Low-Complexity Bit-Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields[1]

Ç. K. Koç and B. Sunar
Electrical & Computer Engineering
Oregon State University
Corvallis, OR 97331, USA
Email: {koc,sunar}@ece.orst.edu

Abstract —

We present a new low-complexity bit-parallel canonical basis multiplier for the field GF(2^m) generated by an all-one-polynomial. The proposed canonical basis multiplier requires $m^2 - 1$ XOR gates and m^2 AND gates. We also extend this canonical basis multiplier to obtain a new bit-parallel normal basis multiplier.

I. Introduction

The arithmetic operations in the Galois field GF(2^m) have several applications in coding theory, computer algebra, and cryptography. In these applications, time and area efficient algorithms and hardware structures are desired for addition, multiplication, squaring, and exponentiation operations. The performance of these operations is closely related to the representation of the field elements. An important advance in this area has been the introduction of the Massey-Omura algorithm [6], which is based on the normal basis representation of the field elements. One advantage of the normal basis is that the squaring of an element is computed by a cyclic shift of the binary representation. Efficient algorithms for the multiplication operation in the canonical basis have also been proposed [5, 3]. The space and time complexities of these bit-parallel canonical basis multipliers are much less than those of the Massey-Omura multiplier.

In this paper [4], we present an alternative design for multiplication in the canonical basis for the field GF(2^m) generated by an all-one-polynomial (AOP). The time complexity of our design is significantly less than similar bit-parallel multiplier designs for the canonical basis [5, 3, 1]. Furthermore, we use the proposed canonical basis multiplier to design a normal basis multiplier, whose space and time complexities are nearly the same as those of the modified Massey-Omura multiplier [2] given for the field GF(2^m) with an AOP. Nevertheless, the proposed normal basis multiplier is based on a different construction from the ones already known, and it has certain advantages.

II. Conclusions

The time complexity of the proposed canonical basis multiplier is significantly less than previously proposed similar multipliers for the field GF(2^m) generated by an AOP. The structure of the canonical basis multiplier is very regular: it consists of $m+1$ identical modules, and some additional XOR and AND gates. It is more regular than the Mastrovito multiplier, and requires significantly less gate delays. The proposed canonical basis multiplier requires m^2 AND gates and $m^2 - 1$ XOR gates.

The normal basis multiplier proposed here and the modified Massey-Omura multiplier [2] require the same number of XOR and AND gates, which is about half of the number of gates required by the Massey-Omura multiplier for the field GF(2^m) with an AOP. Our design [4] requires only 1 more XOR delay than the modified Massey-Omura multiplier. Nevertheless, it is an alternative design, and is based on an entirely different construction. Another advantage is that it is highly modular. Since the proposed normal basis multiplier is based on a canonical basis multiplier, any advances made in canonical basis multiplication using AOPs can be utilized in this design to further reduce the complexity or timing requirements.

Canonical basis multipliers with generating AOPs.

	XOR	AND	Delay
[3]	m^2+2m	m^2+2m+1	$T_A + \lceil \lg m + \lg(m+2) \rceil T_X$
[1]	m^2+m-2	m^2	$T_A + (m + \lceil \lg(m-1) \rceil) T_X$
[4]	m^2-1	m^2	$T_A + (2 + \lceil \lg(m-1) \rceil) T_X$

Normal basis multipliers with generating AOPs.

	XOR	AND	Delay
[6]	$2m^2-2m$	m^2	$T_A + (1 + \lceil \lg(m-1) \rceil) T_X$
[2]	m^2-1	m^2	$T_A + (1 + \lceil \lg(m-1) \rceil) T_X$
[4]	m^2-1	m^2	$T_A + (2 + \lceil \lg(m-1) \rceil) T_X$

References

[1] M. A. Hasan, M. Z. Wang, and V. K. Bhargava. "Modular construction of low complexity parallel multipliers for a class of finite fields GF(2^m)," *IEEE Transactions on Computers*, vol. 41, no. 8, pp. 962-971, August 1992.

[2] M. A. Hasan, M. Z. Wang, and V. K. Bhargava. "A modified Massey-Omura parallel multiplier for a class of finite fields," *IEEE Transactions on Computers*, vol. 42, no. 10, pp. 1278-1280, October 1993.

[3] T. Itoh and S. Tsujii. "Structure of parallel multipliers for a class of finite fields GF(2^m)," *Information and Computation*, vol. 83, pp. 21-40, 1989.

[4] Ç. K. Koç and B. Sunar. "Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields," *IEEE Transactions on Computers*, vol. 47, no. 3, pp. 353-356, March 1998.

[5] E. D. Mastrovito. VLSI architectures for multiplication over finite field GF(2^m). In T. Mora, editor, *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 6th International Conference, AAECC-6*, pp. 297-309, Rome, Italy, July 1988. New York, NY: Springer-Verlag.

[6] J. Omura and J. Massey. "Computational method and apparatus for finite field arithmetic," U.S. Patent Number 4,587,627, May 1986.

[1] This research was supported in part by Intel Corporation.

Proceedings of 1998 IEEE International Symposium on Information Theory,
pages 294-294, MIT, Cambridge, Massachusetts, August 16-21, 1998.