NORMAL AND OPTIMAL NORMAL BASES IN FINITE FIELDS

by
iHSAN TAŞKIN

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University
September 2002

ABSTRACT

Arithmetic operations in finit,e fields have many applications in cryptography, coding theory, and computer algebra. The realization of these operations can often be made more efficient by the normal basis representation of the field elements.

This thesis is aimed at giving a survey of recent results concerning normal bases and efficient ways of multiplication, inversion, and exponentiation when the normal basis representation is used.

ÖZET

Sonlu cisimlerdeki aritmetik işlemlerin kriptografi,kodlama teorisi ve bilgisayar cebirinde birçok uygulaması vardır. Bu işlemlerin gerçeklenmesi, genellikle cisim elemanlanrnn normal baz gösterimi sayesinde daha verimli yapılabilmektedir .

Bu tez,normal bazlar ve normal baz gosterimi kullanılarak yapılan çarpma, ters alma ve üs alma işlemlerinin verimli yollarına dair en son sonuçların incelenerek sunulmasını amaç edinmiştir .

ACKNOWLEDGEMENTS

It is with sincere appreciation that I here express my deepest gratitude to Prof.Dr.S. Alev TOPUZOGLU who expertly and patiently guided my research up to this point and without whom this work would never be finished. I would like to thank my wife for her unfailing support.

I would like to thank to my colleagues at UEKAE for all they have done for me and also thanks to my managers, Önder YETİŞ , Alparslan BABAOĞLU and Murat APOHAN for their patience, support and helps. Finally, I would like to dedicate this thesis to my wife.

TABLE OF CONTENTS
CHAPTER

CHAPTER 1

INTRODUCTION

My thesis consists of five chapters. In the first chapter, we will give some basic definitions, theorems and results related with the normal basis for some finite field. In the second chapter, we will mention the advantages of using normal basis representation and will address some further properties of normal bases which are obtained recently. Moreover, we will give whether there is an advantage of using the pair of dual bases to multiply two elements of finite field. In addition to this, we will examine the complexity of the normal bases for the finite fields $F_{2^{mn}}$ over F_2.

In the third chapter, the concept of optimal normal bases will be introduced. Thus, we will mentione the constructions and types of optimal normal bases over finite fields. It will also be proved in this chapter that all the optimal normal bases in finite fields are completely determined by Theorems 3.1.2 and 3.1.3.

There are many applications of optimal normal bases. In the first section of fourth chapter, we will study a multiplication algorithm by using optimal normal basis and simple permutation of the basis elements. Besides, we will mentione the concept of modified optimal normal bases which also produce efficiency in multiplication. Next, it will be shown that large powers of the generators of optimal normal bases, which have high multiplicative order, can be computed efficiently. Finally, we will give an algorithm finding the multiplicative inverse of a field element efficiently.

In this chapter, we essentially follow the terminology and notation of [20]. F_q denotes the finite field with q elements. A finite extension $F = F_{q^m}$ of the finite

field $K = F_q$ is regarded as a vector space over K. Then F has a dimension m over K, and if $\{\alpha_1, ..., \alpha_m\}$ is a basis of F over K, each element $\alpha \in F$ can be uniquely represented in the form

$$\alpha = c_1\alpha_1 + ... + c_m\alpha_m$$

with $c_j \in K$ for $1 \leq j \leq m$. We introduce a mapping from F to K which we will use frequently.

Definition 1.0.1 *For $\alpha \in F = F_{q^m}$ and $K = F_q$, the Trace function $Tr_{F/K}(\alpha)$ of α over K is defined by $Tr_{F/K}(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{m-1}}$.*

In other words, the trace of α is the sum of the *conjugates* $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ of α with respect to K. Another description of the trace may be obtained as follows. Let $f \in K[x]$ be the *minimal polynomial* of α over K; i.e.; the uniquely determined monic polynomial $f \in K[x]$ generating the ideal $J = \{g \in K[x] : g(\alpha) = 0\}$ of $K[x]$. Then the degree d of f is a divisor of m. The polynomial $g(x) = f(x)^{m/d} \in K[x]$ is called the *characteristic polynomial* of α over K. It is well known (see [20] Theorem 2.14) that, the roots of f in F are given by $\alpha, \alpha^q, ..., \alpha^{q^{d-1}}$, and then this implies that the roots of g in F are precisely the conjugates of α with respect to K. Hence

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 = (x - \alpha)(x - \alpha^q)...(x - \alpha^{q^{m-1}}),$$

and a comparison of coefficients shows that $\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1}$. In particular, $Tr_{F/K}(\alpha)$ is always an element of K.
If $\alpha \in F$ is a root of monic, irreducible polynomial $g(x)$ of degree m, then *trace of* $g(x)$ is defined as the $\mathrm{Tr}_{F/K}(\alpha)$.

The properties of the trace function $\mathrm{Tr}_{F/K}$ are well known. We give them below for the sake of completeness.

Theorem 1.0.2 *Let $K = F_q$ and $F = F_{q^m}$. Then the trace function $Tr_{F/K}$ satisfies the following properties:*

(i) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ for all α, $\beta \in F$;

(ii) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ for all $c \in K$, $\alpha \in F$;

(iii) $Tr_{F/K}$ *is a linear transformation from* F *onto* K*, where both* F *and* K *are viewed as vector spaces over* K*;*

(iv) $Tr_{F/K}(a) = ma$ *for all* $a \in K$*;*

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$ *for all* $\alpha \in F$*.*

Proof. (i) Take any $\alpha, \beta \in F$

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+...+(\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+...+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= Tr_{F/K}(\alpha)+Tr_{F/K}(\beta) \end{aligned}$$

(ii) For $c \in K$ we have $c^{q^j} = c$ for all $j \geq 0$. Hence, we can conclude for any $\alpha \in F$,

$$\begin{aligned} Tr_{F/K}(c\alpha) &= c\alpha+c^q\alpha^q+...+c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha+c\alpha^q+...+c\alpha^{q^{m-1}} \\ &= cTr_{F/K}(\alpha) \end{aligned}$$

(iii) Using first and second properties, together with the fact that $Tr_{F/K} \in K$ for all $\alpha \in F$, show that $Tr_{F/K}$ is a linear transformation from F into K. To prove that this mapping is onto, it suffices then to show the existence of an $\alpha \in F$ with $Tr_{F/K}(\alpha) \neq 0$. Now, $Tr_{F/K}(\alpha) = 0$ if and only if α is a root of the polynomial $x^{q^{m-1}}+...+x^q+x \in K[x]$ in F. However, this polynomial can have at most q^{m-1} roots in F. Indeed, F has q^m elements. Hence there exists an element $\alpha \in F$ such that $\mathrm{Tr}(\alpha)$ is nonzero. Therefore, trace is onto.

(iv)This follows from the definition of the trace function.

(v)Take any $\alpha \in F$. One has $\alpha^{q^m} = \alpha$, and so

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha^q) &= \alpha^q+\alpha^{q^2}+...+\alpha^{q^m} \\ &= \mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

□

Theorem 1.0.3 *Let* F *be a finite extension of the finite field* K*, both considered as vector spaces over* K*. Then the linear transformations from* F *into* K *are exactly the mappings* L_β*,* $\beta \in F$*, where* $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ *for all* $\alpha \in F$*. Furthermore, we have* $L_\beta \neq L_\gamma$ *whenever* β *and* γ *are distinct elements of* F*.*

Proof. Each mapping L_β is a linear transformation from F into K by Theorem 1.0.2(iii). For $\beta, \gamma \in F$ with $\beta \neq \gamma$, we have

$$L_\beta(\alpha) - L_\gamma(\alpha) = Tr_{F/K}(\beta\alpha) - Tr_{F/K}(\gamma\alpha) = Tr_{F/K}((\beta - \gamma)\alpha) \neq 0$$

for suitable $\alpha \in F$ since $\mathrm{Tr}_{F/K}$ maps F onto K, and so the mappings L_β and L_γ are different. If $K = F_q$ and $F = F_{q^m}$, then the mappings L_β produce q^m different linear transformations from F into K. But, every linear transformation from F into K can be obtained by assigning arbitrary elements of K to the m elements of a given basis of F over K. Since this can be done in q^m different ways, the mappings L_β already exhaust all possible linear transformations from F into K.

□

Theorem 1.0.4 *Let F be a finite extension of $K = F_q$. Then for $\alpha \in F$ we have $Tr_{F/K}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in F$.*

Proof. The sufficiency of condition is obvious by Theorem 1.0.2(v). To prove the necessity, suppose $\alpha \in F = F_{q^m}$ with $\mathrm{Tr}_{F/K}(\alpha) = 0$ and β is a root of $x^q - x - \alpha$ in some extension field F. Then $\beta^q - \beta = \alpha$ and

$$\begin{aligned} 0 = Tr_{F/K}(\alpha) &= \alpha + \alpha^q + ... + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + ... + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + ... + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta \end{aligned}$$

so that $\beta \in F$.

□

Let us recall here that the dimension of $F = F_{q^m}$ over $K = F_q$ is called *the degree of the extension*, denoted by $[F : K]$.

Theorem 1.0.5 *Let K be a finite field, let F be a finite extension of K and E a finite extension of F. Then $Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$ for all $\alpha \in E$.*

Proof. Let $K = F_q$, let $[F : K] = m$ and $[E : F] = n$, so that $[E : K] = mn$ by using Theorem 1.84 (in [20]). Then for $\alpha \in E$ we have

$$\begin{aligned} Tr_{F/K}(Tr_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} Tr_{E/F}(\alpha)^{q^i} \\ &= \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \\ &= \sum_{k=0}^{mn-1} \alpha^{q^k} = Tr_{E/K}(\alpha). \end{aligned}$$

□

Definition 1.0.6 *Let K be a finite field and F a finite extension of K. Then two bases $\{\alpha_1, ...\alpha_m\}$ and $\{\beta_1, ..., \beta_m\}$ of F over K are said to be dual bases if for $1 \leq i, j \leq m$ we have*

$$Tr_{F/K}(\alpha_i \beta_j) = \delta_{ij} = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases}$$

Note that, δ_{ij} defined above is called the Kronecker delta function. A basis that is its own dual basis is called a self dual basis. A basis is called weakly self dual, if there exists $\gamma \in F_{q^m}$ and a permutation π of the indices $\{1, 2, ..., m\}$ so that $\beta_i = \gamma \alpha_{\pi(i)}$ for all i, $1 \leq i < m$.

Theorem 1.0.7 *For any basis $\{\alpha_1, ..., \alpha_m\}$ of F over K there exists a unique dual basis $\{\beta_1, ..., \beta_m\}$.*

Proof. If $\{\alpha_1, ..., \alpha_m\}$ is a basis of F over K, we can calculate the coefficients $c_j(\alpha) \in K$, $1 \leq i, j \leq m$, in the unique representation

$$\alpha = c_1(\alpha)\alpha_1 + ... + c_m(\alpha)\alpha_m$$

of an element $\alpha \in F$. We note that $c_j : \alpha \to c_j(\alpha)$ is a linear transformation from F into K, and so according the Theorem 1.0.3, there exists $\beta_j \in F$ such that

$$c_j(\alpha) = Tr_{F/K}(\beta_j \alpha_i)$$

for all $\alpha \in F$. Putting $\alpha = \alpha_i,\ 1 \leq i \leq m$, we see that $\mathrm{Tr}_{F/K}(\beta_j \alpha_i) = 0$ for $i \neq j$ and 1 for $i = j$. Furthermore, $\{\beta_1, ..., \beta_m\}$ is again a basis of F over K, for if

$$d_1\beta_1 + ... + d_m\beta_m = 0$$

with $d_i \in K$ for $1 \leq i \leq m$ then by multiplying by a fixed α_i and applying the trace function $\mathrm{Tr}_{F/K}$, one shows that $d_i = 0$.

Note that the dual basis $\{\beta_1, ..., \beta_m\}$ of a given basis $\{\alpha_1, ..., \alpha_m\}$ is uniquely determined since the elements $\beta_j \in F$ are uniquely determined by the linear transformations c_j according to the Theorem 1.0.3. □ **Example:** Let $\alpha \in F_4$ be a root of the irreducible polynomial $x^2 + x + 1$ in $F_2[x]$. Then $\{\alpha, 1 + \alpha\}$ is a basis of F_4 over F_2. Dual basis of this basis is also itself.

Definition 1.0.8 *Let $K = F_q$ and $F = F_{q^m}$. Then a basis of F over K of the form $\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$, consisting of a suitable element $\alpha \in F$, is called a polynomial basis of F over K. The element α is often taken to be a primitive element of F.*

Definition 1.0.9 *Let $K = F_q$ and $F = F_{q^m}$. A basis of F over K of the form $\{\alpha, \alpha^q, ..., \alpha^{q^{m-1}}\}$, for a suitable element $\alpha \in F$ and its conjugates with respect to K,is called a normal basis of F over K.*

Example: The basis $\{\alpha, \alpha + 1\}$ of F_4 over F_2 is a normal basis of F_4 over F_2 since $1 + \alpha = \alpha^2$.

Theorem 1.0.10 *(Gao 1993) The dual basis of a normal basis is also a normal basis.*

Proof. Let $M = \{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}}\}$ be a normal basis of F_{q^n} over F_q and $N = \{\beta_1, \beta_2, ..., \beta_n\}$ its dual. Let

$$A = \begin{pmatrix} \alpha & \alpha^q & ... & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & ... & \alpha \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \alpha^{q^{n-1}} & \alpha & ... & \alpha^{q^{n-2}} \end{pmatrix}, B = \begin{pmatrix} \beta_1 & \beta_2 & ... & \beta_n \\ \beta_1^q & \beta_2^q & ... & \beta_n^q \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \beta_1^{q^{n-1}} & \beta_2^{q^{n-1}} & ... & \beta_n^{q^{n-1}} \end{pmatrix}.$$

Then $AB = I_n$ and so $BA = I_n$. Observe that

$$(AB)^T = B^T A^T = B^T A = I_n,$$

since A is a symmetric matrix. This means $BA = B^T A = I_n$. Hence $B^T = B$. It follows that $\beta_i = \beta_1^{q^{i-1}}$. Thus N is normal basis.

□

Lemma 1.0.11 *(Artin Lemma). Let $\Psi_1, ..., \Psi_m$ be distinct homomorphisms from a group G into the multiplicative group F^* of an arbitrary field F, and let $a_1, ..., a_m$ be elements of F that are not all 0. Then for some $g \in G$ we have*

$$a_1\Psi_1(g) + ... + a_m\Psi_m(g) \neq 0.$$

Proof. Use induction on m. The case $m = 1$ being trivial. We assume that $m > 1$ and the statement is true for any $m - 1$ distinct homomorphisms. Now take $\Psi_1, ..., \Psi_m$ and $a_1, ..., a_m$ as in the lemma. If $a_1 = 0$, the induction hypothesis immediately produces the result. Thus $a_1 \neq 0$. Suppose we had

$$a_1\Psi_1(g) + ... + a_m\Psi_m(g) = 0 \tag{1.1}$$

for all $g \in G$. Since $\Psi_1 \neq \Psi_m$, there exists $h \in G$ with $\Psi_1(h) \neq \Psi_m(h)$. Then replacing g by hg in (1.1), we get

$$a_1\Psi_1(h)\Psi_1(g) + ... + a_m\Psi_m(h)\Psi_m(g) = 0 \tag{1.2}$$

for all $g \in G$. After multiplication by $\Psi_m(h)^{-1}$ we obtain

$$b_1\Psi_1(g) + ... + b_{m-1}\Psi_{m-1}(g) + a_m\Psi_m(g) = 0$$

for all $g \in G$, where $b_i = a_i\Psi_i(h)\Psi_m(h)^{-1}$ for $1 \leq i \leq m - 1$. By subtracting this identity from (1.1), we arrive

$$c_1\Psi_1(g) + ... + c_{m-1}\Psi_{m-1}(g) = 0$$

for all $g \in G$, where $c_i = a_i - b_i$ for $1 \leq i \leq m - 1$. But $c_1 = a_1 - a_1\Psi_1(h)\Psi_m(h)^{-1} \neq 0$, and we have a contradiction to the induction hypothesis.

□

We want to recall a few concepts and facts from linear algebra.

Definition 1.0.12 *If T is a linear operator on the finite-dimensional vector space V over the arbitrary field K, then a polynomial $f(x) = a_n x^n + ... + a_1 x + a_0 \in K[x]$ is said to annihilate T if $a_n T^n + ... + a_1 T + a_0 I = 0$, where I is the identity operator and 0 is the zero operator on V. The uniquely determined monic polynomial of least positive degree with this property is called the minimal polynomial for T.*

The minimal polynomial for T divides the characteristic polynomial $g(x)$ for T (Cayley Hamilton Theorem), which is given by $g(x) = \det(xI - T)$ and is a monic polynomial of degree equal to the dimension of V.

Definition 1.0.13 *A vector $\alpha \in V$ is called a cyclic vector if the vectors $T^k\alpha$, $k = 0, 1, ...,$ span V.*

Lemma 1.0.14 *Let T be a linear operator on the finite-dimensional vector space V. Then T has a cyclic vector if and only if characteristic and minimal polynomials for T are identical.*

Theorem 1.0.15 *(Normal Basis Theorem). For any finite field K and any finite extension F of K, there exists a normal basis of F over K.*

Proof. Let $K = F_q$ and $F = F_{q^m}$ with $m \geq 2$. From Theorem 2.21 (in [1]) and remarks following it, we know that the distinct automorphisms of F over K are given by $\epsilon, \sigma, \sigma^2, ..., \sigma^{m-1}$, where ϵ is the identity mapping on F, $\sigma(\alpha) = \alpha^q$ for $\alpha \in F$, and a power σ^j refers to the j-fold composition of σ with itself. Because of $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$ for $\alpha, \beta \in F$ and $c \in K$, the mapping σ may also be considered as a linear operator on the vector space F over K. Since $\sigma^m = \epsilon$, the polynomial $x^m - 1 \in K[x]$ annihilates σ. Lemma 1.0.11, applied to $\epsilon, \sigma, \sigma^2, ..., \sigma^{m-1}$ viewed as endomorphisms of F^*, shows that no nonzero polynomial in $K[x]$ of degree less than m annihilates σ. Consequently, $x^m - 1$ is the minimal polynomial for the linear operator σ. Since the characteristic polynomial for σ is a monic polynomial of degree m that is divisible by the minimal polynomial for σ, it follows that the characteristic polynomial for σ is also given by $x^m - 1$. Lemma 1.0.14 implies then existence of an element $\alpha \in F$ such that $\alpha, \sigma(\alpha), \sigma^2(\alpha), ...$ span F. By dropping repeated elements, we see that $\alpha, \sigma(\alpha), \sigma^2(\alpha), ..., \sigma^{m-1}(\alpha)$ span F

and thus form a basis of F over K. Since this basis consists of α and its conjugates with respect to K, it is a normal basis of F over K.

□

CHAPTER 2

NORMAL BASES AND COMPLEXITY

With the development of coding theory and the appearance of several cryptosystems using finite fields, the implementation of finite field arithmetic, in either hardware or software, is needed. These implementations based on finite field multiplications are by the use of normal bases representation. Of course, the advantages of using a normal basis representation has been known for many years. Actually, Hensel [14] noticed the advantage of the normal basis representation in 1888. The complexity of the hardware design of such multiplication schemes is heavily dependent on the choice of the normal bases used [27]. Hence it is essential to find normal bases of "low complexity". This chapter aims at explaining what is meant by complexity of a normal basis.

2.1 A Recent Result on Normal Bases

Before looking at how the addition and multiplication in F_{q^n} can be done, we address some further properties of normal bases which are obtained recently [3]. It is known that when q is a power of a prime p and if either m is a power of p or m itself is a prime different from p having q as one of its primitive roots, then the roots of any irreducible polynomial of degree m and of nonzero trace are linearly independent over F_q. (see [26]) However, converse has been recently proved by Chang, Reed, Truong [3].

Let q be a power of a prime p, and $m \geq 2$ an integer. A monic irreducible

polynomial $f(x) \in F_q[x]$ of degree m is called a *normal polynomial* over F_q if it is a minimal polynomial of a normal element of F_{q^m} over F_q. We know from Chapter 1 that the roots of normal polynomial consist of normal basis elements and the sum of this basis elements is called trace of $f(x)$ which equals to the coefficient of $-x^{m-1}$.

Let q be p^r. Let $m = p^u.k$ with p and k are relatively prime, in F_q, one has

$$x^m - 1 = (x^k - 1)^{p^u} = (h_1(x)...h_t(x))^{p^u}$$

for some distinct irreducible factors $h_i(x) \in F_q[x]$, $i = 1, 2, ..., t$, where $h_1(x) = x-1$. Assume that $h_i(x)$ has degree d_i for $i = 1, 2, ..., t$, and let

$$M_i(x) = (x^m - 1)/h_i(x)$$

for $i = 1, 2, ..., t$. Then $M_1(x) = (x^m-1)/h_1(x) = x^{m-1}+...+x+1$, $M_2(x), ..., M_t(x)$ are the maximal factors of $x^m - 1$, and every proper factor of $x^m - 1$ divides at least one of the these $M_i(x)$'s.

The polynomial $\sum_{i=0}^{n} c_i x^{q^i} \in F[x]$ corresponding with the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$ is called the *linearized* $q-associate$ of $f(x)$ in $F[x]$, denoted by $L_q(f(x))$. A polynomial in $F_q[x]$ is called a $q - polynomial$ over F_q if it is of the form

$$c_n x^{q^n} + ... + c_1 x^q + c_0 x,$$

for some nonnegative integer n and $c_0, c_1, ..., c_n \in F_q$. Two special q-polynomials are used here, namely,

$$L_q(x^m - 1) = x^{q^m} - x,$$

and

$$g_m(x) = L_q(M_1) = L_q(x^{m-1} + ... + x + 1)$$

so $g_m(x) = x^{q^{m-1}} + x^{q^{m-2}} + ... + x^q + x$.

We need the following propositions and lemmas to prove the main result of this section.

Proposition 2.1.1 *(Lidl and Niederreiter) The degree of any irreducible factor of $x^{q^m} - x$ is a divisor of m, and conversely, every monic irreducible polynomial with degree, a divisor of m, is a factor of $x^{q^m} - x$.*

Proof. Assume that $f(x)$ divides $x^{q^m} - x$ where $f(x)$ is an irreducible polynomial in $F_q[x]$. Let α be a root of $f(x)$. Then $\alpha^{q^m} = \alpha$. Hence, $\alpha \in F_{q^m}$. This means $F_q(\alpha) \subseteq F_{q^m}$. Therefore, $\deg(f(x))=[F_q(\alpha) : F_q]$ divides $[F_{q^m} : F_q] = m$ by Theorem 1.84 in [20].

If $\deg(f(x))= n$ divides m, then F_{q^m} contains F_{q^n} as a subfield by Theorem 2.6 in [20]. Hence, $[F_q(\alpha) : F_q] = n$ where α is a root of $f(x)$ and so $F_q(\alpha) = F_{q^n}$. Thus, one has $\alpha \in F_{q^n}$, and $\alpha^{q^m} = \alpha$. This means that $f(x)$ divides $x^{q^m} - x$.

□

Proposition 2.1.2 *(Chang, Truong, Reed and Mullen) Let $f(x) \in F_q[x]$ be a monic irreducible polynomial of degree d, with $d|m$. Then*
(i) $f(x)$ divides $g_m(x)$, if $Tr(f) = 0$.
(ii) $f(x)$ divides $g_m(x)$ if and only if p divides m/d, provided $Tr(f) \neq 0$.

Proof. See [4].

□

Proposition 2.1.2 shows that every monic, trace zero, irreducible polynomial with degree, a divisor of m, is a factor of $g_m(x)$, though its converse is not true.

Corollary 2.1.3 *(i) If m is relatively prime to p, then every irreducible factor of $g_m(x)$ has trace zero.*
(ii) Every m-th degree irreducible factor of $g_m(x)$ has trace zero.

Consider; $r \in F_q$,
$I_q^r(m) =$ *the product of all monic, trace-r, irreducible polynomials in $F_q[x]$ of degree m,*
and
$N_q^r(m) =$ *the number of all monic, trace-r, irreducible polynomials in $F_q[x]$ of degree m,*
We have the following properties of $N_q^r(m)$, which we give without proof and refer the reader to [4].

Proposition 2.1.4 *(Chang, Truong, Reed and Mullen) For any positive integer m and for any nonzero $r \in F_q$ one has*

$$N_q^1(m) = N_q^r(m).$$

Moreover, if m is relatively prime to p, then one has

$$N_q^0(m) = N_q^1(m) = \frac{1}{m}\sum_{d|m}\mu(d)q^{m/d-1},$$

where $\mu(d)$ is

$$\mu(d) = \begin{cases} 1 & if\ n = 1, \\ (-1)^k & if\ d\ is\ the\ product\ of\ k\ distinct\ primes. \\ 0 & if\ d\ is\ divisible\ by\ the\ square\ of\ a\ prime. \end{cases}$$

called Moebius function.

If m is a multiple of p, then for any $r \in F_q$, one has

$$N_q^r(m) = \frac{1}{m}\sum_{\substack{d|m \\ (d,p)=1}}\mu(d)(q^{m/d-1} - \delta_{0r}q^{m/pd}),$$

where δ is the Kronecker delta function.

Now, we can state and prove the main theorem.

Theorem 2.1.5 *(Chang, Truong, Reed 2001) Let q be a power of a prime p and m a positive integer. If every m-th degree irreducible polynomial of nonzero trace is normal over F_q, then m is either a power of p or a prime number different from p that has q as a primitive root.*

Proof.

Let $m = p^u k$ with gcd(p,k) = 1. Suppose the contrary that m is neither a power of p nor a prime number different from p that has q as one of its primitive roots; i.e., m is not a positive integer as assumed in Theorem 2.1.5. Then we show that there exist m-th degree irreducible polynomials of nonzero traces which are not normal over F_q.

Under the above conditions on m, let $h(x)$ be an irreducible factor of $x^m - 1$ other than $x - 1$ but with the smallest degree d. Then $1 \leq d < m - 1$, and

$$M(x) = (x^m - 1)/h(x)$$

is a maximal factor of $x^m - 1$ and $\deg(M(x)) = m - d$. Let $g(x)$ denote the greatest common factor of $M(x)$ and $M_1(x) = x^{m-1} + ... + x + 1$. Then

$$g(x) = (x^m - 1)/((x - 1)h(x)),$$

and the degree of $g(x)$ is $m-(d+1)$. Because $g(x)$ divides $M(x)$, $L_q(g)$ divides $L_q(M)$. Let

$$M^*(x) = L_q(M)/L_q(g).$$

Then $M^*(x)$ and $L_q(g)$ are relatively prime as both $L_q(M)$ and $L_q(g)$ have no repeated factors.

The following lemmas will be used in the proof of Theorem 2.1.5.

Lemma 2.1.6 *(Chang, Reed, Truong) (i) $M^*(x)$ has no irreducible factor of trace zero.*
(ii) Any mth degree irreducible factor of $M^*(x)$ of nonzero trace is not normal.
(iii) $deg(M^*(x)) = (q-1)q^{m-d-1}$.

Proof. (i) When $f(x)$ is an irreducible factor of $M^*(x)$, $f(x)$ divides $L_q(M)$, and the degree of $f(x)$ is a divisor of m by Proposition 2.1.1. When the trace of $f(x)$ is zero, $f(x)$ divides $g_m(x)$ by Proposition 2.1.2 and so $f(x)$ is a factor of $P(x) = \gcd(L_q(M), g_m(x))$ which is a q polynomial. Therefore, $L_q^c(P)$ divides both $M(x)$ and $L_q^c(g_m) = M_1(x)$. This means $L_q^c(P)$ divides $\gcd(M(x), M_1(x)) = g(x)$. This implies that $P(x)$ divides $L_q(g)$. Hence, $f(x)$ is a factor of $L_q(g)$ and so a common factor of $M^*(x)$ and $L_q(g)$, which is a contradiction.
(ii) As $M^*(x)$ divides $L_q(M)$, every factor of $M^*(x)$ has a q polynomial multiple $L_q(M)$, which is not normal.
(iii) $\deg(M^*(x)) = \deg(L_q(M))$-$\deg(L_q(g)) = q^{m-d} - q^{m-d-1} = (q-1)q^{m-d-1}$.

□

Lemma 2.1.7 *(Chang, Reed, Truong) (i) If m is not a prime and θ is the smallest prime factor of m different from p, then*

$$deg(M^*(x)) \geq (q-1)q^{m-\theta}.$$

(ii) If m is a prime number different from p and q not a primitive root of m, then

$$deg(M^*(x)) > (q-1)q^d.$$

Proof. We want to remember the the concept of *cyclotomic polynomial*. The polynomial

$$Q_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \xi^s)$$

is called the *nth cyclotomic polynomial* over the field F where ξ is a primitive n-th root of unity over F and the characteristic of F does not divide n. Then we have $Q_n(x) = \prod_{d|m} Q_d(x) = x^m - 1$ by Theorem 2.45 in [20].

(i) $Q_\theta(x)$ divides $x^m - 1$ as $\theta | m$. Therefore, $d = \deg(h(x)) \leq \deg(Q_\theta(x)) \leq \theta - 1$. Hence, $\deg(M^*(x)) \geq (q-1)q^{m-\theta}$.

(ii) $h(x)$ is a factor of $Q_m(x)$ and $Q_m(x)$ can be factored into $(m-1)/d$ distinct monic irreducible polynomials of the same degree d by Theorem 2.47 in [20]. Since q is not a primitive root of m, $r = (m-1)/d \geq 2$. Hence, $\deg(M^*(x))=(q-1)q^{(m-1)-d} = (q-1)q^{(r-1)d} \geq (q-1)d$.

□

Therefore, Theorem 2.1.5 will be proved once we show that $M^*(x)$ has some mth degree irreducible factors of nonzero trace; by Lemma 2.1.6 (ii) those factors are not normal.

Note that, we can factorize $x^{q^m} - x$ as

$$\begin{aligned} x^{q^m} - x &= \left(\prod_{d|m} I_q^0(d) \right) \cdot \left(\prod_{d|m} \prod_{r \in F_q^*} I_q^r(d) \right) \\ &= \left(\prod_{d|m} I_q^0(d) \right) \cdot \left(\prod_{\substack{d|m \\ (d,p)=1}} \prod_{r \in F_q^*} I_q^r(d) \right) \cdot \left(\prod_{r \in F_q^*} I_q^r(m) \right). \\ &= \text{(I)} \cdot \text{(II)} \cdot \text{(III)} \end{aligned}$$

Since by Lemma 2.1.6(i) each irreducible factor of $M^*(x)$ has a nonzero trace, such a factor must appear in either (II) or (III). If the number of distinct irreducible factors of $M^*(x)$ is more than that in (II), then $M^*(x)$ has at least one factor coming from (III). Since $x^{q^m} - x$ has no repeated factor, $M^*(x)$ also has no repeated factor. Hence, to prove that $M^*(x)$ has more irreducible factors than product (II) is equivalent to showing that the degree of $M^*(x)$, i.e., $(q-1)q^{m-d-1}$, is greater than the degree of (II). In this case, then $M^*(x)$ has at least one factor coming from (III), i.e., an m-th degree irreducible factor $f(x)$ of nonzero trace. According to the Lemma 2.1.6(ii), $f(x)$ is not normal. Hence, we must show $\deg(\text{II}) < \deg(M^*(x))$, and indeed by Lemma 2.1.7 show $\deg(\text{II}) < (q-1)q^{m-\theta}$, where θ is the smallest prime divisor of m.

Observe that, the degree of (III),

$$\deg\left(\prod_{r\in F_q^*} I_q^r(m)\right) = \sum_{r\in F_q^*} deg(I_q^r(m)) = m\cdot\sum_{r\in F_q^*} N_q^r(m)$$

can be simplified. Since by Proposition 2.1.4, the degree of (III) becomes

$$m\cdot\sum_{r\in F_q^*} N_q^1(m) = m\cdot(q-1)\cdot N_q^1(m).$$

Therefore, we can obtain

$$\deg(\text{II}) = q^m - \deg(I) - m(q-1)N_q^1(m).$$

Obviously, we must determine the degree of (I) and the value of $N_q^1(m)$, with both numbers depending on the whether m is relatively prime to p or not.

If m is relatively prime to p, then by Proposition 2.1.2 and Corollary 2.1.3, (I) $= g_m(x)$, and the degree of (I) is q^{m-1}. Indeed, by Proposition 2.1.4

$$N_q^1(m) = \frac{1}{m}\sum_{d|m}\mu(d)q^{m/d-1}.$$

Therefore,

$$\begin{aligned}\deg(\text{II}) &= q^m - \deg(\text{I}) - m(q-1)N_q^1(m)\\ &= \frac{q-1}{q}\left(q^m - \sum_{d|m}\mu(d)q^{m/d}\right).\end{aligned}$$

Using an unpublished result of Chang (see [4]), we can conclude that

$$\deg(\text{II}) < \frac{q-1}{q}\cdot 2\cdot q^{m/\theta} \le (q-1)\cdot q^{m/\theta},$$

where θ is the smallest prime factor of m.

If $m \neq \theta$, then $m-\theta \ge \frac{m}{\theta}$, and so

$$\deg(\text{II}) < (q-1)\cdot q^{m-\theta}.$$

If $m=\theta$ then $\deg(\text{II}) = q-1$ and $\deg(M^*(x)) > q-1$, so, $\deg(\text{II}) < \deg(M^*(x))$.

If m is a multiple of p, e.g., $m = p^u k$, $u \ge 1$, then deg(I) can be determined in the manner shown next. Since

$$(I) = \prod_{d|m} I_q^0(d) = \prod_{i=0}^{u}\left(\prod_{d|k} I_q^0(p^i d)\right),$$

$$\deg(\mathrm{I}) = \sum_{i=0}^{u} \sum_{d|k} deg(I_q^0(p^i d)) = \sum_{i=0}^{u} \sum_{d|k} p^i d \cdot N_q^0(p^i d),$$

It follows that

$$\deg(\mathrm{II}) = q^m - \sum_{i=0}^{u} \sum_{d|k} p^i d \cdot N_q^0(p^i d) - m(q-1)N_q^1(m).$$

To determine the numbers $N_q^0(m)$ and $N_q^1(m)$, we can use the Proposition 2.1.4. The upper bounds for the degree of (II) are obtained in [3]:
If θ is the smallest divisor of k, then

$$(i)\ deg(II) \ < \ 2 \cdot q^{m/\theta} + \frac{q-1}{q} \cdot 2 \cdot q^{m/p}, \tag{2.1}$$

$$(ii)\ deg(II) \ < \ 4 \cdot q^{m/\theta^*},\ where\ \theta^* = min\{p, \theta\}. \tag{2.2}$$

Therefore, we should only treat the cases $p = 2$ and $p \geq 3$. If $p = 2$, then one has $\theta > 2$ and $m \geq 2\theta$. When $m = 2\theta$, use Lemma 2.1.7

$$\deg(M^*(x)) \geq (2-1)2^{2\theta-\theta} = 2^\theta,$$

and using Lemma 2.1.4, we can obtain

$$\deg(\mathrm{II}) < 2^{\theta-1} + 3.$$

This means that $\deg(M^*(x)) - \deg(\mathrm{II}) > 2^{\theta-1} - 3$, so it follows that $\deg(M^*(x)) > \deg(\mathrm{II})$ since $\theta \geq 3$. Otherwise, $m > 2\theta$ and thus $m > 6$. Then by Lemma 2.1(i), one has $\deg(\mathrm{II}) < 2^{m/2+1}$. Since $m > 2\theta$ and m is even, $m - \theta \geq \frac{m}{2} + 1$. Hence,

$$\deg(\mathrm{II}) < 2^{m/2+1} \leq 2^{m-\theta} = (2-1)2^{m-\theta}$$

as required.

If $p \geq 3$, one has by Lemma 2.1(ii) that

$$\deg(\mathrm{II}) < 4 \cdot p^{m/\theta^*} < 2 \cdot p^{m/\theta^*+1}.$$

Since $(m-\theta) - \frac{m}{\theta^*} \geq 1$ for either $\theta^* = p$ or θ, one has finally that

$$\deg(\mathrm{II}) < 2 \cdot q^{m/\theta^*+1} \leq 2 \cdot q^{m-\theta} \leq (q-1) \cdot q^{m-\theta}$$

which proves the Theorem 2.1.5. □

2.2 Arithmetic in Finite Fields and Normal Bases

Let us look at how the addition and multiplication in F_{q^n} can be done in general. We view F_{q^n} as a vector space of dimension n over F_q. Let $\alpha_0, \alpha_1, ..., \alpha_{n-1} \in F_{q^n}$ be linearly independent over F_q. Then every element $A \in F_{q^n}$ can be represented as

$$A = \sum_{i=0}^{n-1} a_i \alpha_i, a_i \in F_q.$$

Recalling that F_{q^n} can be regarded as a vector space over F_q, so, it can be identified as ${F_q}^n$, the set of all n-tuples over F_q, and A can be written as $A = (a_0, a_1, ..., a_{n-1})$. Let $B = (b_0, b_1, ..., b_{n-1})$ be another element in F_{q^n}. Then addition is componentwise and is easy to implement. Multiplication is more complicated. Let $A.B = C = (c_0, c_1, ..., c_{n-1})$. We wish to express the c_i's as simply as possible in terms of the a_i's and b_i's. Suppose

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k, t_{ij}^{(k)} \in F_q. \tag{2.3}$$

Then it is easy to see that

$$c_k = \sum_{i,j} a_i b_j t_{ij}^{(k)} = A T_k B^t, 0 \leq k \leq n-1,$$

where $T_k = (t_{ij}^{(k)})$ is an $n \times n$ matrix over F_q and B^t is the transpose of B. The collection of matrices $\{T_k\}$ is called *multiplication table* for F_{q^n} over F_q.

Observe that the matrices $\{T_k\}$ are independent of A and B. If n is big then this scheme is impractical. Fortunately, there are many available bases of F_{q^n} over F_q. For some bases the corresponding multiplication tables $\{T_k\}$ are simpler than others in the sense that they may have fewer non-zero entries or they may have more regularities so that one may judiciously choose some multiplication algorithm to make a hardware or software design of a finite field for large n. For instance, generalizations [15, 22, 31, 36] of bit-serial multiplication scheme using dual bases are used. However, we give the *Massey Omura Scheme* [21] which uses the symmetry of normal bases.

At this point, we will see the advantage of using normal basis representation. Let $\{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q where $\alpha^{q^i} = \alpha_i$. Then ${\alpha_i}^{q^k} = \alpha_{i+k}$ for any integer k, where indices of α are reduced modulo n. Let us first consider the operation of exponentiation by q.

$$\left(\sum_{i=0}^{n-1} a_i\alpha_i\right)^q = \sum_{i=0}^{n-1} a_i\alpha_{i+1}$$

and

$$\alpha_n = \alpha^{q^n} = \alpha_0.$$

The element A^q has coordinate vector $(a_{n-1}, a_0, a_1, ..., a_{n-2})$. That is, the coordinates of A^q are just a cyclic shift of the coordinates of A, and so the cost of computing A^q is negligible. Computing q-th roots is a cyclic shift in the reverse direction. Consequently, exponentiation using the repeated square and multiply method can be speeded up, especially if $q = 2$. This is very important in the implementation of cryptosystems as the ElGamal cryptosystem [6] and Diffie-Hellman key exchange [5] where one needs to compute large powers of elements in finite fields.

Let the $t_{ij}^{(k)}$ terms be defined by (2.1). Raising both sides of equation to the q^{-l}th power, one finds that

$$t_{ij}^{(l)} = t_{(i-l,j-l)}^{(0)}$$

for any $0 \leq i, j, l \leq n-1$.

Thus each term of C is successively generated by shifting the A and B vectors, and thus C is calculated in n clock cycles. The number of required gates equals the number of non-zero entries in the matrix T_0. Clearly, to aid in implementation, one should select a normal basis such that the number of non-zero entries in T_0 is the smallest possible.

Let

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, 0 \leq i \leq n-1, t_{ij} \in F_q. \tag{2.4}$$

Let $n \times n$ matrix (t_{ij}) be denoted by T. It is easy to prove that

$$t_{ij}^{(k)} = t_{i-j,k-j},$$

for all i, j, k. Therefore, the number of non-zero entries in T_0 is equal to the number of non-zero entries in T. Since the matrices $\{T_k\}$ are uniquely determined by T, we call T the multiplication table of the normal basis N.

Definition 2.2.1 *The number of non-zero entries in T is called the complexity of the normal basis N, denoted by c_N.*

The following theorem gives us a lower bound for c_N.

Theorem 2.2.2 *(Mullin, Onyszchuk, Vanstone 1988) For any normal basis N of F_{q^n} over F_q, $c_N \geq 2n-1$*

Proof. Let $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Then

$$b = \sum_{k=0}^{n-1} \alpha_k = Tr(\alpha) \in F_q.$$

Let

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j.$$

Summing up these equations and comparing the coefficient of α_k we find

$$\sum_{i=0}^{n-1} t_{ij} = \begin{cases} b, & j = 0, \\ 0, & 1 \leq j \leq n-1. \end{cases}$$

Since α is nonzero and $\{\alpha\alpha_i : 0 \leq i \leq n-1\}$ is also a basis of F_{q^n} over F_q, the matrix $T = (t_{ij})$ is invertible. Thus for each j there is at least one nonzero t_{ij}. For each $j \neq 0$, in order for each column j of T to sum to zero there must be at least two nonzero t_{ij}'s. So there are at least $2n-1$ nonzero terms in T, with equality if and only if the element α occurs with a nonzero coefficient in exactly one cross product term $\alpha\alpha_i$ (with coefficient b) and every other member of N occurs exactly two such products, with coefficients that are additive inverses.

□

Let us look at the dual of the normal basis to use the multiplication of the field elements. That is, we want to understand whether there is an advantage of using the dual basis of a normal basis for multiplication or not.

2.3 Complexity of Multiplication with Dual Normal Bases

In this section, the role of dual bases in normal basis multiplication in F_{q^n} is explored. The structure of normal basis multipliers can be made more precise by this approach. In particular, the explicit use of dual normal bases or self dual normal bases do not reduce the complexity of normal basis multiplication [11, 12, 13].

Lemma 2.3.1 *(Geiselmann, Gollmann, 1991) Let* $A = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ *and* $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ *be dual bases of* F_{q^n}*. Then we have for any* $u \in F_{q^n}$

$$u = \sum_{i=0}^{n-1} Tr(\beta_i u)\alpha_i = \sum_{j=0}^{n-1} Tr(\alpha_j u)\beta_j.$$

Proof. Let u be a represented with respect to the basis A by

$$u = \sum_{i=0}^{n-1} u_i \alpha_i.$$

Then

$$\mathrm{Tr}(\beta_k u) = \sum_{i=0}^{n-1} u_i \mathrm{Tr}(\beta_k \alpha_i) = u_k.$$

□

Weakly self dual bases can be characterized by a (pseudo)-symmetry of the representations of the products of basis elements.

Theorem 2.3.2 *(Geiselmann, Gollmann 1991) Let* $A = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ *be a basis of* F_{q^n}*. The following propositions are equivalent:*
(i) The basis A is weakly self dual.
(ii) There exists a permutation π *of indices* $\{0, 1, ..., n-1\}$ *so that*

$$\left(\alpha_k \alpha_{\pi(i)}\right)_j = \left(\alpha_k \alpha_{\pi(j)}\right)_i$$

for all i, j, k, $0 \le i, j, k < n$.

Proof. Let $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ be dual basis of A. Assume that A is weakly self dual. Then, by Lemma 2.3.1,

$$\left(\alpha_k \alpha_{\pi(i)}\right)_j = \mathrm{Tr}(\alpha_k \alpha_{\pi(i)} \beta_j) = \mathrm{Tr}(\alpha_k \alpha_{\pi(i)} \gamma \alpha_{\pi(j)}) = \mathrm{Tr}(\alpha_k \alpha_{\pi(j)} \beta_i) = \left(\alpha_k \alpha_{\pi(j)}\right)_i$$

for all $i, j, k, 0 \le i, j, k < n$. So (ii) holds. Conversely, we get from (ii) for $i = 0$ and for all $j, k, 0 \le j, k < n$, $\mathrm{Tr}(\alpha_k \alpha_{\pi(0)} \beta_j) = tr(\alpha_k \alpha_{\pi(j)} \beta_0)$. Hence

$$tr(\alpha_k(\alpha_{\pi(0)}\beta_j - \alpha_{\pi(j)}\beta_0)) = 0,$$

for all k, $0 \le k < n$.
Then from fact that the number of elements in $\gamma \in F_{q^n}$ such that $\mathrm{Tr}(\gamma) = a$ for every $a \in F_q$ is q^{n-1} implies $\alpha_{\pi(0)}\beta_j = \alpha_{\pi(j)}\beta_0$ and $\beta_j = \gamma \alpha_{\pi(j)}$ with $\gamma = \beta_0/\alpha_{\pi(0)}$.

□

Multiplication is more difficult as the products $\alpha_i\alpha_j$ are, in general, not elements of the normal basis. We know from previous section that, in F_{2^n}, the cost of normal basis multiplication is measured by $\alpha_0\alpha_i$ in the normal basis. Various architectures for normal basis multipliers have been suggested. Multipliers with serial output are derived from the following observations. We get for $u \in F_{q^n}$

$$\{u^{q^i}\}_{n-1} = u_{n-1-i},$$

$0 \leq i < n$.

To obtain $w = u.v$ we thus only require a mapping $F : F_{q^n} \times F_{q^n} \rightarrow F_q$ with $F(u, v) = w_{n-1}$. The remaining coefficients of w follow with

$$w_{n-1-i} = (w^{q^i})_{n-1} = F(u^{q^i}, v^{q^i}).$$

For F_{2^n}, this architecture has become known by the name of its inventors, as the *Massey-Omura* multiplier. We have

$$w_{n-1} = \left(\left(\sum_{i=0}^{n-1} u_i\alpha_i\right)\left(\sum_{j=0}^{n-1} v_j\alpha_j\right)\right)_{n-1} = \sum_{i=0}^{n-1} u_i \sum_{j=0}^{n-1} v_j(\alpha_i\alpha_j)_{n-1}.$$

Using the symbol F also for the symmetric $n \times n$ matrix $F = (\varphi_{ij})$ over F_q, given by

$$\varphi_{ij} = (\alpha_i\alpha_j)_{n-1}, \tag{2.5}$$

we can write $F(u, v)$ as $F(u, v) = \bar{u}.F.\bar{v^t}$, with

$$\bar{u} = (u_0, u_1, ..., u_{n-1})\bar{v} = (v_0, v_1, ..., v_{n-1}) \tag{2.6}$$

where the vector $\bar{v^t}$ is the transpose of $\bar{v}$.

Multipliers with parallel output are based on the following transformations of the product $u.v$

$$\begin{aligned} u.v &= \left(\sum_{i=0}^{n-1} u_i\alpha^{q^i}\right)\left(\sum_{j=0}^{n-1} v_j\alpha^{q^j}\right) \\ &= \sum_{i=0}^{n-1} u_i\left(\alpha.\sum_{j=0}^{n-1} v_j\alpha^{q^{j-i}}\right)^{q^i} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1} u_i \left(\alpha . \sum_{j=0}^{n-1} v_{j+i} \alpha^{q^j} \right)^{q^i} \\
&= \sum_{t=0}^{n-1} u_{n-1-t} \left(\alpha . \sum_{j=0}^{n-1} v_{j-1-t} \alpha^{q^j} \right)^{q^{n-1-t}} .
\end{aligned}
$$

In both equations, the outer index counts time steps while the inner sum represents a power of v that will be replaced at the next time step by its q-th power or its q-th root. At each time step a coefficient of u is read in, the current power of v is multiplied by α and the current coefficient of u. The resulting value is added to the intermediate result. Multiplication is again reduced to computing q-th powers and roots, and multiplication by α. The multiplication $\alpha.v$ can be written as $\bar{v}T\bar{\alpha}^t$, where $T = (t_{ij}), t_{ij} \in F_q$, t_{ij} was defined in the equation 2.4 and

$$\bar{\alpha} = (\alpha_0, \alpha_1, ..., \alpha_{n-1}).$$

We now examine the multiplication matrices F and T. Lemma 2.3.1 gives

$$
\begin{aligned}
F(u,v) = w_{n-1} &= \mathrm{Tr}(\beta_{n-1}.u.v) \\
\varphi_{ij} &= \mathrm{Tr}(\beta_{n-1}\alpha_i\alpha_j) \\
t_{ij} &= \mathrm{Tr}(\beta_j\alpha_0\alpha_i)
\end{aligned}
$$

Theorem 1.0.2(v) implies

$$\mathrm{Tr}(\beta_{n-1}\alpha_i\alpha_j) = \mathrm{Tr}((\beta_{n-1}\alpha_i\alpha_j)^{q^{n-i}}) = \mathrm{Tr}(\beta_{n-i-1}\alpha_0\alpha_{j-i}),$$

and thus

Lemma 2.3.3 *The matrix $F = (\varphi_{ij})$ of the Massey-Omura multiplier and the matrix $T = (t_{ij})$ are related by*

$$\varphi_{ij} = t_{j-i,n-i-1}$$

where indices are computed modulo n.

Let α define a normal basis of F_{q^n}. We know from Theorem 1.0.7 and Theorem 1.0.10 that every normal basis has a dual basis and the dual basis of a normal basis is again a normal basis, generated by some element β. Using this result, we proceed to give a new interpretation of the matrix F of the Massey-Omura multiplier.

Lemma 2.3.4 *(Geiselmann, Gollmann 1991) Let α and β generate a pair of dual normal bases of F_{q^n}. Let the vector $\bar{u}$ and the matrix F be defined (with respect to α) as in equations 2.5 and 2.6 Then the multiplication $\bar{u}.F$ gives the dual basis coefficients of $\beta_{n-1}.u$.*

Proof. The dual basis coefficients of $\beta_{n-1}.u$ are $(\beta_{n-1}.u)_j = \mathrm{Tr}(\alpha_j \beta_{n-1} u)$, hence

$$(\beta_{n-1}.u)_j = \mathrm{Tr}\left(\alpha_j \beta_{n-1} \sum_{i=0}^{n-1} u_i \alpha_i\right) = \sum_{i=0}^{n-1} u_i \mathrm{Tr}(\alpha_j \beta_{n-1} \alpha_i) = \sum_{i=0}^{n-1} u_i \varphi_{ij}.$$

The computation of $\bar{u}.F$ can be seen as the transformation $u \rightarrow \beta_{n-1} u$ with a change of basis representation. The subsequent multiplication $(\bar{u}.F).\bar{v^t}$ is the computation of $\mathrm{Tr}(\beta_{n-1} uv)$, where $\beta_{n-1} u$ and v are given in dual bases.

□

Next we apply Theorem 2.3.2 to normal bases and obtain a simplified proof and extension of a theorem on self-dual normal bases.

Theorem 2.3.5 *(Geiselmann, Gollmann 1991) Let α generate a normal basis N of F_{q^n}. Let the matrix T is the multiplication matrix. Then N is self-dual if and only if T is symmetric and $Tr(\alpha^2) = 1$.*

Proof. We have $t_{ij} = \mathrm{Tr}(\beta_j \alpha_0 \alpha_i)$. Assume first that N is self-dual. Then

$$t_{ij} = \mathrm{Tr}(\beta_j \alpha_0 \alpha_i) = \mathrm{Tr}(\alpha_j \alpha_0 \alpha_i) = \mathrm{Tr}(\beta_i \alpha_0 \alpha_j) = t_{ji},$$

and

$$\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha\beta) = 1.$$

Conversely, assume that T is symmetric. Then

$$t_{n-i,n-i+1} = t_{n-i+1,n-i}$$

and

$$\begin{aligned} t_{n-i,n-i+1} &= \mathrm{Tr}(\beta_{n-i+1} \alpha_0 \alpha_{n-i}) = \mathrm{Tr}(\alpha_i \alpha_0 \beta_1) \\ t_{n-i+1,n-i} &= \mathrm{Tr}(\beta_{n-i} \alpha_0 \alpha_{n-i+1}) = \mathrm{Tr}(\alpha_i \alpha_1 \beta_0) \end{aligned}$$

imply, as in the proof of Theorem 2.3.2, $\alpha_0\beta_1 = \alpha_1\beta_0$ and hence $\beta/\alpha = (\beta/\alpha)^q$. Therefore $\beta = \gamma.\alpha$ with $\gamma \in F_q$. Finally, $\gamma.tr(\alpha^2) = 1$ so $\gamma = 1$ if and only if $\mathrm{Tr}(\alpha^2) = 1$.

□

Theorem 2.3.6 *(Geiselmann, Gollmann 1991) Let N be a normal basis of F_{2^n}. The following statements are equivalent:*

(i) N is self-dual.

(ii) The matrix T is symmetric.

(iii) For all $i > 0$ the number of nonzero entries in the i-th row of T is even.

Proof. We only prove the equivalence of the first and third condition. Consider that $\mathrm{Tr}(\alpha_0\alpha_i)$ is just the i-th coefficient of the representation of α_0 in the dual basis. Therefore

$$\mathrm{Tr}(\alpha_0\alpha_i) = \sum_{j=0}^{n-1} t_{ij}\mathrm{Tr}(\alpha_j) = \sum_{j=0}^{n-1} t_{ij} = |\{j|t_{ij} \neq 0\}| \bmod 2.$$

$|\{j|t_{ij} \neq 0\}| \equiv 0 \bmod 2$ for all $i > 0$ implies $\alpha = \beta$. Conversely, for a self-dual normal basis we have

$$0 = \mathrm{Tr}(\alpha_0\alpha_i) = |\{j|t_{ij} \neq 0\}| \bmod 2.$$

□

Finally, we investigate the potential benefits of employing dual normal basis in a multiplier for F_{q^n}, defining the complexity of normal basis multiplication in previous section.

Let $\alpha \in F_{q^n}$ generate a normal basis and β the respective dual normal basis. Represent u with respect to α and v and $w = u.v$ with respect to β. We get

$$w_{n-1} = \mathrm{Tr}(\alpha_{n-1}.u.v)$$

To take advantage of duality of the bases in computing $\mathrm{Tr}(\alpha_{n-1}.u.v)$, we write $\alpha_{n-1}.u.v$ as the product of two elements represented in dual bases. The two options are $(\alpha_{n-1}u).v$ or $(\alpha_{n-1}v).u$

In the first case, $\alpha_{n-1}u$ has to be given in the basis generated by α and we require the coefficients

$$(\alpha_{n-1}\alpha_j)_i = \mathrm{Tr}(\beta_i\alpha_{n-1}\alpha_j) = \varphi_{n-i-2,j-i-1}.$$

In the second case, $\alpha_{n-1}v$ has to be given in the basis generated by β and we require

$$(\alpha_{n-1}\beta_j)_i = \mathrm{Tr}(\alpha_i\alpha_{n-1}\beta_j) = \varphi_{n-j-2,i-j-1}.$$

In both cases we return to the main problem of normal basis multiplication, i.e. the representation of the elements $\alpha_0\alpha_i$ in the normal basis. If the complexity of multiplication with a pair of dual normal bases is again defined as the number of nonzero coefficients in $(\alpha_{n-1}\alpha_j)_i$ or $(\alpha_{n-1}\beta_j)_i$, then the following theorem holds.

Theorem 2.3.7 *(Geiselmann, Gollmann 1991) The complexity of multiplication with a pair of dual normal bases is the same as the complexity of standard normal basis multiplication.*

2.4 Complexity of Normal Basis for $F_{2^{mn}}$ over F_2

In what follows, we give the relation between the complexities of normal bases for extensions of F_2.

In particular, we study multiplication in fields of the form $F_{2^{mn}}$ where n and m are relatively prime, $m \geq 2$, $n \geq 2$ also. Specifically, we show that normal bases of F_{2^m} and F_{2^n} of respective complexities c_M and c_N can be combined to give a normal bases for $F_{2^{mn}}$ of complexity $c_M c_N$.

Lemma 2.4.1 *Let $m > 1, n > 1$ be two relatively prime integers. Let $B_1 = \{\alpha_i | 0 \leq i \leq m-1\}$ and $B_2 = \{\beta_j | 0 \leq j \leq m-1\}$ be bases, respectively, for F_{2^m} and F_{2^n} over F_2. Then $B = \{\alpha_i\beta_j | 0 \leq i \leq m-1, 0 \leq j \leq m-1\}$ is a basis for $F_{2^{mn}}$ over F_2. Moreover, if B_1 and B_2 are normal bases, then so is B.*

Proof. Let

$$A = \{\sum_i \sum_j a_{ij}\alpha_i\beta_j | a_{ij} \in F_2\},$$

then A is a subring of $F_{2^{mn}}$, hence automatically a subfield, say F_{2^k}. Since $F_{2^n} \subset F_{2^k}$ and $F_{2^m} \subset F_{2^k}$, it follows that $m|k$ and $n|k$, hence $mn|k$ and so $k = mn$. Since dimension of $F_{2^{mn}}$ over F_2 is mn, the result follows.

Next suppose $\alpha_i = \alpha^{2^i}$ and $\beta_j = \beta^{2^j}$ $0 \leq j \leq n-1, 0 \leq i \leq m-1$, then $(\alpha\beta)^{2^k} = \alpha^{2^k}\beta^{2^k}$ where k in α^{2^k} may be reduced modulo m and k in β^{2^k} may be

reduced modulo n. Hence, $(\alpha\beta)^{2^k}$ is of the form $\alpha^{2^i}\beta^{2^j}$, $0 \leq j \leq n-1, 0 \leq i \leq m-1$. To complete the proof, we need only show that the smallest positive integer k for which $(\alpha\beta)^{2^k} = \alpha\beta$ is mn.

If $(\alpha\beta)^{2^k} = \alpha\beta$, then $\alpha^{2^k-1} = (\beta^{-1})^{2^k-1} \in F_2$ since intersections of F_{2^m} and F_{2^n} is F_2. Hence $\alpha^{2^k-1} = \beta^{2^k-1}$ implies that $\beta^{2^k-1} = 1$ and so if M is the order of α, then $M|2^k - 1$. But the smallest positive integer l such that $M|2^l - 1$ is m and so $m|k$. Similarly, we can show $n|k$ and so $mn|k$ and then we are done.

□

Corollary 2.4.2 *(Seguin [28], Semaev [29], Jungnickel [18])Let $mn > 1$, gcd(m, n)=1, $\{\alpha^{2^i}|0 \leq i \leq m-1\}$, $\{\beta^{2^j}|0 \leq j \leq n-1\}$ be normal bases, respectively for F_{2^m} and F_{2^n}. Then $\alpha\beta$ generates a normal basis for $F_{2^{mn}}$ over F_2 with complexity $c_{MN}(\alpha\beta) = c_M(\alpha)c_N(\beta)$.*

Proof. Let

$$\beta^{2^r}\beta^{2^s} = \sum_l \gamma_{r,s}^{(l)}\beta^{2^l}$$

$$\alpha^{2^i}\alpha^{2^j} = \sum_k \lambda_{i,j}^{(k)}\alpha^{2^k}$$

and let $\Lambda_k = (\lambda_{i,j}^{(k)})$, $\Gamma_l = (\gamma_{r,s}^{(l)})$. Multiplying left hand sides of the equations and equating the products, we obtain

$$\begin{aligned}(\alpha\beta)^{2^{u(i,r)}}(\alpha\beta)^{2^{v(j,s)}} &= \alpha^{2^i}\beta^{2^r}\alpha^{2^j}\beta^{2^s} = \sum_k\sum_l \lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}\alpha^{2^k}\beta^{2^l} \\ &= \sum_k\sum_l \lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}(\alpha\beta)^{2^{c(k,l)}}\end{aligned}$$

where $(\alpha\beta)^{2^{u(i,r)}} = \alpha^{2^i}\beta^{2^r}$ etc. Look at the number of ones in the $\lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}$ that occur as i r run over $0, 1, ..., m-1$ and j, s runs over $0, 1, ..., n-1$. But this is the clearly the product of the matrices Λ_k and Γ_l, hence $c_{MN}(\alpha\beta) = c_M(\alpha)c_N(\beta)$. In fact the elements $\lambda_{i,j}^{(k)}\gamma_{r,s}^{(l)}$ define an $mn \times mn$ matrix, which is the usual tensor product of Λ_k and Γ_l.

□

CHAPTER 3

OPTIMAL NORMAL BASES

We recall here that $c_N \geq 2n-1$ for any normal basis N for F_{q^n} over F_q. (Theorem 2.2.2) In view of this fact, normal bases with the smallest complexity are called optimal. In other words,

Definition 3.0.3 *A normal basis N is optimal if $c_N = 2n-1$.*

3.1 Constructions

Theorem 3.1.1 *(Mullin, Onyszchuk, Vanstone 1988) Suppose that F_{p^n} contains $(n+1)$st roots of unity. If the n nonunit roots of unity are linearly independent, then F_{p^n} contains an optimal normal basis.*

Proof. Let β denote a primitive $(n+1)$st root of unity in F_{P^n}. Then the conjugates of β are $\beta^p, \beta^{p^2}, ..., \beta^{p^{n-1}}$. Since $N = \{\beta, \beta^p, \beta^{p^2}, ..., \beta^{p^{n-1}}\}$ is linearly independent , it is a normal basis for F_{p^n}. But N is the set of zeros of

$$p(x) = \frac{x^{n+1}-1}{x-1};$$

that is N is the of n nonunit roots of unity in F_{p^n}. Let $\beta_0 = \beta$, and $\beta_i = \beta^{p^i}$ $i = 1, 2, ..., n-1$. Recall that the number of nonzero terms in the bilinear form for c_0 is also the number of nonzero terms in the expansion of the set $\{\beta_0\beta_i : i = 0, 1, .., n-1\}$ in the basis N. But if $\beta_i \neq \beta_0^{-1}$, then $\beta_0\beta_i = \beta_j$ for some exponent j

(depending on i) whereas

$$\beta_0\beta_0^{-1} = \sum_{i=0}^{n-1} \beta_i.$$

Hence there are $2n-1$ nonzero terms in the expansion, and N is optimal.

□

Theorem 3.1.2 *(Mullin, Onyszchuk, Vanstone, Wilson, 1988, [24]) The field F_{p^n} contains an optimal normal basis consisting of the nonunit $(n+1)$st roots of unity if and only if $n+1$ is a prime and p is primitive in Z_{n+1}.*

Proof. If $n+1$ is a prime, then $n+1$ divides p^n-1 and F_{p^n} contains a primitive $(n+1)$st root of unity β. Since p is primitive in Z_{n+1}, the minimal polynomial of β is

$$\frac{x^{n+1}-1}{x-1}$$

and the nonunit $(n+1)$st roots are linearly independent. Conversely if these roots are independent in F_{p^n} then p has order n modulo $n+1$ and $n+1$ is prime.

□

Theorem 3.1.3 *(Mullin, Onyszchuk, Vanstone, Wilson, 1988, [24]) If either*

(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 residues in Z_{2n+1},

then there exists an optimal normal basis in F_{2^n}.

Proof. Since $2n+1|2^{2n}-1$, there exists a primitive $2n+1$st root of unity, β in F_{2^n}. Let $\gamma = \beta + \beta^{-1}$.
Since $2^n \equiv \pm 1 \bmod (2n+1)$, either $\beta^{-1} = \beta^{2^n}$ or $\beta = \beta^{2^n}$. Now

$$\gamma^{2^n} = (\beta+\beta^{-1})^{2^n} = \beta^{2^n} + \beta^{2^{-n}} = \beta + \beta^{-1} = \gamma.$$

Hence, γ is an element of F_{2^n}. Our claim is:

$$N = \{\gamma, \gamma^2, ..., \gamma^{2^{(n-1)}}\}$$

is an optimal normal basis of F_{2^n}. If

$$\sum_{i=0}^{n-1} \lambda_i \gamma^{2^i} = 0,$$

then

$$\sum_{i=0}^{n-1} \lambda_i(\beta^{2^i} + \beta^{2^{-i}}) = 0$$

Now since either 2 is a generator of the multiplicative group of $Z_{(2n+1)}$ or 2 generates the quadratic residues of $Z_{(2n+1)}$ with $2n+1 \equiv 3 \bmod 4$

$$\sum_{i=0}^{n-1} \lambda_i(\beta^{2^i} + \beta^{2^{-i}}) = \left(\sum_{i=0}^{n-1} \lambda_i \beta^{2^i}\right) + \left(\sum_{i=0}^{n-1} \lambda_i \beta^{2^{-i}}\right) = \sum_{j=1}^{2n} u_j \beta^j$$

where each λ_i occurs in $\{u_1, u_2, ..., u_{2n}\}$. Therefore β is the zero of the polynomial

$$f(X) = \sum_{i=0}^{2n-1} u_{j+1} X^i.$$

Since $f(\beta)$=0, the minimal polynomial of β, $m_\beta(X)$, divides $f(X)$. If hypothesis (1) holds then

$$m_\beta(X) = 1 + X + X^2 + ... + X^{2n}.$$

Since $m_\beta(X)|f(X)$ we conclude that $f(X) = 0$ and all $\lambda_i = 0$. If hypothesis (2) holds then $m_\beta(X)$ has degree n as does $m_{\beta^{-1}}(X)$ and

$$X^{2n+1} - 1 = (X-1)m_\beta(X)m_{\beta^{-1}}(X).$$

But $m_\beta(X)|f(X)$ since $f(\beta) = 0$ and $m_{\beta^{-1}}(X)|f(X)$ since $f(\beta^{-1}) = 0$ and hence, $1+X+X^2+...+X^{2n}|f(X)$ implying that $f(X) = 0$ and that all $\lambda_i = 0$. Therefore, N is a normal basis for F_{2^n}. The cross product terms are

$$\begin{aligned} \gamma^{2^i}\gamma^{2^j} &= (\beta^{2^i} + \beta^{2^j})(\beta^{2^{-i}} + \beta^{2^{-j}}) \\ &= (\beta^{2^i+2^j} + \beta^{-(2^i+2^j)}) + (\beta^{(2^i-2^j)} + \beta^{-(2^i+2^j)}). \end{aligned}$$

Now 2 is primitive modulo $2n+1$ then each nonzero residue has the form 2^k for some integer k satisfying $0 \le k \le 2n-1$, whereas if 2 generates the quadratic residues modulo $2n+1$ and $2n+1$ is congruent to 3 modulo 4, then each nonzero residue has the form of either 2^k or -2^k for some integer k satisfying $0 \le k \le n-1$. Therefore if $2^i \neq 2^j \bmod(2n+1)$ then there exist integers k_1 and k_2 such that

$$2^i + 2^j = \pm 2^{k_1}$$

and

$$2^i - 2^j = \pm 2^{k_2}$$

for at least one choice of the + or - sign in each case. In this event,

$$\gamma^{2^i}\gamma^{2^j} = \gamma^{2^{k_1}} + \gamma^{2^{k_2}}.$$

But, if $2^i = \pm 2^j$, then one of $2^i + 2^j$ is not zero modulo $2n+1$, and so there exists a k such that at least one of the equations

$$\begin{aligned} 2^i + 2^j &= 2^k, \\ 2^i + 2^j &= -2^k, \\ 2^i - 2^j &= 2^k, \\ 2^i - 2^j &= -2^k \end{aligned}$$

is satisfied. In this case, since we are in the field of characteristic 2,

$$\gamma^{2^i}\gamma^{2^j} = \gamma^{2^k}.$$

Let $\gamma_i = \gamma^{2^i}$ for $i = 1, ..., n-1$. Then, since $\gamma_0^2 = \gamma_1$, there at most $2n-1$ terms in the expansion of the set $\{\gamma_0, \gamma_i\}$ in terms of the basis N, and so there are precisely $2n-1$ such terms and N is an optimal normal basis.

□

Definition 3.1.4 *Let $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ be a normal basis of F_{q^n}. Let $\alpha_i = \alpha^{q^i}$ for $i = 1, ..., n-1$. The basis N will be said to be type-I if with the exception of one value of i, there exists an integer k_i satisfying $0 \leq k_i \leq n-1$ such that $\alpha_0\alpha_i = \alpha_{k_i}$. The basis N is said to be of type-II if, for every i satisfying $1 \leq i \leq n-1$, there exists integers k_i and m_i such that*

$$\alpha_0\alpha_i = \alpha_{k_i} + \alpha_{m_i}.$$

Therefore, every optimal basis obtained from using Theorem 3.1.1 is a type-I basis, and every optimal normal basis constructed by the methods of Theorem 3.1.3 is a type-II basis.

Lemma 3.1.5 *(Ash, Vanstone, Blake, 1989, [1]) Let k and n be integers such that $nk+1$ is a prime, and let the order of q modulo $nk+1$ be e. Suppose that $gcd(nk/e, n) = 1$. Let τ be a primitive k-th root of unity in Z_{nk+1}. Then every nonzero element r in Z_{nk+1} can be written uniquely in the form*
$r = \tau^i q^j$, $0 \leq i \leq k-1$, $0 \leq j \leq n-1$.

Proof. Let $e_1 = nk/e$. There is a primitive element g in Z^*_{nk+1} such that $q = g^{e_1}$. As the order of g is nk and the order of τ is k, there is an integer a such that

$$\tau = g^{na}, \gcd\,(a, k) = 1.$$

Suppose that there are $0 \leq i, s \leq k-1$, $0 \leq j, t \leq n-1$, such that

$$\tau^i q^j \equiv \tau^s q^t (\mathrm{mod}\ nk+1),$$

i.e.,

$$\tau^{i-s} \equiv q^{t-j} (\mathrm{mod}\ nk+1)$$

$$g^{na(i-s)} \equiv g^{e_1(t-j)} (\mathrm{mod}\ nk+1).$$

Then

$$na(i-s) \equiv e_1(t-j) (\mathrm{mod}\ nk).$$

As gcd(n,e_1)=1, the last equation implies that $n|(t-j)$. Hence $t = j$. Thus,

$$a(i-s) \equiv 0 (\mathrm{mod}\ k).$$

But gcd(a, k)=1, so $k|(i-s)$. Therefore $i = s$. This proves that

$$\tau^i q^j (\mathrm{mod}\ nk+1),\ i = 0, 1, ..., k-1;\ j = 0, 1, ..., n-1$$

are all distinct. As $\tau^i q^j$ not congruent to 0 modulo $nk+1$, every nonzero element in Z_{nk+1} can be expressed uniquely in the required form.

□

Theorem 3.1.6 *(Wassermann 1989, [37]) Let q be a prime or prime power, and n and k be positive integers such that $nk+1$ is a prime not dividing q. Let β be a primitive $nk+1$th root of unity in $F_{q^{nk}}$. Suppose that gcd(nk/e,n)=1 where e is the order of q modulo $nk+1$. Then, for any primitive k-th root of unity τ in Z_{nk+1},*

$$\alpha = \sum_{i=0}^{k-1} \beta^{\tau^i}$$

generates a normal basis of F_{q^n} over F_q with complexity at most $(k+1)n-k$, and at most $kn-1$ if $k \equiv 0$ (mod p), where p is the characteristic of F_q.

Proof. We first prove that $\alpha \in F_{q^n}$. Since $q^{nk} \equiv 1 \pmod{nk+1}$, q^n is a k-th root of unity in Z_{nk+1}. Thus there is an integer m such that $q^n = \tau^m$. Then

$$\alpha^{q^n} = \sum_{i=0}^{k-1} \beta^{\tau^i q^n} = \sum_{i=0}^{k-1} \beta^{\tau^{i+m}} = \sum_{i=0}^{k-1} \beta^{\tau^i} = \alpha.$$

Therefore α is in F_{q^n}.

We next prove that $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ are linearly independent over F_q. Suppose that

$$\sum_{i=0}^{n-1} \lambda_i \alpha^{q^i} = \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} = 0, \ \lambda_i \in F_q.$$

Note that there exist unique $u_i \in F_q$, $i = 1, 2, ..., kn$ such that the following holds for all $2n+1$-th roots γ of unity:

$$\sum_{i=0}^{n-1} \sum_{j=0}^{k-1} \lambda_i \gamma^{\tau^i q^j} = \sum_{j=1}^{nk} u_j \gamma^j = \gamma \sum_{j=0}^{nk-1} u_{j+1} \gamma^j,$$

since, by Lemma 3.1.5, $\tau^i q^j$ modulo $nk+1$ runs through Z^*_{nk+1} for $j = 0, 1, ..., k-1$ and $i = 0, 1, ..., n-1$. Let

$$f(x) = \sum_{j=0}^{nk-1} u_{j+1} x^j.$$

For any $1 \le r \le nk$, there exist integers u and v such that $r = \tau^u q^v$. As β^r is also a $nk+1$-th primitive root of unity,

$$\begin{aligned} \beta^r f(\beta^r) &= \sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} (\beta^r)^{\tau^j q^i} = \sum_{i=0}^{n-1} \lambda_i \left(\sum_{j=0}^{k-1} \beta^{\tau^{u+j} q^i} \right)^{q^v}, \\ &= \left(\sum_{i=0}^{n-1} \lambda_i \sum_{j=0}^{k-1} \beta^{\tau^j q^i} \right)^{q^v} \\ &= 0. \end{aligned}$$

Therefore β^r is a root of $f(x)$ for $r = 1, 2, ..., nk$, hence

$$\prod_{r=1}^{nk} (x - \beta^r) = \frac{x^{nk+1} - 1}{x - 1} = x^{nk} + ... + x + 1$$

divides $f(x)$. But $f(x)$ has degree at most $nk-1$, and so this is impossible. Thus $\alpha, \alpha^q, ..., \alpha^{q^{n-1}}$ must be linearly independent over F_q, and thus form a normal basis of F_{q^n} over F_q.

Next we compute the multiplication table of this basis. Note that for $0 \le i \le n-1$,

$$\alpha \cdot \alpha^{q^i} = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u + \tau^v q^i} = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u (1 + \tau^{v-u} q^i)} = \sum_{v=0}^{k-1} \left(\sum_{u=0}^{k-1} \beta^{\tau^u (1 + \tau^v q^i)} \right).$$

There is a unique pair (v_0, i_0), $0 \le v_0 \le k-1,\ 0 \le i_0 \le n-1$ such that

$$1 + \tau^{v_0} q^{i_0} \equiv 0 (\text{mod } nk+1).$$

If $(v,i) \neq (v_0, i_0)$, then $1 + \tau^v q^i \equiv \tau^w q^j \pmod{nk+1}$, for some $0 \le w \le k-1,\ 0 \le j \le n-1$, and

$$\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} = \sum_{u=0}^{k-1} \beta^{\tau^{u+w} q^j} = \left(\sum_{u=0}^{k-1} \beta^{\tau^u} \right)^{q^j} = \alpha^{q^j}.$$

If $(v,i) = (v_0, i_0)$, then

$$\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} = k,$$

which is 0 if $k \equiv 0 \pmod{p}$. So for all $i \neq i_0$, the sum

$$\sum_{v=0}^{k-1} \left(\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} \right)$$

is a sum of at most k basis elements. Therefore the complexity of the basis is at most $(n-1)k + n = (k+1)n - k$. If $k \equiv 0 \pmod{p}$ and $i = i_0$, then

$$\sum_{v=0}^{k-1} \left(\sum_{u=0}^{k-1} \beta^{\tau^u (1+\tau^v q^i)} \right)$$

is a sum of at most $k-1$ basis elements. Therefore if $k \equiv 0 \pmod{p}$ then the complexity of the basis is at most $(n-1)k + k - 1 = kn - 1$. The proof is complete.

□

As special cases of Theorem 3.1.6, when $k = 1$ we obtain Theorem 3.1.1, and when $k = 2$ and $q = 2$ we have Theorem 3.1.3. When q is odd, $k = 2$, it is easy to see that the complexity of the normal basis generated by the α in Theorem 3.1.6 is exactly $3n - 2$. The exact complexity is in general difficult to determine. Some special cases are treated in the following theorem ([1]) which we give without proof.

Theorem 3.1.7 *(Ash, Blake, Vanstone, 1989, [1]) Let $q = 2$. Then the normal basis generated by the α of Theorem 2.2.5 has complexity*

(a) $4n - 7$ *if* $k = 3, 4$ *and* $n > 1$;

(b) $6n - 21$ *if* $k = 5$, $n > 2$ *or* $k = 6, n > 12$;

(c) $8n - 43$ *if* $k = 7$, $n > 6$.

3.2 Determination of Optimal Normal Bases

We have seen two constructions of optimal normal bases. A natural question to ask is whether there are any other optimal normal bases. Lenstra [19] proved that if n does not satisfy the criteria for Theorem 3.1.1 or Theorem 3.1.3, then F_{2^n} does not contain an optimal normal basis.

If the ground field F_q is not F_2 we do have other optimal normal bases; suppose N is an optimal normal basis of F_{q^n} over F_q and $a \in F_q$. Then $aN = \{a\alpha : \alpha \in N\}$ is also an optimal normal basis of F_{q^n} over F_q. In fact, the bases N and aN are said to be *equivalent*.

Another way of obtaining optimal normal bases is given by, Lemma 3.2.1 below. For any positive integer s with gcd(n, s) = 1, N remains to be a basis of $F_{q^{ns}}$ over F_{q^s}. Therefore N is an optimal normal basis of $F_{q^{ns}}$ over F_{q^s} provided that gcd(s, n) = 1. The problem now is whether there are any other optimal normal bases. Mullin proved that if the distribution of the nonzero elements of the multiplication table of an optimal normal basis is similar to a type I or type II optimal normal basis then the basis must be either of type I or type II [23]. Later Gao proved that any optimal normal basis of a finite field must be equivalent to a type I or type II optimal normal basis [8]. Finally, Gao and Lenstra extended the result to a any finite Galois extension of an arbitrary field [9].

Lemma 3.2.1 *(Gao, Lenstra 1992, [9]) Let s and n be relatively primes. If $\tilde{B} = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ is a basis for F_{q^n} over F_q, then $\tilde{B}$ is also a basis for $F_{q^{sn}}$ over F_{q^s}.*

Proof. We should prove that $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ are linearly independent over F_{q^s}. Suppose there are $a_i \in F_{q^s}, 1 \leq i \leq n$, such that

$$\sum_{i=0}^{n-1} a_i \alpha_i = 0$$

Note that for any integer j,

$$\left(\sum_{i=0}^{n-1} a_i \alpha_i\right)^{q^{sj}} = \sum_{i=0}^{n-1} a_i^{q^{sj}} \alpha_i q^{sj} = \sum_{i=0}^{n-1} a_i \alpha_i q^{sj}.$$

Since gcd(s, n)=1, when j runs through $0, 1, ..., t-1$ modulo t, sj also runs through $0, 1, ..., t-1$ modulo n. As $\alpha_i \in F_{q^n}$, we have $\alpha_i^{q^n} = \alpha_i$ and so $\alpha_i^{q^r} = \alpha_i^{q^m}$

whenever $r \equiv m \bmod n$.Therefore, by using $\sum_{i=0}^{n-1} a_i\alpha_i = 0$, we have

$$\sum_{i=0}^{n-1} a_i\alpha_i^{q^j} = 0,$$

for each $j, 0 \leq j \leq n-1$, that is,

$$\begin{pmatrix} \alpha_0 & \alpha_1 & ... & \alpha_{n-1} \\ \alpha_0^q & \alpha_1^q & ... & \alpha_{n-1}^q \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \alpha_0^{q^{n-1}} & \alpha_1^{q^{n-1}} & ... & \alpha_{n-1}^{q^{n-1}} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ . \\ . \\ . \\ a_{n-1} \end{pmatrix} = 0. \tag{3.1}$$

Since $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ are linearly independent over F_q, the coefficient matrix of 3.1 is nonsingular. Thus, $a_0, a_1, ..., a_{n-1}$ must be 0. This proves $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ are linearly independent over F_{q^s}.

□

We first prove some properties that hold for any normal basis.

Let as usual $N = \{\alpha_0, \alpha_1, ..., \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q with $\alpha_i = \alpha^{q^i}$. Let

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, 0 \leq i \leq n-1,\ t_{ij} \in F_q.$$

and $T = (t_{ij})$. Raising the last equation to the q^{-i}-th power, we find that

$$t_{ij} = t_{-i,j-i}$$

for all $0 \leq i \leq n-1$.

From Theorem 1.0.10, we know that the dual of a normal basis is also a normal basis. Let $B = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$ be the dual basis of N with $\beta_i = \beta^{q^i}, 0 \leq i \leq n-1$. Suppose that

$$\alpha\beta_i = \sum_{j=0}^{n-1} d_{ij}\beta_j, 0 \leq i \leq n-1,\ d_{ij} \in F_q.$$

We show that

$$d_{ij} = t_{ji},$$

for all $0 \leq i, j \leq n-1$,

i.e, the matrix $D = (d_{ij})$ is the transpose of $T = (t_{ij})$. The reason is as follows. By

definition of a dual basis, we have

$$\mathrm{Tr}(\alpha_i\beta_j) = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases}$$

Consider the quantity $\mathrm{Tr}(\alpha\beta_i\alpha_k)$. On the one hand,

$$\mathrm{Tr}(\alpha\beta_i\alpha_k) = \mathrm{Tr}((\alpha\beta_i)\alpha_k) = \mathrm{Tr}\left(\sum_{j=0}^{n-1} d_{ij}\beta_j\alpha_k\right) = \sum_{j=0}^{n-1} d_{ij}\mathrm{Tr}(\beta_j\alpha_k) = d_{ik}.$$

On the other hand,

$$\mathrm{Tr}(\alpha\beta_i\alpha_k) = \mathrm{Tr}((\alpha\alpha_k)\beta_i) = \mathrm{Tr}\left(\sum_{j=0}^{n-1} t_{kj}\alpha_j\beta_i\right) = \sum_{j=0}^{n-1} t_{kj}\mathrm{Tr}(\alpha_j\beta_i) = t_{ki}.$$

So this proves $d_{ij} = t_{ji}$, for all $0 \leq i, j \leq n-1$.

Theorem 3.2.2 *(Gao, Lenstra, 1992, [9]) Let $N = \{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ be an optimal normal basis of F_{q^n} over F_q. Let $b = Tr_{q^n|q}(\alpha)$, the trace of α in F_q. Then either*

(i) $n+1$ is a prime, q is primitive in Z_{n+1} and $-\alpha/b$ is a primitive $(n+1)$-th root of unity; or
(ii) (a) $q = 2^v$ for some integer v such that gcd(v, n) = 1,
(b) $2n+1$ is a prime, 2 and -1 generate the multiplicative group Z^*_{2n+1}, and
(c) $\alpha/b = \zeta + \zeta^{-1}$ for some primitive $2n+1$-th root ζ of unity.

Proof. Let $\alpha_i = \alpha^{q^i}, 0 \leq i \leq n-1$, and $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ be the dual basis of N with $\beta_i = \beta^{q^i}$. We assume (i,j)- entry of D denoted by $d(i,j)$ where $D = d_{ij}$. Then, we can write

$$d(i,j) = d(i-j, -j),$$

for all $0 \leq i, j \leq n-1$.

We saw from the proof of Theorem 2.2.2 that each row of D (or column of T) has exactly two nonzero entries which are additive inverses, except the first row which has exactly nonzero entry with value b. This is equivalent to saying that for each $i \neq 0, \alpha\beta_i$ is of the form $a\beta_k - a\beta_l$ for some $a \in F_q$ and integers $0 \leq k, l \leq n-1$, and $\alpha\beta_0 = b\beta_m$ for some integer $0 \leq m \leq n-1$. Replacing α by $-\alpha/b$ and β by $-b\beta$ we may, without loss of generality, assume that $\mathrm{Tr}(\alpha) = -1$. Then we have

$$\alpha\beta_0 = -\beta_m$$

Also, from

$$\mathrm{Tr}(\alpha)\mathrm{Tr}(\beta) = \sum_{i,j} \alpha_i \beta_j = \sum_k \mathrm{Tr}(\alpha\beta_k) = 1$$

we see that we have $\mathrm{Tr}(\beta) = -1$.

If $m = 0$ then from $\alpha\beta_0 = b\beta_m$ we see that $\alpha = -1$, so that $n = 1$, a trivial case. Let it henceforth be assumed that $m \neq 0$.

We first deal with the case that $2m \equiv 0 \pmod{n}$. Raising $\alpha\beta_0 = b\beta_m$ to q^m-th power we see that

$$\alpha_m \beta_m = -\beta_{2m} = -\beta_0 = \beta_m/\alpha.$$

Therefore, we have

$$\alpha\alpha_m = 1 = -\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} -\alpha_i.$$

This shows that $d(i, m) = -1$ for all $i = 0, 1, ..., n-1$. This implies that for each $i \neq 0$ there is a unique $i^* \neq m$ such that

$$\alpha\beta_i = \beta_{i^*} - \beta_m.$$

If $i \neq j$ then $\alpha\beta_i \neq \alpha\beta_j$, so $i^* \neq j_*$. Therefore $i \mapsto i^*$ is a bijective map from $\{0, 1, ..., n-1\} - \{0\}$ to $\{0, 1, ..., n-1\} - \{m\}$. Hence each $i^* \neq m$ occurs exactly once, and so

$$\alpha\alpha_{i^*} = \alpha_i \text{ for } i^* \neq m,$$

$$\alpha\alpha_m = 1.$$

It follows that the set $\{1\} \bigcup \{\alpha_i | i = 0, 1, ..., n-1\}$ is closed under multiplication by α. Since it is also closed under the Frobenius map, it is a multiplicative group of order $n+1$. This implies that $\alpha^{n+1} = 1$, and we also have $\alpha \neq 1$. Hence α is a zero of $x^n + ... + x + 1$. Since α has degree n over F_q, the polynomial $x^n + ... + x + 1$ is irreducible over F_q. Therefore $n+1$ is a prime number. This shows that we are in case (i) of Theorem 3.2.2.

For the remainder of the proof we assume that $2m$ is not congruent to 0 modulo n. By $\alpha\beta_0 = -\beta_m$, we have $d(0, i) = -1$ or 0 according as $i = m$ or $i \neq m$. Hence from $d(i, j) = d(i - j, -j)$, for all $0 \leq i, j \leq n-1$ we find that

$$d(i, i) = \begin{cases} -1 & \text{for } i = -m \\ 0 & \text{for } i \neq -m \end{cases}$$

Therefore $\alpha\beta_{-m}$ has a term $-\beta_{-m}$. As $-m \neq 0$, there exists $0 \leq k \leq n-1$ such that

$$\alpha\beta_{-m} = \beta_k - \beta_{-m},\ k \neq -m.$$

We next prove that the characteristic of F_q is 2. Note that

$$\alpha_m(\alpha\beta_0) = \alpha_m(\beta_{-m}) = -(\alpha\beta_0)^{q^m} = -(-\beta_m)^{q^m} = \beta_{2m}.$$

On the other hand,

$$\alpha(\alpha_m\beta_0) = \alpha(\alpha\beta_{-m})^{q^m} = \alpha(\beta_k - \beta_{-m})^{q^m} = \alpha\beta_{k+m} - \alpha\beta_0 = \alpha\beta_{k+m} + \beta_m.$$

Since $\alpha_m(\alpha\beta_0) = \alpha(\alpha_m\beta_0)$ we obtain

$$\alpha\beta_{k+m} = \beta_{2m} - \beta_m.$$

Now we compute $\alpha\alpha_k\beta_{-m}$ in two ways. To this purpose, note that $d(-m-k,-k) = d(-m,k)$, by $\alpha\beta_{-m} = \beta_k - \beta_{-m}, k \neq -m$. Since $k \neq -m$ implies that $-m-k \neq 0$, we may assume that

$$\alpha\beta_{-m-k} = \beta_{-k} - \beta_j$$

for some j is not in the set $\{-k, -m-k\}$, hence $j+k \neq 0, -m$. On the one hand,

$$\begin{aligned}
\alpha_k(\alpha\beta_{-m}) &= \alpha_k(\beta_k - \beta_{-m}) \\
&= (\alpha\beta_0 - \alpha\beta_{-k-m})^{q^k} \\
&= (-\beta_m - \beta_{-k} + \beta_j)^{q^k} \\
&= -\beta_{k+m} - \beta_0 + \beta_{j+k}.
\end{aligned}$$

On the other hand,

$$\alpha(\alpha_k\beta_{-m}) = \alpha(\alpha\beta_{-m-k})^{q^k} = \alpha(\beta_{-k}\beta_j)^{q^k} = \alpha\beta_0 - \alpha\beta_{j+k} = -\beta_m - \alpha\beta_{j+k}.$$

We have

$$\alpha\beta_{j+k} = -\beta_{j+k} + \beta_0 + \beta_{m+k} - \beta_m.$$

As $j+k \neq -m$, β_{j+k} does not appear in $\alpha\beta_{j+k}$ by the definition of $d(i,i)$. Thus $-\beta_{j+k}$ must cancel against one of the last two terms.

If $-\beta_{j+k} + \beta_{m+k} = 0$ then $j+k = m+k$ and thus $\alpha\beta_{m+k} = \beta_0 - \beta_m$. But by $\alpha\beta_{k+m} = \beta_{2m} - \beta_m$, $\beta_0 = \beta_{2m}$ and $2m \equiv 0 \pmod{n}$, contradicting the assumption.

Consequently, $-\beta_{j+k}-\beta_m = 0$ and $\alpha\beta_{j+k} = \beta_{m+k}+\beta_0$. The first relation implies that $j + k = m$ and -2 = 0. Therefore the characteristic of F_q is 2, and

$$\alpha\beta_m = \beta_{m+k} + \beta_0.$$

From now on we assume that $q = 2^v$ for some integer v. The equations $\alpha\beta_0 = -\beta_m$ and $\alpha\beta_{-m} = \beta_k - \beta_{-m}, k \neq -m$ can be written as

$$\alpha\beta = \beta_m,\ \alpha\beta_{-m} = \beta_k + \beta_{-m}.$$

Raising $\alpha\beta_{-m} = \beta_k + \beta_{-m}$ to the q^m-th power and comparing the result to $\alpha\beta_m = \beta_{m+k} + \beta_0$, we find $\alpha_m\beta = \alpha\beta_m$, which is the same as

$$\frac{\alpha}{\beta} = \frac{\alpha_m}{\beta_m} = \left(\frac{\alpha}{\beta}\right)^{q^m}$$

Multiplying the last equation and $\alpha\beta = \beta_m$ we find that $\alpha^2 = \alpha_m = \alpha^{q^m}$. By induction on r one deduces from this that $\alpha^{q^{mr}} = \alpha^{2^r}$ for every nonnegative integer r. Let $r = n/\gcd(m, n)$. Then $\alpha^{2^r} = \alpha$, which means that α is in F_{2^r} and thus of degree at most $r \leq n$ over the prime field F_2 of F_q. As α has degree n over F_q, it has degree at least n over F_2. Hence r must equal to n, and thus $\gcd(m,\ n) = 1$. Also from the fact that α has the same degree over F_2 and F_q for $q = 2^v$, we see immediately that $\gcd(v,\ n) = 1$ and the conjugates of α over F_q are the same as those over F_2, namely $\alpha, \alpha^2, ..., \alpha^{2^{n-1}}$.

Let m_1 be a positive integer such that $mm_1 \equiv 1 \pmod{n}$. Then by repeatedly raising α/β to q^m-th power we have

$$\frac{\alpha}{\beta} = \left(\frac{\alpha}{\beta}\right)^{q^{mm_1}} = \left(\frac{\alpha}{\beta}\right)^{q}$$

(Note that $(\alpha/\beta)^{q^n} = \alpha/\beta$.) This implies that $\alpha/\beta \in F_q$, and since $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta) = -1$ we have in fact $\alpha = \beta$. Thus by $d_{ij} = t_{ji}$, for all $0 \leq i, j \leq n-1$ we see that $d(i, j) = d(j, i)$.

Let now ζ be a zero of $x^2 - \alpha x + 1$ in an extension $F_{q^{2n}}$ of F_q, so that $\zeta + \zeta^{-1} = \alpha$. The multiplicative order of ζ is a factor of $q^{2n}-1$ and is thus odd; let it be $2t+1$. For each integer i, write $\gamma_i = \zeta^i + \zeta^{-i}$, so that $\gamma_0 = 0$ and $\gamma_1 = \alpha$. It can be seen directly that $\gamma_i = \gamma_j$ if and only if $i \equiv \pm j \pmod{2t+1}$. Hence there are exactly t different

nonzero elements among the γ_i, namely $\gamma_1, \gamma_2, ..., \gamma_t$. Each of the n conjugates of α is of the form $\alpha^{2^j} = \zeta^{2^j} + \zeta^{2^{-j}} = \gamma_{2^j}$ for some integer j, and therefore occurs among the γ_i. This implies that $n \leq t$. We show that $n = t$ by proving that, conversely, every nonzero γ_i is a conjugate of α. This is done by induction on i. We have $\gamma_1 = \alpha$ and $\gamma_2 = \alpha^2$, so it suffices to take $3 \leq i \leq t$. We have

$$\alpha\gamma_{i-2} = (\zeta + \zeta^{-1})(\zeta^{i-2} + \zeta^{2-i}) = \gamma_{i-1} + \gamma_{i-3},$$

where by induction hypothesis each of $\gamma_{i-2}, \gamma_{i-1}$ is conjugate to α, and γ_{i-3} is either conjugate to α or equal to zero. Thus when $\alpha\gamma_{i-2}$ is expressed in the normal basis $\{\alpha^{2^i} | i = 0, 1, ..., n-1\}$, then γ_{i-1} occurs with a coefficient 1. By $d_{ij} = t_{ji}$, for all $0 \leq i, j \leq n-1$ implies that when $\alpha\gamma_{i-1}$ is expressed in the same basis, γ_{i-2} likewise occurs with a coefficient 1. Hence from the fact that $\beta = \alpha$ and $\gamma_{i-1} \neq \alpha$ we see that $\alpha\gamma_{i-1}$ is equal to the sum of γ_{i-2} and some other conjugate of α. But since we have $\alpha \cdot \gamma_{i-1} = \gamma_{i-2} + \gamma_i$, that other conjugate of α must be γ_i. This completes the inductive proof that all nonzero γ_i are conjugate to α and that $n = t$.

From the fact that each nonzero γ_i equals a conjugate α^{2^j} of α it follows that for each integer i that is not divisible by $2n + 1$, there is an integer j such that $i \equiv \pm 2^j \pmod{2n+1}$. In particular, every integer i that is not divisible by $2n + 1$ is relatively prime to $2n + 1$, so $2n + 1$ is a prime number, and ${Z_{2n+1}}^*$ is generated by 2 and -1. Thus the conditions (a) and (b) of the Theorem 3.2.2 are satisfied. All assertions of (ii) have been proved.

□

CHAPTER 4

MULTIPLICATION AND INVERSION IN FINITE FIELDS USING NORMAL AND OPTIMAL NORMAL BASES

There are many applications of optimal normal bases. For example, in the paper [32] a new parallel multiplier for F_{2^m} whose elements are represented using the optimal normal basis of type II is presented. As it will be shown below the proposed multiplier requires $1,5(m^2-m)$ XOR gates, as compared to $2(m^2-m)$ XOR gates required by the Massey-Omura multiplier.

Let us recall here the conditions of the Theorem 3.1.3: We assume that $p = 2m+1$ is a prime and either of the following two conditions also holds:
i) 2 is a primitive root modulo p.
ii)$p \equiv 7$ (mod8) and the multiplicative order of 2 modulo p is m.
Then, we have an optimal normal basis of type II in F_{2^m} based on the normal element $\alpha = \gamma + \gamma^{-1}$, where γ is the primitive pth root of unity. The basis is given as

$$M = \{\alpha, \alpha^2, \alpha^4, ..., \alpha^{2^{m-1}}\}.$$

We can show that there exists another basis N which is obtained by a simple permutation of the basis elements in M and construct a new parallel multiplication algorithm in the new basis N. We examine both cases below:

i) If 2 is a primitive root modulo p, then the set of powers of 2 modulo p

$$P_1 = \{2, 2^2, 2^3, ..., 2^{2m-1}, 2^{2m}\} \bmod p$$

is equivalent to

$$Q_1 = \{1, 2, 3, 4, ..., 2m\}.$$

Therefore, a basis element of the form $\gamma^{2^i} + \gamma^{2^{-i}}$ can be written as $\gamma^j + \gamma^{-j}$ for $j \in [1, 2m]$. Moreover, we can rewrite $\gamma^j + \gamma^{-j}$ as $\gamma^{(2m+1)-j} + \gamma^{-(2m+1)+j}$; if $j \geq m+1$, then the power of γ becomes in the range $[1, m]$.

ii) If the multiplicative order of 2 modulo p is m, then the set of powers of 2 modulo p

$$P_1 = \{2, 2^2, 2^3, ..., 2^{2m-1}, 2^{2m}\} \bmod p$$

consists of m distinct integers in the range $[1, 2m]$. If $2^i \pmod p$ is in the range $[1, m]$,then leave as it is. If $2^i \pmod p$ is in the range $[m+1, 2m]$, we write in its place the number $(2m+1) - (2^i \bmod p)$ to bring it to the range $[1, m]$. Since these numbers are all distinct, the set P_2 is equivalent to

$$Q_2 = \{1, 2, 3, 4, ..., 2m\}.$$

As a result, a basis element of the form $\gamma^{2^i} + \gamma^{2^{-i}}$ for $i \in [1, m]$ can be written uniquely as $\gamma^j + \gamma^{-j}$ with $j \in [1, m]$.

Consequently, the bases M and N are given as

$$\begin{aligned} M &= \{\gamma + \gamma^{-1}, \gamma^2 + \gamma^{-2}, \gamma^{2^2} + \gamma^{-2^2}, ..., \gamma^{2^{(m-1)}} + \gamma^{-2^{(m-1)}}\}, \\ N &= \{\gamma + \gamma^{-1}, \gamma^2 + \gamma^{-2}, \gamma^3 + \gamma^{-3}, ..., \gamma^m + \gamma^{-m}\} \end{aligned}$$

are the same. The basis N is obtained from the basis M using a simple permutation. Let A be expressed in the basis M as

$$A = \acute{a_1}\alpha + \acute{a_2}\alpha^2 + \acute{a_3}\alpha^{2^2} + ... + \acute{a_m}\alpha^{2^{m-1}},$$

where $\alpha = \gamma + \gamma^{-1}$. The representation of A in the basis N is given as

$$A = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 + ... + a_m\alpha_m,$$

where $\alpha_i = \gamma^i + \gamma^{-i}$. We can express the permutation between the coefficients $a_j = \acute{a_i}$ as

$$j = \begin{cases} k & \text{if } k \in [1, m], \\ (2m+1) - k & \text{if } k \in [m+1, 2m] \end{cases}$$

where $k = 2^{i-1} \bmod (2m+1)$ for $i = 1, 2, ..., m$. This permutation is the vital part of the algorithm.

The basis N is not a normal basis, it is a shifted form of the canonical basis. Note that the exponents of basis elements of the shifted canonical basis is one more than the ones of the canonical basis. It is constructed an efficient parallel multiplier in the following section using this new basis.

4.1 New Multiplication Algorithm

Using the terminology we introduced in the beginning of this chapter, we present the following algorithm:

1. Convert the elements represented in the basis M to the basis N using the permutation.

2. Multiply the elements in the basis N.

3. Convert the result back to the basis M using the inverse permutation.

The first and third steps are implemented without any gates since the permutation operation requires a simple rewiring. The second step is a multiplication operation in the basis N, which are presented below. Let A, $B \in F_{2^m}$ be represented in the basis N as

$$A = \sum_{i=1}^{m} a_i \alpha_i = \sum_{i=1}^{m} a_i (\gamma^i + \gamma^{-i}),$$
$$B = \sum_{i=1}^{m} b_i \alpha_i = \sum_{i=1}^{m} b_i (\gamma^i + \gamma^{-i}),$$

The product of these two numbers $C = A.B$ is written as

$$C = A.B = \left(\sum_{i=1}^{m} a_i (\gamma^i + \gamma^{-i}) \right) \left(\sum_{j=1}^{m} b_j (\gamma^j + \gamma^{-j}) \right).$$

This product can be transformed to the following form:

$$C = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j (\gamma^{i-j} + \gamma^{-(i-j)}) + \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j (\gamma^{i+j} + \gamma^{-(i+j)}) = C_1 + C_2.$$

The term C_1 has the property that the exponent $(i-j)$ of γ is already with in the proper range, i.e., $-m \leq (i-j) \leq m$ for all $i, j \in [1, m]$. Furthermore, if $i = j$, then $\gamma^{i-j} + \gamma^{-(i-j)} = \gamma^0 + \gamma^0 = 0$. Thus, we can write C_1 as

$$C_1 = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j (\gamma^{i-j} + \gamma^{-(i-j)}) = \sum_{\substack{1 \leq i,j \leq m \\ i \neq j}} a_i b_j (\gamma^{i-j} + \gamma^{-(i-j)}).$$

If $k = |i-j|$, then the product $a_i b_j$ contributes to the basis element $\alpha_k = \gamma^k + \gamma^{-k}$. For example, the coefficients of α_1 are the sum of all $a_i b_j$ for which $|i-j| = 1$. Furthermore, the term C_2 is transformed in to the following:

$$\begin{aligned} C_2 &= \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j (\gamma^{i+j} + \gamma^{-(i+j)}) \\ &= \sum_{i=1}^{m} \sum_{j=1}^{m-i} a_i b_j (\gamma^{i+j} + \gamma^{-(i+j)}) + \sum_{i=1}^{m} \sum_{j=m-i+1}^{m} a_i b_j (\gamma^{i+j} + \gamma^{-(i+j)}) \\ &= D_1 + D_2. \end{aligned}$$

The exponents of the basis elements in D_1 are in the proper range i.e., $1 \leq (i+j) \leq m$ for $i = 1, 2, ..., m$ and $j = 1, 2, ..., m-i$. If $k = i+j$, then the product $a_i b_j$ contributes to the basis element α_k as i and j take these values.
But, the basis elements of D_2 are all out of range. Use the identity $\gamma^{2m+1} = 1$ to bring them to the proper range:

$$D_2 = \sum_{i=1}^{m} \sum_{j=m-i+1}^{m} a_i b_j (\gamma^{i+j} + \gamma^{-(i+j)}) = \sum_{i=1}^{m} \sum_{j=m-i+1}^{m} a_i b_j (\gamma^{2m+1-(i+j)} + \gamma^{-(2m+1-(i+j))}).$$

Hence, if $k = i+j > m$, replace α_k by α_{2m+1-k}. The constructions of C_1, D_1 and D_2 are given below:

The Construction of C_1:

α_1	α_2	...	α_{m-2}	α_{m-1}	α_m
$a_1b_2 + a_2b_1$	$a_1b_3 + a_3b_1$	...	$a_1b_{m-1} + a_{m-1}b_1$	$a_1b_m + a_mb_1$	
$a_2b_3 + a_3b_2$	$a_2b_4 + a_4b_2$	...	$a_2b_m + a_mb_2$		
.	.				
.	.				
.	.				
$a_{m-1}b_m + a_mb_{m-1}$					

The Construction of D_1:

α_1	α_2	α_3	...	α_{m-2}	α_{m-1}	α_m
	a_1b_1	a_1b_2	...	a_1b_{m-3}	a_1b_{m-2}	a_1b_{m-1}
		a_2b_1	...	a_2b_{m-4}	a_2b_{m-3}	a_2b_{m-2}
			.	.	.	
			.	.	.	
			.	.	.	
				$a_{m-3}b_1$	$a_{m-3}b_2$	$a_{m-3}b_3$
					$a_{m-2}b_1$	$a_{m-2}b_2$
						$a_{m-1}b_1$

The Construction of D_2:

α_1	α_2	α_3	...	α_{m-2}	α_{m-1}	α_m
a_mb_m	$a_{m-1}b_m$	$a_{m-2}b_m$	...	a_3b_m	a_2b_m	a_1b_m
	a_mb_{m-1}	$a_{m-1}b_{m-1}$	...	a_4b_{m-1}	a_3b_{m-1}	a_2b_{m-1}
		a_mb_{m-2}	...	a_5b_{m-2}	a_4b_{m-2}	a_3b_{m-2}
			.	.	.	
			.	.	.	
			.	.	.	
				$a_{m-1}b_4$	$a_{m-2}b_4$	$a_{m-3}b_4$
				a_mb_3	$a_{m-1}b_3$	$a_{m-2}b_3$
					a_mb_2	$a_{m-1}b_2$
						a_mb_1

4.1.1 Details of Multiplication and Complexity Analysis

If these three arrays C_1, D_1 and D_2 are inspected closely, the following observations can be made:

1. All three arrays are composed of the elements of the form $a_i b_j$ for $i, j \in [1, m]$

2. The height of the ith column in the array C_1 is $2(m-i)$ for $i = 1, 2, ..., m$. This is the number of the terms of the form $a_i b_j$ to be summed in the ith column.

3. The height of the ith column in the array D_1 is $i - 1$.

4. The height of the ith column in the array D_2 is i.

5. Therefore, the height of the ith column in the entire array representing the total sum C is found as $2(m-i) + i - 1 + i = 2m - 1$.

6. If there is an element $a_i b_j$ is present in a column, then the element $a_j b_i$ is also present in the same column. This is true for all arrays C_1, D_1 and D_2.

7. An element of the form $a_i b_i$ is present only once in a column of either D_1 or D_2.

8. A column of the entire array representing the total sum C contains a single element of the form $a_i b_i$ and $2m - 2$ elements of the form $a_i b_j$, where $a_j b_i$ is also present.

The proposed multiplication algorithm first computes the terms $a_i b_j$ for $i, j \in [1, m]$ using exactly m^2 two-input AND gates. Let $t_{ij} = a_i b_j + a_j b_i$ for $i = 1, 2, ..., m-$

1 and $j = i+1, i+2, ..., m$. Compute the terms t_{ij} using

$$(m-1) + (m-2) + ... + 2 + 1 = m(m-1)/2$$

two input XOR gates. The ith column of the entire array contains exactly $(2m-2)/2 = m-1$ terms of the form t_{ij} and also a single element of the form $a_i b_i$. These m numbers are summed using a binary XOR tree, which requires $m-1$ XOR gates. Due to the parallelism, all m columns require $m(m-1)$ XOR gates. Hence, the construction of the product C requires

AND Gates $= m^2$,

XOR Gates $= m(m-1)/2 + m(m-1) = 3/2m(m-1)$,

But, the parallel Massey-Omura algorithm uses m^2 AND gates and $2m(m-1)$ XOR gates. Therefore, the proposed algorithm requires 25 % fewer XOR gates than the Massey-Omura algorithm.

4.2 Fast Operation Method in F_{2^n} Using a Modified Optimal Normal Basis

In this section, we show how to construct an optimal normal basis over finite field of high degree. We have two methods for fast operations in some finite field F_{2^n}. The first method is to use an optimal normal basis of F_{2^n} over F_2. On the other hand, the second method which regards the finite field F_{2^n} as an extension field of F_{2^s} and F_{2^t} is to use an optimal normal basis of F_{2^t} over F_2 when $n = st$ where s and t are relatively primes. Using a polynomial basis, the multiplication of two elements in F_{2^n} is a product of two polynomials modulo an irreducible polynomial. The inverse of an element is easily computed using the Euclid algorithm.

Moreover, another fast operation method is suggested [25]. In case of $n = st$ where s and t are relatively primes, F_{2^n} is regarded as a vector space of dimension t over F_{2^s}. Each element of F_{2^n} is represented by a polynomial basis which is generated by an irreducible polynomial of degree t over F_{2^s}. It is called a *modified polynomial basis*.

Let $f(x)$ be a monic irreducible polynomial of degree n over F_2 denoted by

$$f(x) = d_0 + d_1 x + ... + d_{n-1} x^{n-1} + x^n,$$

where $d_0, d_1, ..., d_{n-1} \in F_2$.

Then we construct the finite field F_{2^n} as $F_2[x]/(f(x))$. Let $\tilde{B} = \{\gamma_0, \gamma_1, ..., \gamma_{n-1}\}$ be a basis for F_{2^n} over F_2. Every element A of F_{2^n} is identified with the vector $A = (a_0, a_1, ..., a_{n-1})$ e.g.

$$A = \sum_{i=0}^{n-1} a_i \gamma_i, a_i \in F_2.$$

Now we investigate an addition and multiplication of two elements of F_{2^n} for polynomial (canonical) basis. Let α be a root of an irreducible polynomial $f(x)$. Then $\tilde{C} = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ forms a basis for F_{2^n}. Let A be the same above and

$$B = \sum_{i=0}^{n-1} b_i \alpha_i = (b_0, b_1, ..., b_{n-1}).$$

Then

$$A + B = \sum_{i=0}^{n-1} (a_i + b_i)\alpha_i,$$

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

Using the fact that α is a root of $f(x)$, i.e.

$$d_0 + d_1\alpha + d_2\alpha^2 + ... + d_{n-1}\alpha^{n-1} = 0,$$

we can obtain

$$A.B = \left(\sum_{i=0}^{n-1} a_i \alpha_i\right)\left(\sum_{j=0}^{n-1} b_j \alpha_j\right) = \sum_{k=0}^{n-1} c_k \alpha_k.$$

Observe that addition has the same complexity as an optimal normal basis, because in both cases there is a component-wise addition. However, multiplication using polynomial basis is much more complex than using optimal normal basis.

In case that s and t are relatively prime, we may consider the field F_{2^n} as an extension field of two subfields F_{2^s} and F_{2^t}.

Theorem 4.2.1 *(Gao 1994) Let s and t be relatively prime. If $\tilde{N} = \{\alpha, \alpha^2, ..., \alpha^{2^{t-1}}\}$ is a normal basis for F_{2^t} over F_2, then $\tilde{N}$ is also a normal basis for $F_{2^{st}}$ over F_{2^s}.*

Proof. Follows by the Lemma 3.2.1.

□

Let $\tilde{N}$ be an optimal normal basis of the form $\tilde{N} = \{\alpha, \alpha^2, ..., \alpha^{2^{t-1}}\}$.

Since every multiplication group $F^*_{(2^s)}$ is cyclic, there exists a generator ξ of $F^*_{2^s}$

(since s is practically small, it is very simple to find a ξ). So every element of $F_{2^s}^*$ is represented by ξ^{a_i} for some integer $0 \leq a_i < 2^s$. Let us denote the zero element of F_{2^s} as -1. Thus any element A of $F_{2^{st}}$ is represented with respect to $\tilde{N}$ by

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

We denote it by $A = (a_0, a_1, ..., a_{t-1})$. If z_i is zero, put -1 in the i-th coordinate. $(-1, -1, ..., -1)$ is the zero element of $F_{2^{st}}$ over F_{2^s}. So addition of two elements in $F_{2^{st}}$ is reduced to the addition of $2t$ elements of F_{2^s}. Thus we need the table of addition of elements of F_{2^s}. Using an irreducible polynomial which defines F_{2^s}, each element ξ^{a_i} can be represented by a polynomial basis. We denote ξ^{a_i} by the extended vector representation $(p_0, p_1, ..., p_{s-1}, a_i)$ which consists of the polynomial representation and its exponent a_i. So the addition table is composed of 2^s rows and $(s+1)$ columns. In order to add two elements of F_{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

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

It is just the cyclic shifts of the original A. Let $C = AB = (c_0, c_1, ..., c_{t-1})$. Then

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

where $t_{ij} \in F_2$ and subscripts on a and b are taken modulo t. Since s and t are relatively prime, k varies from 0 to $t-1$. So all c_i's are obtained by s times cyclic shifts of A and B.

Results of implementation

In this section, we will compare the complexity of $F_{2^{1018}}$ with that of $F_{2^{904}} = F_{2^{8 \cdot 113}}$. According to the Theorem 3.1.1 (type I), $F_{2^{1018}}$ has an optimal normal basis. This optimal normal basis is generated by a root α of $f(x) = 1 + x + x^2 + ... + x^{1018}$.

Since $F_{2^{1018}}$ has an optimal normal basis, the matrix of multiplication has two 1's for each row except for the last row(the last row has one 1). Using the matrix,

we compute the multiplication of two elements of $F_{2^{1018}}$ and an exponentiation of one element of $F_{2^{1018}}$.

Let $n = 904 = 8.113, s = 8$ and $t = 113$. Then $F_{2^{904}}$ is regarded as an extension field of F_{2^8} and $F_{2^{113}}$. Take a primitive polynomial $p(x) = 1+x+x^3+x^4+x^8$, then its root ξ generates ${F_{2^8}}^*$. By the Theorem 3.1.3, $F_{2^{113}}$ has an optimal normal basis. Let $f(x) = 1 + x + x^2 + ... + x^{226}$. If β is its root then $\alpha = \beta + \beta^{-1}$ generates an optimal normal basis of $F_{2^{113}}$. This normal basis is also a self-dual normal basis.

Table [25] 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 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. The time required for making matrix of $F_{2^{904}}$ is huge. Since it is a preparation step, it can be ignorable for an operation speed.

	operation speed for $F_{2^{1018}}$	operation speed for $F_{2^{904}}$	memory size for $F_{2^{1018}}$	memory size for $F_{2^{904}}$
making matrix	9.66 sec	3 hour 18 min 22.37 sec	2 x 1018- 1 byte	2 x 113 -1 byte
one element			1018 byte	113 byte
making addition table		0.02 sec		255 x 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})		

4.3 Orders of Optimal Normal Basis Generators

In several cryptographic systems (such as, Diffie Hellmann [5]), a fixed element of a group needs to be repeatedly raised to many different large powers. To make such system secure, the fixed element must have high order. In any implementation of these systems, there should be an efficient algorithm for computing large powers of the fixed element. Therefore, Gao and Vanstone [10] show by experimental results

that the optimal normal basis generators given in Type II Construction have exactly this desired property: They have very high multiplicative orders, and large powers of them can be computed efficiently, as indicated by the following result.

Theorem 4.3.1 *(Gao, Vanstone 1995) Let α be an optimal normal basis generator in type II construction. Then, for any integer e, α^e can be computed in $O(n.w(e))$ bit operations, where $w(e)$ is the number of 1's in the binary representation of e which is called the Hamming weight of the element e.*

As $w(e) \leq n$ for $0 \leq e \leq 2^n - 1$, α^e can be computed in $O(n^2)$ bit operations. To compare, we should mention that for an arbitrary $\beta \in F_{2^n}$, if F_{2^n} is represented by an optimal normal basis, Stinson [30] and Von Zur Gathen [34] showed that β^e can be computed in about $O(n^3/log_2 n)$ bit operations in F_{2^n},

In the following, we assume the conditions in Construction II are satisfied. Our goal is to determine the multiplicative order of $\alpha = \gamma + \gamma^{-1}$.

Here, the standard algorithm for the determining the multiplicative order of elements in finite fields is used. To apply this algorithm for computing the multiplicative order of an element in F_{2^n}, one needs to know the complete factorization of the integer $2^n - 1$.

The optimal normal basis generated by α is $\{\alpha, \alpha^2, ..., \alpha^{2^{n-1}}\}$. Here, we arrange the elements of the basis in a different order. For an integer i, define $\gamma_i = \gamma^i + \gamma^{-i}$. We recall that (Section 4.1),

$$\{\alpha, \alpha^2, ..., \alpha^{2^{n-1}}\} = \{\gamma_1, \gamma_2, ..., \gamma_n\}.$$

To facilitate multiplication of elements represented under this basis, we define a new function from the set of integers to the set $\{0, 1, ..., n\}$. For any integer i, define $s(i)$ to be the unique integer such that

$$0 \leq s(i) \leq n, \text{and } \ i \equiv s(i) \text{mod } 2n+1 \text{or } i \equiv -s(i) \text{mod } 2n+1.$$

Obviously, $s(0) = 0$, $s(i) = -s(i)$ and

$$\gamma_i = \gamma_{s(i)}, \alpha^{2^i} = \gamma_{s(2^i)}$$

for all i.

As

$$\gamma_i.\gamma_j = \gamma_{i+j} + \gamma_{i-j}$$

for all i, j, we have

$$\gamma_i.\gamma_j = \gamma_{s(i+j)} + \gamma_{s(i-j)},$$

$1 \le i, j \le n$.

Next we show how to compute the product $\gamma_i.A$, where $1 \le i \le n$ and A is an arbitrary element in F_{2^n}. Suppose that $A = \sum_{k=1}^{n} a_k\gamma_k$, where $a_k \in F_2$. Then

$$\gamma_i.A = \sum_{k=1}^{n} a_k\gamma_i.\gamma_k = \sum_{k=1}^{n} a_k(\gamma_{s(k+i)} + \gamma_{s(k-i)}).$$

Note that

$$\begin{aligned}
\sum_{k=1}^{n} a_k\gamma_{s(k+i)} &= \sum_{k=1}^{n-i} a_k\gamma_{k+i} + \sum_{k=n+1-i}^{n} a_k\gamma_{2n+1-(k+i)} && (4.1)\\
&= \sum_{k=i+1}^{n} a_{k-i}\gamma_k + \sum_{k=n+1-i}^{n} a_{2n+1-(k+i)}\gamma_k && (4.2)\\
&= \sum_{k=i+1}^{n} a_{s(k-i)}\gamma_k + \sum_{k=n+1-i}^{n} a_{s(k+i)}\gamma_k, && (4.3)\\
\sum_{k=1}^{n} a_k\gamma_{s(k-i)} &= \sum_{k=1}^{i} a_k\gamma_{i-k} + \sum_{k=i+1}^{n} a_k\gamma_{k-i} && (4.4)\\
&= \sum_{k=1}^{i} a_{i-k}\gamma_k + \sum_{k=1}^{n-i} a_{k+i}\gamma_k && (4.5)\\
&= \sum_{k=1}^{i} a_{s(k-i)}\gamma_k + \sum_{k=1}^{n-i} a_{s(k+i)}\gamma_k, && (4.6)
\end{aligned}$$

We assume that $a_0 = 0$ everywhere. We see that

$$\begin{aligned}
\gamma_i.A &= \sum_{k=1}^{n}(a_{s(k-i)} + a_{s(k+i)})\gamma_k && (4.7)\\
&= \sum_{k=1}^{c}(a_{i-k} + a_{i+k})\gamma_k + \sum_{k=c+1}^{d} f(k)\gamma_k + \sum_{k=d+1}^{n}(a_{k-i} + a_{2n+1-(k+i)})\gamma_k,
\end{aligned}$$

where $c = \min\{i, n-i\}$, $d = \max\{i, n-i\} = n - c$ and

$$f(k) = \begin{cases} a_{i-k} + a_{2n+1-(k+i)} & \text{if } i > n-i, \\ a_{k-i} + a_{k+i} & \text{if } i < n-i. \end{cases}$$

This shows that $\gamma_i.A$ can be computed in $O(n)$ bit operations.

Now, to compute α^e we can assume that $0 \leq e < 2^n - 1$, as $\alpha^{2^n-1} = 1$. Write $e = \sum_{k=0}^{n-1} e_k 2^k$, where $e_k \in \{0, 1\}$. Then

$\alpha^e = \Pi_{k=0}^{n-1}(\alpha^{2^k})^{e_k} = \Pi_{k=0}^{n-1}(\gamma_{s(2^k)})^{e_k}$.

This suggests that α^e can be computed iteratively as follows:

Algorithm:

Input: An integer e with $0 \leq e \leq 2^n - 1$.

Output: α^e represented in the basis $(\gamma_1, ..., \gamma_n)$.

Step 1. Set $A := 1 = \sum_{k=1}^{n} \gamma_k$ and compute the binary representation: $e = \sum_{k=0}^{n-1} e_k 2^k$;

Step 2. For k from 0 to $n-1$, if $e_k = 1$ then set $A := \gamma_{s(2^k)}.A$;

Step 3. Return A;

End.

The correctness of the algorithm is obvious. The major cost is incurred at Step2 where $w(e)$ products of the form $\gamma_k.A$ are computed. Since we have shown that each such product can be computed in $O(n)$ bit operations, the total cost is $O(n.w(e))$ bit operations. Therefore, α^e can be computed in $O(n.w(e))$ bit operations as claimed by the Theorem 4.3.1

□

By using the algorithm described above, S. Gao and S. Vanstone [10] have computed the multiplicative order of α for $n \leq 1200$ where the conditions of Construction II are satisfied and complete factorization of $2^n - 1$ is known.

Experiments indicate that the multiplicative order of α is at least $O((2^n - 1)/n)$. This means that α always has very high multiplicative order. Besides, one can check that if n is prime, then α is primitive.

4.4 A Fast Algorithm for Multiplicative Inversion Using Normal Basis

It is known that multiplicative inversion is much more time-consuming than multiplication. Several algorithms have been proposed for multiplicative inversion in F_{2^m}. N. Takagi, J. Yoshiki and K. Takagi [33] proposed a new fast algorithm for

multiplicative inversion in $F(2^m)$ using normal basis. The new method is an improvement of the algorithm proposed by Chang [2] et al.

From Fermat's theorem, for any nonzero element $\beta \in F_{2^m}$, $\beta^{-1} = \beta^{2^m-2}$ holds. But $2^m - 2 = 2^1 + 2^2 + ... + 2^{m-1}$ and

$$\beta^{-1} = \beta^{2^m-2} = \beta^{2^1} \times \beta^{2^2} \times ... \times \beta^{2^{m-1}}.$$

Wang et al.[35] proposed an algorithm using this expression. This algorithm requires $m-2$ multiplications as well as taking $m-1$ squares.

As we mentioned before, squaring is just cyclic shift by using normal basis and, so is much faster than multiplication. Hence, it is important to reduce the number of multiplications for accelerating the exponentiation.

Itoh and Tsujii [16], [17] decreased the number of required multiplications to $O(\log m)$. We can call this algorithm Algorithm[IT]. Algorithm[IT] requires $l(m-1)+w(m-1)-2$ multiplications and $l(m-1)+w(m-1)-1$ (multiple-bit) cyclic shifts, where $l(m-1) = q$ is the number of bits of the binary representation of $m-1$ and $w(m-1)$ is the number of 1's in the representation which is defined before.

Feng [7] proposed a similar algorithm, which requires the same number of multiplications and cyclic shifts as Algorithm[IT].

Chang [2] improved the Algorithm[IT]. Hereafter, we call the algorithm proposed by Chang as the Algorithm[Chang]. Algorithm[Chang] requires $(l(s)+w(s)-2)+(l(t)+w(t)-2)$ multiplications and $(l(s)+w(s)-1)+(l(t)+w(t)-2)$ (multiple-bit) cyclic shifts where $m-1 = s \times t$ and l and w defined above.

Algorithm[Chang] is efficient, but it is not applicable if $m-1$ is a prime number. N. Takagi, J. Yoshiki and K. Takagi [33] proposed a new algorithm which is applicable to the case where $m-1$ is prime.

Since

$$\begin{aligned} 2^m - 2 &= 2^{m-1} + 2^{m-1} - 2 = 2^{m-1} + 2^{m-2} + ... + 2^{m-h} + 2^{m-h} - 2, \\ \beta^{-1} &= \beta^{2^m-2} = \beta^{2^{m-1}} \times \beta^{2^{m-2}} \times ... \times \beta^{2^{m-h}} \times \beta^{2^{m-h}-2} \end{aligned}$$

$\beta^{2^{m-i}}$ can be calculated by i-bit cyclic shift. Therefore, β^{-1} can be found from $\beta^{2^{m-h}-2}$ by h multiplications. Indeed, $\beta^{2^{m-h}-2}$ can be calculated by Algorithm[IT] or Algorithm[Chang] by replacing m by $m-h$.

By this method, the number of multiplications required is reduced for some integers m. Moreover, it is decreased by factorizing $m-1$ into more than two factors. Thus, this method is adopted when $m-h-1$ can be factorized into more than two factors. Hence, the principle that decomposing $m-1$ into several factors and a small remainder h can be recursively applied to one of the factors of $m-h-1$.

When $m-1$ is decomposed as $m-1=\prod_{j=1}^{k} s_j + h$ and s_1 is not decomposed, the number of multiplications required is $\sum_{j=1}^{k}(l(s_j)+w(s_j)-2)+h$. This is because the number of multiplications required corresponding to the factor s_j is $l(s_j)+w(s_j)-2$. When the first factor s_1 is decomposed further, we can calculate the number of multiplications required by using this formula iteratively.

The number of multiplications required depends on the way of decomposition. There may exist several decompositions which minimize the number of multiplications. We call the decomposition which minimizes the number of multiplications required and consists of the fewest factors as the *optimal decomposition*. More than one optimal decompositions may exist.

The following propositions can be used for finding optimal decomposition(s) of $m-1$.

Proposition 4.4.1 *When $m-1=2^n$, the optimal decomposition is $m-1$ itself (nondecomposition) and the number of required multiplications is n.*

Proposition 4.4.2 *When $m-1=2^{\tilde{n}}s+h$, where s is odd, the smallest number of required multiplications by a decomposition of $m-1$ as $\prod_{j=1}^{k} s_j + h$ (either s_1 is decomposed further or not) is $\tilde{n}+h+MR(s)$ where $MR(s)$ is the number of required multiplications by the optimal decomposition of s.*

When $s_j = 2^{\tilde{n_j}}\tilde{s_j}$, the number of required multiplications corresponding to s_j and that corresponding to $2^{\tilde{n_j}} \times \tilde{s_j}$ are identical, i.e., $l(\tilde{s_j})+w(\tilde{s_j})-2+\tilde{n}$. Therefore, the optimal decomposition of $m-1$ does not include a power of 2 as a factor unless it is in the form $S \times 2^{\tilde{n}}+h$ and S is a decomposition of s with a nonzero remainder, where $m-1=2^{\tilde{n}}s+h$.

When $m-1=2^n+c$ $(0<c<2^n)$, the decomposition of $m-1$ as 2^n+c does not decrease the number of required multiplications because the number of

multiplications becomes $n+c$, that is, not less than $l(m-1)+w(n-1)-2 = n+w(c)$. Hence, in the optimal decomposition of $m-1$, the remainder h must be smaller than c and, so,

$$l(m-h-1) = l(m-1) = n+1.$$

When $m-1$ is decomposed as $\prod_{j=1}^{k} s_j + h$ and s_1 is not decomposed further, the number of required multiplications is at least

$$\sum_{j=1}^{k} l(s_j) + h \geq l(m-1) + h$$

because $w(s_j) \geq 2$. When the first factor s_1 is decomposed further, the number of required multiplications corresponding to the optimal decomposition of s_1 is at least $l(s_1)$ and, hence, the number of required multiplications by the optimal decomposition of $m-1$ is also at least $l(m-1)+h$. Therefore, we have the following propositions also.

Proposition 4.4.3 *In the optimal decomposition of $m-1$, the remainder h must be smaller than $w(m-1)-2$.*

Proposition 4.4.4 *When $m-1 = 2^n + 2^{\tilde{n}}$, where $n > \tilde{n}$, i.e., $w(m-1) = 2$, the optimal decomposition is $m-1$ itself and the number of required multiplications is $n+1$.*

In practical applications, m is usually chosen as a power of 2. When $m = 2^n, m-1 = 2^n - 1$ and $l(m-1) = w(m-1) = n$. If we do not decompose $m-1$, Algorithm[IT] requires $2n-2$ multiplications. If n is even, then $2^n - 1$ can be factorized as $(2^{n/2}+1) \times (2^{n/2}-1)$ and, when $n/2$ is even again, $2^{n/2}-1$ can be factorized further. The number of multiplications is decreased in this case. However, $2^n - 1$ can be a prime number. In this case, as n is odd, we can always decompose $2^n - 1$ as $2(2^{(n-1)/2}+1) \times (2^{(n-1)/2}-1)+1$ and reduce the number of multiplications by Takagi's algorithm.

In conclusion, the proposed algorithm reduces the number of required multiplications by decomposing $m-1$ into several factors and a small remainder.

CHAPTER 5

CONCLUSION

In many cryptographic and coding techniques, it is necessary to implement finite field arithmetic such as addition, squaring and multiplication of two elements. Especially, multiplication of two field elements is difficult and time consuming. The actualization of these arithmetic operations can be done more efficiently by a suitable choice of field representation. For instance, using normal basis, the squaring of an element is just a cyclic shift operation of itself. In my thesis, first we gave some basic definitions, theorems and results related with the normal basis in some finite field. After that, we mentioned the advantages of using normal basis representation. Moreover, we gave whether there is an advantage of using the pair of dual bases in the multiplication operation.

However, Mullin, Onyszchuk and Vanstone proved that there is a lower bound for the complexity of the normal basis. Hence, the concept of optimal normal bases was introduced. Next, we gave the answers of questions that how we can construct the optimal normal bases and what the ways of determination of optimal normal bases.

There are many applications of optimal normal bases. Therefore, we studied a multiplication algorithm by using optimal normal basis. Besides, we gave the concept of modified optimal normal bases which also produce efficiency in multiplication. Next, it was shown that large powers of the generators of optimal normal bases, which have high multiplicative order, can be computed efficiently. Con-

sequently, we presented an algorithm finding the multiplicative inverse of a field element efficiently.

Eventually, we point out some some problems related with my thesis. By our classification, not all finite fields have optimal normal bases. For fields without optimal normal bases, it is desirable to have a normal basis of low complexity. Therefore, the following question is of interest: What is the minimal complexity of normal bases in F_{q^n} over F_q, and how to construct a normal basis of minimal complexity when there is no optimal normal basis in F_{q^n} over F_q? For cryptographic purposes it is important to have either a primitive element or an element of high multiplicative order in F_{2^n}. Another interesting problem is the following: Let n be a positive integer and γ a $2n+1$-th primitive root of unity in some extension of F_2. Determine the multiplicative order of $\alpha = \gamma + \gamma^{-1}$.

The following problem is the converse of the above problem.

Let α be an element in an extension field of F_2. Given the multiplicative order of α, determine the order of γ, where $\alpha = \gamma + \gamma^{-1}$.

REFERENCES

[1] Ash, D.W., Blake, I.F. and Vanstone, S.A. *Low Complexity Normal Bases.* Discrete Applied Math. **25** (1989). 191-210.

[2] Chang, Y., Lu, E., Lee, Y., Leu, Y., and Shyu, H. *Two Algorithms for Computing Multiplicative Inverses in $GF(2^m)$.* accepted by Information Processing Letters

[3] Chang, Y., Truong, T.K., and Reed I.S. *Normal Bases Over $GF(q)$.* Journal of Algebra **241** (2001). 89-101

[4] Chang, Y., Truong, T.K., Reed, I.S., and Mullen, G.L. *The Number of Irreducible Polynomials of Fixed Degree and Trace Over $GF(q)$.* submitted for publication

[5] Coutinho, S.C. *The Mathematics of Ciphers.* Num. th., RSA

[6] Elgamal, T. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.* IEEE Trans. Info. Th. **31** (1985). 469-472

[7] Feng, G.L. *A VLSI Architecture for Fast Inversion in $GF(2^m)$.* IEEE Trans. Comput. **38** (1989). 1383-1386

[8] Gao, S. *The Determination of Optimal Normal Bases Over Finite Fields.* CORR 92-01. Department of Combinatorics and Optimization. University of Waterloo. 1992

[9] Gao, S., and Lenstra, H.W., Jr. *Optimal Normal Bases.* Designs, Codes and Cryptography. **2** (1992). 315-323

[10] Gao, S., and Vanstone, S. *On Orders of Optimal Normal Basis Generators.* Math. Comp. **64** (1995). no.211. 1227-1233

[11] Geisellmann, W., and Gollmann, D. *Symmetry and Duality in Normal Basis Multiplication.* AAECC-6. Lecture Notes in Computer Science. **357** (1989). Springer-Verlag. 230-238

[12] Geisellmann, W., and Gollmann, D. *Self Dual Bases in F_q.* 1992. preprint

[13] Geisellmann, W., and Gollmann, D. *Duality and Normal Basis Multiplication.* Cryptography and coding III. (Cirencester 1991. 187-195

[14] Hensel, K. *Uber die Darstellung der Zahlen eines Gattungsbereiches fur einen Beliebigen Primdivisor.* J. Reine Angew. Math. **103** (1888). 230-237

[15] Hsu, I.S., Truong, T.K., Deutsch, L.J., and Reed, I.S. *A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases.* IEEE Trans. Comp. vol.C-37. No.6 (1988). 735-739

[16] Itoh, T., and Tsukii, S. *A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Basis.* Information and Computing. **78** (1988). 171-177

[17] Itoh, T., and Tsukii, S. *A Fast Algorithm for Computing Multiplicative Inverses in Finite Fields Using Normal Basis.* IEICE Trans. (A). **J70-A** (1989). 1637-1644

[18] Jungnickel, D. *Trace-orthogonal Normal Bases.* Discrete Applied Math. to appear

[19] Lenstra, H.W., Jr. *Optimal Normal Bases Over the Field of Two Elements.* preprint. 1991

[20] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and Their Applications.* Cambridge University Press. 1986

[21] Massey, J.L., and Omura, J.K. *Computational Method and Apparatus for Finite Field Arithmetic.* U.S.patent #4,587,627,. May 1986

[22] Morii, M., Kasahara, M., and Whiting, D. *Efficient Bit-serial Multiplication and the Discrete-time Wiener-Hopf Equation Over Finite Fields.* IEEE Trans. Info. Th. bf 35 (1989). 1177-1183

[23] Mullin, R.C. *A Characterization of the Extremal Distributions of Optimal Normal Bases.* to appear in *Proc. Marshall Hall Memorial Conference*, Burlington, Vermont. 1990

[24] Mullin, R., Onyszchuk, I., Vanstone, S., and Wilson, R. *Optimal Normal Bases in $GF(p^n)$.* Discrete Applied Math. **22** (1988 / 1989). 149-161

[25] Park, I.W., Jung, S.W., Kim, H.J., and Lim, J.I. *Fast Operation Method in $GF(2^n)$ Using a Modified Optimal Normal Basis.* Comm. Korean Math. Soc. **12** (1997). No.3. 531-538

[26] Pei, D., Wang, C., and Omura, J. *Normal Bases of Finite Field $GF(2^m)$.* IEEE Trans. Inform. Theory **32** (1986). 285-287

[27] Pott, A. *On the Complexity of Normal Bases.* Bull. Inst. Combin. Appl. **4** (1992). 51-52

[28] Seguin, G.E. *Low Complexity Normal Bases for $F_{2^{mn}}$.* Discrete Applied Math. **28** (1990). 309-312

[29] Semaev, I.A. *Construction of Polynomials Irreducible Over a Finite Field with Linearly Independent Roots.* Math. USSR Sbornik. **63** (1989). 507-519

[30] Stinson, D.R. *Some Observations on Parallel Algorithms for Fast Exponentiation in $GF(2^n)$.* SIAM J.Comput. **19** (1990). 711-717

[31] Stinson, D.H. *On Bit-serial Multiplication and Dual Bases in $GF(2^m)$.* IEEE Trans. Info. Th. **37** (1991). 1733-1736

[32] Sunar, B., and Koc, C.K. *An Efficient Optimal Normal Basis Type II Multiplier.* IEEE Transactions on Computers. **50(1)** (2001). 83-87

[33] Takagi, N., Yoshiki, Y., and Takagi, K. *A Fast Algorithm for Multiplicative Inversion in $GF(2^m)$ Using Normal Basis.* IEEE Transactions on Computers. Vol.50 No.5 (2001)

[34] Von zur gathen, J. *Efficient and Optimal Exponentiation in Finite Fields.* Comput. Complexity. **1** (1991). 360-394

[35] Wang, C.C., Truong, T.K., Shao, H.M., Deutsch, L.J., Omura, J.K., and Reed, I.S. *VLSI Architecture for Computing Multiplications and Inverses in $GF(2^m)$.* IEEE Trans. Computers. **34** (1985). 709-716

[36] Wang, M., and Blake, I.F. *Bit-serial Multiplication in Finite Fields.* SIAM J. Disc. Math. **3** (1990). 140-148

[37] Wassermann, A. *Konstruktion von Normalbasen.* Bayreuther Mathematische Schriften. **31** (1990). 155-164

REFERENCES

[1] Ash, D.W., Blake, I.F. and Vanstone, S.A. *Low Complexity Normal Bases.* Discrete Applied Math. **25** (1989). 191-210.

[2] Chang, Y., Lu, E., Lee, Y., Leu, Y., and Shyu, H. *Two Algorithms for Computing Multiplicative Inverses in $GF(2^m)$.* accepted by Information Processing Letters

[3] Chang, Y., Truong, T.K., and Reed I.S. *Normal Bases Over $GF(q)$.* Journal of Algebra **241** (2001). 89-101

[4] Chang, Y., Truong, T.K., Reed, I.S., and Mullen, G.L. *The Number of Irreducible Polynomials of Fixed Degree and Trace Over $GF(q)$.* submitted for publication

[5] Coutinho, S.C. *The Mathematics of Ciphers.* Num. th., RSA

[6] Elgamal, T. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.* IEEE Trans. Info. Th. **31** (1985). 469-472

[7] Feng, G.L. *A VLSI Architecture for Fast Inversion in $GF(2^m)$.* IEEE Trans. Comput. **38** (1989). 1383-1386

[8] Gao, S. *The Determination of Optimal Normal Bases Over Finite Fields.* CORR 92-01. Department of Combinatorics and Optimization. University of Waterloo. 1992

[9] Gao, S., and Lenstra, H.W., Jr. *Optimal Normal Bases.* Designs, Codes and Cryptography. **2** (1992). 315-323

[10] Gao, S., and Vanstone, S. *On Orders of Optimal Normal Basis Generators.* Math. Comp. **64** (1995). no.211. 1227-1233

[11] Geisellmann, W., and Gollmann, D. *Symmetry and Duality in Normal Basis Multiplication.* AAECC-6. Lecture Notes in Computer Science. **357** (1989). Springer-Verlag. 230-238

[12] Geisellmann, W., and Gollmann, D. *Self Dual Bases in F_q.* 1992. preprint

[13] Geisellmann, W., and Gollmann, D. *Duality and Normal Basis Multiplication.* Cryptography and coding III. (Cirencester 1991. 187-195

[14] Hensel, K. *Uber die Darstellung der Zahlen eines Gattungsbereiches fur einen Beliebigen Primdivisor.* J. Reine Angew. Math. **103** (1888). 230-237

[15] Hsu, I.S., Truong, T.K., Deutsch, L.J., and Reed, I.S. *A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases.* IEEE Trans. Comp. vol.C-37. No.6 (1988). 735-739

[16] Itoh, T., and Tsukii, S. *A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Basis.* Information and Computing. **78** (1988). 171-177

[17] Itoh, T., and Tsukii, S. *A Fast Algorithm for Computing Multiplicative Inverses in Finite Fields Using Normal Basis.* IEICE Trans. (A). **J70-A** (1989). 1637-1644

[18] Jungnickel, D. *Trace-orthogonal Normal Bases.* Discrete Applied Math. to appear

[19] Lenstra, H.W., Jr. *Optimal Normal Bases Over the Field of Two Elements.* preprint. 1991

[20] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and Their Applications.* Cambridge University Press. 1986

[21] Massey, J.L., and Omura, J.K. *Computational Method and Apparatus for Finite Field Arithmetic.* U.S.patent #4,587,627,. May 1986

[22] Morii, M., Kasahara, M., and Whiting, D. *Efficient Bit-serial Multiplication and the Discrete-time Wiener-Hopf Equation Over Finite Fields.* IEEE Trans. Info. Th. bf 35 (1989). 1177-1183

[23] Mullin, R.C. *A Characterization of the Extremal Distributions of Optimal Normal Bases.* to appear in *Proc. Marshall Hall Memorial Conference*, Burlington, Vermont. 1990

[24] Mullin, R., Onyszchuk, I., Vanstone, S., and Wilson, R. *Optimal Normal Bases in $GF(p^n)$.* Discrete Applied Math. **22** (1988 / 1989). 149-161

[25] Park, I.W., Jung, S.W., Kim, H.J., and Lim, J.I. *Fast Operation Method in $GF(2^n)$ Using a Modified Optimal Normal Basis.* Comm. Korean Math. Soc. **12** (1997). No.3. 531-538

[26] Pei, D., Wang, C., and Omura, J. *Normal Bases of Finite Field $GF(2^m)$.* IEEE Trans. Inform. Theory **32** (1986). 285-287

[27] Pott, A. *On the Complexity of Normal Bases.* Bull. Inst. Combin. Appl. **4** (1992). 51-52

[28] Seguin, G.E. *Low Complexity Normal Bases for $F_{2^{mn}}$.* Discrete Applied Math. **28** (1990). 309-312

[29] Semaev, I.A. *Construction of Polynomials Irreducible Over a Finite Field with Linearly Independent Roots.* Math. USSR Sbornik. **63** (1989). 507-519

[30] Stinson, D.R. *Some Observations on Parallel Algorithms for Fast Exponentiation in $GF(2^n)$.* SIAM J.Comput. **19** (1990). 711-717

[31] Stinson, D.H. *On Bit-serial Multiplication and Dual Bases in $GF(2^m)$.* IEEE Trans. Info. Th. **37** (1991). 1733-1736

[32] Sunar, B., and Koc, C.K. *An Efficient Optimal Normal Basis Type II Multiplier.* IEEE Transactions on Computers. **50(1)** (2001). 83-87

[33] Takagi, N., Yoshiki, Y., and Takagi, K. *A Fast Algorithm for Multiplicative Inversion in $GF(2^m)$ Using Normal Basis.* IEEE Transactions on Computers. Vol.50 No.5 (2001)

[34] Von zur gathen, J. *Efficient and Optimal Exponentiation in Finite Fields.* Comput. Complexity. **1** (1991). 360-394

[35] Wang, C.C., Truong, T.K., Shao, H.M., Deutsch, L.J., Omura, J.K., and Reed, I.S. *VLSI Architecture for Computing Multiplications and Inverses in $GF(2^m)$.* IEEE Trans. Computers. **34** (1985). 709-716

[36] Wang, M., and Blake, I.F. *Bit-serial Multiplication in Finite Fields.* SIAM J. Disc. Math. **3** (1990). 140-148

[37] Wassermann, A. *Konstruktion von Normalbasen.* Bayreuther Mathematische Schriften. **31** (1990). 155-164