Comm. Korean Math. Soc. **12** (1997), No. 3, pp. 531–538

FAST OPERATION METHOD IN $GF(2^n)$ USING A MODIFIED OPTIMAL NORMAL BASIS

IL-WHAN PARK, SEOK-WON JUNG, HEE-JEAN KIM, JONG-IN LIM

ABSTRACT. In this paper, we show how to construct an optimal normal basis over finite field of high degree and compare two methods for fast operations in some finite field $GF(2^n)$. The first method is to use an optimal normal basis of $GF(2^n)$ over $GF(2)$. In case of $n = st$ where s and t are relatively primes, the second method which regards the finite field $GF(2^n)$ as an extension field of $GF(2^s)$ and $GF(2^t)$ is to use an optimal normal basis of $GF(2^t)$ over $GF(2)$. In section 4, we tabulate implementation result of two methods.

1. Introduction

In many coding, cryptographic and signal processing techniques, it is required to implement finite field arithmetic. The realization of arithmetic operations in these structures, in either hardware or software, can often be made more efficient by an astute choice of field representation and operational algorithm.

Using a polynomial basis, the multiplication of two elements in $GF(2^n)$ is a product of two polynomials modulo an irreducible polynomial. The inverse of an element is easily computed using the Euclid algorithm.

But using a normal basis, the squaring of an element is easily obtained from cyclic shift operation. However new multiplier is needed for a multiplication of elements [4]. In order to effeciently reduce a multiplication complexity, Mullin *et al.* suggested a new concept of optimal normal bases [6].

Received December 11, 1996. Revised May 15, 1997.
1991 Mathematics Subject Classification: Primary : 12Y05.
Key words and phrases: finite fields, normal bases, complexity.
This paper was partially supported by BSRI96-1408.

Recently another fast operation method is suggested [2]. In case of $n = st$ where s and t are relatively primes, $GF(2^n)$ is regarded as a vector space of dimension t over $GF(2^s)$. Each element of $GF(2^n)$ is represented by a polynomial basis which is made by an irreducible polynomial of degree t over $GF(2^s)$. It is called a modified polynomial basis.

In this paper, we use an optimal normal basis instead of a modified polynomial basis. We call it an modified optimal normal basis. We show how to construct an modified optimal normal basis and compare operation speed using an optimal normal basis of $GF(2^{1018})$ with one using an modified optimal normal basis of $GF(2^{8\cdot 113})$.

2. Operation using an optimal normal basis

Let $f(x)$ be a monic irreducible polynomial of degree n over $GF(2)$ and denote it by

$$f(x) = d_0 + d_1 x + \cdots + d_{n-1}x^{n-1} + x^n, \quad \text{where } d_0, d_1, \cdots, d_{n-1} \in GF(2).$$

Then we can construct the finite field $GF(2^n)$ as $GF(2)[x]/(f(x))$. From another point of view, $GF(2^n)$ can be regarded as a vector space of dimension n over $GF(2)$. So there exist bases. Let $\tilde{B} = \{\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\}$ be a basis for $GF(2^n)$ over $GF(2)$. Every element A of $GF(2^n)$ with the representation

$$A = \sum_{i=0}^{n-1} c_i \gamma_i \ , \ c_i \in GF(2)$$

is identified with the vector $A = (c_0, c_1, \cdots, c_{n-1})$.

Now we investigate an addition and a multiplication of two elements of $GF(2^n)$ for some special bases. Let α be a root of an irreducible polynomial $f(x)$. Then $\tilde{C} = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ forms a basis for $GF(2^n)$. It is called a polynomial basis or a canonical basis. Let $A = \sum_{i=0}^{n-1} a_i \alpha^i = (a_0, a_1, \cdots, a_{n-1})$ and $B = \sum_{i=0}^{n-1} b_i \alpha^i = (b_0, b_1, \cdots, b_{n-1})$. Then

$$\begin{aligned} A + B &= \sum_{i=0}^{n-1} (a_i + b_i)\alpha^i \\ &= (a_0 + b_0, a_1 + b_1, \cdots, a_{n-1} + b_{n-1}). \end{aligned}$$

Using the fact that α is a root of $f(x)$, i.e. $d_0+d_1\alpha+d_2\alpha^2+\cdots+\alpha^n=0$, we can obtain

$$\begin{aligned} A \cdot B &= (\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{j=0}^{n-1} b_j\alpha^j) \\ &= \sum_{k=0}^{n-1} c_k\alpha^k. \end{aligned}$$

But this multiplication takes many bit operations. So we introduce the concept of a normal basis in order to reduce the hardware complexity of multiplying field elements. A normal basis in $GF(2^n)$ is a basis $\tilde{N}$ of the form

$$\tilde{N} = \{\beta, \beta^2, \beta^{2^2}, \cdots, \beta^{2^{n-1}}\}$$

It is well known that a normal basis exists in every finite fields [3]. Let $A = \sum_{i=0}^{n-1} a_i\beta^{2^i} = (a_0, a_1, \cdots, a_{n-1})$ and $B = \sum_{i=0}^{n-1} b_i\beta^{2^i} = (b_0, b_1, \cdots, b_{n-1})$. Then

$$A + B = (a_0 + b_0, a_1 + b_1, \cdots, a_{n-1} + b_{n-1}).$$

It has the same complexity as a polynomial basis. But using the fact that $\beta^{2^n} = \beta$, A^2 has the representation $(a_{n-1}, a_0, a_1 \cdots, a_{n-2})$. So squaring of an element needs only one cyclic shift operation.

Let $C = A \cdot B = (c_0, c_1, \cdots, c_{n-1})$ with respect to a basis $\tilde{N}$. Then there exists $\lambda_{ij} \in GF(2)$ such that

$$c_k = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \lambda_{ij} a_{i+k} b_{j+k} \ , \ k = 0, 1, \cdots, n-1 \quad \text{- - - (1)}$$

where the subscripts on a and b are taken modulo n. Thus $c_0 = A\lambda B^T$, $\lambda = (\lambda_{ij})$, B^T is the transpose of B, and remaining coefficients of C can be found using the same matrix but with A and B cyclically shifted. So if the matrix λ has many zero elements, the multiplication of two elements of $GF(2^n)$ is much faster. Define $C_{\tilde{N}}$ by the number of nonzero element of λ which is referred to as the complexity of multiplication with respect to a basis $\tilde{N}$. It is well known fact that $C_{\tilde{N}} \geq 2n - 1$ [6]. In optimal case of $C_{\tilde{N}} = 2n - 1$, a normal basis $\tilde{N}$ is called an optimal normal basis. But it does not always exists for any n. The following two theorems produce optimal normal bases [6].

THEOREM 2.1. *The field $GF(2^n)$ contains an optimal normal basis consisting of the nonunit (n+1)st root of unity if and only if n+1 is a prime and 2 is primitive in Z_{n+1}.*

THEOREM 2.2. *If*
(1) *2 is primitive in Z_{2n+1}, or*
(2) *$2n+1$ is a prime congruent to 3 modulo 4 and 2 generates the quadratic residue in Z_{2n+1},*
then there exists an optimal normal basis in $GF(2^n)$.

Complete computer searches for optimal normal bases in $GF(2^n)$, $2 \leq n \leq 30$ were performed. No other optimal normal bases were found [6]. Gao and Lenstra proved that if n does not satisfy the criteria for the Theorem 2.1 and the Theorem 2.2, then $GF(2^n)$ does not contain an optimal normal basis [1].

3. Operation using a modified optimal normal basis

In case that s and t are relatively primes, we may consider the field $GF(2^n)$ as an extension field of two subfields $GF(2^s)$ and $GF(2^t)$.

LEMMA 3.1. [5] *Let s and t be relatively primes. If $\tilde{B} = \{\alpha_0, \alpha_1, \cdots, \alpha_{t-1}\}$ be a basis for $GF(2^t)$ over $GF(2)$ then $\tilde{B}$ is also a basis for $GF(2^{st})$ over $GF(2^s)$.*

THEOREM 3.1. *Let s and t be relatively primes. If $\tilde{N} = \{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{t-1}}\}$ be a normal basis for $GF(2^t)$ over $GF(2)$, then $\tilde{N}$ is also a normal basis for $GF(2^{st})$ over $GF(2^s)$.*

PROOF. By the Lemma 3.1, it is clear. □

Let $\tilde{N}$ be an optimal normal basis of the form

$$\tilde{N} = \{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{t-1}}\}.$$

Since every multiplication group $GF(2^s)^*$ is cyclic, there exists a generator ξ of $GF(2^s)^*$ (since practically s is small, it is very simple to find a ξ). So every element of $GF(2^s)$ except 0 is represented by ξ^{a_i} for some integer $0 \leq a_i < 2^s$. As a matter of convenience, we denote the zero element of

$GF(2^s)$ by -1. Thus any element A of $GF(2^{st})$ is represented with respect to $\tilde{N}$ by

$$A = \sum_{i=0}^{t-1} z_i \xi^{a_i} \alpha^{2^i}, \quad z_i \in \{0,1\}, \quad 0 \le a_i < 2^s.$$

We denote it by $A = (a_0, a_1, \cdots, a_{t-1})$. If z_i is zero, put -1 in the ith coordinate. ($(-1,-1,\cdots,-1)$ is the zero element of $GF(2^{st})$ over $GF(2^s)$.) So the addition of two elements in $GF(2^{st})$ is reduced the addition of $2t$ elements of $GF(2^s)$. Thus we need the table of addition of elements of $GF(2^s)$. Using an irreducible polynomial which defines $GF(2^s)$, each element ξ^{a_i} can be represented by a polynomial basis. We denote ξ^{a^i} by the extended vector representation $(p_0, p_1, \cdots, p_{s-1}, a_i)$ which consists of the polynomial representation and it's exponent a_i. So the addition table is composed of 2^s rows and $(s+1)$ columns. In order to add two elements of $GF(2^s)$, first find elements of table for two elements, add to use a polynomial basis and find the exponent of an element of the table matching its result.

Using $\xi^{2^s} = \xi$ and $\alpha^{2^t} = \alpha$, we obtain

$$\begin{aligned} A^{2^s} &= (z_0\xi^{a_0}\alpha + z_1\xi^{a_1}\alpha^2 + z_2\xi^{a_2}\alpha^{2^2} + \cdots + z_{t-1}\xi^{a_{t-1}}\alpha^{2^{t-1}})^{2^s} \\ &= z_0\xi^{a_0}\alpha^{2^s} + z_1\xi^{a_1}\alpha^{2^{s+1}} + z_2\xi^{a_2}\alpha^{2^{s+2}} + \cdots + z_{t-1}\xi^{a_{t-1}}\alpha^{2^{s+t-1}} \\ &= (a_{t-s}, a_{t-s+1}, \cdots, a_{t-1-s}). \end{aligned}$$

It is easily computed by s times cyclic shifts. Let $C = AB = (c_0, c_1, \cdots, c_{t-1})$. Then

$$c_k = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} \lambda_{ij} a_{i+k} b_{j+k}, \quad k \equiv 0, s, 2s, \cdots, (t-1)s \bmod t$$

where λ is defined in (1) and the subscripts on a and b are taken modulo t. Since s and t are relatively primes, k varies 0 to $t-1$. So all c_i's are obtained by s times cyclic shifts of A and B.

4. Results of implementation

In this section, we will compare the complexity of $GF(2^{1018})$ with that of $GF(2^{904}) = GF(2^{8\cdot 113})$. By the Theorem 2.1, $GF(2^{1018})$ has an optimal normal basis. This optimal normal basis is generated by α which is a

zero of $f(x) = 1 + x + x^2 + \cdots + x^{1018}$. In order to find the matrix of multiplication, the following two theorems are needed [7].

THEOREM 4.1. *The matrix of multiplication generated by* $f(x) = 1 + x + x^2 + \cdots + x^n$ *has 1's at row* i *and column* j *satisfying*

$$(2^{\overline{i-n/2+1}} + 2^{\overline{j-n/2+1}}) \equiv 0 \text{ or } n \bmod (n+1)$$

where $\bar{i}$ *denote* i *mod* n.

THEOREM 4.2. *For the matrix of multiplication generated by* $f(x) = 1 + x + x^2 + \cdots + x^n$,
(1) *the* $(n-2, n-2)$ *entry is* 1,
(2) *the* (i, i) *entry is* 0 *for* $i \neq n-2$,
(3) *the* $(k, \overline{n/2+k})$ *entry is* 1 *for* $k = 0, 1, \cdots, n-1$,
(4) *the* $(0, n/2-1)$ *entry is* 1,
where $\bar{k}$ *denote* k *mod* n.

Since $GF(2^{1018})$ has an optimal normal basis, the matrix of multiplication has two 1's for each row except the last row(the last row has one 1). We find 1's satisfying the Theorem 4.2 and find remainders to use the Theorem 4.1. Using this matrix, we compute the multiplication of two elements of $GF(2^{1018})$ and an exponentiation of one element of $GF(2^{1018})$.

Let $n = 904 = 8 \cdot 113$, $s = 8$ and $t = 113$. Then $GF(2^{904})$ is regarded as an extension field of $GF(2^8)$ and $GF(2^{113})$. Take a primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^8$, then its root ξ generates $GF(2^8)^*$. By the Theorem 2.2 (1), $GF(2^{113})$ has an optimal normal basis. Let $f(x) = 1 + x + x^2 + \cdots + x^{226}$. If β is its root then $\alpha = \beta + \beta^{-1}$ generates an optimal normal basis of $GF(2^{113})$. This normal basis is also a self-dual normal basis. So the following theorem makes the triangular symmetric matrix $\lambda = (\lambda_{ij})$ of multiplication [7].

THEOREM 4.3. (1) $\lambda_{ij} = Tr(\alpha^{2^i}\alpha^{2^j}\alpha^{2^{n-1}})$,
(2) $\lambda_{i,n-1} = \lambda_{n-1,i} = \delta_{i0}$,
(3) $\lambda_{ij} = \lambda_{(n-1+i-j)(n-j-2)} = \lambda_{(j-i-1)(n-i-2)}$,
where $0 \leq i < j \leq n-1$.

Table 1 shows the comparison of operation speed of the above two cases. It is shown that an operation speed using a modified optimal normal basis is more faster than that using an optimal normal basis. The memory size is almost the same as in the case of a modified optimal normal basis and an optimal normal basis.

	operation speed for $GF(2^{1018})$	operation speed for $GF(2^{904})$	memory size for $GF(2^{1018})$	memory size for $GF(2^{904})$
making matrix	9.66 sec	3 hour 18 min 22.37 sec	$2 \times 1018 - 1$ byte	$2 \times 113 - 1$ byte
one element			1018 byte	113 byte
making addition table		0.02 sec		255×9 byte
multiplication	4.4 sec	0.01 sec		
exponentiation	57.3 sec (exponent is about 2^{25})	0.36 sec (exponent is about 2^{30})		

TABLE 1. Comparison of $GF(2^{1018})$ and $GF(2^{904})$

Note: The time required for making matrix of $GF(2^{904})$ is huge. Since it is a preparation step, it can be negligible for an operation speed.

ACKNOWLEDGEMENTS: We would like to thank the referee for helpful comments.

References

[1] S. Gao and H. Lenstra, *Optimal Normal Bases*, Design. Coded and Cryptography **2** (1992), 315-323.

[2] G. Harper, A. Menezes and S. Vanstone, *Public-key Cryptosystems with very small key lenghths*, Advances in Cryptology - Eurocrypt'92, LNCS 658, Spring-Verlag, 1993.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

[4] J. L. Massey and J. K. Omura, Patent Application of *Computational Method and Apparatus for Finite Field Arithmetic*, submitted in 1981.

[5] A. J. Menezes, *Applications of Finite Fields*, Kluwer Academic Publishers 71-72, 1994.

[6] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone and R. M. Wilson, *Optimal Normal Bases in $GF(p^n)$*, Discrete Applied Math. **22** (1988/89), 149-161, North-Holland.

[7] C. C. Wang, *Exponentiation in Finite Fields*, Univ. of California, Los Angeles, Ph. D., 1985.

Il-Whan Park
Electronics and Telecommunications Research Institute
P.O.Box 106, Yusung Post Office
Taejean 305-600, Korea

Seok-Won Jung and Hee-Jean Kim
Department of Mathematics
Korea University
Seoul 136-701, Korea

Jong-In Lim
Department of Mathematics
Korea University
Choongnam 339-700, Korea