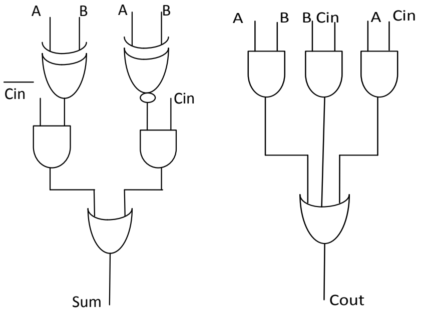


Figure 6. Implementation of full adder using Shannon theorem

4. Results and comparison

Starting with a Verilog HDL circuit description synthesis results are taken from the Xilinx ISE 9.2i and the Simulation results are taken from the Mentor Graphics Model sim 6.5d and the gate level synthesis results were taken from Synopsys Design Compiler C-2009.06-SP4 using SAED 90nm technology library. No hand-optimization has been involved. Thus, it is wanted to ensure that the results can be reproduced easily and that the circuits can be integrated in any system without additional effort for changing an existing design flow.

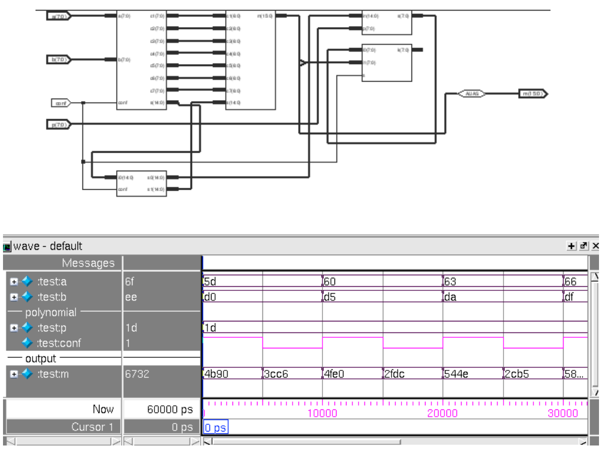
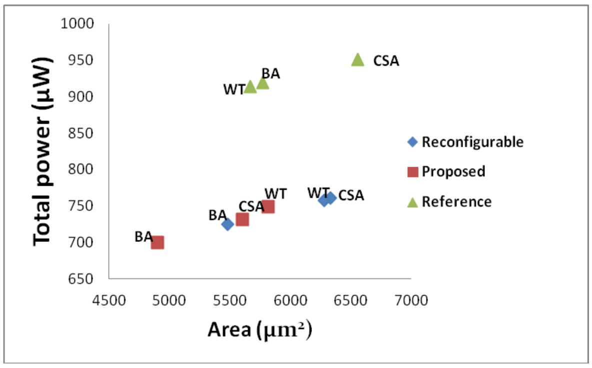


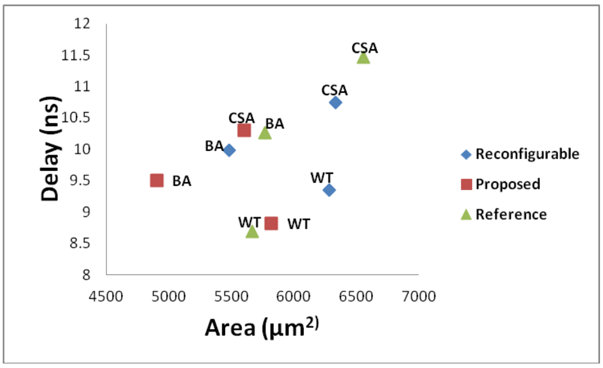
Figure 7. Synthesis and simulation results of WT&MGF reconfigurable multipliers based on Shannon adder

Table 1. Comparison of conventional adder and high speed adder based reconfigurable multipliers

Structure type	Design model	Area (μm^2)	Total power (μW)	Delay (ns)
CSA & MGF	Reference	6559.05	950.7	11.47
	Reconfigurable	6333.13	761.27	10.74
	Proposed	5603.11	731.76	10.3
BA & MGF	Reference	5768.96	919.25	10.26
	Reconfigurable	5480.1	724.29	9.98
	Proposed	4905.14	699.22	9.5
WT & MGF	Reference	5667.41	913.57	8.69
	Reconfigurable	6282.0	757.18	9.35
	Proposed	5819.34	749.31	8.82



(a)



(b)

Figure 8. (a) Area and Total power dissipation (b) Area and Delay comparison graphs for combination of different integer field multipliers with MGF

Reconfigurable architectures turn out to be most recommendable compare to the reference architectures. The BA&MGF architectures require less area around 5480.93µm^2 and less power consumption around 724.29µW than the other reconfigurable structures and the WT&MGF is the most favorable solutions when timing and power constraints are much more important than area constraint and also found that reconfigurable structures using high speed Shannon adder based structures have 10% reduction in area 3-4% less in delay and power values compare to conventional adder based reconfigurable structures.

5. Conclusion

In this paper, performance results for three reference and reconfigurable unsigned integer and GF multipliers are presented. The reconfigurable circuits were constructed based on both high speed Shannon adder and conventional adder in a straightforward way. The effects of special structural particularities of the individual multiplier models on the resulting circuits are analyzed and discussed. An important contribution of this work is the evidence, that function-specific reconfigurable circuits can be constructed which improve three design objectives. This places some of the resulting designs very close to standard ASIC solutions. Precisely, we found that reconfigurable multiplier of BA&MGF achieves small area as well as high speed and low power dissipation.

The study confirms that the design for reconfigurable structures based on high speed adders leads to results improving the design objectives considerably than the conventional adder based structures. In addition, the results highly depend on the quality of the input circuits and on the way they are combined.

References

[1] H. Hinkelmann, Peter Zipf, Jia Li, Guifang Liu, Manfred Glesner, “On the design of reconfigurable multipliers for integer and Galois field multiplication”, *Microprocessors and Microsystems*, Feb 2009, Vol. 33, pp. 2–12.

[2] P. Kitsos, G. Theodoridis, O. Koufopavlou, “An efficient reconfigurable multiplier Architecture for Galois field GF (2^m)”, *Microelectronics Journal*, Oct 2003, Vol. 34, pp. 975–980.

[3] C. Senthilpari, A. K. Singh, K. Diwakar, “Design of a low power, high Performance, 8 × 8 bit multiplier using a Shannon-based adder cell”, *Microelectronics Journal*, May 2008, Vol. 39, pp.812-821.

[5] William Stallings,*Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hall, 2005.

[6] Shu Lin, Daniel J. Costello, *Error Control Coding: Fundamentals and Applications*, Prentice Hall, 1983.

[7] W. Drescher, G. Fettweis, “VLSI architectures for multiplication in GF(2^m) for Application tailored digital signal processors”, *IEEE Workshop on VLSI Signal Processing*, Nov 1996, pp. 55–64.

[8] Raminder Preet Pal Singh, Parveen Kumar, Balwinder Singh, Performance Analysis of 32-Bit Array Multiplier with a Carry Save Adder and with a Carry-Look-Ahead Adder, *IEEE International Journal of Recent Trends in Engineering*, Nov 2009, Vol. 2, No. 6.

[9] C.S. Wallace, “A suggestion for a fast multiplier”, *IEEE Transactions on Electronic Computers*, Dec 1964, Vol. EC-13, pp. 14–17.