Normal Bases over Finite Fields

by

Shuhong Gao

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 1993

Abstract

Interest in normal bases over finite fields stems both from mathematical theory and practical applications. There has been a lot of literature dealing with various properties of normal bases (for finite fields and for Galois extension of arbitrary fields). The advantage of using normal bases to represent finite fields was noted by Hensel in 1888. With the introduction of optimal normal bases, large finite fields, that can be used in secure and efficient implementation of several cryptosystems, have recently been realized in hardware. The present thesis studies various theoretical and practical aspects of normal bases in finite fields.

We first give some characterizations of normal bases. Then by using linear algebra, we prove that F_{q^n} has a basis over F_q such that any element in F_q represented in this basis generates a normal basis if and only if some groups of coordinates are not simultaneously zero. We show how to construct an irreducible polynomial of degree 2^n with linearly independent roots over F_q for any integer n and prime power q. We also construct explicitly an irreducible polynomial in $F_p[x]$ of degree p^n with linearly independent roots for any prime p and positive integer n. We give a new characterization of the minimal polynomial of α^t for any integer t when the minimal polynomial of α is given. When $q \equiv 3 \bmod 4$, we present an explicit complete factorization of $x^{2^n} - 1$ over F_q for any integer n.

The principal result in the thesis is the complete determination of all optimal normal bases in finite fields, which confirms a conjecture by Mullin, Onyszchuk, Vanstone and Wilson. Finally, we present some explicit constructions of normal bases with low complexity and some explicit constructions of self-dual normal bases.

Acknowledgements

I count myself as being the most fortunate to be able to work under the supervision of Ronald C. Mullin. His enthusiasm for mathematics and his high level of expectation have greatly influenced me. I found him always encouraging, supportive and patient with me. The same acknowledgement should also go to Ian F. Blake who has acted as my second supervisor (though not officially!) and I deeply appreciate the insight I gained through my association with him.

I express many thanks to Hendrik W. Lenstra, Jr., Gary L. Mullen, Scott A. Vanstone and Wandi Wei; I greatly benefited from conversations, electronic communications and joint works with them. Thanks are also due to Dieter Jungnickel, Helmut Meyn, Paul Schellenberg and Jeff Shallit for their useful comments on my thesis.

I am grateful to Mert Cramer, Charles Haff and David Jackson, who were very helpful in the early days of my graduate study at Waterloo. I would like to thank my previous office mate Bill Martin for his help and friendship.

I acknowledge Kluwer Academic Publishers for permission to use, in part, material from *Applications of Finite Fields* by A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian, 1993. I also acknowledge the Government of Ontario for financial support through an Ontario Graduate Scholarship.

Finally, this thesis might not exist at all without the love and support of my family. My wife Suhua Zhang made countless sacrifices so that I could focus on my study; for her love, encouragement and inspiration I can never thank her enough. My twin boys Ian (Qiying) and Phillip (Qifei) made my life much more cheerful and colorful: typically they would climb on my shoulders and say “Ride on, Cowboy! Yee——Ha!!”

Contents

Chapter 1

Introduction

In this chapter we explain why we are interested in normal bases and give a brief overview of the thesis. We will assume that one is familiar with the basic concepts for field extensions; our standard reference is Jacobson [69].

Let F be field and E be a finite Galois extension of F of degree n and Galois group G. A *normal basis* of E over F is a basis of the form $\{\sigma\alpha : \sigma \in G\}$ where $\alpha \in E$. That is, a normal basis consists of all the algebraic conjugates of some element with the property that they are linearly independent over the ground field. For finite fields, let q be a prime power and n a positive integer. Let F_q and F_{q^n} be finite fields of q and q^n elements, respectively. The field F_{q^n} is viewed as an extension of F_q. The Galois group of F_{q^n} over F_q is cyclic and is generated by the Frobenius map: $\alpha \mapsto \alpha^q$ for $\alpha \in F_{q^n}$. A normal basis of F_{q^n} over F_q is thus of the form: $\{\alpha, \alpha^q, \ldots, \alpha^{q^n-1}\}$ for some $\alpha \in F_{q^n}$.

Interest in normal bases stems both from mathematical theory and practical applications. The notion of normal bases appeared in the last century. A possible reason for the early interest in normal bases may be the fact that Gauss [54] used normal bases to solve the problem of when a regular polygon can be drawn with ruler and compass alone. Actually Gauss used normal bases (which he called *periods*) to construct the subfields of a cyclotomic field. In general, normal bases can be used to realize the Galois correspondence between intermediate fields of a finite Galois extension of fields and the subgroups of its Galois group. We will dwell on this in the next section.

At the practical aspect, 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 required. Work in this area has resulted in several hardware and software designs or implementations [41, 45, 121, 145, 146, 151], including single-chip exponentiators for the fields $F_{2^{127}}$ [152], $F_{2^{155}}$ [3], and $F_{2^{332}}$ [56], and an encryption processor for $F_{2^{593}}$ [114] for public key cryptography. These products are based on multiplication schemes due to Massey and Omura [95] and Mullin, Onyszchuk and Vanstone [105] by using normal bases to represent finite fields and choosing appropriate algorithms for the arithmetic. Interestingly, the advantage of using a normal basis representation was noticed by Hensel [61] in 1888, long before finite field theory found its practical applications. The complexity of the hardware design of such multiplication schemes is heavily dependent on the choice of the normal basis used.

1.1 Galois Correspondence

Let F be any field and E a finite Galois extension of F, with Galois group G. The main theorem of Galois theory [48] guarantees that there is a bijective correspondence between the subgroups of G and the intermediate fields of E over F: if H is a subgroup of G then the fixed subfield

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha, \text{ for all } \sigma \in H\}$$

of E relative to H is a subfield of E containing F such that

$$H = \mathrm{Aut}(E/E^H)$$

where $\mathrm{Aut}(E/E^H)$ denotes the set of all automorphisms of E that fix E^H. If K is an intermediate field of E over F then $\mathrm{Aut}(E/K)$ is a subgroup of G and

$$K = E^{\mathrm{Aut}(E/K)}.$$

Moreover, for any subgroup H of G, we have

$$|H| = [E : E^H], \quad [G : H] = [E^H : F]$$

and E^H is normal over F if and only if H is normal in G.

The problem is to realize the correspondence constructively, that is, to find $\mathrm{Aut}(E/K)$ when given K, and E^H when given H. Here we assume that we are given the extension E of F

and its Galois group $G = \mathrm{Aut}(E/F)$. By "given E over F", we mean that we have a basis $A = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ of E over F and the n^2 cross products $\alpha_i\alpha_j$ expressed as linear combinations of A with coefficients from F. By "given G", we mean that we know the matrix representation of each automorphism in G under the same basis A.

We follow the approaches by Pohst and Zassenhaus [110, pp. 171-173] and van der Waerden [141, pp. 169]. For the first part of the problem, suppose that $K = F(\beta_1, \cdots, \beta_k)$ where $\beta_i \in E$ is expressed in the basis A for $1 \le i \le k$. Then $\mathrm{Aut}(K/F)$ simply consists of those automorphisms σ in G such that $\sigma\beta_i = \beta_i$ for all i with $1 \le i \le k$; for they will fix all rational functions of $\beta_1, \ldots, \beta_k$ as well.

For the second part of the problem, we show in the sequel that normal bases offer an elegant solution. Let $N = \{\sigma\alpha : \sigma \in G\}$ be a normal basis of E over F and H be a subgroup of G. Let $n = [G : H]$ and let the right coset decomposition of G relative to H be

$$G = \bigcup_{i=1}^{n} Hg_i$$

where $g_i \in G$. The *Gauss periods* of N with respect to H are defined to be

$$\zeta_i = \sum_{\sigma \in H} \sigma g_i \, \alpha, \quad i = 1, 2, \cdots, n. \tag{1.1}$$

Note that $\zeta_1, \zeta_2, \cdots, \zeta_n$ are linearly independent over F since they are non-overlapping F-linear combinations of N. For any element

$$\xi = \sum_{\sigma \in G} u_\sigma \, \sigma\alpha, \quad u_\sigma \in F,$$

of E, it is fixed by all elements in H if and only if it has constant coefficients on every right coset of G relative to H. This implies that $\zeta_i \in E^H$ and every element of E^H is an F-linear combination of $\zeta_1, \zeta_2, \cdots, \zeta_n$. Thus we have proved that the Gauss periods (1.1) form a basis of E^H over F, i.e.

$$E^H = F\zeta_1 \oplus F\zeta_2 \oplus \cdots \oplus F\zeta_n. \tag{1.2}$$

Moreover, if H is normal in G then the Gauss periods are conjugate to each other and thus they form a normal basis for E^H over F. This solves the second part of the problem if we know how to construct a normal basis for E over F.

Let us look at the special case of cyclotomic fields which were first studied by C.F. Gauss [54] in connection with his investigation into the constructability of regular polygons. This is why the elements in (1.1) are called Gauss periods. Let m be a prime number and β an mth primitive root of unity in the field of complex numbers. Then

$$\beta^{m-1} + \cdots + \beta + 1 = 0$$

and β generates the mth cyclotomic field

$$E_m = \mathbb{Q}(\beta),$$

where $\mathbb{Q}$ is the field of rational numbers. It can be proved that

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

is a normal basis of E_m over $\mathbb{Q}$. Let τ be a primitive element of $\mathbb{Z}_m$, i.e. τ is an integer such that

$$\{1, 2, \cdots, m-1\} \equiv \{\tau, \tau^2, \cdots, \tau^{m-1}\} \bmod m.$$

Then the Galois group of E_m over $\mathbb{Q}$ is generated by the automorphism ϱ which carries β to β^τ, that is,

$$G =< \varrho >= \{1 = \varrho^0, \varrho, \varrho^2, \cdots, \varrho^{m-2}\}.$$

For any factor n of $m-1$, let $m-1 = nk$. Then

$$H = \{1, \varrho^n, \varrho^{2n}, \cdots, \varrho^{(k-1)n}\}$$

is a subgroup of G of index n. The Gauss periods of N with respect to H are

$$\zeta_i = \sum_{j=0}^{k-1} \varrho^{jn} \varrho^i \beta = \sum_{j=0}^{k-1} \beta^{\tau^{jn+i}}, \quad 0 \le i \le n-1, \tag{1.3}$$

which form a normal basis of the unique subfield of E_m of degree n over $\mathbb{Q}$. If $m-1$ has only small prime factors then one can construct E_m by building a sequence of subfields, where each of them has a small degree over the preceding one, by using Gauss periods. This is the basic idea that was used by C.F. Gauss [54] to determine when a regular polygon can be drawn with ruler and compass alone. In particular, he discovered how to draw a regular 17-gon with ruler and compass, which had remained as an unsolved problem for more than 2000 years.

We will show in Chapter 4 that under certain conditions Gauss periods (1.3) give a family of normal bases with low *complexity* in finite fields, including essentially all the *optimal normal bases*. The definition for the complexity of normal bases and for optimal normal bases is given in the next section. We mention that Gauss periods are also useful in integer factorization [12] and construction of irreducible polynomials [1] (refer to section 4.3).

1.2 Finite Field Arithmetic

Let q be a prime power and n a positive integer. Let F_q and F_{q^n} be finite fields of q and q^n elements, respectively. Let us first look at how 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 $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in F_{q^n}$ be linearly independent over F_q. Then every element $A \in F_{q^n}$ can be represented as $A = \sum_{i=0}^{n-1} a_i \alpha_i$ where $a_i \in F_q$. Thus F_{q^n} can be identified as F_q^n, the set of all n-tuples over F_q, and $A \in F_{q^n}$ can written as $A = (a_0, a_1, \ldots, a_{n-1})$. Let $B = (b_0, b_1, \ldots, b_{n-1})$ be another element in F_{q^n}. Then addition is component-wise and is easy to implement. Multiplication is more complicated. Let $A \cdot B = C = (c_0, c_1, \ldots, c_{n-1})$. We wish to express the c_i's as simply as possible in terms of the a_i's and b_i's. Suppose

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k, \quad t_{ij}^{(k)} \in F_q. \tag{1.4}$$

Then it is easy to see that

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

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 a *multiplication table* for F_{q^n} over F_q.

Observe that the matrices $\{T_k\}$ are independent of A and B. An obvious implementation of multiplication in F_{q^n} is to build n circuits corresponding to the T_k's such that each circuit outputs a component of $C = A \cdot B$ on input A and B. If n is big then this scheme is impractical. Fortunately, there are many bases available 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 regularity so that one may judiciously choose some multiplication algorithm to make a hardware or software design of a finite field feasible for large n. One example is the bit-serial multiplication scheme due to Berlekamp [16], see also [97], and its generalizations [101, 55, 57, 143, 63, 134] using a pair of (dual) bases. In the following we examine the Massey-Omura scheme [95] which exploits the symmetry of normal bases.

A normal basis of F_{q^n} over F_q is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ for some $\alpha \in F_{q^n}$. Let $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q with $\alpha_i = \alpha^{q^i}$ for $0 \leq i \leq n-1$. 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. The element A^q has coordinate vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. 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. 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 such cryptosystems as the Diffie-Hellman key exchange [42] and ElGamal cryptosystem [44] where one needs to compute large powers of elements in a fixed finite field.

Let the $t_{ij}^{(k)}$ terms be defined by (1.4). Raising both sides of equation (1.4) to the $q^{-\ell}$-th power, one finds that

$$t_{ij}^{(\ell)} \;=\; t_{i-\ell,j-\ell}^{(0)}, \quad \text{for any } 0 \leq i, j, \ell \leq n-1.$$

Consequently, if a circuit is built to compute c_0 with inputs A and B, then the same circuit with inputs $A^{q^{-\ell}}$ and $B^{q^{-\ell}}$ yields the product term c_ℓ. ($A^{q^{-\ell}}$ and $B^{q^{-\ell}}$ are simply cyclic shifts of the vector representations of A and B.) 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 gates required in this circuit 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 as small as possible.

Let

$$\alpha\alpha_i \;=\; \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \leq i \leq n-1, \;\; t_{ij} \in F_q. \tag{1.5}$$

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

$$t_{ij}^{(k)} = t_{i-j,k-j}, \quad \text{for all } i, j, k.$$

Therefore the number of non-zero entries in T_0 is equal to the number of non-zero entries in T. Following Mullin, Onyszchuk, Vanstone and Wilson [103], we call the number of non-zero entries in T the *complexity* of the normal basis N, denoted by c_N. Since the matrices $\{T_k\}$ are uniquely determined by T, we call T the multiplication table of the normal basis N. The following theorem gives us a lower bound for c_N.

Theorem 1.2.1 (Mullin et al. [103]) *For any normal basis N of F_{q^n} over F_q, $c_N \geq 2n-1$.*

Proof: Let $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Then $b = \sum_{k=0}^{n-1} \alpha_k = Tr(\alpha) \in F_q$. Summing up the equations (1.5) 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 non-zero 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 non-zero 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 non-zero t_{ij}'s. So there are at least $2n-1$ non-zero terms in T, with equality if and only if the element α occurs with a non-zero coefficient in exactly one cross-product term $\alpha\alpha_i$ (with coefficient b) and every other member of N occurs in exactly two such products, with coefficients that are additive inverses. □

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

A major concern for a hardware implementation is the interconnections between registers containing the elements A, B and C. The *fanout* of a cell is the number of connections to the cell, and should be as small as possible. Agnew, Mullin, Onyszchuk and Vanstone [2] designed a different architecture with a low fanout, and they successfully implemented the field $F_{2^{593}}$ in hardware (see [114]). Since this scheme is more complicated, we omit its description here. We only remark that the complexity of this scheme also depends on the number of non-zero entries in T.

1.3 A Brief Overview

In Chapter 2, we investigate the structural properties of normal bases. We begin with some characterizations of normal bases. We then use linear algebra to decompose F_{q^n} into a direct sum of subspaces over F_q such that an element α in F_{q^n} generates a normal basis if and only if the projections of α in some subspaces are nonzero. This means that F_{q^n} has a basis over F_q such that any element in F_q represented in this basis generates a normal basis if and only if some groups of coordinates are not simultaneously zero. In particular, we can obtain all the normal elements in F_{q^n} if we can factor $x^n - 1$ over F_q. We present an explicit complete factorization of $x^{2^e} - 1$ over F_p when $p \equiv 3 \bmod 4$ is a prime.

In Chapter 3, we briefly survey various algorithms for constructing normal bases in finite fields, where the complexity issue is ignored. We show that if $x^n - a$, where $a \in F_q$, is irreducible over F_q then $ax^n - (x-1)^n$ is irreducible and has linearly independent roots over F_q. In particular, if $q \equiv 1 \pmod 4$ then $ax^{2^n} - (x-1)^{2^n}$ is irreducible with linearly independent roots over F_q for any quadratic nonresidue $a \in F_q$ and any integer n. When a prime $p \equiv 3$ (mod4), we show that if $x^2 - bx - c \in F_p[x]$, with $b \neq 2$ and c a quadratic residue in F_p, is irreducible over F_p, then the polynomial

$$(x-1)^{2^{k+1}} - b(x-1)^{2^k} x^{2^k} - cx^{2^k}$$

is irreducible with roots being linearly independent over F_p for every integer $k \geq 0$. For any prime p and positive integer n, we construct explicitly an irreducible polynomial in $f_p[x]$ of degree p^n with linearly independent roots. We give a new characterization of the minimal polynomial of α^t for any integer t when the minimal polynomial of α is given. When $q \equiv 3 \pmod 4$, we present an explicit complete factorization of $x^{2^n} - 1$ over F_q for any integer n, which enables us to compute efficiently $u \in F_p$ such that the roots of $x^2 - 2ux - 1$ are quadratic nonresidues in F_{q^2}.

In Chapter 4, we completely determine all the optimal normal bases in finite fields, thus confirming a conjecture by Mullin, Onyszchuk, Vanstone and Wilson. We show that there is an optimal normal basis in F_{q^n} over F_q if and only if either **(i)** $n+1$ is a prime and q is primitive in $\mathbb{Z}_{n+1}$ or **(ii)** $q = 2^v$ for some integer v such that $\gcd(v, n) = 1$, $2n+1$ is a prime and $\mathbb{Z}^*_{2n+1}$ is generated by 2 and -1.

Finally, in Chapter 5, we present some explicit constructions of normal bases with low complexity and some explicit constructions of self-dual normal bases. For example, we show that, for any $\beta \in F_q^*$ with $\mathrm{Tr}_{q|p}(\beta) = 1$, the polynomial $x^p - x^{p-1} - \beta^{p-1}$ is irreducible over F_q and its roots form a self-dual normal basis with complexity at most $3p - 2$ of F_q over F_p where p is the characteristic of F_q. We also prove that, for any divisor n of $q-1$ and $a = \beta^{(q-1)/n}$ where $\beta \in F_q$ with multiplicative order t such that $\gcd(n, (q-1)/t) = 1$, the polynomial $x^n - \beta(x - a + 1)^n$ is irreducible over F_q and its roots constitute a normal basis with complexity at most $3n-2$ of F_{q^n} over F_q.

1.4 Some Notes

In this thesis we will focus our attention exclusively on normal bases in finite fields. For completeness, we give a brief survey here on the results for normal bases in the general setting of Galois extensions of arbitrary fields. We also mention some results on primitive normal bases in finite fields which will not be discussed in the thesis.

Theorem 1.4.1 (The normal basis theorem) *There is a normal basis for any finite Galois extension of fields.*

The normal basis theorem for finite fields was conjectured by Eisenstein [43] in 1850 and partly proved by Schönemann [118] in 1850. The first complete proof was given by Hensel [61] in 1888. The normal basis theorem for Galois extension of arbitrary fields was proved by Noether [104] in 1932 and Deuring [40] in 1933. This theorem is included in most algebra textbooks, see for example, Albert [7], Bourbaki [27], Cohn [36], Hungerford [64], Jacobson [69], Lang [78], Rédei [112] and van der Waerden [141]. For different proofs of the normal basis theorem, see Artin [8], Berger and Reiner [15], Krasner [76], Waterhouse [149] and Childs and Orzech [33]. Lenstra [86] generalizes the normal basis theorem to infinite Galois extensions. Bshouty and Seroussi [29] and Scheerhorn [116] give generalizations of the normal basis theorem for finite fields in different directions. Blessenohl and Johnsen [25] prove that for each finite Galois extension E of F there exists an element $\alpha \in E$ that gives a normal basis over each intermediate field (see [24] for a simpler proof).

For finite fields, there is another refinement of the normal basis theorem.

Theorem 1.4.2 *For any prime power q and positive integer n, there is a primitive normal basis in F_{q^n} over F_q.*

Here by a *primitive normal basis* of F_{q^n} over F_q we mean a normal basis $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ such that α also generates the multiplicative group of F_{q^n}. This result was proved by Carlitz

[32] in 1952 for q^n sufficiently large, by Davenport [38] in 1968 for the case that q is a prime and by Lenstra and Schoof [87] in 1987 for the general case. For the construction of primitive normal bases and primitive elements, see Cohen [34], Hachenberger [60], Shoup [129], Stepanov and Shparlinskiy [131, 132, 133].

An important class of normal bases are self-dual normal bases. More generally, one has the concept of self-dual bases, which is useful for construction of devices for arithmetic of finite fields [16, 55, 142] and in applications to coding theory [47], cryptography [42] and the discrete Fourier transform [18]. Let E be a finite Galois extension of F with Galois group G. The trace function $\mathrm{Tr} : E \mapsto F$ is defined as

$$\mathrm{Tr}(\alpha) = \sum_{\sigma \in G} \sigma\alpha.$$

A basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of E over F is said to be dual to the basis $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ if $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{i,j}$ (which by definition is equal to 0 if $i \neq j,$ and 1 if $i = j$). It is easy to prove that each basis in E over F has a unique dual basis and the dual basis of a normal basis is again a normal basis. If a basis coincides with its dual basis then it is said to be self-dual, i.e., a basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is called *self-dual* if $\mathrm{Tr}(\alpha_i\alpha_j) = \delta_{i,j}$. Existence results of self-dual bases can be found in Serre [125] and Kahn [73, 74]. As to the existence of self-dual normal bases, we have the following two theorems.

Theorem 1.4.3 *Let E be a Galois extension of F of degree n. If n is odd then E has a self-dual normal basis over F.*

Theorem 1.4.4 *Let E be a Galois extension of F of degree n and Galois group G. Assume that G is Abelian.*

(a) *If $\mathrm{Char}(F) \neq 2$, then E has a self-dual normal basis over F if and only if n is odd.*

(b) *If $\mathrm{Char}(F) = 2$, then E has a self-dual normal basis over F if and only if the exponent of G is not divisible by 4.*

The exponent of a group G is defined to be the smallest integer m such that $g^m = 1$ for all $g \in G$. For finite fields, Theorem 1.4.4 says that F_{q^n} has a self-dual normal basis over F_q if and only if both n and q are odd or q is even and n is not divisible by 4.

The above two theorems are proved by Bayer-Fluckiger and Lenstra [13, 14]. Partial results were obtained earlier by Lempel, and Weinberger [79, 80, 82], Imamura and Morii [67, 100], Beth, Fummy and Mühlfeld [19], Kersten and Michaliček [75], Conner and Perlis [37]. For enumeration of self-dual normal bases, see Lempel and Seroussi [81] and Jungnickel, Menezes and Vanstone [72].

In designing finite field multipliers it is sometime useful to consider weakly self-dual bases [20, 101, 143]. Let $A = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ be a basis of E over F and let $B = \{\beta_0, \beta_1, \dots, \beta_{n-1}\}$ be its dual basis. Then A is said to be *weakly self-dual* if there exists a $\gamma \in E$ and a permutation π of the indices $\{0, 1, \dots, n-1\}$ so that $\beta_i = \gamma\alpha_{\pi(i)}$ for all i with $0 \leq i \leq n-1$. Obviously self-dual bases are weakly self-dual. The existence of weakly self-dual polynomial basis (by definition it is of the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$) is determined by Geiselmann and Gollmann [57] (their argument for finite fields is applicable to arbitrary fields). The existence of weakly self-dual normal bases is determined by Lenstra [83]. To state this result, we need the notion of equivalence of bases. Two Bases A and B of E over F are called equivalent if $A = cB$ for some $c \in F$.

Theorem 1.4.5 *Let E be a Galois extension of F of degree n and Galois group G. Assume that G is Abelian. Then E has a weakly self-dual normal basis over F that is not equivalent to a self-dual normal basis if and only if $E = M(i)$ where $[M, F]$ is odd, $i^2 = -1$ and i is not in F.*

In particular, the field F_{q^n} has a weakly self-dual normal basis over F_q that is not self-dual if and only if n is exactly divisible by 2 and $q \equiv 3 \bmod 4$.

Chapter 2

Basics on Normal Bases

In this chapter, we will focus on the structural properties of normal bases, where the complexity issue is usually ignored.

2.1 Introduction

For convenience, we first make some conventions and recall some definitions in this section.

In this thesis, we assume that p is a prime number, q is a power of p, and F_q denotes the finite field of q elements. Thus the characteristic of F_q is p. The field F_{q^n} is always considered as an n-dimensional extension of F_q and is thus a vector space of dimension n over F_q. The Galois group of F_{q^n} over F_q is cyclic and is generated by the Frobenius mapping $\sigma(\alpha) = \alpha^q,\ \alpha \in F_{q^n}$.

A normal basis of F_{q^n} over F_q is a basis of the form $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$, i.e., a basis consisting of all the algebraic conjugates of a fixed element. We say that α *generates* the normal basis N, or α is a *normal element* of F_{q^n} over F_q. In either case we are referring to the fact that the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over F_q.

In the following context, when we mention a normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, we always assume that $\alpha_i = \alpha^{q^i}$ for $\alpha \in F_{q^n}$ with $i = 0, 1, \ldots, n-1$.

Let $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Then for any i, j, $0 \le i, j \le n-1$,

$\alpha_i\alpha_j$ is a linear combination of $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ with coefficients in F_q. In particular,

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = T \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} \tag{2.1}$$

where T is an $n \times n$ matrix over F_q. We call (2.1) or T the *multiplication table* of the normal basis N. If α is a normal element, the multiplication table of the normal basis generated by α is also referred to as the multiplication table of α. As in section 1.2, the number of non-zero entries in T is called the *complexity* of the normal basis N, denoted by C_N. If α generates N, C_N is also denoted as C_α.

We call a polynomial in $F_q[x]$ an *N-polynomial* if it is irreducible and its roots are linearly independent over F_q. The minimal polynomial of any element in a normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is $m(x) = \prod_{i=0}^{n-1}(x - \alpha_i) \in F_q[x]$, which is irreducible over F_q. The elements in a normal basis are exactly the roots of an N-polynomial. Hence an N-polynomial is just another way of describing a normal basis.

The *trace function* of F_{q^n} over F_q is

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}.$$

The trace function is a linear functional of F_{q^n} to F_q. For brevity, we sometimes denote the trace function by $Tr_{q^n|q}$ or simply Tr if the fields are clear from context. The trace of an element over its characteristic subfield is called the *absolute trace*.

If $\bar{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\bar{\beta} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ are bases of F_{q^n} over F_q, $\bar{\beta}$ is referred to as the *dual basis* of $\bar{\alpha}$ if

$$Tr(\alpha_i\beta_j) = \delta_{ij}, \quad 1 \le i, j \le n.$$

(δ_{ij} denotes the Kronecker delta function, i.e., $\delta_{ij} = 0$ if $i \neq j$, and $\delta_{ij} = 1$ if $i = j$.) It is a standard result that for any given basis $\bar{\alpha}$ there exists a unique dual basis. If the dual basis of $\bar{\alpha}$ happens to be $\bar{\alpha}$ itself, then $\bar{\alpha}$ is called a self-dual basis.

We sometimes say that α is self-dual normal if α generates a self-dual normal basis.

In this chapter, we are mainly concerned with the problem of which elements in F_{q^n} generate a normal basis over F_q. In section 2.2, we give some characterizations of normal elements and also give a method to compute the element that generates the dual basis of a given normal basis. In Section 2.3, we show how to construct normal bases from normal bases over smaller fields. In Section 2.4, we determine how all the normal elements are distributed in the whole space, and thus we show that F_{q^n} has a basis over F_q such that any element in F_{q^n} represented in this basis generates a normal basis if and only if some groups of coordinates are not simultaneously zero. In Section 2.5, we discuss when an irreducible polynomial is an N-polynomial, i.e., an irreducible polynomial with linearly independent roots. In some special cases, one can tell immediately from the coefficients of an irreducible polynomial whether it is an N-polynomial.

2.2 Characterization of Normal Elements

In this section, we give some characterizations of normal elements and show how to compute the element that generates the dual basis of a given normal basis.

We begin with a characterization for a set of n elements in F_{q^n} to form a basis of F_{q^n} over F_q. For this purpose, we define the *discriminant* $\Delta(\alpha_1, \dots, \alpha_n)$ of the elements $\alpha_1, \dots, \alpha_n$ in F_{q^n} by the determinant:

$$\Delta(\alpha_1, \dots, \alpha_n) = \det \begin{pmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) & \cdots & Tr(\alpha_1\alpha_n) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) & \cdots & Tr(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ Tr(\alpha_n\alpha_1) & Tr(\alpha_n\alpha_2) & \cdots & Tr(\alpha_n\alpha_n) \end{pmatrix},$$

where Tr is understood to be $\mathrm{Tr}_{q^n|q}$. Obviously, $\Delta(\alpha_1, \dots, \alpha_n) \in F_q$.

Theorem 2.2.1 (Theorem 2.37, [89]) *For any n elements $\alpha_1, \dots, \alpha_n$ in F_{q^n}, they form a basis of F_{q^n} over F_q if and only if $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$.*

Proof: First assume that $\alpha_1, \dots, \alpha_n$ form a basis for F_{q^n} over F_q. We prove that $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$ by showing that the row vectors of the matrix in the definition of $\Delta(\alpha_1, \dots, \alpha_n)$ are linearly independent over F_q. For suppose that

$$c_1\mathrm{Tr}(\alpha_1\alpha_j) + \cdots + c_n\mathrm{Tr}(\alpha_n\alpha_j) = 0 \ \text{ for } 1 \leq j \leq n,$$

where $c_1, \ldots, c_n \in F_q$. Then with $\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$ we get $\mathrm{Tr}(\beta\alpha_j) = 0$ for $1 \le j \le n$, and since $\alpha_1, \ldots, \alpha_n$ span F_{q^n}, it follows that $\mathrm{Tr}(\beta\alpha) = 0$ for all $\alpha \in F_{q^n}$. However, this is only possible if $\beta = 0$, and then $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$ implies that $c_1 = \cdots = c_n = 0$.

Conversely, assume that $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ and $c_1\alpha_1 + \cdots + c_n\alpha_n = 0$ for some $c_1, \ldots, c_n \in F_q$. Then

$$c_1\alpha_1\alpha_j + \cdots + c_n\alpha_n\alpha_j = 0 \quad \text{for } 1 \le j \le n,$$

and by applying the trace function we get

$$c_1 \mathrm{Tr}(\alpha_1\alpha_j) + \cdots + c_n \mathrm{Tr}(\alpha_n\alpha_j) = 0 \quad \text{for } 1 \le j \le n.$$

But since the row vectors of the matrix in $\Delta(\alpha_1, \ldots, \alpha_n)$ are linearly independent over F_q, it follows that $c_1 = \cdots = c_n = 0$. Therefore $\alpha_1, \ldots, \alpha_n$ are linearly independent over F_q. □

Corollary 2.2.2 *The set of elements $\bar{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of F_{q^n} over F_q if and only if the matrix A is nonsingular where*

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{pmatrix}.$$

Proof: It suffices to note that $\Delta(\alpha_1, \ldots, \alpha_n) = \det(A^tA) = (\det A)^2$. □

We need the the following standard result for the remaining part of this section.

Lemma 2.2.3 *Let F be any field. For any n elements $a_0, a_1, \ldots, a_{n-1} \in F$, the $n \times n$ circulant matrix*

$$c[a_0, a_1, \ldots, a_{n-1}] = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

is nonsingular if and only if the polynomial $\sum_{i=0}^{n-1} a_i x^i$ is relatively prime to $x^n - 1$.

Proof: Let A be the following $n \times n$ permutation matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Then it is easy to see that

$$c[a_0, a_1, \ldots, a_{n-1}] = \sum_{i=0}^{n-1} a_i A^i = f(A),$$

where $f(x) = \sum_{i=0}^{n-1} a_i x^i$. Note that the minimal polynomial of A is $x^n - 1$. Assume that $f(x)$ and $x^n - 1$ are relatively prime. Then there are polynomials $a(x), b(x)$ such that

$$a(x)f(x) + b(x)(x^n - 1) = 1,$$

and hence

$$a(A)f(A) = I_n,$$

as $A^n - 1 = 0$. This implies that $f(A)$ is invertible and so nonsingular. Now assume that $\gcd(f(x), x^n - 1) = d(x) \neq 1$. Let $f(x) = f_1(x)d(x)$ and $x^n - 1 = h(x)d(x)$. Since $\deg h(x) < n$, we have $h(A) \neq 0$. As $h(A)d(A) = 0$, we see that $d(A)$ is singular. Therefore $f(A) = f_1(A)d(A)$ is singular. This shows that $f(A)$ is nonsingular if and only if $f(x)$ is relatively prime to $x^n - 1$. □

Theorem 2.2.4 (Hensel [61]) *For $\alpha \in F_{q^n}$, α generates a normal basis of F_{q^n} over F_q if and only if the polynomial $\alpha^{q^{n-1}} x^{n-1} + \cdots + \alpha^q x + \alpha \in F_{q^n}[x]$ is relatively prime to $x^n - 1$.*

Proof: Note that α generates a normal basis if and only if the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over F_q. By Corollary 2.2.2, this is true if and only if

$$\begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \cdots & \alpha^{q^{n-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \cdots & \alpha \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^{q^{n-1}} & \alpha & \alpha^q & \cdots & \alpha^{q^{n-2}} \end{pmatrix} \tag{2.2}$$

is non-singular. Note that if we reverse the order of the rows in (2.2) from the second row to the last row, we get the circulant matrix $c[\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}]$, which is non-singular if and only if (2.2) is non-singular. By Lemma 2.2.3, $c[\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}]$ is non-singular if and only if $x^n - 1$ and $\alpha^{q^{n-1}}x^{n-1} + \cdots + \alpha^q x + \alpha$ are relatively prime. □

Theorem 2.2.5 *Let $\alpha \in F_{q^n}$, $\alpha_i = \alpha^{q^i}$, and $t_i = Tr_{q^n|q}(\alpha_0\alpha_i)$, $0 \le i \le n-1$. Then α generates a normal basis of F_{q^n} over F_q if and only if the polynomial $N(x) = \sum_{i=0}^{n-1} t_i x^i \in F_q[x]$ is relatively prime to $x^n - 1$.*

Proof: By Theorem 2.2.1, we know that $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ form a basis if and only if $\Delta(\alpha_0, \dots, \alpha_{n-1}) \neq 0$. Since $Tr(\alpha_i\alpha_{i+j}) = Tr(\alpha_0\alpha_j)$, we see that

$$\Delta(\alpha_0, \dots, \alpha_{n-1}) = \det \begin{pmatrix} t_0 & t_1 & \dots & t_{n-1} \\ t_{n-1} & t_0 & \dots & t_{n-2} \\ \vdots & \vdots & & \vdots \\ t_1 & t_2 & \dots & t_0 \end{pmatrix}.$$

By Lemma 2.2.3, $\Delta(\alpha_0, \dots, \alpha_{n-1}) \neq 0$ if and only if $x^n - 1$ and $N(x) = \sum_{i=0}^{n-1} t_i x^i$ are relatively prime. □

Theorem 2.2.6 (Perlis [108]) *Let $N = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Then an element $\gamma = \sum_{i=0}^{n-1} a_i\alpha_i$, where $a_i \in F_q$, is a normal element if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_i x^i \in F_q[x]$ is relatively prime to $x^n - 1$.*

Proof: Note that

$$\begin{pmatrix} \gamma \\ \gamma^q \\ \vdots \\ \gamma^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}.$$

The n elements $\gamma, \gamma^q, \dots, \gamma^{q^{n-1}}$ are linearly independent if and only if the circulant matrix $c[a_0, a_1, \dots, a_{n-1}]$ is nonsingular, that is, if and only if the polynomial $\gamma(x) = \sum_{i=0}^{n-1} a_i x^i \in F_q[x]$ is relatively prime to $x^n - 1$. □

From this theorem we see that if there is a normal basis of F_{q^n} over F_q then the number of normal elements in F_{q^n} over F_q is equal to the number of polynomials in $F_q[x]$ of degree less than n that are relatively prime to $x^n - 1$.

Theorem 2.2.7 *The dual basis of a normal basis is a normal basis.*

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

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

Then, by definition, $AB = I_n$ and so $BA = I_n$. Note that

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

since A is a symmetric matrix. From $BA = I_n = B^T A$ we conclude that $B = B^T$. It follows that $\beta_i = \beta_1^{q^{i-1}}$ and hence that $\bar{\beta}$ is a normal basis. □

The following theorem describes a method of computing the dual basis of a normal basis (which by Theorem 2.2.7 is also a normal basis).

Theorem 2.2.8 *Let $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q. Let $t_i = Tr_{q^n|q}(\alpha_0\alpha_i)$, and $N(x) = \sum_{i=0}^{n-1} t_i x^i$. Furthermore, let $D(x) = \sum_{i=0}^{n-1} d_i x^i$, $d_i \in F_q$, be the unique polynomial such that $N(x)D(x) \equiv 1(\mathrm{mod}\ x^n - 1)$. Then the dual basis of N is generated by $\beta = \sum_{i=0}^{n-1} d_i\alpha_i$.*

Proof: Note that

$$\begin{aligned} N(x)D(x) &= \sum_{0 \le i,j \le n-1} t_i d_j x^{i+j} \\ &\equiv \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} d_k t_{i-k} x^i \pmod{x^n - 1}. \end{aligned}$$

It follows from $N(x)D(x) \equiv 1(\mathrm{mod}\ x^n - 1)$ that

$$\sum_{k=0}^{n-1} d_k t_{i-k} = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Thus

$$\begin{aligned} Tr(\alpha_i\beta^{q^j}) &= Tr\left(\alpha_i(\sum_{k=0}^{n-1} d_k\alpha_{j+k})\right) = \sum_{k=0}^{n-1} d_k Tr(\alpha_i\alpha_{j+k}) \\ &= \sum_{k=0}^{n-1} d_k Tr(\alpha_0\alpha_{i-j-k}) = \sum_{k=0}^{n-1} d_k t_{i-j-k} \\ &= \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

That is, $\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ is the dual basis of N. □

Theorem 2.2.9 *Let N and $D(x)$ be as in Theorem 2.2.8. Let $\gamma = \sum_{i=0}^{n-1} a_i\alpha_i$, where $a_i \in F_q$, be a normal element in F_{q^n} and let $\delta(x) = \sum_{i=0}^{n-1} b_i x^i$ be the unique polynomial such that $\gamma(x)\delta(x) \equiv 1 \pmod{x^n - 1}$, where $\gamma(x) = \sum_{i=0}^{n-1} a_i x^i$. Define*

$$c_i = \sum_{k=0}^{n-1} b_k d_{i+k}, \quad 0 \le i \le n-1.$$

Then $\delta = \sum_{i=0}^{n-1} c_i\alpha_i$ generates the dual basis of the normal basis generated by γ.

Proof: Let $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ be the dual basis of N. Then one can check, similar to the proof of Theorem 2.2.8, that

$$\delta = \sum_{i=0}^{n-1} b_{-i}\beta_i \tag{2.3}$$

generates the dual basis of the normal basis generated by γ. By Theorem 2.2.8, $\beta = \sum_{i=0}^{n-1} d_i\alpha_i$. Substituting β into (2.3), we obtain the theorem immediately. □

2.3 Composition of Normal Bases

It is reasonable to ask the following question: if we are given normal bases of some fields, say F_{q^t} over F_q and F_{q^v} over F_q, how can we construct a normal basis of a larger field, say $F_{q^{vt}}$ over F_q? We start with the opposite direction, that is, given a normal basis of $F_{q^{vt}}$ over F_q to construct a normal basis for F_{q^t} (or F_{q^v}) over F_q. The results are stated in terms of normal elements.

Theorem 2.3.1 (Perlis [108]) *Let t and v be any positive integers. If α is a normal element of $F_{q^{vt}}$ over F_q then $\gamma = Tr_{q^{vt}|q^t}(\alpha)$ is a normal element of F_{q^t} over F_q. Moreover, if α is self-dual normal then so is γ.*

Proof: The conjugates of $\gamma = \sum_{i=0}^{v-1} \alpha^{q^{ti}}$ are non-overlapping sums of the vt conjugates of α, which are assumed to be linearly independent over F_q. So they must also be linearly independent over F_q. The latter statement is easily checked directly. □

We remark that the multiplication table of the normal basis generated by γ in Theorem 2.3.1 is easily derived from that of α. Actually, assume that

$$\alpha\alpha^{q^i} = \sum_{j=0}^{vt-1} c(i,j)\alpha^{q^j}, \quad 0 \le i \le vt-1.$$

Then

$$\gamma\gamma^{q^i} = \sum_{j=0}^{t-1} d(i,j)\gamma^{q^j}, \quad 0 \le i \le t-1,$$

where

$$d(i,j) = \sum_{k=0}^{v-1}\sum_{\ell=0}^{v-1} c(t(\ell-k)+i, j-tk).$$

Before we go to the next theorem, we prove a lemma which itself is interesting.

Lemma 2.3.2 *Let $\gcd(v,t) = 1$. Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_v\}$ be a basis of F_{q^v} over F_q. Then A is also a basis of $F_{q^{vt}}$ over F_{q^t}.*

Proof: We need to prove that $\alpha_1, \alpha_2, \ldots, \alpha_v$ are linearly independent over F_{q^t}. Suppose there are $a_i \in F_{q^t}$, $1 \le i \le v$, such that

$$\sum_{i=1}^{v} a_i\alpha_i \;=\; 0. \tag{2.4}$$

Note that for any integer j,

$$\left(\sum_{i=1}^{v} a_i\alpha_i\right)^{q^{tj}} \;=\; \sum_{i=1}^{v} a_i^{q^{tj}}\alpha_i^{q^{tj}} \;=\; \sum_{i=1}^{v} a_i\alpha_i^{q^{tj}}.$$

Since $\gcd(v,t)=1$, when j runs through $0,1,\ldots,v-1$ modulo v, tj also runs through $0,1,\ldots,v-1$ modulo v. Note that since $\alpha_i \in F_{q^v}$, we have $\alpha_i^{q^v}=\alpha_i$ and thus $\alpha_i^{q^u}=\alpha_i^{q^k}$ whenever $u \equiv k \pmod{v}$. So (2.4) implies that

$$\sum_{i=1}^{v} a_i \alpha_i^{q^j} = 0, \quad \text{for each } j, \quad 0 \le j \le v-1,$$

that is,

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_v \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_v^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{v-1}} & \alpha_2^{q^{v-1}} & \cdots & \alpha_v^{q^{v-1}} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_v \end{pmatrix} = 0. \tag{2.5}$$

As $\alpha_1,\alpha_2,\ldots,\alpha_v$ are linearly independent over F_q, the coefficient matrix of (2.5) is nonsingular, by Corollary 2.2.2. Thus $a_1,a_2,\ldots,a_v$ must be 0, which proves that $\alpha_1,\alpha_2,\ldots,\alpha_v$ are linearly independent over F_{q^t}. □

Theorem 2.3.3 (Pincin [109], Semaev [123]) *Let $n=vt$ with v and t relatively prime. Then, for $\alpha \in F_{q^v}$ and $\beta \in F_{q^t}$, the element $\gamma=\alpha\beta \in F_{q^n}$ is a normal element of F_{q^n} over F_q if and only if α and β are normal elements of F_{q^v} and F_{q^t}, respectively, over F_q.*

Proof: First assume that γ is a normal element of F_{q^n} over F_q. Then by Theorem 2.3.1,

$$Tr_{q^n|q^t}(\gamma) \;=\; \beta Tr_{q^n|q^t}(\alpha) \;=\; \beta Tr_{q^v|q}(\alpha)$$

is a normal element of F_{q^t} over F_q. Note that $Tr_{q^v|q}(\alpha)$ must not be zero (otherwise γ would not be normal) and is in F_q. So β is a normal element of F_{q^t} over F_q. Similarly, α is a normal element of F_{q^v} over F_q.

Now assume that both of α and β are normal elements of F_{q^v} and F_{q^t}, respectively, over F_q. We prove that $\gamma=\alpha\beta$ is a normal element of F_{q^n} over F_q. As $\gcd(v,t)=1$, by the Chinese remainder theorem, for any $0 \le i \le v-1$ and $0 \le j \le t-1$ there is a unique integer k such that

$$k \equiv i \pmod{v} \quad \text{and} \quad k \equiv j \pmod{t},$$

and hence

$$\gamma^{q^k} \;=\; \alpha^{q^i}\beta^{q^j}.$$

Thus the conjugates of γ are:

$$\alpha^{q^i}\beta^{q^j}: \quad 0 \le i \le v-1, \quad 0 \le j \le t-1. \tag{2.6}$$

Now we prove that the elements of (2.6) are linearly independent over F_q. Suppose there are $a_{ij} \in F_q$ such that

$$\sum_{\substack{0 \le i \le v-1 \\ 0 \le j \le t-1}} a_{ij}\alpha^{q^i}\beta^{q^j} \;=\; 0. \tag{2.7}$$

Let $b_j = \sum_{i=0}^{v-1} a_{ij}\alpha^{q^i}$, $0 \le j \le t-1$. Then $b_j \in F_{q^v}$ and (2.7) implies that

$$\sum_{j=0}^{t-1} b_j\beta^{q^j} \;=\; 0.$$

But by Lemma 2.3.2, $\beta, \beta^q, \ldots, \beta^{q^{t-1}}$ are linearly independent over F_{q^v}, so $b_j = 0$, $0 \le j \le t-1$. However $\alpha, \alpha^q, \ldots, \alpha^{q^{v-1}}$ are linearly independent over F_q, and hence $b_j = 0$ implies $a_{ij} = 0$ for all i, j. Therefore the elements in (2.6) form a basis of F_{q^n} over F_q and this completes the proof. □

Theorem 2.3.4 (Semaev [123], Séguin [122], Jungnickel [70]) *Let α, β and γ be as in Theorem 2.3.3. Then*

(a) *the complexity of the normal basis generated by γ is equal to the product of the complexities of those of α and β;*

(b) *the normal basis generated by γ is self-dual if and only if the normal bases generated by α and β are both self-dual.*

Proof: Let $\bar{\alpha}$ be the column vector $(\alpha, \alpha^q, \ldots, \alpha^{q^{v-1}})^t$ and $\bar{\beta}$ the column vector $(\beta, \beta^q, \ldots, \beta^{q^{t-1}})^t$. Then the Kronecker product $\bar{\alpha} \otimes \bar{\beta}$ is a column vector of length vt, consisting of the elements in the normal basis generated by $\gamma = \alpha\beta$, ordered in a different way. Assume that

$$\alpha\bar{\alpha} = A\bar{\alpha} \quad \beta\bar{\beta} = B\bar{\beta},$$

where A and B are $v \times v$ and $t \times t$ matrices over F_q, respectively. Then by the property of Kronecker product of matrices, we have

$$\begin{aligned} \gamma\bar{\gamma} &= \alpha\beta\,\bar{\alpha} \otimes \bar{\beta} = (\alpha\bar{\alpha}) \otimes (\beta\bar{\beta}) \\ &= (A\bar{\alpha}) \otimes (B\bar{\beta}) = (A \otimes B)(\bar{\alpha} \otimes \bar{\beta}). \end{aligned}$$

The number of nonzero entries in $A \otimes B$ is obviously equal to the product of those in A and B. Part (a) is thus proved.

For part (b), Theorem 2.3.1 shows that if γ is self-dual normal over F_q then both α and β are self-dual normal over F_q. Assume that α and β are self-dual normal over F_q. By Theorem 2.3.1, we just need to prove that $\gamma = \alpha\beta$ is self-dual. Note that, for any $0 \le i \le v-1$ and $0 \le j \le t-1$,

$$\mathrm{Tr}_{q^{vt}|q}(\alpha\beta\,\alpha^{q^i}\beta^{q^j}) = \mathrm{Tr}_{q^v|q}(\alpha\alpha^{q^i})\mathrm{Tr}_{q^t|q}(\beta\beta^{q^j}) = \begin{cases} 1, & \text{if } i = j = 0, \\ 0, & \text{otherwise.} \end{cases}$$

That is, the normal basis generated by γ is self-dual. □

The proof of Theorem 2.3.3 shows that one can easily get a multiplication table of a normal basis of $F_{q^{vt}}$ (with v and t relatively prime) from multiplication tables of normal bases of F_{q^v} and F_{q^t}, respectively, over F_q. If we are given two N-polynomials of degree v and t, respectively, then the following theorem tells us how to construct an N-polynomial of degree vt.

Theorem 2.3.5 *Let $f(x) = \sum_{i=0}^{v} a_i x^i$, $g(x) = \sum_{j=0}^{t} b_j x^j \in F_q[x]$ be two N-polynomials of degree v and t respectively, with v and t relatively prime. Let A, B be the companion matrices of $f(x)$, $g(x)$ respectively, and let $C = A \otimes B$ be the Kronecker product of A and B. Then the characteristic polynomial*

$$\det(Ix - C) \;=\; \det\left(\sum_{j=0}^{t} b_j x^j A^{t-j}\right) \;=\; \det\left(\sum_{i=0}^{v} a_i x^i B^{v-i}\right)$$

is an N-polynomial of degree vt over F_q.

Proof: Let α be a root of $f(x)$ and β a root of $g(x)$. Then α is a normal element of F_{q^v} over F_q and β a normal element of F_{q^t} over F_q. Note that $\alpha, \alpha^q, \ldots, \alpha^{q^{v-1}}$ are the eigenvalues of A and $\beta, \beta^q, \ldots, \beta^{q^{t-1}}$ are the eigenvalues of B. It is easy to see that the eigenvalues of $C = A \otimes B$ are $\alpha^{q^i}\beta^{q^j}$, $i = 0, 1, \ldots, v-1$, $j = 0, 1, \ldots, t-1$. therefore

$$\det(Ix - C) = \prod_{\substack{0 \le i \le v-1 \\ 0 \le j \le t-1}} (x - \alpha^{q^i}\beta^{q^j}),$$

and it is an N-polynomial by Theorem 2.3.3. We prove that $\det(xI - C) = \det(\sum_{i=0}^{v} a_i x^i B^{v-i})$; the other equation is proved similarly. Denote $\alpha_i = \alpha^{q^i}$ for $0 \le i \le v-1$. Let D be the diagonal matrix

$$D = \begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_v \end{pmatrix}.$$

Then there is an invertible matrix P such that $A = PDP^{-1}$ and thus

$$\begin{aligned}
\det(xI_{vt} - C) &= \det(xI_{vt} - (PDP^{-1}) \otimes B) \\
&= \det(xI_{vt} - (P \otimes I_t)(D \otimes B)(P^{-1} \otimes I_t)) \\
&= \det((P \otimes I_t)(xI_{vt} - D \otimes B)(P \otimes I_t)^{-1}) \\
&= \det(xI_{vt} - D \otimes B) \\
&= \det \begin{pmatrix} (xI_t - \alpha_0 B) & & & \\ & (xI_t - \alpha_1 B) & & \\ & & \ddots & \\ & & & (xI_t - \alpha_{v-1} B) \end{pmatrix} \\
&= \prod_{i=0}^{v-1} \det(xI_t - \alpha_i B) \; = \; \det \prod_{i=0}^{v-1} (xI_t - \alpha_i B) \\
&= \det(\sum_{i=0}^{v} a_i x^i B^{v-i}),
\end{aligned}$$

as required. □

2.4 Distribution of Normal Elements

In this section we will show how normal elements are distributed in the whole space. We prove that there is a basis of F_{q^n} over F_q such that, with respect to this basis representation, normal elements are just the elements with some groups of the coordinates not simultaneously zero. Consequently one can easily count the total number of normal elements and hence the number of normal bases of F_{q^n} over F_q.

We view F_{q^n} as a vector space of dimension n over F_q. Recall that the Frobenius map:

$$\sigma : \quad \eta \mapsto \eta^q, \quad \eta \in F_{q^n}$$

is a linear transformation of F_{q^n} over F_q. This linear transformation plays an essential role in the following context.

Before proceeding we review some concepts from linear algebra. Our standard reference to linear algebra is Hoffman and Kunze [62]. Let T be a linear transformation on a finite-dimensional vector space V over a (arbitrary) field F. A polynomial $f(x) = \sum_{i=0}^{m} a_i x^i$ in $F[x]$ is said to *annihilate* T if $a_m T^m + \cdots + a_1 T + a_0 I = 0$, where I is the identity map and 0 is the zero map on V. The uniquely determined monic polynomial of least degree with this property is called the *minimal polynomial for* T. It divides any other polynomial in $F[x]$ annihilating T. In particular, the minimal polynomial for T divides the characteristic polynomial for T (Cayley-Hamilton Theorem).

A subspace $W \subseteq V$ is called T*-invariant* if $Tu \in W$ for every $u \in W$. For any vector $u \in V$, the subspace spanned by $u, Tu, T^2u, \ldots$ is a T-invariant subspace of V, called the T*-cyclic subspace generated by* u, denoted by $Z(u,T)$. It is easily seen that $Z(u,T)$ consists of all vectors of the form $g(T)u$, $g(x)$ in $F[x]$. If $Z(u,T) = V$, then u is called a *cyclic vector of* V *for* T.

For any polynomial $g(x) \in F[x]$, $g(T)$ is also a linear transformation on V. The *null space* (or kernel) of $g(T)$ consists of all vectors u such that $g(T)u = 0$; we also call it the null space of $g(x)$. On the other hand, for any vector $u \in V$, the monic polynomial $g(x) \in F[x]$ of smallest degree such that $g(T)u = 0$ is called the T*-Order* of u (some authors call it the T-annihilator, or minimal polynomial of u). We denote this polynomial by $\mathrm{Ord}_{u,T}(x)$, or $\mathrm{Ord}_u(x)$ if the transformation T is clear from context. Note that $\mathrm{Ord}_u(x)$ divides any polynomial $h(x)$ annihilating u (i.e., $h(T)u = 0$), in particular the minimal polynomial for T or the characteristic polynomial for T. It is not difficult to see that the degree of $\mathrm{Ord}_{u,T}(x)$ is equal to the dimension of $Z(u,T)$.

Next we summarize the results we need from linear algebra in the following lemma. The proof is direct, so omitted.

Lemma 2.4.1 *Let T be a linear transformation on a finite-dimensional vector space V over a field F. Assume that the minimal and characteristic polynomials for T are the same, say $f(x)$.*
(i) *Let $g(x) \in F[x]$ and W be its null space. Let $d(x) = \gcd(f(x), g(x))$ and $e(x) = f(x)/d(x)$. Then the dimension of W is equal to the degree of $d(x)$ and*

$$W \;=\; \{u \in V \mid d(T)u = 0\} \;=\; \{e(T)u \mid u \in V\}.$$

(ii) *Let $f(x)$ have the following factorization*

$$f(x) \;=\; \prod_{i=1}^{r} f_i^{d_i}(x),$$

where $f_i(x) \in F[x]$ are the distinct irreducible factors of $f(x)$. Let V_i be the null space of $f_i^{d_i}(x)$. Then

$$V \;=\; V_1 \oplus V_2 \oplus \cdots \oplus V_r.$$

Furthermore, let $\Psi_i(x) = f(x)/f_i^{d_i}(x)$. Then, for any $u_j \in V_j, u_j \neq 0$,

$$\Psi_i(T)u_j \begin{cases} \neq 0, & \textit{if } i = j, \\ = 0, & \textit{otherwise.} \end{cases}$$

Returning to our subject, we consider F_{q^n} as a vector space of dimension n over F_q and the Frobenius map σ is a linear transformation.

Lemma 2.4.2 *The minimal and characteristic polynomial for σ are identical, both being $x^n - 1$.*

Proof: We know that $\sigma^n \eta = \eta^{q^n} = \eta$ for every $\eta \in F_{q^n}$. So $\sigma^n - I = 0$. We prove that $x^n - 1$ is the minimal polynomial of σ.

Assume there is a polynomial $f(x) = \sum_{i=0}^{n-1} f_i x^i \in F_q[x]$ of degree less than n that annihilates σ, that is,

$$\sum_{i=0}^{n-1} f_i \sigma^i \;=\; 0.$$

Then, for any $\eta \in F_{q^n}$,

$$\left(\sum_{i=0}^{n-1} f_i \sigma^i\right) \eta \;=\; \sum_{i=0}^{n-1} f_i \eta^{q^i} = 0,$$

i.e., η is a root of the polynomial $F(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$. This is impossible, since $F(x)$ has degree at most q^{n-1} and cannot have $q^n > q^{n-1}$ roots in F_{q^n}. Hence the minimal polynomial for σ is $x^n - 1$.

Since the characteristic polynomial of σ is monic of degree n and is divisible by the minimal polynomial for σ, they must be identical, both being $x^n - 1$. □

Our objective is to locate the normal elements in F_{q^n} over F_q. Let $\alpha \in F_{q^n}$ be a normal element. Then $\alpha, \sigma\alpha, \dots, \sigma^{n-1}\alpha$ are linearly independent over F_q. So there is no polynomial of degree less than n that annihilates α with respect to σ. Hence the σ-order of α must be $x^n - 1$, that is, α is a cyclic vector of F_{q^n} over F_q with respect to σ. So an element $\alpha \in F_{q^n}$ is a normal element over F_q if and only if $\mathrm{Ord}_{\alpha,\sigma}(x) = x^n - 1$.

Recall that p denotes the characteristic of F_q. Let $n = n_1 p^e$ with $\gcd(p, n_1) = 1$ and $e \geq 0$. For convenience we denote p^e by t. Suppose that $x^n - 1$ has the following factorization in $F_q[x]$:

$$x^n - 1 \ = \ (\varphi_1(x)\varphi_2(x)\cdots\varphi_r(x))^t, \tag{2.8}$$

where $\varphi_i(x) \in F_q[x]$ are the distinct irreducible factors of $x^n - 1$. We assume that $\varphi_i(x)$ has degree d_i, $i = 1, 2, \dots, r$. Let

$$\Phi_i(x) \ = \ (x^n - 1)/\varphi_i(x) \tag{2.9}$$

and

$$\Psi_i(x) \ = \ (x^n - 1)/\varphi_i^t(x) \tag{2.10}$$

for $i = 1, 2, \dots, r$. Then we have a useful characterization of the normal elements in F_{q^n}.

Theorem 2.4.3 (Schwarz [119]) *An element $\alpha \in F_{q^n}$ is a normal element if and only if*

$$\Phi_i(\sigma)\alpha \ \neq \ 0, \quad i = 1, 2, \dots, r. \tag{2.11}$$

Proof: By definition, α is normal over F_q if and only if $\alpha_i = \alpha^{q^i} = \sigma^i(\alpha)$, $i = 0, 1, \dots, n-1$, are linearly independent over F_q, that is, the σ-order of α is equal to $x^n - 1$. This is true if and only if no proper factor of $x^n - 1$ annihilates α, hence if and only if (2.11) holds. □

Corollary 2.4.4 (Perlis [108]) *Let $n = p^e$. Then $\alpha \in F_{q^n}$ is a normal element over F_q if and only if $Tr_{q^n|q}(\alpha) \neq 0$.*

Proof: When $n = p^e$, $x^n - 1 = (x - 1)^n$. So, in (2.8), $r = 1$, $\varphi_1(x) = x - 1$ and $\Phi_1(x) = x^{n-1} + \cdots + x + 1$. By Theorem 2.4.3, $\alpha \in F_{q^n}$ is a normal element over F_q if and only if

$$\Phi_1(\sigma)\alpha \ = \ \sum_{i=0}^{n-1} \alpha^{q^i} \ = \ Tr_{q^n|q}(\alpha) \ \neq \ 0. \qquad \square$$

The following theorem decomposes F_{q^n} into a direct sum of subspaces, half of which are σ-invariant subspaces. The theorem enables us to see where the normal elements of F_{q^n} lie.

Theorem 2.4.5 *Let W_i be the null space of $\varphi_i^t(x)$ and $\widetilde{W_i}$ the null space of $\varphi_i^{t-1}(x)$. Let $\overline{W_i}$ be any subspace of W_i such that $W_i = \overline{W_i} \oplus \widetilde{W_i}$. Then*

$$F_{q^n} \ = \ \sum_{i=1}^{r} \overline{W_i} \oplus \widetilde{W_i}$$

is a direct sum where $\overline{W_i}$ has dimension d_i and $\widetilde{W_i}$ has dimension $(t-1)d_i$. Furthermore, an element $\alpha \in F_{q^n}$ with $\alpha = \sum_{i=1}^{r}(\overline{\alpha}_i + \widetilde{\alpha}_i)$, $\overline{\alpha}_i \in \overline{W_i}$, $\widetilde{\alpha}_i \in \widetilde{W_i}$, is a normal element over F_q if and only if $\overline{\alpha}_i \neq 0$ for each $i = 1, 2, \ldots, r$.

Proof: The first statement follows from Lemma 2.4.1. We only need to prove the second statement. Note that if $i \neq j$ then $\varphi_j^t(x)|\Phi_i(x)$. Hence for any $\alpha_j \in W_j$, $\Phi_i(\sigma)\alpha_j = 0$. So

$$\Phi_i(\sigma)\alpha \ = \ \Phi_i(\sigma)(\overline{\alpha}_i + \widetilde{\alpha}_i) \ = \ \Phi_i(\sigma)\overline{\alpha}_i + \Phi_i(\sigma)\widetilde{\alpha}_i \ = \ \Phi_i(\sigma)\overline{\alpha}_i,$$

as $\Phi_i(x) = \Psi_i(x)\varphi_i^{t-1}(x)$ is divisible by $\varphi_i^{t-1}(x)$. Therefore, by Theorem 2.4.3, α is a normal element over F_q if and only if $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ for each $i = 1, 2, \ldots, r$.

Now we prove that $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ if and only if $\overline{\alpha}_i \neq 0$. Obviously, if $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$ then $\overline{\alpha}_i \neq 0$. Conversely, let $\overline{\alpha}_i \neq 0$. Then $\overline{\alpha}_i \in W_i \setminus \widetilde{W_i}$, whence

$$\varphi_i^t(\sigma)\overline{\alpha}_i \ = \ 0$$

and

$$\varphi_i^{t-1}(\sigma)\overline{\alpha}_i \ \neq \ 0.$$

As $\Psi_i(x)$ and $\varphi_i(x)$ are relatively prime, there exist polynomials $a(x)$ and $b(x)$ in $F_q[x]$ such that

$$a(x)\varphi_i(x) + b(x)\Psi_i(x) \ = \ 1.$$

Hence

$$\overline{\alpha}_i \ = \ a(\sigma)\varphi_i(\sigma)\overline{\alpha}_i + b(\sigma)\Psi_i(\sigma)\overline{\alpha}_i,$$

and so

$$\begin{aligned}
\varphi_i^{t-1}(\sigma)\overline{\alpha}_i \ &= \ a(\sigma)\varphi_i^t(\sigma)\overline{\alpha}_i + b(\sigma)\varphi_i^{t-1}(\sigma)\Psi_i(\sigma)\overline{\alpha}_i \\
&= \ b(\sigma)\Phi_i(\sigma)\overline{\alpha}_i \\
&= \ b(\sigma)(\Phi_i(\sigma)\overline{\alpha}_i).
\end{aligned}$$

Since $\varphi_i^{t-1}(\sigma)\overline{\alpha}_i \neq 0$, one must have that $\Phi_i(\sigma)\overline{\alpha}_i \neq 0$. This completes the proof. □

If we have a basis for each of the subspaces $\overline{W_i}$ and $\widetilde{W_i}$, then by putting them together we have a basis for F_{q^n} over F_q with the properties that an element in F_{q^n} represented in this basis generates a normal basis if and only if its coordinates corresponding to the subspace $\overline{W_i}$ are not simultaneously zero for each i. Since the dimension of the subspace $\overline{W_i}$ is $d_i \geq 1$, the following corollary is another immediate consequence from Theorem 2.4.5.

Corollary 2.4.6 (Normal Basis Theorem for Finite Fields) *There always exists a normal basis of F_{q^n} over F_q.*

As another consequence of Theorem 2.4.5, we count the number of normal elements, and thus the number of normal bases of F_{q^n} over F_q.

Corollary 2.4.7 (Hensel [61], Ore [106]) *The total number of normal elements in F_{q^n} over F_q is*

$$v(n,q) \;=\; \prod_{i=1}^{r} q^{d_i(t-1)}(q^{d_i}-1),$$

and the number of normal bases of F_{q^n} over F_q is $v(n,q)/n$.

Proof: The first statement is obvious from Theorem 2.4.5 and the second one follows from the fact that every element in a normal basis generates the same basis. □

We remark that computing $v(n,q)$ does not require the factorization of x^n-1. The only thing one needs is the degrees of all the irreducible factors. Write $n = n_1p^e$ as above. Then it is shown in [5] and [52] that

$$v(n,q) \;=\; q^{n-n_1}\prod_{d|n_1}(q^{\tau(d)}-1)^{\phi(d)/\tau(d)},$$

where the product is over all divisors d of n_1 with $1 \leq d \leq n_1$, $\tau(d)$ is the order of q modulo d, and $\phi(d)$ is the Euler totient function.

In the special case that n and q are relatively prime, we have $t = 1$, $\widetilde{W_i} = \{0\}$ and $\overline{W_i} = W_i$ in Theorem 2.4.5. We restate this as a corollary.

Corollary 2.4.8 (Pincin [109], Semaev [123]) *Let* $\gcd(n, q) = 1$ *and let*

$$x^n - 1 \;=\; \varphi_1(x)\varphi_2(x)\cdots\varphi_r(x)$$

be a complete factorization in $F_q[x]$*. Let* W_i *be the null space of* $\varphi_i(x)$*. Then*

$$F_{q^n} \;=\; W_1 \oplus W_2 \oplus \cdots \oplus W_r \tag{2.12}$$

is a direct sum of σ*-invariant subspaces; the dimension of* W_i *equals the degree of* $\varphi_i(x)$*. Furthermore* $\alpha = \sum_{i=1}^{r} \alpha_i \in F_{q^n}$*,* $\alpha_i \in W_i$*, is a normal element of* F_{q^n} *over* F_q *if and only if* $\alpha_i \neq 0$ *for each* i*.*

Assume now that $\gcd(n, q) = 1$. Note that each W_i in the decomposition (2.12) in Corollary 2.4.8 is a σ-invariant subspace and every element in W_i is annihilated by $\varphi_i(\sigma)$. As $\varphi_i(x)$ is irreducible, W_i has no proper σ-invariant subspaces. In this case, we say that W_i is an *irreducible* σ-invariant subspace. The decomposition (2.12) is unique in the sense that if F_{q^n} is decomposed into a direct sum of irreducible σ-invariant subspaces

$$F_{q^n} \;=\; V_1 \oplus V_2 \oplus \cdots \oplus V_s,$$

then $s = r$ and, after rearranging the order of V_i's if necessary, $V_i = W_i$ for $i = 1, 2, \ldots, r$. As an application of this observation, we look at a special case of the degree n when there exists an element $a \in F_q$ such that $x^n - a$ is irreducible over F_q.

We first introduce some notation. A *cyclotomic coset* mod n with respect to q that contains an integer ℓ is the set

$$M_\ell \;=\; \{\ell, \ell q, \ldots, \ell q^{m-1}\} \bmod n$$

where m is the smallest positive integer such that $\ell q^m \equiv \ell (\text{mod } n)$. Let S be a subset of $\{0, 1, \ldots, n-1\}$ such that M_{ℓ_1} and M_{ℓ_2} are disjoint for any ℓ_1, $\ell_2 \in S$, $\ell_1 \neq \ell_2$, and

$$\{0, 1, \ldots, n-1\} \;=\; \bigcup_{\ell \in S} M_\ell.$$

Any subset S satisfying this property is called a *complete set of representatives* of all the cyclotomic cosets mod n.

Theorem 2.4.9 (Semaev [123]) *Let* $\gcd(n,q)=1$*, and assume that there exists* $a \in F_q$ *such that* $x^n - a$ *is irreducible over* F_q*. Let* α *be a root of* $x^n - a$ *and* S *a complete set of representatives of all the cyclotomic cosets mod* n*. For* $\ell \in S$*, let* V_ℓ *be the subspace of* F_{q^n} *spanned over* F_q *by the elements of the set* $\{\alpha^m \mid m \in M_\ell\}$*. Then*

$$F_{q^n} = \sum_{\ell \in S} V_\ell \tag{2.13}$$

is a direct sum of irreducible σ*-invariant subspaces. Therefore an element* $\theta = \sum_{\ell \in S} \theta_\ell$*,* $\theta_\ell \in V_\ell$*, is a normal element if and only if* $\theta_\ell \neq 0$ *for each* $\ell \in S$*.*

Proof: As $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of F_{q^n} over F_q, (2.13) is a direct sum. Obviously, each V_ℓ is σ-invariant. We just need to prove that V_ℓ is irreducible. Let n_ℓ be the cardinality of M_ℓ. Note that the number of irreducible factors of $x^n - 1$ of degree m is equal to the number of $\ell \in S$ such that $n_\ell = m$. If $f_\ell(x)$ is the characteristic polynomial of σ on V_ℓ, then

$$x^n - 1 = \prod_{\ell \in S} f_\ell(x).$$

Hence, the polynomials $f_\ell(x)$ are irreducible over F_q. Therefore (2.13) is an irreducible σ-invariant decomposition. □

2.5 Characterization of N-Polynomials

In Section 2.1 we saw that irreducible polynomials with linearly independent roots are called N-polynomials and the construction of normal bases is equivalent to the construction of N-polynomials. A natural problem is: when is an irreducible polynomial an N-polynomial? This section is devoted to the discussion of this problem.

A direct way to verify whether an irreducible polynomial $f(x)$ is an N-polynomial is as follows. Let α be a root of $f(x)$. Then $1, \alpha, \ldots, \alpha^{n-1}$ form a polynomial basis of F_{q^n} over F_q and $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are all the roots of $f(x)$ in F_{q^n}. Express each α^{q^i}, $0 \leq i \leq n-1$, in the polynomial basis:

$$\alpha^{q^i} = \sum_{j=0}^{n-1} b_{ij}\alpha^j, \quad b_{ij} \in F_q. \tag{2.14}$$

If the $n \times n$ matrix $B = (b_{ij})$ is nonsingular then $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent, and hence $f(x)$ is an N-polynomial.

This does give us a polynomial-time algorithm to test if $f(x)$ is an N-polynomial. However (2.14) requires a lot of computations. A natural question is whether there is a simple criterion to identify N-polynomials. The answer is yes in certain cases.

Actually, Theorem 2.4.3 gives us another way to check if an irreducible polynomial is an N-polynomial. Noting that $c(\sigma)\alpha = \sum_{i=0}^{m} c_i \alpha^{q^i}$ for any polynomial $c(x) = \sum_{i=0}^{m} c_i x^i \in F_q[x]$, we can restate Theorem 2.4.3 as follows.

Theorem 2.5.1 (Schwarz [119]) *Let $f(x)$ be an irreducible polynomial of degree n over F_q and α a root of it. Let $x^n - 1$ factor as in (2.8) and let $\Phi_i(x)$ be as in (2.9). Then $f(x)$ is an N-polynomial over F_q if and only if*

$$L_{\Phi_i}(\alpha) \neq 0 \text{ for each } i = 1, 2, \ldots, r,$$

where $L_{\Phi_i}(x)$ is the linearized polynomial, defined by $L_{\Phi_i}(x) = \sum_{i=0}^{m} t_i x^{q^i}$ if $\Phi_i(x) = \sum_{i=0}^{m} t_i x^i$.

In general, checking the conditions in Theorem 2.5.1 is equivalent to computing (2.14). But, in certain cases, the conditions in Theorem 2.5.1 are very simple, as indicated by the following four corollaries.

Corollary 2.5.2 (Perlis [108]) *Let $n = p^e$ and $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over F_q. Then $f(x)$ is an N-polynomial if and only if $a_1 \neq 0$.*

Proof: It follows from Corollary 2.4.4 by noting that $a_1 = -Tr_{q^n|q}(\alpha)$ for any root of $f(x)$. □

Corollary 2.5.3 *Let $f(x) = x^2 + a_1 x + a_2$ be an irreducible quadratic polynomial over F_q. Then $f(x)$ is an N-polynomial if and only if $a_1 \neq 0$.*

Proof: Note that $x^2 - 1 = (x-1)(x+1)$ and apply Theorem 2.2.4. □

Corollary 2.5.4 (Pei, Wang and Omura [107]) *Let r be a prime different from p. Suppose that q is a primitive element modulo r. Then an irreducible polynomial $f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$ is an N-polynomial over F_q if and only if $a_1 \neq 0$.*

Proof: Note that

$$x^r - 1 \ = \ (x-1)(x^{r-1} + \cdots + x + 1).$$

Since q is primitive modulo r, $x^{r-1}+\cdots+x+1$ is irreducible over F_q. Hence, in (2.8), $\varphi_1(x) = x-1$ and $\varphi_2(x) = x^{r-1}+\cdots+x+1$. Thus $\Phi_1(x) = \varphi_2(x)$ and $\Phi_2(x) = \varphi_1(x)$. Let α be a root of $f(x)$. By Theorem 2.5.1, $f(x)$ is an N-polynomial if and only if

$$\Phi_1(\sigma)\alpha \ = \ \alpha^{q^{r-1}} + \cdots + \alpha^q + \alpha \ = \ Tr_{q^r|q}(\alpha) \ = \ -a_1 \ \neq \ 0 \tag{2.15}$$

and

$$\Phi_2(\sigma)\alpha \ = \ \alpha^q - \alpha \ \neq \ 0. \tag{2.16}$$

But (2.16) is obviously true, since $\alpha \notin F_q$. □

Corollary 2.5.5 *Let $n = p^e r$ where r is a prime different from p and q is a primitive element modulo r. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be an irreducible polynomial over F_q and α a root of $f(x)$. Let $u = \sum_{i=0}^{p^e-1} \alpha^{q^{ir}}$. Then $f(x)$ is an N-polynomial if and only if $a_1 \neq 0$ and $u \notin F_q$.*

Proof: In this case, the following factorization is complete:

$$x^n - 1 \ = \ (x^r-1)^{p^e} \ = \ (x-1)^{p^e}(x^{r-1}+\cdots+x+1)^{p^e}.$$

Hence

$$\Phi_1(x) \ = \ \frac{x^n-1}{x-1} \ = \ \sum_{i=0}^{n-1} x^i,$$

and

$$\begin{aligned}\Phi_2(x) \ &= \ \frac{x^n-1}{x^{r-1}+\cdots+x+1} \ = \ (x-1)\frac{x^{p^e r}-1}{x^r-1} \\ &= \ (x-1)\left(\sum_{i=0}^{p^e-1} x^{ir}\right) \\ &= \ \sum_{i=0}^{p^e-1} x^{ir+1} - \sum_{i=0}^{p^e-1} x^{ir}.\end{aligned}$$

It follows that

$$L_{\Phi_1}(\alpha) \ = \ Tr_{q^n|q}(\alpha) \ = \ -a_1,$$

and

$$\begin{aligned} L_{\Phi_2}(\alpha) &= \left(\sum_{i=0}^{p^e-1} \alpha^{q^{ir}}\right)^q - \sum_{i=0}^{p^e-1} \alpha^{q^{ir}} \\ &= u^q - u. \end{aligned}$$

Note that $u^q - u \neq 0$ if and only if $u \notin F_q$. The result now follows immediately from Theorem 2.5.1.

□

Chapter 3

Construction of Normal Bases

In this Chapter, we present various algorithms for constructing normal bases. We also construct explicitly some families of irreducible polynomials with linearly independent roots.

3.1 Randomized Algorithms

We begin with a brief discussion of randomized algorithms. The simplest algorithm which comes to mind for constructing a normal basis is to repeatedly select a random element α in F_{q^n} until $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a linearly independent set over F_q. This is a probabilistic polynomial-time algorithm since von zur Gathen and Giesbrecht [56] have shown that the probability, κ, that α is normal over F_q satisfies $\kappa \geq 1/34$ if $n \leq q^4$, and $\kappa > (16 \log_q n)^{-1}$ if $n \geq q^4$.

A better probabilistic algorithm is based on the following theorem.

Theorem 3.1.1 (Artin [9]) *Let $f(x)$ be an irreducible polynomial of degree n over F_q and α a root of $f(x)$. Let*

$$g(x) \ = \ \frac{f(x)}{(x-\alpha)f'(\alpha)}.$$

Then there are at least $q - n(n-1)$ elements u in F_q such that $g(u)$ is a normal element of F_{q^n} over F_q.

Proof: Let σ_i be the automorphism $\theta \to \theta^{q^i}$, $\theta \in F_{q^n}$, for $i = 1, \ldots, n$. Then $\alpha_i = \sigma_i(\alpha)$ is also a root of $f(x)$, $1 \le i \le n$. Let

$$g_i(x) \;=\; \sigma_i(g(x)) \;=\; \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)},$$

and note that $\sigma_i\sigma_j(g(x)) = \sigma_{i+j}(g(x))$. Then $g_i(x)$ is a polynomial in $F_{q^n}[x]$ having α_k as a root for $k \ne i$ and $g_i(\alpha_i) = 1$. Hence

$$g_i(x)g_k(x) \equiv 0 \pmod{f(x)}, \quad \text{for } i \ne k. \tag{3.1}$$

Note that

$$g_1(x) + g_2(x) + \cdots + g_n(x) - 1 \;=\; 0, \tag{3.2}$$

since the left side is a polynomial of degree at most $n-1$ and has $\alpha_1,\ \alpha_2,\ \ldots, \alpha_n$ as roots. Multiplying (3.2) by $g_i(x)$ and using (3.1) yields

$$(g_i(x))^2 \equiv g_i(x) \pmod{f(x)}. \tag{3.3}$$

We next compute the determinant, $D(x)$, of the matrix

$$D \;=\; [\sigma_i\sigma_j(g(x))], \quad 1 \le i, j \le n.$$

From (3.1), (3.2) and (3.3), we see that the entries of D^TD modulo $f(x)$ are all 0, except on the main diagonal, where they are all 1. Hence

$$(D(x))^2 \;=\; \det(D^TD) \;\equiv\; 1 \pmod{f(x)}.$$

This proves that $D(x)$ is a non-zero polynomial of degree at most $n(n-1)$. Therefore $D(x)$ has at most $n(n-1)$ roots in F_q. The proof is completed by noting that, by Theorem 2.2.2, for $u \in F_q$, $g(u)$ is a normal element of F_{q^n} over F_q if and only if $D(u) \ne 0$. □

Now the algorithm is very simple. Choose $u \in F_q$ at random, and let $\theta = g(u)$. Then test if θ is a normal element of F_{q^n} over F_q. Theorem 3.1.1 tells us that if $q > 2n(n-1)$, then θ is a normal element with probability at least 1/2. The entire computation takes $O((n + \log q)(n \log q)^2)$ bit operations, as shown by Bach, Driscoll and Shallit [11].

Frandsen [46] shows that when $q > 2n(n-1)$, an arbitrary element in F_{q^n} is a normal element with probability $\ge 1/2$. In general, he proves that a random element in F_{q^n} is a normal element with probability at least $(1-q^{-1})/(e(1+\log_q(n)))$.

3.2 Deterministic Algorithms

Next we turn to deterministic algorithms for constructing normal bases for F_{q^n} over F_q. We will assume that an irreducible polynomial $f(x)$ of degree n over F_q is given. Let α be a root of $f(x)$. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of F_{q^n} over F_q. Thus we may compute the matrix representation of the Frobenius map $\sigma : x \to x^q$, $x \in F_{q^n}$. Von zur Gathen and Shoup [53] give an efficient way to do this.

An obvious deterministic algorithm follows from Theorem 2.4.5. One first factors $x^n - 1$ over F_q to get the factorization (2.8). Then one computes a basis for each subspace in the decomposition of F_{q^n} in Theorem 2.4.5. Thus one obtains a basis for the whole space F_{q^n} over F_q and normal elements are just those whose coordinates corresponding to each $\overline{W_i}$ are not simultaneously zero. One advantage of this algorithm is that it produces all the normal elements. However it is not efficient, since there is currently no deterministic polynomial time algorithm known to factor $x^n - 1$ when p is large.

In the following we will present two deterministic polynomial time algorithms due to Lüneburg [92] and Lenstra [85]. As shown by Bach, Driscoll and Shallit [11], both algorithms have the same complexity. In both algorithms we need to find the σ-Order $\mathrm{Ord}_\theta(x)$ of an arbitrary element θ in F_{q^n}. Note that the degree of $\mathrm{Ord}_\theta(x)$ is the least positive integer k such that $\sigma^k\theta$ belongs to the F_q-linear span of $\{\sigma^i\theta \mid 0 \le i < k\}$. If $\sigma^k\theta = \sum_{i=0}^{k-1} c_i\sigma^i\theta$ for that k, then $\mathrm{Ord}_\theta(x) = x^k - \sum_{i=0}^{k-1} c_i x^i$. This shows that $\mathrm{Ord}_\theta(x)$ can be computed in polynomial time (in n and $\log q$).

Lüneburg's algorithm is very simple. For each $i = 0, 1, \ldots, n-1$, compute the σ-Order $f_i = \mathrm{Ord}_{\alpha^i}(x)$. Then $x^n - 1 = \mathrm{lcm}(f_0, f_1, \ldots, f_{n-1})$. Now apply factor refinement [11] to the list of polynomials f_0, f_1, $\ldots$, f_{n-1}. This will give pairwise relatively prime polynomials g_1, g_2, $\ldots$, g_r and integers e_{ij}, $0 \le i \le n-1$, $1 \le j \le r$, such that

$$f_i \;=\; \prod_{1\le j\le r} g_j^{e_{ij}}, \quad i = 0, 1, \ldots, n-1.$$

For each j, $1 \le j \le r$, find an index $i(j)$ for which e_{ij} is maximized. Let

$$h_j = f_{i(j)}/g_j^{e_{i(j)j}},$$

and take $\beta_j = h_j(\sigma)\alpha^{i(j)}$. Then

$$\beta \;=\; \sum_{j=1}^{r} \beta_j$$

is a normal element of F_{q^n} over F_q. The reason is that the σ-Order of β_j is $g_j^{e_{i(j)j}}$ for $j = 1, \ldots, r$. As $g_1, g_2, \ldots, g_r$ are pairwise relatively prime, the σ-Order of β must be

$$\prod_{j=1}^{r} g_j^{e_{i(j)j}} \; = \; x^n - 1,$$

that is, β is a normal element. Bach, Driscoll and Shallit show that this algorithm takes $O((n^2 + \log q)(n \log q)^2)$ bit operations.

Lenstra's algorithm is more complicated to describe, but has more of a linear algebra flavour. Its complexity is the same as Lüneburg's algorithm. Before proceeding to describe this algorithm, we need two lemmas.

Lemma 3.2.1 *Let* $\theta \in F_{q^n}$ *with* $\mathrm{Ord}_\theta(x) \neq x^n - 1$. *Let* $g(x) = (x^n - 1)/\mathrm{Ord}_\theta(x)$. *Then there exists* $\beta \in F_{q^n}$ *such that*

$$g(\sigma)\beta \; = \; \theta. \tag{3.4}$$

Proof: Let γ be a normal element of F_{q^n} over F_q. Then there exists $f(x) \in F_q[x]$ such that $f(\sigma)\gamma = \theta$. Since $\mathrm{Ord}_\theta(\sigma)\theta = 0$, we have $(\mathrm{Ord}_\theta(\sigma)f(\sigma))\gamma = 0$. So $\mathrm{Ord}_\theta(x)f(x)$ is divisible by $x^n - 1$. Therefore $f(x)$ is divisible by $g(x)$. Let $f(x) = g(x)h(x)$. Then

$$g(\sigma)(h(\sigma)\gamma) \; = \; \theta.$$

This proves that $\beta = h(\sigma)\gamma$ is a solution of (3.4). □

Lemma 3.2.2 *Let* $\theta \in F_{q^n}$ *with* $\mathrm{Ord}_\theta(x) \neq x^n - 1$. *Assume that there exists a solution* β *of (3.4) such that* $\deg(\mathrm{Ord}_\beta(x)) \leq \deg(\mathrm{Ord}_\theta(x))$. *Then there exists a non-zero element* $\eta \in F_{q^n}$ *such that*

$$g(\sigma)\eta \; = \; 0, \tag{3.5}$$

where $g(x) = (x^n - 1)/\mathrm{Ord}_\theta(x)$. *Moreover any such* η *has the property that*

$$\deg(\mathrm{Ord}_{\theta+\eta}(x)) \; > \; \deg(\mathrm{Ord}_\theta(x)). \tag{3.6}$$

Proof: Let γ be a normal element in F_{q^n} over F_q. It is easy to see that $\eta = \mathrm{Ord}_\theta(\sigma)\gamma \neq 0$ is a solution of (3.5). We prove that (3.6) holds for any non-zero solution η of (3.5).

From (3.4) it follows that $\mathrm{Ord}_\theta(x)$ divides $\mathrm{Ord}_\beta(x)$, so the hypothesis that $\deg(\mathrm{Ord}_\beta(x)) \leq \deg(\mathrm{Ord}_\theta(x))$ implies that $\mathrm{Ord}_\beta(x) = \mathrm{Ord}_\theta(x)$. Hence $g(x)$ must be relatively prime to $\mathrm{Ord}_\theta(x)$. Note that $\mathrm{Ord}_\eta(x)$ is a divisor of $g(x)$, and consequently $\mathrm{Ord}_\theta(x)$ and $\mathrm{Ord}_\eta(x)$ are relatively prime. This implies that

$$\mathrm{Ord}_{\theta+\eta}(x) = \mathrm{Ord}_\theta(x)\mathrm{Ord}_\eta(x),$$

and then (3.6) follows from the fact that $\eta \neq 0$. The proof is now complete. □

We are now ready to describe Lenstra's algorithm for finding a normal element of F_{q^n} over F_q.

Algorithm Construct a normal element of F_{q^n} over F_q.

Step 1. Take any element $\theta \in F_{q^n}$ and determine $\mathrm{Ord}_\theta(x)$.

Step 2. If $\mathrm{Ord}_\theta(x) = x^n - 1$ then the algorithm stops.

Step 3. Calculate $g(x) = (x^n-1)/\mathrm{Ord}_\theta(x)$, and then solve the system of linear equations $g(\sigma)\beta = \theta$ for β.

Step 4. Determine $\mathrm{Ord}_\beta(x)$. If $\deg(\mathrm{Ord}_\beta(x)) > \deg(\mathrm{Ord}_\theta(x))$ then replace θ by β and go to Step 2; otherwise if $\deg(\mathrm{Ord}_\beta(x)) \leq \deg(\mathrm{Ord}_\theta(x))$ then find a non-zero element η such that $g(\sigma)\eta = 0$, replace θ by $\theta + \eta$ and determine the order of the new θ, and go to Step 2.

The correctness of the algorithm follows from Lemmas 3.2.1 and 3.2.2, since with each replacement of θ the degree of $\mathrm{Ord}_\theta(x)$ increases by at least 1.

3.3 Factoring $x^e - 1$

To realize the decomposition in Theorem 2.4.5, we need to factor polynomials of the type $x^e - 1$ in $F_q[x]$. Polynomial factorization is, of course, of independent interest; it has important applications in computer algebra, coding theory and cryptography. For surveys on this topic, the reader is referred to [89, Chapter 4] or [99, Chapter 2] and the references given there.

We will not try to give the best algorithms for this problem. Instead we present some results that are of interest from a theoretical point of view. A result due to Daykin [39] shows that if one knows the minimal polynomial $f(x)$ of a primitive e-th root α of unity then all the irreducible factors of $x^e - 1$ can be obtained by computing the minimal polynomials of α^t for $t = 1, 2, \ldots, e$. We give a new characterization of the minimal polynomial of α^t in terms of the coefficients of the quotient polynomial $(x^e - 1)/f(x)$. When $e = r^k$, where r is a prime, we show that $x^{r^k} - 1$ can be factored in polynomial time (in r^k, and $\log q$) if an irreducible factor of $(x^r - 1)/(x-1)$ and an irreducible polynomial of degree r are given. Finally, we present an explicit complete factorization of $x^{2^k} - 1$ over F_q when $q \equiv 3 \bmod 4$.

3.3.1 A Theorem of Daykin

Let $f(x) \in F_q[x]$ with $f(0) \neq 0$. The *period* of $f(x)$ is defined to be the smallest positive integer e such that $f(x)$ divides $x^e - 1$. Recall the definition for cyclotomic cosets on page 30.

Theorem 3.3.1 (Daykin [39]) *Let $f(x)$ be an irreducible polynomial over F_q of degree n and period e. Let α be a root of $f(x)$ and $f_t(x)$ be the minimal polynomial of α^t over F_q for any integer t. Let $\Delta \subset \mathbb{Z}_e$ be a complete set of representatives of the cyclotomic classes mod e with respect to q. Then*

$$x^e - 1 = \prod_{t \in \Delta} f_t(x).$$

In order to factor $x^e - 1$ in F_{q^n}, one problem here is to find efficiently an irreducible polynomial $f(x) \in F_{q^n}[x]$ whose roots are primitive e-th roots of unity. There are at present no deterministic polynomial time (in $\log q$ and $\deg f(x)$) algorithms to solve this problem. In this respect, the following result seems interesting.

Theorem 3.3.2 *Let r be an odd prime that does not divide q, and let m be the order of q modulo r. Suppose that an irreducible factor of $(x^r - 1)/(x - 1)$ and an irreducible polynomial of degree r in $F_q[x]$ are given. Then, for any positive integer k, an irreducible polynomial in $F_{q^n}[x]$ whose roots are primitive r^k-th roots of unity can be found deterministically in time polynomial in r, k and $\log q$.*

Proof: We only give a sketch of the proof. Let α be a root of the given irreducible factor of $(x^r - 1)/(x - 1)$, and β a root of the given irreducible polynomial of degree r. Then

$$\{\alpha^i \beta^j \mid 0 \leq i \leq m-1,\ \ 0 \leq j \leq r-1\}$$

is a basis of $F_{q^{mr}}$ over F_q. Henceforth, we assume that elements in $F_{q^{mr}}$ are represented with respect to this basis.

Let $q^m - 1 = r^t l$ with $\gcd(l, r) = 1$. Then r^{t+1} divides $q^{mr} - 1$. As α has multiplicative order r, the equation

$$x^{q^m-1} = \alpha \tag{3.7}$$

has at least one solution in $F_{q^{mr}}$, say γ_0. It is easy to see that the multiplicative order of γ_0 is divisible by r^{t+1}. Hence $\gamma = \gamma_0^{(q^{mr}-1)/r}$ is in F_{q^m} and has multiplicative order r^t. Let $f(x)$ be the minimal polynomial of γ over F_q. For any positive integer k, as $x^{r^k} - \gamma$ is irreducible in $F_{q^m}[x]$, we see that $f(x^{r^k})$ is irreducible over F_q. It is easy to see that the roots of $f(x^{r^k})$ have multiplicative order r^{t+k} for all integers $k \geq 0$.

Note that (3.7) can be written as

$$x^{q^m} = x\alpha. \tag{3.8}$$

Since (3.8) is a system of linear equations in the coordinates of x, it can be solved in polynomial time. So γ can be computed in polynomial time. Also the minimal polynomial of γ can be easily computed by the method in [58]. The theorem is thus proved. □

3.3.2 A Characterization of Minimal Polynomials

Another problem is to compute the minimal polynomials $f_t(x)$ from $f(x)$. Let $C_t(x)$ be the characteristic polynomial of α^t in F_{q^n} over F_q (α^t is viewed as the linear transformation of multiplying α^t on the elements of F_{q^n}.) Then it is easy to see that $C_t(x) = (f_t(x))^r$, where $r = n/d$ and d is the degree of $f_t(x)$. In fact d is equal to the smallest positive integer k such that $tq^k \equiv t \bmod e$. If t is relatively prime to e, then d is equal to n. Thus if $\gcd(t, e) = 1$ then $f_t(x) = C_t(x)$. Several methods of computing $C_t(x)$ are given by Alanen and Knuth [6], Daykin [39], Rifà and Borrell [113] and Thiong Ly [136]. We will not discuss these methods here. Instead we will show that the coefficients of $f_t(x)$ are a unique solution of a system of linear equations whose coefficients are from the coefficients of the quotient polynomial $(x^e - 1)/f(x)$. Though Theorem 3.3.3 seems not provide any advantages in computing $f_t(x)$, it is interesting in itself.

For a polynomial $g(x) = \sum_{i=0}^{e-1} g_i x^i$, the associated column vector $(g_0, g_1, \cdots, g_{e-1})^t$ of $g(x)$ is denoted by g. The polynomial $g(x)$ can be written as $(1, x, \cdots, x^{e-1})g$. Let u be a column vector. We will use $u^{[i]}$ to denote the column vector obtained by cyclic shifting u downwardly i positions.

Theorem 3.3.3 *Let $f(x)$ be an irreducible polynomial of degree n and period e over F_q. Let $x^e - 1 = f(x)h(x)$, say $h(x) = \sum_{i=0}^{e-n} h_i x^i$. Let h denote the column vector $(h_0, h_1, \cdots, h_{e-n}, 0, \cdots, 0)^t$ of length e. Let α be a root of $f(x)$ in some extension field of F_q. Then, for any non-negative integer t, the minimal polynomial of α^t over F_q is $m(x) = \sum_{i=0}^{d} m_i x^i$, where d is the smallest positive integer d such that $tq^d \equiv t \bmod e$ and $X = (m_0, m_1, \cdots, m_d)^t$ is the unique solution of the following system of linear equations:*

$$\begin{pmatrix} h & h^{[t]} & \ldots & h^{[dt]} \end{pmatrix} X = 0, \tag{3.9}$$

with $m_d = 1$.

Proof: First note that the degree of the minimal polynomial $m(x)$ of α^t over F_q is equal to the smallest positive integer k such that $(\alpha^t)^{q^k} = \alpha^t$, or equivalently the smallest integer k such that $tq^k \equiv t \pmod{e}$, as the order of α is e. Hence the degree of $m(x)$ is d.

Now $m(\alpha^t) = 0$ implies that α is a root of $m(x^t)$. It follows that $f(x)$ divides $m(x^t)$. Thus $x^e - 1$ divides $m(x^t)h(x)$, that is,

$$m(x^t)h(x) \equiv 0 \pmod{x^e - 1}. \tag{3.10}$$

Write $h(x)$ as $(1, x, \cdots, x^{e-1})h$. It is easy to see that

$$x^i h(x) \equiv (1, x, \cdots, x^{e-1})h^{[i]} \pmod{x^e - 1}.$$

Hence

$$\begin{aligned} m(x^t)h(x) &= \sum_{i=0}^{d} m_i (x^{it} h(x)) \\ &\equiv \sum_{i=0}^{d} m_i (1, x, \cdots, x^{e-1}) h^{[it]} \pmod{x^e - 1} \\ &\equiv (1, x, \cdots, x^{e-1}) \sum_{i=0}^{d} m_i h^{[it]} \pmod{x^e - 1}. \end{aligned}$$

The equation (3.10) is equivalent to

$$\sum_{i=0}^{d} m_i h^{[it]} = 0. \tag{3.11}$$

So we have proved that the coefficients of the minimal polynomial of α^t over F_q must be a solution of the equation (3.9), and the equation (3.10) is equivalent to the equation (3.9).

Finally, we only need to prove that (3.9) has a unique solution within a scalar multiple. Since (3.9) and (3.10) are equivalent, for any nonzero solution $A = (a_0, a_1, \cdots, a_d)^T$ of (3.9), the associated polynomial $A(x) = \sum_{i=0}^{d} a_i x^i$ has degree at most d and satisfies

$$A(x^t)h(x) \equiv 0 \pmod{x^e - 1}. \tag{3.12}$$

Plug α in (3.12), we have

$$A(\alpha^t)h(\alpha) = 0. \tag{3.13}$$

As $e|(q^n - 1)$, e is relatively prime to q. This implies that $x^e - 1$ has no multiple roots, thus $h(\alpha) \neq 0$. Hence we have from (3.13) that $A(\alpha^t) = 0$, that is, α^t is a root of $A(x)$. One sees that $A(x)$ is divisible by the minimal polynomial $m(x)$ of α^t over F_q which has degree d. Therefore $a_d \neq 0$ and $A(x) = a_d m(x)$, that is, the equation (3.9) has only one solution $(a_0, a_1, \cdots, a_d)$ with $a_d = 1$. This completes the proof. □

3.3.3 Factoring $x^{2^k} - 1$

In this section, we consider the problem of completely factoring $x^{2^k} - 1$ over F_q for $q \equiv 3 \bmod 4$. As $x^{2^t} - 1 = (x - 1)\prod_{i=0}^{t-1}(x^{2^i} + 1)$, we just need to factor $x^{2^k} + 1$. As the roots of $x^{2^k} + 1$ are primitive 2^{k+1}th roots of unity (in some extension field of F_q), every irreducible factor of $x^{2^k} + 1$ is of the same degree, a power of 2. Also let $q = p^m$ where p is a prime. Then m must be odd and $p \equiv 3 \bmod 4$. We only need to factor $x^{2^k} + 1$ over F_p, since its irreducible factors in $F_p[x]$ will remain irreducible over F_q.

We assume that p is a prime such that $2^a|(p+1)$, $2^{a+1} \nmid (p+1)$ with $a \geq 2$. Then 2^{a+1} is the highest power in $p^2 - 1$. We first quote the following result due to J.A. Serret [126], see also [89, Theorem 3.75].

Lemma 3.3.4 *Let $a \in F_q^*$ with multiplicative order e. Then the binomial $x^t - a$ is irreducible in $F_q[x]$ if and only if the integer $t \geq 2$ satisfies the following conditions:*
(i) $\gcd(t, (q-1)/e) = 1$,
(ii) each prime factor of t divides e,
(iii) if $4|t$ then $4|(q-1)$.

Theorem 3.3.5 *Let $H_1 = \{0\}$. Recursively define*

$$H_k = \{\pm(\frac{u+1}{2})^{(p+1)/4} \ : \ u \in H_{k-1}\}$$

for $k = 2, 3, \cdots, a-1$ and

$$H_a = \{\pm(\frac{u-1}{2})^{(p+1)/4} \ : \ u \in H_{a-1}\}.$$

Then, for $1 \leq k \leq a-1$, H_k has cardinality 2^{k-1},

$$x^{2^k} + 1 = \prod_{u \in H_k} (x^2 - 2ux + 1), \tag{3.14}$$

and for any integer $e \geq 0$,

$$x^{2^{a+e}} + 1 = \prod_{u \in H_a} (x^{2^{e+1}} - 2ux^{2^e} - 1). \tag{3.15}$$

All the factors in the above products are irreducible over F_p.

Proof: First note that F_{p^2} contains all the 2^{a+1}th roots of unity, since $2^{a+1}|(p^2-1)$. Since $2^2 \nmid (p-1)$, for $1 \leq k \leq a$, every primitive 2^{k+1}th root of unity is of degree 2 over F_p. We prove (3.14) and (3.15) by induction on k.

For $k = 1$, note that $p \equiv 3 \bmod 4$, -1 is a quadratic nonresidue in F_p. Hence $x^2 + 1$ is irreducible over F_p. Therefore (3.14) is true for $k = 1$.

Assume that (3.14) is true for k with $1 \leq k < a$. For $k+1$, we prove that (3.14) is true if $k+1 < a$ and (3.15) with $e = 0$ is true if $k+1 = a$. Substituting the x in (3.14) by x^2 yields

$$x^{2^{k+1}} + 1 = \prod_{u \in H_k} (x^4 - 2ux^2 + 1).$$

and for a complete factorization it is required to factor

$$x^4 - 2ux^2 + 1 \tag{3.16}$$

for any $u \in H_k$.

Let β be a root of (3.16). Then β is of order 2^{k+2}. As $k+2 \leq a+1$, β is of degree 2 over F_p. The minimal polynomial of β is of the form

$$x^2 - 2rx + s, \tag{3.17}$$

where $r, s \in F_p$. As β is a root of both (3.16) and (3.17), we have

$$\beta^2 + s = 2r\beta, \tag{3.18}$$

and

$$\beta^4 = 2u\beta^2 - 1. \tag{3.19}$$

Squaring (3.18) gives

$$\beta^4 = (4r^2 - 2s)\beta^2 - s^2. \tag{3.20}$$

From (3.19) and (3.20) we have

$$(4r^2 - 2s)\beta^2 - s^2 = 2u\beta^2 - 1.$$

As $\beta^2 \notin F_p$ (since β^2 has order 2^{k+1} and $2^{k+1} \nmid (p-1)$), we must have $4r^2 - 2s = 2u$ and $s^2 = 1$. So

$$s = \pm 1, \tag{3.21}$$

and

$$r = \pm\sqrt{\frac{u+s}{2}} = \pm(\frac{u+s}{2})^{(p+1)/4}. \tag{3.22}$$

The last equation follows from the fact that if w is a quadratic residue in F_p then $w^{(p+1)/4}$ is a square root of w. We prove that s must be 1 if $k < a-1$, and -1 if $k = a-1$.

Case 1 $k < a-1$. Then $k+1 \leq a-1$ and $k+3 \leq a+1$. Suppose $s = -1$ in (3.21) and (3.22). Then, from (3.17), $x^2 - 2rx - 1$ is irreducible and its roots are primitive 2^{k+2}th roots of unity. Hence the roots of $x^4 - 2rx^2 - 1$ are primitive 2^{k+3}th roots of unity. As $k+3 \leq a+1$, $x^4 - 2rx^2 - 1$ has two irreducible factors of degree 2, and assume $x^2 - 2\bar{r}x + \bar{s}$ is one of them. Then, by a similar argument leading to (3.21) and (3.22), we find that

$$\bar{s}^2 = -1 \tag{3.23}$$

and

$$4\bar{r}^2 - 2\bar{s} = 2r \tag{3.24}$$

have at least one solution $(\bar{r}, \bar{s}) \in F_p \times F_p$. This is impossible , as -1 is a quadratic nonresidue in F_p.

Therefore $s = 1$ in (3.21) and (3.22). Since (3.16) has irreducible factors of degree 2, for every $u \in H_k$, $(u + 1)/2$ must be a quadratic residue in F_p. Let $u_1 = ((u + 1)/2)^{(p+1)/4}$. Then

$$x^4 - 2ux^2 + 1 = (x^2 - 2u_1x + 1)(x^2 - 2(-u_1)x + 1).$$

So (3.14) is true for $k + 1$.

Case 2 $k = a - 1$. In this case, $k + 2 = a + 1, k + 3 = a + 2 > a + 1$. Suppose $s = 1$ in (3.21) and (3.22). Then both $x^2 - 2rx + 1$ and $x^2 + 2rx + 1$ are irreducible and have roots being primitive 2^{a+1}th roots of unity. Thus the roots of

$$x^4 - 2rx^2 + 1 \tag{3.25}$$

and

$$x^4 + 2rx^2 + 1 \tag{3.26}$$

are primitive 2^{a+2}th roots of unity. Since p has order 4 modulo 2^{a+2}, a primitive 2^{a+2}th root of unity is of degree 4 over F_p. So (3.25) and (3.26) must be irreducible over F_p.

It is easy to see that if $(r + 1)/2 = \bar{r}^2$ for some $\bar{r} \in F_p$, then $x^2 - 2\bar{r}x + 1$ divides (3.25); if $(r - 1)/2 = \tilde{r}^2$ for some $\tilde{r} \in F_p$, then $x^2 - 2\tilde{r}x - 1$ divides (3.25). So for (3.25) to be irreducible, both $(r+1)/2$ and $(r-1)/2$ must be quadratic nonresidues. Similarly, for (3.26) to be irreducible, both of $(-r + 1)/2$ and $(-r - 1)/2$ must also be quadratic nonresidues. This is impossible, since -1 is a quadratic nonresidue in F_p and one of $(r + 1)/2$ and $-(r + 1)/2$ is a quadratic residue in F_p.

Therefore $s = -1$ in (3.21) and (3.22). Hence, for each $u \in H_k$, $(u-1)/2$ is a quadratic residue in F_p. Let $u_1 = ((u - 1)/2)^{(p+1)/4}$. Then

$$x^4 - 2ux^2 + 1 = (x^2 - 2u_1x - 1)(x^2 - 2(-u_1)x - 1).$$

So (3.15) is true for $e = 0$.

This proves by induction that (3.14) and (3.15) with $e = 0$ hold. As the factors in (3.14) and (3.15) (with $e = 0$) are minimal polynomials of roots of unity, they are all irreducible over F_p. For $e > 0$, (3.15) obviously holds as it is true for $e = 0$. We just need to prove that every factor in (3.15) is irreducible over F_p. For any $u \in H_a$, we have proved that $x^2 - 2ux - 1$ is irreducible over F_p. Let α_1, α_2 be its two roots. We know that $\alpha_1, \alpha_2 \in F_{p^2}$ and have order 2^{a+1}. By Lemma 3.3.4, $x^{2^e} - \alpha_1$ and $x^{2^e} - \alpha_2$ are irreducible over F_{p^2} for any integer $e \geq 1$. Hence

$$(x^{2^e} - \alpha_1)(x^{2^e} - \alpha_2) = x^{2^{e+1}} - 2ux^{2^e} - 1$$

is irreducible over F_p.

This completes the proof. □

Note that when $p \equiv -1(\text{mod}8)$ (so $a > 2$), $1/2$ is a quadratic residue in F_p. From the above proof we see that if $k < a - 1$ then, for every $u \in H_k$, $(u + 1)/2$ is a quadratic residue in F_p, thus $u + 1$ is a quadratic residue. Observe that the irreducibility of $x^2 - 2ux + 1 = (x - u)^2 - (u^2 - 1)$ implies that $u^2 - 1 = (u - 1)(u + 1)$ is a quadratic nonresidue. So $u - 1$ is a quadratic nonresidue. Similarly, for $u \in H_{a-1}$, $u-1$ is a quadratic residue and $u+1$ is a quadratic nonresidue. For $u \in H_a$, we can only say that $u^2 + 1$ is a quadratic nonresidue due to the irreducibility of $x^2 - 2ux - 1$. In summary, we have

Corollary 3.3.6 *If $p \equiv -1(\text{mod}8)$ (hence $a > 2$), then*

(a) *for each $1 \leq k < a-1$ and $u \in H_k$, $u+1$ is a quadratic residue in F_p and $u-1$ is a quadratic nonresidue in F_p;*

(b) *for each $u \in H_{a-1}$, $u - 1$ is a quadratic residue in F_p and $u + 1$ is a quadratic nonresidue in F_p;*

(c) *for each $u \in H_a$, $u^2 + 1$ is a quadratic nonresidue in F_p.*

This solves, in a theoretical sense, a problem arising from primality testing [35, (11.6)(a)] and [26, section 5], as remarked by Lenstra [85, page 344].

Corollary 3.3.7 *For $1 \leq k \leq a$, let $u \in H_k$. Define*

$$v = \begin{cases} (1 - u^2)^{(p+1)/4}, & \text{if } k < a, \\ (-1 - u^2)^{(p+1)/4}, & \text{if } k = a. \end{cases}$$

Then $u + iv \in F_{p^2} = F_p(i)$ is a 2^{k+1}th primitive root of unity where $i = \sqrt{-1}$.

Proof: For $u \in H_k$ with $k < a$, we know from Corollary 3.3.6 that $1 - u^2$ is a quadratic residue in F_p. So $v = (1-u^2)^{(p+1)/4}$ is a square root of $1 - u^2$, that is, $v^2 = 1 - u^2$. Hence $u + iv$ is a root of $x^2 - 2ux + 1$. By Theorem 3.3.5, $u + iv$ is a 2^{k+1}th primitive root of unity. For $u \in H_a$, the proof is similar. □

As $x^{2^t} - 1 = (x-1)\prod_{i=0}^{t-1}(x^{2^i} + 1)$, the following corollary is an immediate consequence of Theorem 3.3.5.

Corollary 3.3.8 *For any integer $t \geq 1$, the following factorization over F_p is complete:*

(a) *if $t < a + 1$, then*

$$x^{2^t} - 1 = (x-1)(x+1)\prod_{i=1}^{t-1}\prod_{u \in H_i}(x^2 - 2ux + 1);$$

(b) *if $t \geq a + 1$, then*

$$x^{2^t} - 1 = (x-1)(x+1)\prod_{\substack{u \in H_i \\ 1 \leq i \leq a-1}}(x^2 - 2ux + 1)\prod_{\substack{u \in H_a \\ 0 \leq r \leq t-a-1}}(x^{2^{r+1}} - 2ux^{2^r} - 1).$$

In concluding this section, we mention a possible application of the above results in applying the Fast Fourier Transform (FFT) over finite fields [91, Chapter IX] and [4, Chapter 7]. The FFT is widely used in many areas including computing the convolution of data, digital signal processing and computing products of polynomials or integers. In [91], to apply the FFT over finite fields one chooses an appropriately large $N = 2^e$ and a prime p of the form $Nk + 1$. If an Nth root of unity ω in F_p is given, then the FFT evaluates a polynomial in $F_p[x]$ of degree at most N at the N points $1, \omega, \omega^2, \ldots, \omega^{N-1}$ in time $O(N \log N)$. The problem here is that, when an integer e and a prime $p = 2^e k + 1$ are given, there is currently no deterministic polynomial time (in $\log p$ and e) algorithm to construct a 2^eth primitive root of unity in F_p. It is suggested in [4] to apply the FFT over the ring $\mathbb{Z}_m$ of integers modulo m where $m = 2^{N/2} + 1$ (which is not necessarily a prime). One advantage of $\mathbb{Z}_m$ is that 2 is known to be a primitive Nth root of unity in $\mathbb{Z}_m$. Since the number m is exponential in N, the computation in $\mathbb{Z}_m$ may be expensive for large N. In the following we show that such problems do not exist if one operates the FFT over F_{p^2}.

Let $e \geq 1$ be a positive integer and $N = 2^e$. Let p be any prime of the form $2Nk - 1$. Define $u = u_e$ inductively: $u_1 = 0$ and

$$u_k = (\frac{1 + u_{k-1}}{2})^{(p+1)/4}, \quad k = 2, 3, \ldots, e.$$

Let

$$v = (1 - u^2)^{(p+1)/4}.$$

Then, by Theorem 3.3.5 and Corollary 3.3.7, $\omega = u + iv \in F_{p^2} = F_p(i)$ is a 2^eth primitive root of unity where $i = \sqrt{-1}$. Here the number of F_p-operations needed to get $u + iv$ is $O(e \log p)$. So one can compute a 2^eth primitive root of unity in F_{p^2} quickly for any given integer e and prime p of the form $2Nk - 1$. Also, for fixed $N = 2^e$, the prime number theorem in arithmetic progressions [88] implies that the number of primes $2Nk - 1 \leq N^2$ is approximately $N/(2e \log 2)$. This means that primes of the required form exist in reasonable abundance and their sizes can be bounded by N^2. So the problems encountered in [4] and [91] are avoided when the FFT is applied over F_{p^2}.

3.4 Specific Constructions

In this section, we shall present several families of N-polynomials (irreducible polynomials whose roots are linearly independent).

3.4.1 For n whose prime factors divides $q - 1$

The following result shows how to construct an infinite family of N-polynomials whose degrees have prime factors from $q - 1$.

Theorem 3.4.1 *Let $a \in F_q$ be such that $x^n - a$ is irreducible in $F_q[x]$. Then the polynomial*

$$ax^n - (x-1)^n$$

is irreducible and has linearly independent roots over F_q.

Proof: Let α be a root of $x^n - a$. Then

$$\frac{1}{1-\alpha} = \frac{1}{1-a}(1 + \alpha + \cdots + \alpha^{n-1}).$$

By Theorem 2.4.9, we see that $(1-\alpha)^{-1}$ is a normal element in F_{q^n} over F_q. It is easy to check that $(1-\alpha)^{-1}$ is a zero of $ax^n - (x-1)^n$. Therefore $ax^n - (x-1)^n$ is a scalar multiple of the minimal polynomial of $(1-\alpha)^{-1}$, and thus an N-polynomial. □

By Lemma 3.3.4, we have the following corollary.

Corollary 3.4.2 *Let a be a primitive element in F_q and $n = \prod_{i=1}^{k} r_i^{l_i}$ where $r_1, r_2, \ldots, r_k$ are distinct prime factors of $q-1$. We assume that $q \equiv 1 (\mathrm{mod}\ 4)$ if some $r_i = 2$. Then the polynomial*

$$ax^n - (x-1)^n$$

is irreducible and has linearly independent roots over F_q for all positive integers $l_1, l_2, \ldots, l_k$.

Example 3.4.3 As 2 is primitive in F_5, and by Corollary 3.4.2, the polynomial $2x^{2^k} - (x-1)^{2^k}$ is irreducible with linearly independent roots over F_5 for all integers $k \geq 1$.

Example 3.4.4 Over F_{13}, the following polynomials are N-polynomials for all integer $k, \ell \geq 0$:

a. $ax^{2^k} - (x-1)^{2^k}$, $a \in \{\pm 2, \pm 5, \pm 6\}$;

b. $ax^{3^k} - (x-1)^{3^k}$, $a \in \{\pm 2, \pm 3, \pm 4, \pm 6\}$;

c. $ax^{2^\ell 3^k} - (x-1)^{2^\ell 3^k}$, $a \in \{\pm 2, \pm 6\}$.

3.4.2 For n being a power of 2

In this section, we show how to construct an N-polynomial of degree any power of 2. If $q \equiv 1 \bmod 4$, then by Theorem 3.4.1, for any quadratic nonresidue a in F_q, the polynomial $ax^{2^k} - (x-1)^{2^k}$ is an N-polynomial for every integer $k \geq 0$. If $q \equiv 3 \bmod 4$, we just need to consider the problem over the prime field F_p, since if p is the characteristic of F_q then $p \equiv 3 \bmod 4$ and $q = p^m$ for odd m, and further, any N-polynomial of degree a power of 2 in $F_p[x]$ remains an N-polynomial in $F_q[x]$.

Theorem 3.4.5 *Let $p \equiv 3 \bmod 4$ be a prime. Assume that $x^2 - bx - c \in F_p[x]$ is irreducible with $b \neq 2$ and c a quadratic residue in F_p. Then the polynomial*

$$(x-1)^{2^{k+1}} - b(x-1)^{2^k} x^{2^k} - cx^{2^k} \tag{3.27}$$

is irreducible with roots being linearly independent over F_p for every integer $k \geq 0$.

Before proceeding to the proof of Theorem 3.4.5, we look at a corollary and some examples.

Corollary 3.4.6 *Let* $p \equiv 3 \bmod 4$ *be a prime and let* a *be the largest integer such that* $2^a|(p+1)$*. Let the set* $H_a \subset F_p$ *be defined as in Theorem 3.3.5. Then for any* $u \in H_a$*,* $u \neq 1$*, the polynomial*

$$(x-1)^{2^{k+1}} - 2u(x-1)^{2^k} x^{2^k} - x^{2^{k+1}}$$

is an N*-polynomial over* F_p *of degree* 2^{k+1} *for every integer* $k \geq 0$*.*

Example 3.4.7 Let $p = 3$. Then $a = 2$. We have $H_1 = \{0\}$, $H_2 = \{\pm 1\}$. So by Corollary 3.4.6, the polynomial

$$(x-1)^{2^{k+1}} + 2(x-1)^{2^k} x^{2^k} - x^{2^{k+1}}$$

is an N-polynomial over F_3 of degree 2^{k+1} for every integer $k \geq 0$.

Example 3.4.8 Let $p = 7$. Then $a = 3$. We have $H_1 = \{0\}$, $H_2 = \{\pm 2\}$, and $H_3 = \{\pm 2, \pm 4\}$. Hence for every $u \in H_3$, the polynomial

$$(x-1)^{2^{k+1}} - 2u(x-1)^{2^k} x^{2^k} - x^{2^{k+1}}$$

is an N-polynomial over F_7 of degree 2^{k+1} for every integer $k \geq 0$.

Proof of Theorem 3.4.5: Let α be a root of (3.27). Then $\theta = (\alpha - 1)/\alpha$ is a root of

$$x^{2^{k+1}} - bx^{2^k} - c. \tag{3.28}$$

The polynomial (3.27) is irreducible over F_p if and only if the polynomial (3.28) is irreducible over F_p. To see that (3.28) is irreducible, let γ be a root of $x^2 - bx - c$ in F_{p^2}. As $x^2 - bx - c$ is irreducible over F_p, we have $\gamma^p + \gamma = b$ and $\gamma^p \gamma = \gamma^{p+1} = -c$. Since $-c$ is a quadratic nonresidue in F_p, the multiplicative order of $-c$ is divisible by 2. Let $p + 1 = 2^a h_1$ for h_1 odd. Then $p^2 - 1 = 2^{a+1} h_2$ for h_2 odd. The multiplicative order of γ must be divisible by 2^{a+1}. Hence γ, and thus γ^p, is a quadratic nonresidue in F_{p^2}. It follows from Lemma 3.3.4 that $x^{2^k} - \gamma$ and $x^{2^k} - \gamma^p$ are irreducible over F_{p^2} for every integer $k \geq 0$. Consequently

$$(x^{2^k} - \gamma)(x^{2^k} - \gamma^p) = x^{2^{k+1}} - bx^{2^k} - c,$$

is irreducible over F_p for every integer $k \geq 0$. It remains to prove that the 2^{k+1} roots of (3.27) in $F_{p^{2^{k+1}}}$ are linearly independent over F_p, that is, we have to prove that α is a normal element in $F_{p^{2^{k+1}}}$ over F_p.

To establish this, we shall use Corollary 2.4.8. We first factor $x^{2^{k+1}} - 1$ over F_p, then we decompose $F_{p^{2^{k+1}}}$ into the direct sum of irreducible invariant subspaces under the Frobenius map $\sigma : \beta \mapsto \beta^p$, $\beta \in F_{p^{2^{k+1}}}$, and at the same time we prove that the projection of α in each of the subspaces is not zero. Our approach is motivated by Semaev [123, §3].

First some notations are in order. We fix that $p^2 - 1 = 2^{a+1}h_1$, $p + 1 = 2^a h_2$ and $p - 1 = 2h_3$ where h_1, h_2, h_3 are odd integers. Obviously, $h_1 = h_2 h_3$, $h_2 = (1 + h_3)/2^{a-1}$. Let E be the multiplicative subgroup of order 2^{a+1} in F_{p^2} and let $E_i \subset E$ be the set of elements in F_{p^2} with multiplicative order exactly 2^i for $i = 0, 1, 2, \ldots, a + 1$. Then $E = E_0 \cup E_1 \cup \cdots \cup E_{a+1}$. For an integer ℓ, we use $v(\ell)$ to denote the largest integer v such that $2^v | \ell$, that is, $\ell = 2^{v(\ell)}\ell_1$ where ℓ_1 is odd. When $\ell = 0$ we define $v(\ell) = \infty$.

By Corollary 3.3.8, the irreducible factors of $x^{2^{k+1}} - 1$ over F_p have the following forms:

(a) $x - 1$, $x + 1$;

(b) $x^2 + 1$;

(c) $x^2 - (\omega + \omega^{-1})x + 1$, for $\omega \in E_3 \cup E_4 \cup \cdots \cup E_{\min\{a,k+1\}}$;

(d) $x^2 - (\omega - \omega^{-1})x - 1$ for $\omega \in E_{a+1}$, if $k \geq a$;

(e) $x^{2^{r+1}} - (\omega - \omega^{-1})x^{2^r} - 1$ for $\omega \in E_{a+1}$ and $1 \leq r \leq k - a$.

This could be seen as follows. Let β be a root of $x^{2^{k+1}} - 1$. Then β has multiplicative order 2^i for some i with $0 \leq i \leq k + 1$. The minimal polynomial $m_\beta(x)$ of β over F_p is an irreducible factor of $x^{2^{k+1}} - 1$. If $i \leq 1$ then $m_\beta(x)$ is either $x - 1$ or $x + 1$. If $2 \leq i \leq a$, then $\beta \in E \setminus E_{a+1}$ and $\beta^{2^a} = 1$. As $2^a | (p + 1)$, we have $\beta^{p+1} = 1$, hence $\beta^p = \beta^{-1} \neq \beta$. So $m_\beta(x)$ is of the form (b) or (c). If $i > a$, then $\omega = \beta^{2^{i-a-1}} \in E_{a+1}$. In this case, $\omega^{2^a} = -1$, and $\omega^{p+1} = \omega^{2^a h_2} = (-1)^{h_2} = -1$, as h_2 is odd. Hence $\beta^p = -\beta^{-1}$. Since $x^{2^{i-a-1}} - \omega$ and $x^{2^{i-a-1}} - \omega^p$ are irreducible over F_p by Lemma 3.3.4, the polynomial

$$(x^{2^{i-a-1}} - \omega)(x^{2^{i-a-1}} - \omega^p) = x^{2^{i-a}} - (\omega - \omega^{-1})x^{2^{i-a-1}} - 1$$

is irreducible over F_p. However this polynomial has β as a zero, we see that $m_\beta(x)$ is of the form (d) or (e).

Now we proceed to decompose $F_{p^{2^{k+1}}}$ into the direct sum of irreducible σ-invariant subspaces. For convenience, we denote $t = 2^k$. We use t and 2^k interchangeably. Thus $2t = 2^{k+1}$. Let $\gamma = \theta^t$. Then γ is a root of $x^2 - bx - c$ and

$$\sigma(\gamma) = \gamma^p = -c/\gamma, \quad \gamma^2 = b\gamma + c, \quad \gamma^{p+1} = -c. \tag{3.29}$$

Since $-c$ is a quadratic nonresidue in F_p, γ is a quadratic nonresidue in F_{p^2}. Thus $\gamma^{h_1 m} \in E_{a+1}$ for any odd integer m. We also have

$$\alpha = \frac{1}{1-\theta} = \frac{1}{1-\gamma^2}(1 + \theta + \cdots + \theta^{t-1} + \gamma + \gamma\theta + \cdots + \gamma\theta^{t-1}). \tag{3.30}$$

Since θ has degree $2t$ over F_p, the $2t$ elements

$$1, \theta, \ldots, \theta^{t-1}, \gamma, \gamma\theta, \ldots, \gamma\theta^{t-1} \tag{3.31}$$

form a basis for $F_{p^{2t}}$ over F_p.

For ℓ such that $0 \le \ell \le t - 1 = 2^k - 1$, let

$$M_\ell = \{\ell p^i \bmod t : \ i = 0, 1, 2, \ldots\}$$

be the cyclotomic class modulo t containing ℓ. Note that $M_0 = \{0\}$, and for $\ell \neq 0$, the size of M_ℓ is equal to the smallest positive integer i such that $\ell \equiv \ell p^i \bmod 2^k$, i.e., $1 \equiv p^i \bmod 2^{k-v(\ell)}$. As 2 and 2^{a+1} divide exactly $p-1$ and p^2-1, respectively, we see that

$$|M_\ell| = \begin{cases} 1, & \text{if } \ell = 0, \\ 1, & \text{if } v(\ell) = k-1, \\ 2, & \text{if } k - a \le v(\ell) \le k-2, \\ 2^{k-v(\ell)-a}, & \text{if } v(\ell) < k - a. \end{cases}$$

Let V_ℓ be the subspace of $F_{p^{2t}}$ spanned over F_p by the elements of the set

$$\{\theta^r, \gamma\theta^r : \ r \in M_\ell\}.$$

Then V_ℓ is of dimension $2|M_\ell|$ over F_p, and V_ℓ is also a subspace over F_{p^2} of dimension $|M_\ell|$. Let

$$\{0, 1, \ldots, t-1\} = \bigcup_{\ell \in L} M_\ell$$

be a disjoint union for some subset L of $\{0, 1, \ldots, t-1\}$. Then

$$F_{p^{2t}} = \sum_{\ell \in L} V_\ell$$

is a direct sum. Let

$$\alpha_\ell = \frac{1}{1-\gamma^2}\Big(\sum_{r \in M_\ell} \theta^r + \gamma\theta^r\Big).$$

Then $\alpha_\ell \in V_\ell$ and

$$\alpha = \sum_{\ell \in L} \alpha_\ell.$$

For each $\ell \in L$, we shall prove that V_ℓ is either an irreducible σ-invariant subspace or a direct sum of two irreducible σ-invariant subspaces. Thus we obtained all the irreducible σ-invariant subspaces of $F_{p^{2t}}$ over F_p. To prove that α is a normal element, it suffices to check that the projection of α in each of the subspaces is not zero. In the first case, the projection of α in V_ℓ is $\alpha_\ell \neq 0$, nothing to check. In the latter case, we need to find the projection of α_ℓ in each of the two irreducible subspaces of V_ℓ and verify that it is not zero. We are going to discuss in the following cases, corresponding to the types of polynomials (a)–(e):

(A) $\ell = 0$;

(B) $v(\ell) = k-1$, then $\ell = 2^{k-1}$;

(C) $k - a + 1 \leq v(\ell) \leq k-2$;

(D) $v(\ell) = k - a$;

(E) $v(\ell) < k - a$.

We proceed in the order A,B,E,C,D, since the cases (C) and (D) are more complicated.

Case (A). Obviously, $V_0 = F_p \oplus \gamma F_p = F_{p^2}$. Hence V_0 is a σ-invariant subspace with $x^2 - 1$ as annihilating polynomial. As $x^2 - 1 = (x-1)(x+1)$, V_0 splits into two irreducible σ-invariant subspaces. One is evidently F_p with $x - 1$ as annihilating polynomial. Since $\sigma(\gamma + c/\gamma) = -(\gamma + c/\gamma)$, the other must be $(\gamma + c/\gamma)F_p$ with $x + 1$ as annihilating polynomial. Therefore

$$V_0 = F_p \oplus (2\gamma - b)F_p.$$

(Note that $2\gamma - b = \gamma + c/\gamma$.) It can be checked that

$$\alpha_0 = \frac{1}{1-\gamma^2}(1+\gamma) = \frac{b-2}{2(b+c-1)} + \left(-\frac{1}{2(b+c-1)}\right)(2\gamma - b).$$

As $b \neq 2$ by assumption, the projections of α_0 (or α) into the irreducible σ-invariant subspaces with annihilating polynomials $x-1$ and $x+1$ do not vanish.

Case (B). Note that $\theta^{2^k} = \gamma \in F_{p^2}$, we have $\left(\theta^{2^{k-1}(p^2-1)}\right)^2 = \left(\theta^{2^k}\right)^{p^2-1} = 1$. It follows that $\theta^{2^{k-1}(p^2-1)} = -1$, as $\theta^{2^{k-1}} \notin F_{p^2}$. Hence

$$\begin{aligned} (\sigma^2+1)(\theta^{2^{k-1}}) = \theta^{2^{k-1}}\left(\theta^{2^{k-1}(p^2-1)}+1\right) &= 0, \\ (\sigma^2+1)(\gamma\theta^{2^{k-1}}) = \gamma\theta^{2^{k-1}}\left(\theta^{2^{k-1}(p^2-1)}+1\right) &= 0. \end{aligned}$$

Therefore $V_{2^{k-1}}$ spanned by $\theta^{2^{k-1}}$ and $\gamma\theta^{2^{k-1}}$ over F_p is a σ-invariant subspace with x^2+1 as annihilating polynomial. As the dimension of $V_{2^{k-1}}$ is 2, equal to the degree of x^2+1, $V_{2^{k-1}}$ is the irreducible invariant subspace annihilated by x^2+1. The projection of α in $V_{2^{k-1}}$ is $\alpha_{2^{k-1}} \neq 0$.

Case (E). Let $\ell = 2^{v(\ell)}\ell_1$ for ℓ_1 odd and let $p_1 = p^{2^{k-v(\ell)-a}}$. Since $k - v(\ell) - a \geq 1$, we have $p_1 = 1 + 2^{k-v(\ell)}m$ for m odd and

$$p_1^2 = 1 + 2^{k-v(\ell)+1}(m + 2^{k-v(\ell)-1}m^2).$$

Note that $(p^2-1)|(p_1-1)$, we have $h_1|m$. Let $b_\ell = \gamma^{m\ell_1}$. Then $b_\ell = (\gamma^{h_1})^{\ell_1 m/h_1} \in E_{a+1}$. Now let

$$\psi_\ell(x) = x^{2^{k-v(\ell)-a+1}} - (b_\ell - b_\ell^{-1})x^{2^{k-v(\ell)-a}} - 1.$$

Then $\psi_\ell(x)$ is irreducible over F_p. We show that V_ℓ is annihilated by $\psi_\ell(\sigma)$. Note that

$$\begin{aligned} \psi_\ell(\sigma)\theta^\ell &= \theta^\ell\left(\theta^{\ell(p_1^2-1)} - (b_\ell - b_\ell^{-1})\theta^{\ell(p_1-1)} - 1\right) \\ &= \theta^\ell\left(\theta^{2^{k+1}(m+2^{k-v(\ell)-1}m^2)\ell_1} - (b_\ell - b_\ell^{-1})\theta^{2^k m\ell_1} - 1\right) \\ &= \theta^\ell\left(\gamma^{2m\ell_1} - (b_\ell - b_\ell^{-1})\gamma^{m\ell_1} - 1\right) \\ &= 0, \end{aligned}$$

as $\theta^{2^k} = \gamma \in F_{p^2}$ and $\gamma^{2^{k-v(\ell)}m^2\ell_1} = 1$. If $r \in M_\ell$, then $r \equiv \ell p^s \bmod t$ for some integer s. Note that $v(\ell) = v(r)$ and $r = 2^{v(\ell)}\ell_1 p^s$. By a similar argument, we have

$$\psi_r(\sigma)\theta^r = 0,$$

where

$$\psi_r(x) = x^{2^{k-v(r)-a+1}} - (b_r - b_r^{-1})x^{2^{k-v(r)-a}} - 1,$$

with $b_r = \gamma^{m\ell_1 p^s}$. Since

$$b_r = (b_\ell)^{p^s} = \begin{cases} b_\ell & \text{if } s \text{ is even,} \\ -b_\ell^{-1} & \text{if } s \text{ is odd,} \end{cases}$$

we have $b_r - b_r^{-1} = b_\ell - b_\ell^{-1}$. Thus $\psi_r(x) = \psi_\ell(x)$ for $r \in M_\ell$. This implies that $\psi_\ell(\sigma)\theta^r = 0$ for each $r \in M_\ell$.

Note that, for any $r \in M_\ell$, $\psi_\ell(\sigma)(\gamma\theta^r) = \gamma\psi_\ell(\sigma)(\theta^r) = 0$. Therefore all the elements in the basis $\{\theta^r, \gamma\theta^r : r \in M_\ell\}$ of V_ℓ are annihilated by $\psi_\ell(\sigma)$. So V_ℓ is annihilated by $\psi_\ell(\sigma)$. Since $\psi_\ell(x)$ has degree $2^{k-v(\ell)-a+1}$, which is equal to the dimension of V_ℓ over F_p, the irreducibility of $\psi_\ell(x)$ implies that V_ℓ is the irreducible σ-invariant subspace annihilated by $\psi_\ell(x)$. The projection of α in V_ℓ is $\alpha_\ell \neq 0$.

Common for Cases (C) and (D). In both cases, we shall show that V_ℓ splits into two irreducible σ-invariant subspaces of dimension 2. Let $\ell = 2^{v(\ell)}\ell_1$ for ℓ_1 odd. We have

$$k - a \leq v(\ell) \leq k - 2.$$

Hence

$$2 \leq k - v(\ell) \leq a.$$

Note that $\ell(p+1) = 2^{v(\ell)+a}\ell_1 h_2 \equiv 2^k \pmod{t}$, as $v(\ell) + a \geq k$. We see that $\ell p \equiv 2^k - \ell \ (\mathrm{mod} t)$. Thus

$$M_\ell = \{\ell, 2^k - \ell\}.$$

The basis for V_ℓ over F_p is

$$\{\theta^\ell, \theta^{2^k-\ell}, \gamma\theta^\ell, \gamma\theta^{2^k-\ell}\} = \{\theta, \gamma\theta^{-\ell}, \gamma\theta^\ell, \gamma^2\theta^{-\ell}\}.$$

It is easy to see that

$$V_\ell = \theta^\ell F_{p^2} \oplus \theta^{-\ell} F_{p^2},$$

since $F_{p^2} = F_p(\gamma) = F_p \oplus \gamma F_p$. Let $b_\ell = \gamma^{2^{a-k} h_1 \ell}$. Then

$$b_\ell = \gamma^{2^{a+v(\ell)-k} h_1 \ell_1} \in E \setminus (E_0 \cup E_1 \cup E_2),$$

and

$$\theta^{p^2 \ell} = \theta^\ell \theta^{\ell(p^2-1)} = \theta^\ell \theta^{2^{a+1} h_1 \ell} = \theta^\ell (\theta^{2^k})^{2^{a+1-k} h_1 \ell} = \theta^\ell \gamma^{2^{a-k+1} h_1 \ell} = \theta^\ell b_\ell^2.$$

Let $c_\ell = \gamma^{2^{a-k} h_2 \ell}$. Then

$$\theta^{p\ell} = \theta^{-\ell} \theta^{\ell(p+1)} = \theta^{-\ell} \theta^{2^a h_2 \ell} = \theta^{-\ell} \left(\theta^{2^k}\right)^{2^{a-k} h_2 \ell} = \theta^{-\ell} \gamma^{2^{a-k} h_2 \ell} = \theta^{-\ell} c_\ell.$$

Denote $b_\ell c_\ell$ by d_ℓ. Then

$$d_\ell = b_\ell c_\ell = \gamma^{2^{a-k}(h_1+h_2)\ell} = \gamma^{2^{a-k} h_2 (1+h_3)\ell} = \gamma^{2^{a-k+a-1+v(\ell)} h_2^2 \ell_1}.$$

Case (C). Assume that we are in case (C). Then $v(\ell) + a - k \geq 1$. Hence $b_\ell \in E \setminus E_{a+1}$ and

$$d_\ell = \left(\gamma^{p+1}\right)^{2^{a+v(\ell)-k-1} h_2 \ell_1} = c^{2^{a+v(\ell)-k-1} h_2 \ell_1} \in F_p.$$

For $\delta = 1, 2$, let

$$\psi_{\ell\delta}(x) = x^2 + (-1)^\delta (b_\ell + b_\ell^{-1}) x + 1.$$

Then $\psi_{\ell\delta}(x)$ is irreducible in $F_p[x]$. Let $V_{\ell\delta} \subseteq V_\ell$ be the subspace spanned over F_p by

$$\alpha_{\ell\delta}^{(1)} = \theta^\ell - (-1)^\delta d_\ell \theta^{-\ell}, \;\; \alpha_{\ell\delta}^{(2)} = c\gamma^{-1}\theta^\ell + (-1)^\delta d_\ell \gamma \theta^{-\ell}.$$

Then $V_\ell = V_{\ell 1} \oplus V_{\ell 2}$. Since

$$\begin{aligned}
\psi_{\ell\delta}^{(\sigma)}(\alpha_{\ell\delta}^{(1)}) &= \theta^{p^2\ell} + (-1)^\delta (b_\ell + b_\ell^{-1}) \theta^{p\ell} + \theta^\ell - (-1)^\delta d_\ell \theta^{-p^2\ell} \\
&\quad -(-1)^\delta (b_\ell + b_\ell^{-1})(-1)^\delta d_\ell \theta^{-p\ell} - (-1)^\delta d_\ell \theta^{-\ell} \\
&= \theta^\ell b_\ell^2 + (-1)^\delta (b_\ell + b_\ell^{-1}) \theta^{-\ell} c_\ell + \theta^\ell \\
&\quad -(-1)^\delta d_\ell \theta^{-\ell} b_\ell^{-2} - d_\ell (b_\ell + b_\ell^{-1}) \theta^\ell c_\ell^{-1} - (-1)^\delta d_\ell \theta^{-\ell} \\
&= \theta^\ell b_\ell (b_\ell + b_\ell^{-1})(1 - d_\ell c_\ell^{-1} b_\ell^{-1}) - (-1)^\delta \theta^{-\ell} b_\ell^{-1} (b_\ell + b_\ell^{-1})(d_\ell - c_\ell b_\ell) \\
&= 0,
\end{aligned}$$

and

$$\begin{aligned}
\psi_{\ell\delta}^{(\sigma)}(\alpha_{\ell\delta}^{(2)}) &= c\gamma^{-1}\theta^{p^2\ell} + (-1)^{\delta}(b_\ell + b_\ell^{-1})(-\gamma)\theta^{p\ell} + c\gamma^{-1}\theta^{\ell} + (-1)^{\delta} d_\ell \gamma \theta^{-p^2\ell} \\
&\quad + (-1)^{\delta}(b_\ell + b_\ell^{-1})(-1)^{\delta} d_\ell(-c\gamma^{-1})\theta^{-p\ell} + (-1)^{\delta} d_\ell \gamma \theta^{-\ell} \\
&= c\gamma^{-1}\theta^{\ell} b_\ell^2 - (-1)^{\delta}(b_\ell + b_\ell^{-1})\gamma\theta^{-\ell} c_\ell + c\gamma^{-1}\theta^{\ell} \\
&\quad + (-1)^{\delta} d_\ell \gamma \theta^{-\ell} b_\ell^{-2} - d_\ell(b_\ell + b_\ell^{-1}) c\gamma^{-1}\theta^{\ell} c_\ell^{-1} + (-1)^{\delta} d_\ell \gamma \theta^{-\ell} \\
&= c\gamma^{-1}\theta^{\ell} b_\ell(b_\ell + b_\ell^{-1})(1 - d_\ell c_\ell^{-1} b_\ell^{-1}) + (-1)^{\delta}\gamma\theta^{-\ell} b_\ell^{-1}(b_\ell + b_\ell^{-1})(d_\ell - c_\ell b_\ell) \\
&= 0,
\end{aligned}$$

we see that $V_{\ell\delta}$ is annihilated by $\psi_{\ell\delta}(\sigma)$. As the dimension of $V_{\ell\delta}$ equals the degree of $\psi_{\ell\delta}(x)$, it follows that $V_{\ell\delta}$ is the irreducible σ-invariant subspace of $\psi_{\ell\delta}(\sigma)$ for $\delta = 1, 2$.

Now it can be checked that

$$\begin{aligned}
\alpha_\ell &= \frac{1}{1-\gamma^2}(\theta^{\ell} + \gamma\theta^{-\ell} + \gamma\theta^{\ell} + \gamma^2\theta^{-\ell}) \\
&= \frac{1}{1-\gamma}(\theta^{\ell} + \gamma\theta^{-\ell}) \\
&= x_1\alpha_{\ell 1}^{(1)} + x_2\alpha_{\ell 1}^{(2)} + y_1\alpha_{\ell 2}^{(1)} + y_2\alpha_{\ell 2}^{(2)}
\end{aligned}$$

where

$$\begin{aligned}
x_1 &= \frac{d_\ell + c}{2d_\ell(1-b-c)}, \qquad x_2 = \frac{d_\ell - 1}{2d_\ell(1-b-c)}, \\
y_1 &= \frac{d_\ell - c}{2d_\ell(1-b-c)}, \qquad y_2 = \frac{d_\ell + 1}{2d_\ell(1-b-c)}.
\end{aligned}$$

Since $c \neq -1$ (as -1 is a quadratic nonresidue in F_p),

$$x_1 - x_2 = y_2 - y_1 = \frac{c+1}{2d_\ell(1-b-c)} \neq 0.$$

Therefore

$$(x_1, x_2) \neq (0,0), \quad (y_1, y_2) \neq (0,0),$$

that is, the projections of α_ℓ (or α) in $V_{\ell 1}$ and $V_{\ell 2}$ do not vanish.

Case (D). Finally, assume that we are in case (D), that is, $v(\ell) = k - a$. Then $b_\ell = \gamma^{h_1\ell_1} \in E_{a+1}$ and $c_\ell b_\ell = \gamma^{2^{a-1}h_2^2\ell_1}$. We have

$$(c_\ell b_\ell)^{p-1} = \gamma^{2^a h_2^2 \ell_1 h_3} = \left(\gamma^{2^a h_1}\right)^{h_2\ell_1} = \left(\gamma^{(p^2-1)/2}\right)^{h_2\ell_1} = (-1)^{h_2\ell_1} = -1,$$

since γ is a quadratic nonresidue and $h_2\ell_1$ is odd. Thus

$$\sigma(c_\ell b_\ell) = (c_\ell b_\ell)^p = -c_\ell b_\ell.$$

Let $\epsilon = (c_\ell b_\ell)/(\gamma + c\gamma^{-1})$. Then $\epsilon \in F_p$, as $\sigma(\epsilon) = \epsilon$. For $\delta = 1, 2$, let

$$\psi_{\ell\delta}(x) = x^2 + (-1)^\delta (b_\ell - b_\ell^{-1})x - 1.$$

Then $\psi_{\ell\delta}(x)$ is irreducible in $F_p[x]$. Let $V_{\ell\delta} \subseteq V_\ell$ be the subspace spanned over F_p by the two elements

$$\begin{aligned}
\alpha_{\ell\delta}^{(1)} &= \theta^\ell + (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\theta^{-\ell}, \\
\alpha_{\ell\delta}^{(2)} &= c\gamma^{-1}\theta^\ell - (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell}.
\end{aligned}$$

Then $V_\ell = V_{\ell 1} \oplus V_{\ell 2}$. Note that

$$\begin{aligned}
\psi_{\ell\delta}^{(\sigma)}(\alpha_{\ell\delta}^{(1)}) &= \theta^{p^2\ell} + (-1)^\delta (b_\ell - b_\ell^{-1})\theta^{p\ell} - \theta^\ell + (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\theta^{-p^2\ell} \\
&\quad +(-1)^\delta (b_\ell - b_\ell^{-1})(-1)^\delta \epsilon(-c\gamma^{-1} - \gamma)\theta^{-p\ell} - (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\theta^{-\ell} \\
&= \theta^\ell b_\ell^2 + (-1)^\delta (b_\ell - b_\ell^{-1})\theta^{-\ell} c_\ell - \theta^\ell + (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\theta^{-\ell} b_\ell^{-2} \\
&\quad -\epsilon(b_\ell - b_\ell^{-1})(\gamma + c\gamma^{-1})\theta^\ell c_\ell^{-1} - (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\theta^{-\ell} \\
&= \theta^\ell b_\ell (b_\ell - b_\ell^{-1})(1 - \epsilon(\gamma + c\gamma^{-1})c_\ell^{-1} b_\ell^{-1}) \\
&\quad -(-1)^\delta \theta^{-\ell} b_\ell^{-1}(b_\ell - b_\ell^{-1})(\epsilon(\gamma + c\gamma^{-1}) - c_\ell b_\ell) \\
&= 0,
\end{aligned}$$

and

$$\begin{aligned}
\psi_{\ell\delta}^{(\sigma)}(\alpha_{\ell\delta}^{(2)}) &= c\gamma^{-1}\theta^{p^2\ell} + (-1)^\delta (b_\ell - b_\ell^{-1})(-\gamma)\theta^{p\ell} - c\gamma^{-1}\theta^\ell - (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-p^2\ell} \\
&\quad -(-1)^\delta (b_\ell - b_\ell^{-1})(-1)^\delta \epsilon(-c\gamma^{-1} - \gamma)(-c\gamma^{-1})\theta^{-p\ell} + (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell} \\
&= c\gamma^{-1}\theta^\ell b_\ell^2 - (-1)^\delta (b_\ell - b_\ell^{-1})\gamma\theta^{-\ell} c_\ell - c\gamma^{-1}\theta^\ell - (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell} b_\ell^{-2} \\
&\quad -(b_\ell - b_\ell^{-1})\epsilon(\gamma + c\gamma^{-1})c\gamma^{-1}\theta^\ell c_\ell^{-1} + (-1)^\delta \epsilon(\gamma + c\gamma^{-1})\gamma\theta^{-\ell} \\
&= c\gamma^{-1}\theta^\ell b_\ell (b_\ell - b_\ell^{-1})(1 - \epsilon(\gamma + c\gamma^{-1})c_\ell^{-1} b_\ell^{-1}) \\
&\quad +(-1)^\delta \gamma\theta^{-\ell} b_\ell^{-1}(b_\ell - b_\ell^{-1})(\epsilon(\gamma + c\gamma^{-1}) - c_\ell b_\ell) \\
&= 0.
\end{aligned}$$

We see that $V_{\ell\delta}$ is annihilated by $\psi_{\ell\delta}(\sigma)$. As the dimension of $V_{\ell\delta}$ equals the degree of $\psi_{\ell\delta}(x)$, it follows that $V_{\ell\delta}$ is the irreducible σ-invariant subspace of $\psi_{\ell\delta}(\sigma)$ for $\delta = 1, 2$.

It is direct to check that

$$\begin{aligned}\alpha_\ell &= \frac{1}{1-\gamma^2}(\theta^\ell + \gamma\theta^{-\ell} + \gamma\theta^\ell + \gamma^2\theta^{-\ell}) \\ &= \frac{1}{1-\gamma}(\theta^\ell + \gamma\theta^{-\ell}) \\ &= x_1\alpha_{\ell 1}^{(1)} + x_2\alpha_{\ell 1}^{(2)} + y_1\alpha_{\ell 2}^{(1)} + y_2\alpha_{\ell 2}^{(2)}\end{aligned}$$

where

$$\begin{aligned}x_1 &= \frac{1}{2}\left(\frac{1}{1-b-c} + \frac{c(b-2)}{\epsilon(1-b-c)(b^2+4c)}\right), \\ x_2 &= \frac{1}{2}\left(\frac{1}{1-b-c} + \frac{2c+b}{\epsilon(1-b-c)(b^2+4c)}\right), \\ y_1 &= \frac{1}{2}\left(\frac{1}{1-b-c} - \frac{c(b-2)}{\epsilon(1-b-c)(b^2+4c)}\right), \\ y_2 &= \frac{1}{2}\left(\frac{1}{1-b-c} - \frac{2c+b}{\epsilon(1-b-c)(b^2+4c)}\right).\end{aligned}$$

Note that

$$x_1 - x_2 = y_2 - y_1 = \frac{(c-1)b - 4c}{2\epsilon(1-b-c)(b^2+4c)}.$$

We prove that $(c-1)b - 4c \neq 0$. Suppose in the contrary that $(c-1)b - 4c = 0$. Then $c \neq 1$ and thus $b = 4c/(c-1)$. Hence the discriminant $b^2 + 4c = 4c(c+1)^2/(c-1)^2$. The irreducibility of $x^2 - bx - c$ would imply that c were a quadratic nonresidue in F_p, contradicting to the assumption that c is a quadratic residue in F_p. Therefore

$$(x_1, x_2) \neq (0,0), \quad (y_1, y_2) \neq (0,0),$$

that is, the projections of α_ℓ (or α) in $V_{\ell 1}$ and $V_{\ell 2}$ do not vanish.

This completes the proof. □

3.4.3 For n being a power of p

Let p be the characteristic of F_q. For each positive integer k, we shall construct an irreducible polynomial of degree p^k with linearly independent roots. We need some results from Varshamov [137, 138, 139].

Lemma 3.4.9 (Varshamov) *Let $P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ be an irreducible polynomial over F_q, and let $b \in F_q$. Let p be the characteristic of F_q. Then the polynomial $P(x^p - x - b)$ is irreducible over F_q if and only if $Tr_{q|p}(nb - c_{n-1}) \neq 0$.*

A proof of this lemma can be found in [89, 99]. The next theorem is due to Varshamov [139], where no proof is given.

Theorem 3.4.10 (Varshamov) *Let p be a prime and let $f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ be irreducible over F_p. Suppose that there exists an element $a \in F_p$, $a \neq 0$, such that $(na + c_{n-1})f'(a) \neq 0$. Let $g(x) = x^p - x + a$ and define $f_0(x) = f(g(x))$, and $f_k(x) = f_{k-1}^*(g(x))$ for $k \geq 1$, where $f^*(x)$ is the reciprocal polynomial of $f(x)$. Then for each $k \geq 0$, $f_k(x)$ is irreducible over F_p of degree np^{k+1}.*

Proof: The following proof can be found in [142]. From Lemma 3.4.9, $f_0(x) = f(g(x))$ is irreducible if and only if $Tr_{p|p}(na + c_{n-1}) = na + c_{n-1} \neq 0$. Induction is used to show that the coefficient of x in $f_k(x)$, denoted $[x]f_k(x)$, is not 0 and $f_k'(a) \neq 0$. First consider $f_0(x)$:

$$\begin{aligned}
[x]f_0(x) &= \frac{d}{dx} f_0(x)|_{x=0} = \frac{d}{dx}\left(\sum_{i=0}^{n} c_i g^i(x)\right)|_{x=0} \\
&= \sum_{i=0}^{n} c_i i g^{i-1}(x) g'(x)|_{x=0} \\
&= -\sum_{i=0}^{n} c_i i a^{i-1} \quad (\text{since } g(0) = a,\ g'(0) = -1) \\
&= -f'(a),
\end{aligned}$$

which by assumption is non-zero. Similarly note that

$$\begin{aligned}
f_0'(a) &= \sum_{i=0}^{n} c_i i g^{i-1}(a) g'(a) \\
&= -\sum_{i=0}^{n} c_i i a^{i-1} \quad (\text{since } g(a) = a,\ g'(a) = -1) \\
&= -f'(a),
\end{aligned}$$

which again by assumption is non-zero.

Now assume that $f_k(x)$ is irreducible over F_p and that $[x]f_k(x) \neq 0$ and $f_k'(a) \neq 0$. We prove the statement true for $f_{k+1}(x)$. Note that both $f_k(x)$ and $f_k^*(x)$ have degree $np^{k+1} = n_k$. When

$f_k^*(x)$ is made monic, its coefficient of x^{n_k-1} is $[x]f_k(x)/f_k(0) \neq 0$. It follows from Lemma 3.4.9 that $f_{k+1}(x) = f_k^*(g(x))$ is irreducible over F_q. Let

$$f_k(x) \;=\; \sum_{i=0}^{n_k} u_i x^i.$$

Then

$$f_{k+1}(x) \;=\; \sum_{i=0}^{n_k} u_i g^{n_k-i}(x),$$

and

$$\begin{aligned} f'_{k+1}(x) \;&=\; \sum_{i=0}^{n_k} u_i(n_k - i)g^{n_k-i-1}(x)g'(x) \\ &=\; -\sum_{i=0}^{n_k} u_i(n_k - i)g^{n_k-i-1}(x). \end{aligned}$$

Note that since $g(x)$ is constant on F_p, so are $f_k(x)$ and $f'_k(x)$. Thus

$$[x]f_{k+1}(x) \;=\; f'_{k+1}(0) \;=\; f'_k(a^{-1})a^{n_k-1} \;=\; f'_k(a)a^{n_k-1},$$

which is non-zero by the induction hypothesis. Similarly

$$f'_{k+1}(a) \;=\; a^{n_k-1}f'_k(a^{-1}) \;=\; a^{n_k-1}f'_k(a),$$

which is again non-zero. This completes the proof. □

Since $x^p - x - 1$ is irreducible over F_p, substituting x by $1/(x-1)$, it is seen that

$$f(x) \;=\; (x-1)^p + (x-1)^{p-1} - 1 \;=\; x^p + x^{p-1} + \cdots + x - 1$$

is irreducible over F_p. By taking $g(x) = x^p - x - 1$ in Theorem 3.4.10, we obtain the following result.

Corollary 3.4.11 *Let p be a prime. Define $f_{-1}(x) = x^p+x^{p-1}+\cdots+x-1$, $f_0(x) = f_{-1}(x^p-x-1)$ and $f_k(x) = f^*_{k-1}(x^p - x - 1)$ for $k \geq 1$. Then $f_k(x)$ is irreducible over F_p of degree p^{k+2} for every $k \geq -1$. Moreover, the roots of $f_k^*(x)$ are linearly independent over F_p.*

For the latter statement, by Corollary 2.5.2, one just need to check that the coefficient of the next highest term in each polynomial $f_k^*(x)$ is nonzero. However, the proof of Theorem 3.4.10 shows that this is indeed true.

When $p = 2$, we have an another construction as follows. Define polynomials $a_k(x)$ and $b_k(x)$ recursively:

$$\begin{aligned} a_0(x) = x, \qquad & b_0(x) = 1, \\ a_{k+1}(x) \quad &= \quad a_k(x)b_k(x), \\ b_{k+1}(x) \quad &= \quad a_k^2(x) + b_k^2(x), \end{aligned}$$

for $k \geq 0$. Then we claim that $a_k(x) + b_k(x)$ is irreducible over F_2 of degree 2^k and its roots are linearly independent over F_2 for every $k \geq 1$. We will prove this result by proving the more general Theorem 3.4.13.

Lemma 3.4.12 *Let $q = 2^m$ and let $P(x) = \sum_{i=0}^n c_i x^i \in F_q[x]$ be irreducible over F_q of degree n. Then*
(i) $x^n P(x + x^{-1})$ is irreducible over F_q if and only if $Tr_{q|2}(c_1/c_0) \neq 0$.
(ii) $x^n P^*(x + x^{-1})$ is irreducible over F_q if and only if $Tr_{q|2}(c_{n-1}/c_n) \neq 0$.

Proof: Only (i) is proved here; the proof of (ii) is similar. Let α be a root of $P(x)$. Then it is easy to show that $x^n P(x+x^{-1})$ is irreducible over F_q if and only if $x^2+1-\alpha x = \alpha^2[(x/\alpha)^2 - x/\alpha + \alpha^{-2}]$ is irreducible over F_{q^n}. By Lemma 3.4.9, this is true if and only if

$$\begin{aligned} Tr_{q^n|2}(\alpha^{-2}) \quad &= \quad (Tr_{q^n|2}(\alpha^{-1}))^2 \\ &= \quad (Tr_{q|2}(Tr_{q^n|q}(\alpha^{-1})))^2 \\ &= \quad (Tr_{q|2}(-c_1/c_0))^2 \;=\; (Tr_{q|2}(c_1/c_0))^2 \;\neq\; 0. \end{aligned}$$ □

Part (i) of Theorem 3.4.12 was obtained by Meyn [98] in the present general form; in the case that $q = 2$, it was previously obtained by Varshamov and Garakov [140].

The next theorem appears in a different form in [98], special cases were proved by Varshamov [139] and Wiedemann [150].

Theorem 3.4.13 *Let $q = 2^m$ and let $f(x) = \sum_{i=0}^n c_i x^i$ be irreducible over F_q of degree n. Suppose that $Tr_{q|2}(c_1/c_0) \neq 0$ and $Tr_{q|2}(c_{n-1}/c_n) \neq 0$. Then*

$$f_k(x) \;=\; (b_k(x))^n f(a_k(x)/b_k(x))$$

is irreducible over F_q of degree $n2^k$ for all $k \geq 0$.

Proof: Note that for $k \geq 0$,

$$\frac{a_{k+1}(x)}{b_{k+1}(x)} = \frac{a_k(x)/b_k(x)}{1+(a_k(x)/b_k(x))^2}.$$

It is easily proved by induction that

$$\frac{a_k(x/(1+x^2))}{b_k(x/(1+x^2))} = \frac{a_k(x)/b_k(x)}{1+(a_k(x)/b_k(x))^2}$$

for $k \geq 0$. Then one sees that $f_k(x)$ satisfy the following recursive relation:

$$\begin{aligned} f_0(x) &= f(x), \\ f_{k+1}(x) &= (1+x^2)^{n2^k} f_k(x/(1+x^2)), \quad k \geq 0. \end{aligned}$$

For the sake of convenience let $n_k = n2^k$ and $f_k(x) = \sum_{i=0}^{n_k} c_i^{(k)} x^i$, $k \geq 0$. By Theorem 3.4.12(ii), if $f_k(x)$ is irreducible over F_q then $f_{k+1}(x)$ is irreducible over F_q if and only if

$$Tr_{q|2}(c_{n_k-1}^{(k)}/c_{n_k}^{(k)}) \neq 0. \tag{3.32}$$

Since $c_{n_0-1}^{(0)} = c_{n-1}$ and $c_{n_0}^{(0)} = c_n$, (3.32) is true for $k = 0$ by assumption, and so $f_1(x)$ is irreducible over F_q. To prove that $f_k(x)$ is irreducible over F_q for $k > 1$, by Theorem 3.4.12(ii) it suffices to prove that

$$c_{n_k}^{(k)} = c_0, \quad c_{n_k-1}^{(k)} = c_1, \quad \text{for all } k \geq 1, \tag{3.33}$$

since $Tr_{q|2}(c_1/c_0) \neq 0$ by assumption. To prove (3.33) it is enough to observe that if $M(x) = \sum_{i=0}^{l} m_i x^i$ is an arbitrary polynomial over F_q, then

$$(1+x^2)^l M(x/(1+x^2)) = \sum_{i=0}^{l} m_i x^i (1+x^2)^{l-i}$$

is self-reciprocal of degree $2l$, the coefficients of x and x^{2l-1} are both m_1, and the leading coefficient of x^{2l} is m_0. The proof is completed by induction on k. □

Now for $m = 1$ and $f(x) = x + 1$, we see from the above proof that the coefficient of the next highest term in $a_k(x) + b_k(x)$ is not zero. Therefore, by Corollary 2.5.2, we have the following result.

Corollary 3.4.14 *For any integer $k \geq 0$,*

$$a_k(x) + b_k(x)$$

is irreducible over F_2 of degree 2^k and its roots are linearly independent over F_2.

Chapter 4

Optimal Normal Bases

In this chapter, we first give a general constructions for normal bases of low complexity, including optimal normal bases. We then determine all the optimal normal bases in finite fields.

4.1 Constructions

We have seen in Chapter 1 that normal bases of low complexity are desirable in hardware or software implementation of finite fields. Presently we do not have many techniques for finding normal bases of a required complexity. In this section we will describe a quite general construction that gives all the optimal normal bases and a large family of normal bases of low complexity. Let us begin with the constructions of optimal normal bases discovered by Mullin, Onyszchuk, Vanstone and Wilson [103].

Theorem 4.1.1 *Suppose $n+1$ is a prime and q is primitive in $\mathbb{Z}_{n+1}$, where q is a prime or prime power. Then the n nonunit $(n+1)$th roots of unity are linearly independent and they form an optimal normal basis of F_{q^n} over F_q.*

Theorem 4.1.2 *Let $2n+1$ be a prime and assume that either*
(1) 2 is primitive in $\mathbb{Z}_{2n+1}$, or
(2) $2n+1 \equiv 3 (\mathrm{mod}\ 4)$ and 2 generates the quadratic residues in $\mathbb{Z}_{2n+1}$.

Then $\alpha = \gamma + \gamma^{-1}$ *generates an optimal normal basis of* F_{2^n} *over* F_2*, where* γ *is a primitive* $(2n+1)$*th root of unity.*

Theorem 4.1.1 and Theorem 4.1.2 will be proved as consequences of Theorem 4.1.4. We first examine the multiplication tables of these bases.

For Theorem 4.1.1, let α be a primitive $(n+1)$th root of unity. Then α is a root of the polynomial $x^n + \cdots + x + 1$. As $n+1$ is a prime, $n+1$ divides $q^n - 1$ and all the $(n+1)$th roots of unity are in F_{q^n}. Since q is primitive in $\mathbb{Z}_{n+1}$, there are n distinct conjugates of α, each of which is also a nonunit $(n+1)$th root of unity, i.e.,

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\} = \{\alpha, \alpha^2, \ldots, \alpha^n\}.$$

Hence N is a normal basis of F_{q^n} over F_q. Note that

$$\alpha\alpha^i = \alpha^{i+1} \in N, \quad 1 \le i < n,$$

and

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

Therefore there are $2n-1$ non-zero terms in all the cross-products, and thus N is optimal. The matrix T corresponding to this basis has the following properties: there is exactly one 1 in each row, except for one row where all the n entries are -1's; all other entries are 0's. We call any optimal normal basis obtained by this construction a *type I* optimal normal basis.

For Theorem 4.1.2, it will be proved that $\alpha \in F_{2^n}$ and $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$ are linearly independent over F_2. So $N = \{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ is a normal basis of F_{2^n} over F_2. By the conditions in Theorem 4.1.2, it is easy to see that

$$N = \{\gamma + \gamma^{-1}, \gamma^2 + \gamma^{-2}, \ldots, \gamma^n + \gamma^{-n}\}.$$

The cross-product terms are

$$\begin{aligned} \alpha(\gamma^i + \gamma^{-i}) &= (\gamma + \gamma^{-1})(\gamma^i + \gamma^{-i}) \\ &= (\gamma^{(1+i)} + \gamma^{-(1+i)}) + (\gamma^{(1-i)} + \gamma^{-(1-i)}), \end{aligned}$$

which is a sum of two distinct elements in N except when $i = 1$. If $i = 1$, the sum is just α^2 which is in N. Thus N is an optimal normal basis of F_{2^n} over F_2. The matrix T corresponding to this basis has the following properties: there are exactly two 1's in each row, except for the first row in which there is exactly one 1; all other entries are 0's. We call any optimal normal basis obtained by this construction a *type II* optimal normal basis.

We next look at the minimal polynomials of these optimal normal bases. For a type I optimal normal basis, its minimal polynomial is obviously $x^n + \cdots + x + 1$, which is irreducible over F_q if and only if $n+1$ is a prime and q is primitive in $\mathbb{Z}_{n+1}$. For the minimal polynomial of a type II optimal normal basis, we consider a more general situation. Let n be any positive integer and γ a $(2n+1)$th primitive root of unity in an arbitrary field. Let

$$f_n(x) \;=\; \prod_{j=1}^{n}(x - \gamma^j - \gamma^{-j}). \tag{4.1}$$

(Note that $f_n(x)$ is the minimal polynomial of $\alpha = \gamma + \gamma^{-1}$ under the conditions of Theorem 4.1.2.) We will find an explicit formula for $f_n(x)$. For any $0 \le j \le n$, γ^j is also a $(2n+1)$th root of unity. Hence

$$(\gamma^j)^n + (\gamma^j)^{-n} \;=\; (\gamma^j)^{n+1} + (\gamma^j)^{-(n+1)}. \tag{4.2}$$

By Waring's formula, for any positive integer k,

$$(\gamma^j)^k + (\gamma^j)^{-k} \;=\; \sum_{i=0}^{[k/2]} \frac{k}{k-i}\binom{k-i}{i}(-1)^i(\gamma^j + \gamma^{-j})^{k-2i}.$$

Let

$$D_k(x) \;=\; \sum_{i=0}^{[k/2]} \frac{k}{k-i}\binom{k-i}{i}(-1)^i x^{k-2i},$$

which is a special kind of Dickson polynomial. Then by (4.2), we see that $\gamma^j + \gamma^{-j}$ is a root of $D_{n+1}(x) - D_n(x)$ for $j = 0, 1, \ldots, n$. As $D_{n+1}(x) - D_n(x)$ has degree $n+1$ and $\gamma^j + (\gamma^j)^{-1}$ are different for $j = 0, 1, \ldots, n$, we see that $D_{n+1}(x) - D_n(x) = f_n(x)(x-2)$. Therefore

$$f_n(x) = \sum_{j=0}^{[(n-1)/2]} (-1)^j \binom{n-1-j}{j} x^{n-(2j+1)} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.$$

We point out that $f_n(x)$ is irreducible over F_q if and only if the multiplicative group $\mathbb{Z}_{2n+1}^*$ is generated by q and -1, and $f_n(x)$ is irreducible over the field of rational numbers whenever $2n+1$ is a prime.

In practical applications, we need optimal normal bases over F_2. It would be nice if we had simple rules to test the hypotheses in Theorems 4.1.1 and 4.1.2. In this regard, the following results (see [88], p. 68) are useful:

(a) 2 is primitive in $\mathbb{Z}_r$ for a prime r if $r = 4s + 1$ and s is an odd prime.

(b) 2 is primitive in $\mathbb{Z}_r$ for a prime r if $r = 2s + 1$ where s is a prime congruent to 1 modulo 4.

(c) 2 generates the quadratic residues in $\mathbb{Z}_r$ for a prime r if $r = 2s + 1$ where s is a prime congruent to 3 modulo 4.

For convenience, we list in Table 4.1 all the values of $n \leq 2000$ for which there is an optimal normal basis of F_{2^n} over F_2. In the table, $\star$ indicates the existence of a type I optimal normal basis, † indicates the existence of both type I and type II optimal normal bases, otherwise there exists only a type II optimal normal basis.

The constructions in Theorems 4.1.1 and 4.1.2 are generalized by Ash, Blake and Vanstone [10] and further by Wassermann [148] to construct normal bases of low complexity as in Theorem 4.1.4. To establish this result, we first prove a lemma.

Lemma 4.1.3 *Let k, 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 $\mathbb{Z}_{nk+1}$. Then every non-zero element r in $\mathbb{Z}_{nk+1}$ can be written uniquely in the form*

$$r = \tau^i q^j, \quad 0 \leq i \leq k-1, \quad 0 \leq j \leq n-1.$$

Proof: Let $e_1 = nk/e$. There is a primitive element g in $\mathbb{Z}_{nk+1}^*$ 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

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

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

$$\tau^i q^j \equiv \tau^s q^t \pmod{nk+1},$$

i.e.,

$$\begin{aligned} \tau^{i-s} &\equiv q^{t-j} \pmod{nk+1}, \\ g^{na(i-s)} &\equiv g^{e_1(t-j)} \pmod{nk+1}. \end{aligned}$$

2†	113	293	473	676⋆	873	1110	1310	1533	1790
3	119	299	483	683	876⋆	1116⋆	1323	1539	1791
4⋆	130⋆	303	490⋆	686	879	1118	1329	1541	1806
5	131	306	491	690	882⋆	1119	1331	1548⋆	1811
6	134	309	495	700⋆	891	1121	1338	1559	1818
9	135	316⋆	508⋆	708⋆	893	1122⋆	1341	1570⋆	1821
10⋆	138⋆	323	509	713	906⋆	1133	1346	1583	1829
11	146	326	515	719	911	1134	1349	1593	1835
12⋆	148⋆	329	519	723	923	1146	1353	1601	1838
14	155	330	522⋆	725	930	1154	1355	1618⋆	1845
18†	158	338	530	726	933	1155	1359	1620⋆	1850
23	162⋆	346⋆	531	741	935	1166	1370	1626	1854
26	172⋆	348⋆	540⋆	743	938	1169	1372⋆	1636⋆	1859
28⋆	173	350	543	746	939	1170⋆	1380⋆	1649	1860⋆
29	174	354	545	749	940⋆	1178	1394	1653	1863
30	178⋆	359	546⋆	755	946⋆	1185	1398	1659	1866†
33	179	371	554	756⋆	950	1186⋆	1401	1661	1876⋆
35	180⋆	372⋆	556⋆	761	953	1194	1409	1666⋆	1883
36⋆	183	375	558	765	965	1199	1418	1668⋆	1889
39	186	378†	561	771	974	1211	1421	1673	1898
41	189	378⋆	562⋆	772⋆	975	1212⋆	1425	1679	1900⋆

50	191	386	575	774	986	1218	1426⋆	1685	1901
51	194	388⋆	585	779	989	1223	1430	1692⋆	1906⋆
52⋆	196⋆	393	586⋆	783	993	1228⋆	1439	1703	1923
53	209	398	593	785	998	1229	1443	1706	1925
58⋆	210†	410	606	786⋆	1013	1233	1450⋆	1730	1926
60⋆	221	411	611	791	1014	1236⋆	1451	1732⋆	1930⋆
65	226⋆	413	612⋆	796⋆	1018⋆	1238	1452⋆	1733	1931
66⋆	230	414	614	803	1019	1251	1454	1734	1938
69	231	418⋆	615	809	1026	1258⋆	1463	1740⋆	1948⋆
74	233	419	618†	810	1031	1265	1469	1745	1953
81	239	420⋆	629	818	1034	1269	1478	1746⋆	1955
82⋆	243	426	638	820⋆	1041	1271	1481	1749	1958
83	245	429	639	826⋆	1043	1274	1482⋆	1755	1959
86	251	431	641	828⋆	1049	1275	1492⋆	1758	1961
89	254	438	645	831	1055	1276⋆	1498⋆	1763	1965
90	261	441	650	833	1060⋆	1278	1499	1766	1972⋆
95	268⋆	442⋆	651	834	1065	1282⋆	1505	1769	1973
98	270	443	652⋆	846	1070	1289	1509	1773	1978⋆
99	273	453	653	852⋆	1090⋆	1290⋆	1511	1778	1983
100⋆	278	460⋆	658⋆	858⋆	1103	1295	1518	1779	1986⋆
105	281	466⋆	659	866	1106	1300⋆	1522⋆	1785	1994
106⋆	292⋆	470	660⋆	870	1108⋆	1306⋆	1530⋆	1786⋆	1996⋆

Table 4.1: Values of $n \leq 2000$ for which there exists an optimal normal basis in F_{2^n} over F_2.

Then

$$na(i-s) \;\equiv\; e_1(t-j) \quad (\text{mod } nk). \tag{4.3}$$

As $\gcd(n, e_1) = 1$, equation (4.3) implies that $n \mid (t-j)$. Hence $t = j$. Thus from (4.3),

$$a(i-s) \;\equiv\; 0 \quad (\text{mod } k).$$

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

$$\tau^i q^j \quad (\text{mod } nk+1), \quad i = 0, 1, \ldots, k-1, \quad j = 0, 1, \ldots, n-1$$

are all distinct. As $\tau^i q^j \not\equiv 0(\text{mod } nk+1)$, every non-zero element in $\mathbb{Z}_{nk+1}$ can be expressed uniquely in the required form. □

Theorem 4.1.4 *Let q be a prime or prime power, and n, 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 $\mathbb{Z}_{nk+1}$,*

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

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 $k \equiv 0(\text{mod } p)$, where p is the characteristic of F_q.

Proof: We first prove that $\alpha \in F_{q^n}$. Since $q^{nk} \equiv 1(\text{mod } nk+1)$, q^n is a k-th root of unity in $\mathbb{Z}_{nk+1}$. Thus there is an integer ℓ such that $q^n = \tau^\ell$. Then

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

Therefore α is in F_{q^n}.

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

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

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

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

since, by Lemma 4.1.3, $\tau^j q^i$ modulo $nk+1$ runs through $\mathbb{Z}^*_{nk+1}$ for $j = 0, 1, \ldots, k-1$ and $i = 0, 1, \ldots, n-1$. 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 $r = 1, 2, \ldots, nk$, whence

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

divides $f(x)$. But $f(x)$ has degree at most $nk-1$, and so this is impossible. Thus $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ 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 $0 \le i \le n-1$,

$$\begin{aligned} \alpha \cdot \alpha^{q^i} &= \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u + \tau^v q^i} = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} \beta^{\tau^u (1 + \tau^{v-u} q^i)} \\ &= \sum_{v=0}^{k-1} \left(\sum_{u=0}^{k-1} \beta^{\tau^u (1 + \tau^v q^i)} \right). \end{aligned} \tag{4.4}$$

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 $1 + \tau^{v_0} q^{i_0} \equiv 0 \pmod{nk+1}$. If $(v, i) \ne (v_0, i_0)$, then $1 + \tau^v q^i \equiv \tau^w q^j (\text{mod } nk+1)$, 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 $k \equiv 0 (\text{mod } p)$. So for all $i \ne i_0$, the sum (4.4) 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 $k \equiv 0 (\text{mod } p)$ and $i = i_0$, then (4.4) is a sum of at most $k-1$ basis elements. Therefore if $k \equiv 0 (\text{mod } p)$ 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 4.1.4, when $k = 1$ we obtain Theorem 4.1.1, and when $k = 2$ and $q = 2$ we have Theorem 4.1.2. When q is odd, $k = 2$, it is easy to see that the complexity of the normal basis generated by the α in Theorem 4.1.4 is exactly $3n - 2$. The exact complexity is in general difficult to determine. Here we just quote the following result from [10], without proof.

Theorem 4.1.5 *Let $q = 2$. Then the normal basis generated by the α of Theorem 4.1.4 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* $k = 7, n > 6$.

4.2 Determination of all Optimal Normal Bases

We have seen two constructions of optimal normal bases in the last section. A natural question is whether there are any other optimal normal bases. In [103], complete computer searches were performed for optimal normal bases in F_{2^n}, $2 \leq n \leq 30$, and no new optimal normal bases were found. This evidence led the authors to conjecture that if n does not satisfy the criteria for Theorem 4.1.1 or Theorem 4.1.2, then F_{2^n} does not contain an optimal normal basis. Lenstra [84] proved that this is indeed true. 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. The two bases N and aN are said to be *equivalent*. In addition, by Lemma 5.1.1, for any positive integer v with $\gcd(v, n) = 1$, N remains a basis of $F_{q^{nv}}$ over F_{q^v}. Therefore N is an optimal normal basis of $F_{q^{nv}}$ over F_{q^v} provided that $\gcd(v, n) = 1$. The problem now is whether there are any other optimal normal bases. Mullin [102] 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 a type II optimal normal basis then the basis must be either of type I or type II. Later Gao [49] proved that any optimal normal basis of a finite field must be equivalent to a type I or a type II optimal normal basis. Finally, Gao and Lenstra [50] extended the result to any finite Galois extension of an arbitrary field.

In this section we prove that all the optimal normal bases in finite fields are completely determined by Theorems 4.1.1 and 4.1.2. The proof given here is a combination of the proofs in [49] and [50]. We first prove some properties that hold for any normal basis.

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

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \le i \le n-1, \quad t_{ij} \in F_q. \tag{4.5}$$

Let $T = (t_{ij})$. Raising (4.5) to the q^{-i}-th power, we find that

$$t_{ij} = t_{-i,j-i}, \quad \text{for all } 0 \le i, j \le n-1. \tag{4.6}$$

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

$$\alpha\beta_i = \sum_{j=0}^{n-1} d_{ij}\beta_j, \quad 0 \le i \le n-1, \quad d_{ij} \in F_q. \tag{4.7}$$

We show that

$$d_{ij} = t_{ji}, \quad \text{for all } 0 \le i, j \le n-1, \tag{4.8}$$

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

$$Tr(\alpha_i\beta_j) = \begin{cases} 0, & \text{if } i \ne j, \\ 1, & \text{if } i = j. \end{cases}$$

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

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

On the other hand,

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

This proves (4.8).

Theorem 4.2.1 *Let $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ 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 $\mathbb{Z}_{n+1}$ 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 $\mathbb{Z}^*_{2n+1}$, 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 $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ be the dual basis of N with $\beta_i = \beta^{q^i}$. We assume (4.5) and (4.7) with the (i,j)-entry of D denoted by $d(i,j)$. Then, by (4.6) and (4.8), we have

$$d(i,j) \;=\; d(i-j, -j), \quad \text{for all } 0 \leq i, j \leq n-1. \tag{4.9}$$

We saw from the proof of Theorem 1.2.1 that each row of D (or column of T) has exactly two non-zero entries which are additive inverses, except the first row which has exactly one non-zero entry with value b. This is equivalent to saying that for each $i \neq 0$, $\alpha\beta_i$ is of the form $a\beta_k - a\beta_\ell$ for some $a \in F_q$ and integers $0 \leq k, \ell \leq n-1$, 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 $Tr(\alpha) = -1$. Then we have

$$\alpha\beta_0 \;=\; -\beta_m. \tag{4.10}$$

Also, from $Tr(\alpha)Tr(\beta) = \sum_{i,j} \alpha_i\beta_j = \sum_k Tr(\alpha\beta_k) = 1$ we see that we have $Tr(\beta) = -1$.

If $m = 0$ then from (4.10) 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 $2m \equiv 0 (\text{mod } n)$. Raising (4.10) to q^m-th power we see that

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

Therefore, we have

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

This shows that $d(i,m) = -1$ for all $i = 0, \ldots, n-1$. 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 $\{0, 1, \ldots, n-1\} - \{0\}$ to $\{0, 1, \ldots, n-1\} - \{m\}$. Hence each $i^* \neq m$ occurs exactly once, and so

$$\begin{aligned} \alpha\alpha_{i^*} &= \alpha_i \ \text{ for } i^* \neq m, \\ \alpha\alpha_m &= 1. \end{aligned}$$

It follows that the set $\{1\} \cup \{\alpha_i | i = 0, 1, \ldots, n-1\}$ 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 $x^n + \cdots + x + 1$. Since α has degree n over F_q, the polynomial $x^n + \cdots + x + 1$ is irreducible over F_q. Therefore $n+1$ is a prime number. This shows that we are in case (i) of Theorem 4.2.1.

For the remainder of the proof we assume that $2m \not\equiv 0 (\text{mod } n)$. By (4.10) we have $d(0, i) = -1$ or 0 according as $i = m$ or $i \neq m$. Hence from (4.9) we find that

$$d(i, i) = \begin{cases} -1, & \text{if } i = -m, \\ 0, & \text{if } i \neq -m. \end{cases} \tag{4.11}$$

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

$$\alpha\beta_{-m} = \beta_\ell - \beta_{-m}, \quad \ell \neq -m. \tag{4.12}$$

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,

$$\begin{aligned} \alpha(\alpha_m\beta_0) &= \alpha(\alpha\beta_{-m})^{q^m} = \alpha(\beta_\ell - \beta_{-m})^{q^m} \\ &= \alpha\beta_{\ell+m} - \alpha\beta_0 = \alpha\beta_{\ell+m} + \beta_m. \end{aligned}$$

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

$$\alpha\beta_{\ell+m} = \beta_{2m} - \beta_m. \tag{4.13}$$

Now we compute $\alpha\alpha_\ell\beta_{-m}$ in two ways. To this purpose, note that $d(-m-\ell, -\ell) = d(-m, \ell) = 1$, by (4.12). Since $\ell \neq -m$ implies that $-m - \ell \neq 0$, we may assume that

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

for some $j \notin \{-\ell, -m-\ell\}$ (hence $j+\ell \neq 0, -m$). On the one hand,

$$\begin{aligned}\alpha_\ell(\alpha\beta_{-m}) &= \alpha_\ell(\beta_\ell - \beta_{-m}) \;=\; (\alpha\beta_0 - \alpha\beta_{-m-\ell})^{q^\ell} \\ &= (-\beta_m - \beta_{-\ell} + \beta_j)^{q^\ell} \;=\; -\beta_{m+\ell} - \beta_0 + \beta_{j+\ell}.\end{aligned}$$

On the other hand,

$$\begin{aligned}\alpha(\alpha_\ell\beta_{-m}) &= \alpha(\alpha\beta_{-m-\ell})^{q^\ell} \;=\; \alpha(\beta_{-\ell} - \beta_j)^{q^\ell} \\ &= \alpha\beta_0 - \alpha\beta_{j+\ell} \;=\; -\beta_m - \alpha\beta_{j+\ell}.\end{aligned}$$

We have

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

As $j+\ell \neq -m$, $\beta_{j+\ell}$ does not appear in $\alpha\beta_{j+\ell}$ by (4.11). Thus $-\beta_{j+\ell}$ must cancel against one of the last two terms.

If $-\beta_{j+\ell} + \beta_{m+\ell} = 0$ then $j+\ell = m+\ell$ and thus $\alpha\beta_{m+\ell} = \beta_0 - \beta_m$. But by (4.13), $\alpha\beta_{m+\ell} = \beta_{2m} - \beta_m$. Therefore $\beta_0 = \beta_{2m}$ and $2m \equiv 0 \pmod n$, contradicting the assumption.

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

$$\alpha\beta_m \;=\; \beta_{m+\ell} + \beta_0. \tag{4.14}$$

From now on we assume that $q = 2^v$ for some integer v. The equations (4.10) and (4.12) can be rewritten as

$$\alpha\beta \;=\; \beta_m, \tag{4.15}$$

$$\alpha\beta_{-m} \;=\; \beta_\ell + \beta_{-m}. \tag{4.16}$$

Raising (4.16) to q^m-th power and comparing the result to (4.14), we find $\alpha_m\beta = \alpha\beta_m$, which is the same as

$$\frac{\alpha}{\beta} \;=\; \frac{\alpha_m}{\beta_m} \;=\; \left(\frac{\alpha}{\beta}\right)^{q^m}. \tag{4.17}$$

Multiplying (4.17) and (4.15) we find that $\alpha^2 = \alpha_m = \alpha^{q^m}$. By induction on k one deduces from this that $\alpha^{q^{mk}} = \alpha^{2^k}$ for every non-negative integer k. Let $k = n/\gcd(m,n)$. Then $\alpha^{2^k} = \alpha$, which means that α is in F_{2^k} and thus of degree at most $k \leq n$ 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 k 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 $\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}$.

Let m_1 be a positive integer such that $mm_1 \equiv 1 (\text{mod } n)$. Then by repeatedly raising (4.17) 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 $Tr(\alpha) = Tr(\beta) = -1$ we have in fact $\alpha = \beta$. Thus by (4.8) we see that

$$d(i, j) = d(j, i) \quad \text{for all } 0 \leq i, j \leq n-1. \tag{4.18}$$

Let now ζ be a zero of $x^2 - \alpha x + 1$ in an extension $F_{q^{2n}}$ of F_{q^n}, 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 non-zero elements among the γ_i, namely $\gamma_1, \gamma_2, \ldots, \gamma_t$. 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 non-zero 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 the 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 $\{\alpha^{2^i} | i = 0, 1, \ldots, n-1\}$, then γ_{i-1} occurs with a coefficient 1. By (4.18), this 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 non-zero γ_i are conjugate to α and that $n = t$.

From the fact that each non-zero 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 $i \equiv \pm 2^j (\text{mod } 2n+1)$. 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 $\mathbb{Z}_{2n+1}^*$ is generated by 2 and -1. Thus the conditions (a) and (b) of the theorem are satisfied. All assertions of (ii) have been proved. □

4.3 Constructing Irreducible Polynomials under ERH

The α in Theorem 4.1.4 has classical origins and is called a *Gauss period* [147, 110]. Gauss periods are used to realize the Galois correspondence between subfields of a cyclotomic field and subgroups of its Galois group, as shown in section 1.1. Gauss periods are also useful for integer factorization algorithms [12]. In this section, we show how Theorem 4.1.4 can be used to solve the problem of constructing irreducible polynomials deterministically in polynomial time, assuming the Extended Riemann Hypothesis (ERH), as shown in [1].

Suppose that the conditions in Theorem 4.1.4 are satisfied. Then the α has degree n over F_q. The minimal polynomial of α over F_q is an irreducible polynomial of degree n. Let $\alpha_i = \alpha^{q^i}$ for $i = 0, 1, \dots, n-1$. By the equation (4.4) and its following arguments, we see that the products $\alpha\alpha^{q^i} = \sum_{j=0}^{n-1} t_{ij}\alpha_j$, where t_{ij}'s are integers and $i = 0, 1, \dots, n-1$, can be computed in time polynomial in $m = kn+1$. The minimal polynomial of α is just the characteristic polynomial of the $n \times n$ matrix (t_{ij}), since $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ is a basis for F_{q^n} over F_q. Thus we see that the minimal polynomial of α can be found in time polynomial in $m = kn+1$.

About the smallest $m = kn+1$ such that the conditions of Theorem 4.1.4 are satisfied, we quote Proposition 3 in [1] which is a variant of Theorem 3 in [12].

Lemma 4.3.1 *Assuming the Extended Riemann Hypothesis (ERH), there is a constant $c > 0$ such that for all prime p and positive integer n such that $\gcd(n,p) = 1$, there is a prime $m = kn+1$ with $m < cn^4(\log(np))^2$ such that $\gcd(kn/e, n) = 1$ where e is the multiplicative order of p modulo m.*

Note that the conditions in the above lemma are the same as in Theorem 4.1.4 and can be tested in time polynomial in m and $\log p$. Therefore, we have

Theorem 4.3.2 (Adleman and Lenstra [1]) *Assuming Extended Riemann Hypothesis, an irreducible polynomial of degree n in $F_p[x]$ can be constructed deterministically in polynomial time* *(in n and $\log p$) for any prime p and positive integer n.*

Finally, we give some comments on computing the matrix (t_{ij}) and its connection with *cyclotomic numbers*. From the argument following the equation (4.4) we see that t_{ij} is the number of solutions of $1+\tau^v q^i \equiv \tau^w q^j (\mathrm{mod} nk+1)$ with $0 \leq v, w \leq k-1$ (except for $i = i_0$ where $1+\tau^{v_0} q^{i_0} \equiv 0(\mathrm{mod} nk+1)$). These numbers are called *cyclotomic numbers* in the theory of cyclotomy and their values are determined for many small values of n, for detail see [135]. We remark that $\alpha_i = \alpha^{q^i} = \sum_{v=0}^{k-1} \beta^{\tau^v q^i}$ does not depends on the particular τ and q, it depends only on the coset $\{q^i, q^i\tau, \ldots, q^i\tau^{k-1}\}(\mathrm{mod} m = kn+1)$ of the unique subgroup $<\tau>$ of order k of the multiplicative group $\mathbb{Z}_m^*$. Also the value of β is not important. We can just think of β as a symbol x with $x^m = 1$ and $x \neq 1$, that is, we may work in the ring $\mathbb{Z}_m[x]/(x^{m-1}+\cdots+x+1)$.

Let us look at an example. Let $n=4$, $k=3$ and $m = 4\times 3+1 = 13$. The subgroup of order 3 in $\mathbb{Z}_{13}$ is $\{1,3,9\}$. Its cosets are

$$\{1,3,9\}, \quad \{2,5,6\}, \quad \{4,10,12\}, \quad \{7,8,11\}.$$

We have

$$\begin{aligned} \alpha_0 &= \beta+\beta^3+\beta^9, \\ \alpha_1 &= \beta^2+\beta^5+\beta^6, \\ \alpha_2 &= \beta^4+\beta^{10}+\beta^{12}, \\ \alpha_3 &= \beta^7+\beta^8+\beta^{11}, \end{aligned}$$

and

$$\begin{aligned} \alpha_0\alpha_0 &= \alpha_1+2\alpha_2, \\ \alpha_0\alpha_1 &= \alpha_0+\alpha_1+\alpha_3, \\ \alpha_0\alpha_2 &= -3\alpha_0-2\alpha_1-3\alpha_2-2\alpha_3, \\ \alpha_0\alpha_3 &= \alpha_0+\alpha_2+\alpha_3. \end{aligned}$$

The matrix (t_{ij}) is

$$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 \\ -3 & -2 & -3 & -2 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Its characteristic polynomial is $f(x) = x^4 + x^3 + 2x^2 - 4x + 3$. Let $E = \{2, 5, 6, 7, 8, 11\}$. Then, for each $a \in E$, the multiplicative order e of a satisfies $\gcd(12/e, 4) = 1$. Hence by Theorem 4.1.4, the polynomial $f(x)$ is irreducible over F_q for all prime powers q such that $q \equiv a \bmod 13$ for some $a \in E$.

4.4 A Simple Proof of the Law of Quadratic Reciprocity

In this section, we show another application of Gauss periods in the proof of the law of quadratic reciprocity.

Let p be prime. For an integer a, the *Legendre symbol* (a/p) is defined to be 1 if a is a quadratic residue in $\mathbb{Z}_p$, -1 if a is a quadratic nonresidue in $\mathbb{Z}_p$, and zero if $p|a$. If q is another prime, then there is a remarkable relationship between (p/q) and (q/p), called the law of quadratic reciprocity, discovered by Euler and first completely proved by Gauss.

Theorem 4.4.1 (Law of Quadratic Reciprocity) *Let p and q be odd primes. Then*

(a) $(-1/p) = (-1)^{(p-1)/2}$,

(b) $(2/p) = (-1)^{(p^2-1)/8}$,

(c) $(p/q) = (-1)^{((p-1)/2)((q-1)/2)}(q/p)$.

Proof: It is our purpose to give a proof of (c), the proof of (a) and (b) can be found in [68]. Note that $q|(p^{q-1} - 1)$. There is a primitive q-th root of unity in $F_{p^{q-1}}$, say ξ. As $\xi \neq 1$, ξ must be a root of $(x^q - 1)/(x - 1)$, that is,

$$\sum_{i=0}^{q-1} \xi^i = 0.$$

Now let S be the set of quadratic residues in F_q and $N = F_q^* \setminus S$ the set of quadratic nonresidues. Then $uS = S$ if $u \in S$ and $uS = N$ if $u \in N$. Define

$$\alpha_0 = \frac{1}{2} + \sum_{u \in S} \xi^u, \quad \alpha_1 = \frac{1}{2} + \sum_{u \in N} \xi^u.$$

Then we have

$$\alpha_0 + \alpha_1 = 0.$$

Note that

$$\begin{aligned}\alpha_0\alpha_1 &= \frac{1}{4}+\frac{1}{2}\left(\sum_{u\in S}\xi^u+\sum_{u\in N}\xi^u\right)+\sum_{\substack{u\in S\\ v\in N}}\xi^{u+v}\\ &= -\frac{1}{4}+\sum_{d=0}^{q-1}a_d\xi^d.\end{aligned}$$

where a_d is the number of pairs $(u,v)\in S\times N$ such that

$$u+v=d. \tag{4.19}$$

We claim that a_d is a constant for $d\neq 0$. The reason is that for any $d_1=\sigma d\neq 0$, every solution $(u,v)\in S\times N$ of (4.19) corresponds to a solution $(u_1,v_1)\in S\times N$ for $u_1+v_1=d_1$ where (u_1,v_1) is $(\sigma u,\sigma v)$ if σ is a quadratic residue or $(\sigma v,\sigma u)$ if σ is a quadratic nonresidue. Let $a=a_d$ be the constant for $d\neq 0$. The number a_0 is easy to determine. We know that if $q\equiv 1 \pmod 4$ then $-1\in S$ and $-S=S$, $-N=N$; if $q\equiv 3 \pmod 4$ then $-1\in N$ and $-S=N$, $-N=S$. Hence

$$a_0=\begin{cases}0, & \text{if } q\equiv 1 \pmod 4,\\ |S|=|N|=\frac{q-1}{2}, & \text{if } q\equiv 3 \pmod 4.\end{cases}$$

Note that

$$a_0+(q-1)a=\sum_{i=0}^{q-1}a_i=\left(\frac{q-1}{2}\right)^2,$$

which is the total number of pairs $(u,v)\in S\times N$. We have

$$a=\begin{cases}\frac{q-1}{4}, & \text{if } q\equiv 1 \pmod 4,\\ |S|=|N|=\frac{q-1}{4}-\frac{1}{2}, & \text{if } q\equiv 3 \pmod 4.\end{cases}$$

Therefore

$$\alpha_0\alpha_1=-\frac{1}{4}+a_0+a\sum_{i=1}^{q-1}\xi^i=-\frac{1}{4}+a_0-a=-(-1)^{(q-1)/2}\frac{q}{4}.$$

Consider the irreducibility of the following polynomial

$$f(x)=(x-\alpha_0)(x-\alpha_1)=x^2-(-1)^{(q-1)/2}\frac{q}{4}$$

in $F_p[x]$. On the one hand, obviously, $f(x)$ is irreducible in $F_p[x]$ if and only $(-1)^{(q-1)/2}q$ is a quadratic nonresidue in F_p. On the other hand, $f(x)$ is irreducible in $F_p[x]$ if and only if $\alpha_0\notin F_p$, or equivalently $\alpha_0^p \neq \alpha_0$. However,

$$\alpha_0^p = \left(\frac{1}{2} + \sum_{u\in S} \xi^u\right)^p = \frac{1}{2} + \sum_{u\in S} \xi^{pu} = \begin{cases} \alpha_0, & \text{if } (p/q) = 1, \\ \alpha_1, & \text{if } (p/q) = -1. \end{cases}$$

This means that $f(x)$ is irreducible in $F_p[x]$ if and only if p is a quadratic nonresidue in F_q. Consequently, we have

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{(q-1)/2}q}{p}\right) = (-1)^{((q-1)/2)((p-1)/2)}\left(\frac{q}{p}\right),$$

which is what we want to prove! □

The reader may have realized that the second terms of α_0 and α_1 are Gauss periods for $n = 2$. In [68, page 85], there is a proof on the same line based on finite fields using *Gauss sums.* It seems that Gauss periods are easier to manipulate than Gauss sums in this circumstance.

Chapter 5

Normal Bases of Low Complexity

This chapter is devoted to a family of normal bases, considered by Sidel'nikov [130], with the property that all the elements in a basis can be obtained from one element by repeatedly applying to it a linear fractional function of the form $\varphi(x) = (ax+b)/(cx+d)$, $a, b, c, d \in F_q$. Sidel'nikov proved that the cross products for such a basis $\{\alpha_i\}$ are of the form $\alpha_i \alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$, $i \neq j$, where $e_k, \gamma \in F_q$. We will show that every such basis can be formed by the roots of an irreducible factor of $F(x) = cx^{q+1} + dx^q - ax - b$. We will construct: (a) a normal basis of F_{q^n} over F_q with complexity at most $3n-2$ for each divisor n of $q-1$ and for $n = p$ where p is the characteristic of F_q; (b) a self-dual normal basis of F_{q^n} over F_q for $n = p$ and for each odd divisor n of $q-1$ or $q+1$. When $n = p$, the self-dual normal basis constructed of F_{q^p} over F_q also has complexity at most $3p-2$. In all cases, we will give the irreducible polynomials and the multiplication tables explicitly.

For this purpose, some properties of linear fractional functions and the complete factorization of $F(x)$ are discussed in sections 5.1 and 5.2, respectively.

5.1 On Linear Fractional Functions

In this section, we discuss some properties of the linear fractional function $\varphi(x) = (ax+b)/(cx+d)$ with $a, b, c, d \in F_q$ and $ad - bc \neq 0$. It is easy to see that $\varphi(x)$ defines a permutation on $F_q \cup \{\infty\}$, where

$$\begin{aligned} \frac{a\infty+b}{c\infty+d} &:= \frac{a}{c}, && \text{if } c \neq 0, \\ \frac{a\infty+b}{c\infty+d} &:= \infty, && \text{if } ad \neq 0, c = 0, \\ \frac{a}{0} &:= \infty, && \text{if } a \neq 0. \end{aligned}$$

Actually, $\varphi(x)$ induces a permutation on $F_{q^n} \cup \{\infty\}$, for any $n \geq 1$. The inverse of $\varphi(x)$ is $\varphi^{-1}(x) = (-dx+b)/(cx-a)$.

For any two linear fractional functions φ and ψ, the composition $\varphi\psi$, defined as $\varphi\psi(x) = \varphi(\psi(x))$, is still a linear fractional function. It is well known that all the linear fractional functions over F_q form a group under composition and is isomorphic to the projective general linear group $PGL(2,q)$. The order of φ is the smallest positive integer t such that $\varphi^t(x) = x$, i.e., φ^t is the identity map.

For our purpose, we will deal with a linear fractional function $\varphi(x) = (ax+b)/(cx+d)$ with $c \neq 0$. The fixed points of $\varphi(x)$ satisfy

$$cx^2 - (a-d)x - b = 0. \tag{5.1}$$

The following two lemmas are easily checked.

Lemma 5.1.1 *Let $\varphi(x) = ax+b$ with $a \neq 0, 1$, be a linear mapping. Then*

$$\varphi = h^{-1}\psi h,$$

where $\psi(x) = ax$ and $h(x) = x + b/(a-1)$.

Lemma 5.1.2 *Let $\varphi(x) = (ax+b)/(cx+d)$ with $c \neq 0$ and $ad - bc \neq 0$. Let $\Delta = (a-d)^2 + 4bc$. Then*

$$\varphi = h^{-1}\psi h,$$

where $h(x)$ and $\psi(x)$ are defined as follows:

(a) *When $\Delta = 0$, let x_0 be the only solution of (5.1) in F_q, that is, x_0 satisfies $cx_0^2 = -b$ and $2cx_0 = a-d$. Then $h(x) = (a/c - x_0)/(x - x_0)$ and $\psi(x) = x+1$.*

(b) *When $\Delta \neq 0$, let x_0, x_1 be the two solutions of (5.1) in F_{q^2} and let $\xi = (a - cx_0)/(a - cx_1)$. Then*

$$h(x) = \frac{x - x_0}{x - x_1}, \quad \psi(x) = x\xi.$$

The order of φ is now easy to determine. The order of φ is equal to the order of ψ. If ψ is of the form $x+1$ then the order of ψ is equal to the additive order p of 1 in F_q, where p is the characteristic of F_q. If ψ is of the form ξx, then the order of ψ is equal to the multiplicative order of ξ. In case **(b)** of Lemma 5.1.2, if Δ is a quadratic residue in F_q, then $x_0, x_1 \in F_q$, and $\xi \in F_q$. Hence $\xi^{q-1} = 1$ and the order of ξ is a divisor of $q-1$. If Δ is a quadratic nonresidue in F_q, then $x_0, x_1 \in F_{q^2} \setminus F_q$ and $x_0^q = x_1, x_1^q = x_0$. Thus $\xi^q = ((a-cx_0)/(a-cx_1))^q = (a-cx_0^q)/(a-cx_1^q) = (a-cx_1)/(a-cx_0) = 1/\xi$. So $\xi^{q+1} = 1$ and the order of ξ divides $q+1$. Therefore the order of φ is always a divisor of p, $q-1$ or $q+1$.

Lemma 5.1.3 *Let $a, b, c, d \in F_q$ with $c \neq 0$ and $ad - bc \neq 0$. Let $\varphi(x) = (ax+b)/(cx+d)$ with order t. Then, for $1 \leq i \leq t-1$,*

$$\varphi^i(x) = \frac{e_i x + b/c}{x - e_{t-i}}, \quad e_i + e_{t-i} = \frac{a-d}{c} \tag{5.2}$$

where $e_1 = a/c$ and $e_{i+1} = \varphi(e_i)$ for $i = 1, \ldots, t-2$.

Proof: It is routine to prove by induction on i that there exist $e_i, f_i \in F_q$ with $e_1 = a/c$, $f_1 = d/c$ such that

$$\varphi^i(x) = \frac{e_i x + b/c}{x + f_i},$$

and

$$e_i - f_i = \frac{a-d}{c}, \quad e_i = \varphi(e_{i-1})$$

for $i = 1, \ldots, t-1$, where $e_0 = \infty$. Note that

$$\frac{e_{t-i}x + b/c}{x + f_{t-i}} = \varphi^{t-i}(x) = \varphi^{-i}(x) = (\varphi^i)^{-1}(x) = \frac{-f_i x + b/c}{x - e_i}.$$

We see that $f_i = -e_{t-i}$. This completes the proof. □

Lemma 5.1.4 *With the same notation as in Lemma 5.1.3, we have*

$$\sum_{j=1}^{t-1} e_j = \begin{cases} (t-1)(a-d)/(2c), & \textit{if } p \neq 2, \\ a/c = d/c, & \textit{if } p = 2 \textit{ and } t = 2, \\ (a-d)/c, & \textit{if } p = 2 \textit{ and } t \equiv 3 \bmod 4, \\ 0, & \textit{if } p = 2 \textit{ and } t \equiv 1 \bmod 4, \end{cases} \tag{5.3}$$

where p is the characteristic of F_q.

Proof: We consider two cases according to the type of $\varphi(x)$.

Case I $\Delta = (a-d)^2 + 4bc = 0$. Then $t = p$ and, by Lemma 5.1.2, $\varphi(x) = h^{-1}\psi h(x)$ where

$$\psi(x) = x + 1, \quad h(x) = \frac{a/c - x_0}{x - x_0}, \quad h^{-1}(x) = x_0 + \frac{a/c - x_0}{x},$$

with x_0 satisfying $2cx_0 = a - d$ and $cx_0^2 = -b$. Note that $\psi^i(x) = x + i$. We have

$$\begin{aligned} \varphi^i(x) &= h^{-1}\psi^i h(x) \\ &= h^{-1}\left(\frac{a/c - x_0}{x - x_0} + i\right) \\ &= \frac{(a/c - x_0 - ix_0)x - ix_0^2}{ix + (a/c - x_0 - ix_0)}. \end{aligned}$$

So

$$e_i = \frac{a/c - x_0}{i} + x_0, \quad \text{for } 1 \leq i \leq t-1.$$

Therefore

$$\begin{aligned} \sum_{i=1}^{p-1} e_i &= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i^{-1} \\ &= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i \\ &= \begin{cases} (p-1)x_0 = (t-1)(a-d)/(2c), & \text{if } p \neq 2, \\ a/c = d/c, & \text{if } p = 2. \end{cases} \end{aligned}$$

Case II $\Delta = (a-d)^2 + 4bc \neq 0$. In this case, the order t of $\varphi(x)$ is a factor of $q-1$ or $q+1$. So $t \in F_q^*$. By Lemma 5.1.2, $\varphi(x) = h^{-1}\psi h(x)$ where

$$h(x) = \frac{x - x_0}{x - x_1}, \quad \psi(x) = \xi x, \quad \xi = \frac{a/c - x_0}{a/c - x_1},$$

with $x_0+x_1 = (a-d)/c$ and $x_0x_1 = -b/c$. Note that $h^{-1}(x) = (x_1x-x_0)/(x-1)$ and $\psi^i(x) = \xi^i x$, we have

$$\begin{aligned}\varphi^i(x) &= h^{-1}\psi^i h(x)\\ &= h^{-1}\left(\xi^i \frac{x-x_0}{x-x_1}\right)\\ &= \frac{(x_1\xi^i - x_0)x - x_0x_1(\xi^i-1)}{(\xi^i-1)x + x_1 - x_0\xi^i}.\end{aligned}$$

So

$$e_i = \frac{x_1\xi^i - x_0}{\xi^i - 1} = x_1 + \frac{x_1 - x_0}{\xi^i - 1}, \quad \text{for } 1 \le i \le t-1,$$

and

$$\sum_{i=1}^{t-1} e_i = (t-1)x_1 + (x_0 - x_1)\sum_{i=1}^{t-1}\frac{1}{1-\xi^i}.$$

As ξ is a t-th primitive root of unity, we have

$$\prod_{i=1}^{t-1}(x-\xi^i) = (x^t-1)/(x-1) = x^{t-1} + x^{t-2} + \cdots + x + 1. \tag{5.4}$$

Letting $x = 1$ in equation (5.4), we get

$$\prod_{i=1}^{t-1}(1-\xi^i) = t. \tag{5.5}$$

Taking derivatives with respect to x on both sides of (5.4), we have

$$\prod_{i=1}^{t-1}(x-\xi^i)(\sum_{i=1}^{t-1}\frac{1}{x-\xi^i}) = (t-1)x^{t-2} + (t-2)x^{t-3} + \cdots + 2x + 1. \tag{5.6}$$

Letting $x = 1$ in (5.6), we see that

$$\sum_{i=1}^{t-1}\frac{1}{1-\xi^i} = (\sum_{i=1}^{t-1} i)/t = \begin{cases} (t-1)/2, & \text{if } p \ne 2,\\ 1, & \text{if } p = 2 \text{ and } t \equiv 3 \bmod 4,\\ 0, & \text{if } p = 2 \text{ and } t \equiv 1 \bmod 4,\end{cases}$$

(Note that t is odd when $p = 2$.) Therefore

$$\sum_{i=1}^{t-1} e_i = \begin{cases} ((t-1)/2)(x_0+x_1) = (t-1)(a-d)/(2c), \quad \text{if } p \ne 2,\\ x_0 - x_1 = (a-d)/c, \quad \text{if } p = 2 \text{ and } t \equiv 3 \bmod 4,\\ 0, \quad \text{if } p = 2 \text{ and } t \equiv 1 \bmod 4.\end{cases}$$

This completes the proof. □

The following theorem is proved by Sidel'nikov [130, Theorem 2]:

Theorem 5.1.5 *Let $a, b, c, d \in F_q$ with $c \neq 0$ and $ad - bc \neq 0$. Let θ be a root of $F(x) = cx^{q+1} + dx^q - ax - b$ in some extension field of F_q, not fixed by $\varphi(x) = (ax+b)/(cx+d)$ whose order is assumed to be t. Then*

$$\theta, \varphi(\theta), \cdots, \varphi^{t-1}(\theta)$$

are linearly independent over F_q, if $\sum_{i=0}^{t-1} \varphi^i(\theta) \neq 0$.

This theorem indicates that if we can factor $F(x)$ then we will obtain normal bases over F_q. The factorization of $F(x)$ is discussed in the next section.

5.2 Factorization of $cx^{q+1}+dx^q-ax-b$

The complete factorization of $F(x)=cx^{q+1}+dx^q-ax-b$, $a,b,c,d\in F_q$, into irreducible factors was established by Ore [106, pp. 264–270] by using his theory of linearized polynomials. In this section, we briefly discuss how this can be done without resorting to linearized polynomials. The detail can be found in [22]. To exclude the trivial cases, we assume that $ad-bc\neq 0$. Let $\varphi(x)=(ax+b)/(cx+d)$ be the linear fractional function associated with $F(x)$. As noted in section 5.1, $\varphi(x)$ induces a permutation on $F_{q^n}\cup\{\infty\}$, for any $n\geq 1$. We assume that the order of φ is t in this section.

Let θ be a root of $F(x)=(cx+d)x^q-(ax+b)$. Then

$$\theta^q=\frac{a\theta+b}{c\theta+d}=\varphi(\theta).$$

Note that

$$\theta^{q^2}=(\varphi(\theta))^q=\varphi(\theta^q)=\varphi(\varphi(\theta))=\varphi^2(\theta).$$

By induction we see that $\theta^{q^i}=\varphi^i(\theta)$, $i\geq 0$. So

$$\theta,\varphi(\theta),\cdots,\varphi^{t-1}(\theta) \tag{5.7}$$

are all the conjugates of θ over F_q. If θ is a fixed point of $\varphi(x)$ then $\theta\in F_q$, and $x-\theta$ is a factor of $F(x)$. If θ is not a fixed point of $\varphi(x)$, then, by Theorem 5.1.5, the elements of (5.7) are distinct and θ is of degree t over F_q. In the latter case, the minimal polynomial of θ over F_q is an irreducible factor of $F(x)$ of degree t. So an irreducible factor of $F(x)$ is either linear or of degree t. We first deal with two special cases.

Theorem 5.2.1 *Let $\xi\in F_q\setminus\{0\}$ with multiplicative order t. Then the following factorization over F_q is complete:*

$$x^{q-1}-\xi=\prod_{j=1}^{(q-1)/t}(x^t-\beta_j),$$

where β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t}-\xi$ in F_q.

Proof: Let θ be a root of $x^{q-1}-\xi$ in some extension field of F_q. Then $\theta^{q^i}=\theta\xi^i, i\geq 1$. All the distinct conjugates of θ over F_q are $\theta,\theta\xi,\ldots,\theta\xi^{t-1}$. The minimal polynomial of θ over F_q is

$$\prod_{i=0}^{t-1}(x-\theta\xi^i)=x^t-\theta^t,$$

which divides $x^{q-1} - \xi$. This means that any irreducible factor of $x^{q-1} - \xi$ is of the form $x^t - \beta$ where $\beta \in F_q$. One can prove that $x^t - \beta$ divides $x^{q-1} - \xi$ if and only if β is a root of $x^{(q-1)/t} - \xi$. This completes the proof. □

Theorem 5.2.2 *For $x^q - (x + b)$ with $b \in F_q^*$, the following factorization over F_q is complete:*

$$x^q - (x + b) = \prod_{j=1}^{q/p} (x^p - b^{p-1}x - b^p\beta_j) \tag{5.8}$$

where β_j are the distinct elements of F_q with $Tr_{q/p}(\beta_j) = 1$ and p is the characteristic of F_q.

Remark: The factorization in (5.7) is better than that in Theorem 3.80 in [90, page 128].

Proof: Let θ be a root of $F(x) = x^q - (x + b)$. Then $\theta^{q^i} = \theta + ib, i \geq 1$. So the conjugates of θ over F_q are $\theta, \theta + b, \ldots, \theta + (p-1)b$. The minimal polynomial of θ over F_q is

$$\begin{aligned}
\prod_{i=0}^{p-1} [x - (\theta + ib)] &= b^p \prod_{i=0}^{p-1} [\frac{x - \theta}{b} - i] \\
&= b^p[(\frac{x - \theta}{b})^p - \frac{x - \theta}{b}] \\
&= x^p - b^{p-1}x + \theta(b^{p-1} - \theta^{p-1}).
\end{aligned}$$

Hence an irreducible factor of $x^q - (x + b)$ is of the form

$$x^p - b^{p-1}x - \beta, \quad \beta \in F_q. \tag{5.9}$$

Let γ be a root of (5.9) in some extension field of F_q. Then we have

$$(\frac{\gamma}{b})^{p^i} - (\frac{\gamma}{b})^{p^{i-1}} = (\frac{\beta}{b^p})^{p^{i-1}}, \quad 1 \leq i \leq m, \tag{5.10}$$

where $q = p^m$. Summing (5.10) yields

$$\gamma^{p^m} - \gamma = b\mathrm{Tr}_{q/p}(\frac{\beta}{b^p}).$$

Consequently (5.9) divides $F(x) = x^{p^m} - x - b$ if and only if $\mathrm{Tr}_{q/p}(\beta/b^p) = 1$. Note that there are $q/p = p^{m-1}$ elements β in F_q with trace 1, and the proof is completed. □

In general we show that the factorization of $F(x)$ can be reduced to factoring $x^q - x - 1$, $x^{q-1} - \xi$ or $x^{q+1} - \xi$. Let $\varphi = h^{-1}\psi h$ as in Lemmas 5.1.1 and 5.1.2. For any root θ of $F(x)$ that is not fixed by φ, we have

$$h(\theta^q) = \psi(h(\theta)). \tag{5.11}$$

If Δ is a quadratic residue in F_q, then $h(\theta^q) = (h(\theta))^q$. Thus $\eta = h(\theta)$ is a root of $x^q - x - 1$ or $x^q - \xi x = x(x^{q-1} - \xi)$ according as $\psi(x) = x + 1$ or $\psi(x) = \xi x, \xi \in F_q$. So by the factorization of $x^q - x - 1$ and $x^{q-1} - \xi$ as in Theorems 5.2.1 and 5.2.2 we obtain the factorization of $F(x)$ as follows.

Theorem 5.2.3 *For $a, b \in F_q$ with $a \neq 0, 1$, the following factorization over F_q is complete:*

$$x^q - (ax + b) = (x - \frac{b}{a-1}) \prod_{j=1}^{(q-1)/t} ((x - \frac{b}{a-1})^t - \beta_j),$$

where t is the multiplicative order of a and β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t} - a$.

Remark: Compare this with Theorem 3.83 in [90, page 129].

Theorem 5.2.4 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc = 0$, the following factorization over F_q is complete:*

$$\begin{aligned} &(cx + d)x^q - (ax + b) \\ &= (x - x_0) \prod_{j=1}^{q/p} [(x - x_0)^p + \frac{1}{\beta_j}(a/c - x_0)(x - x_0)^{p-1} - \frac{1}{\beta_j}(a/c - x_0)^p] \end{aligned}$$

where $x_0 \in F_q$ is the unique solution of (5.1) and β_j are all the q/p distinct elements of F_q with $Tr_{q/p}(\beta_j) = 1$.

Theorem 5.2.5 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic residue in F_q, the following factorization over F_q is complete:*

$$\begin{aligned} &(cx + d)x^q - (ax + b) \\ &= (x - x_0)(x - x_1) \prod_{j=1}^{(q-1)/t} \frac{1}{1 - \beta_j}[(x - x_0)^t - \beta_j(x - x_1)^t] \end{aligned}$$

where $x_0, x_1 \in F_q$ are the two distinct roots of (5.1), t is the multiplicative order of $\xi = (a - cx_0)/(a - cx_1)$ and β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t} - \xi$ in F_q.

If Δ is not a quadratic residue in F_q, the situation is a little more complicated, as in this case $x_0, x_1, \xi \notin F_q$. Noting that $x_0^q = x_1$ and $x_1^q = x_0$, we have $h(\theta^q) = (1/h(\theta))^q$. The equation (5.11) implies that $\eta = 1/h(\theta)$ is a root of $x^{q+1} - \xi$. So by factoring $x^{q+1} - \xi$ over F_{q^2} we can obtain the factorization of $F(x)$ over F_{q^2}. Then by "combining" these factors we get the factorization of $F(x)$ over F_q as in Theorem 5.2.6.

Theorem 5.2.6 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic nonresidue in F_q, the following factorization over F_q is complete:*

$$\begin{aligned} F(x) &= (cx+d)x^q - (ax+b) \\ &= \prod_{j=1}^{(q+1)/t} \frac{1}{1-\beta_j}[(x-x_0)^t - \beta_j(x-x_1)^t] \end{aligned} \tag{5.12}$$

where $x_0, x_1 \in F_{q^2}$ are the two distinct roots of (5.1), t is the multiplicative order of $\xi = (a - cx_1)/(a - cx_0)$ and β_j are all the $(q+1)/t$ distinct roots of $x^{(q+1)/t} - \xi$ in F_{q^2}.

Let $f(x)$ be any nonlinear irreducible factor of $F(x)$ of degree t and let α be a root of $f(x)$. From the discussion at the beginning of this section, we see that $\varphi^i(\alpha), i = 0, 1, \ldots, t-1$ are all the roots of $f(x)$ and, by Theorem 5.1.5, they are linearly independent over F_q if $\mathrm{Tr}(\alpha) \neq 0$. But $\mathrm{Tr}(\alpha)$ is just the negative of the coefficient of x^{t-1} in $f(x)$. By examining the factors in the above explicit factorizations, we have

Theorem 5.2.7 *Let $F(x) = (cx+d)x^q - (ax+b)$ with $a, b, c, d \in F_q$, $c \neq 0$ and $ad - bc \neq 0$. Then a monic nonlinear irreducible factor $f(x)$ of $F(x)$ of degree t has linearly dependent roots over F_q if and only if the coefficient of x^{t-1} in $f(x)$ is zero. The latter happens only if $\Delta = (a-d)^2 + 4bc \neq 0$ and $f(x)$ is of the form*

$$\frac{1}{x_1 - x_0}[x_1(x-x_0)^t - x_0(x-x_1)^t],$$

where x_0 and x_1 are solutions of (5.1).

This shows that every nonlinear irreducible factor of $F(x)$, except for possibly one, has linearly independent roots.

5.3 Normal Bases

As Theorem 5.2.7 shows, when $c \neq 0$ the roots of an irreducible nonlinear factor of $F(x)$ form a normal basis over F_q (except possibly for one factor). This section is devoted to discussing the properties of these bases. We will show how to construct a normal basis of F_{q^n} over F_q with complexity at most $3n - 2$ for $n = p$ and for each divisor n of $q - 1$. For this purpose we first compute the multiplication tables of the normal bases formed by the roots of an irreducible factor of $F(x)$.

Without loss of generality, we assume that $F(x) = x^{q+1} + dx^q - ax - b$ with $a, b, d \in F_q$ and $b \neq ad$. Assume that $\varphi(x) = (ax+b)/(x+d)$ has order n and that, by Lemma 5.1.3, $\varphi^i(x) = (e_i x + b)/(x - e_{n-i})$ with $e_i = \varphi^{i-1}(a)$, $1 \le i \le n-1$. Let $f(x)$ be any irreducible nonlinear factor of $F(x)$ and α a root of $f(x)$. Then $f(x)$ has degree n and its roots are

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha), \quad i = 0, 1, \cdots, n-1,$$

and they form a normal basis of F_{q^n} over F_q if the coefficient of x^{n-1} in $f(x)$ is not zero (or $\mathrm{Tr}(\alpha) \neq 0$), by Theorem 5.2.7.

Theorem 5.3.1 *Let $F(x) = x^{q+1} + dx^q - (ax+b)$ with $a, b, d \in F_q$ and $b \neq ad$. Let $f(x)$ be an irreducible factor of $F(x)$ of degree $n > 1$ and let α be a root of it. Then all the roots of $f(x)$ are*

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha), \quad i = 0, 1, \cdots, n-1, \tag{5.13}$$

where $\varphi(x) = (ax+b)/(x+d)$. If $\tau = \sum_{i=0}^{n-1} \alpha_i$, the negative of the coefficient of x^{n-1} in $f(x)$, is not zero, then (5.13) form a normal basis of F_{q^n} over F_q such that

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \cdots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} + \begin{pmatrix} b^* \\ b \\ b \\ \vdots \\ b \end{pmatrix} \tag{5.14}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ $(i \ge 1)$, $b^* = -b(n-1)$ and $\tau^* = \tau - \epsilon$ with

$$\epsilon = \sum_{i=1}^{n-1} e_i = \begin{cases} (n-1)(a-d)/2, & \text{if } p \neq 2, \\ a = d, & \text{if } p = n = 2, \\ a - d, & \text{if } p = 2 \text{ and } n \equiv 3 \bmod 4, \\ 0, & \text{if } p = 2 \text{ and } n \equiv 1 \bmod 4. \end{cases}$$

Proof: We just need to prove (5.14). By Lemma 5.1.3, for $i \ge 1$,

$$\alpha_i = \varphi^i(\alpha) = \frac{e_i \alpha_0 + b}{\alpha_0 - e_{n-i}}.$$

So

$$\alpha_0 \alpha_i = e_i \alpha_0 + e_{n-i} \alpha_i + b.$$

For $i = 0$, we have

$$\alpha_0 \alpha_0 = \alpha_0 (\tau - \sum_{j=1}^{n-1} \alpha_j) = (\tau - \sum_{j=1}^{n-1} e_j) \alpha_0 - \sum_{j=1}^{n-1} e_{n-j} \alpha_j - b(n-1).$$

The theorem follows from Lemma 5.1.4. □

The next theorem can be viewed as the "converse" of Theorem 5.3.1.

Theorem 5.3.2 *Let* $n > 2$ *and* $\alpha_i = \alpha^{q^i}$ *for* $0 \leq i \leq n-1$. *Suppose that* $\{\alpha_i\}$ *is a normal basis of* F_{q^n} *over* F_q *and satisfies*

$$\alpha_i \alpha_j = a_{ij} \alpha_i + b_{ij} \alpha_j + \gamma_{ij}, \quad \textit{for all } 0 \leq i \neq j \leq n-1, \tag{5.15}$$

where $a_{ij}, b_{ij}, \gamma_{ij} \in F_q$. *Then there are constants* $\gamma, e_1, e_2, \ldots, e_{n-1} \in F_q$ *such that*

(a) $e_i = \varphi(e_{i-1})$, *for* $2 \leq i \leq n-1$, *and*

$$a_{ij} = e_{j-i}, b_{ij} = e_{i-j}, \gamma_{ij} = \gamma, \quad \textit{for all } i \neq j,$$

where $\varphi(x) = (e_1 x + \gamma)/(x - e_{n-1})$ *and the subscripts of* e *are calculated modulo* n;

(b) *the minimal polynomial of* α *is a factor of* $F(x) = x^{q+1} - e_{n-1} x^q - (e_1 x + \gamma)$, *and thus* n *must be a factor of* p, $q-1$ *or* $q+1$.

Proof: Let $e_k = a_{0k}$ and $\gamma_k = \gamma_{0k}$ for $k = 1, 2, \cdots, n-1$. Then

$$\alpha_0 \alpha_k = e_k \alpha_0 + b_{0k} \alpha_k + \gamma_k. \tag{5.16}$$

Raising (5.16) to the q^{n-k}-th power on both sides, we have

$$\alpha_0 \alpha_{n-k} = b_{0k} \alpha_0 + e_k \alpha_{n-k} + \gamma_k. \tag{5.17}$$

Subtracting (5.17) from (5.16), with the k in (5.16) replaced by $n-k$, gives

$$(e_{n-k} - b_{0k}) \alpha_0 + (b_{0\,n-k} - e_k) \alpha_{n-k} + \gamma_{n-k} - \gamma_k = 0. \tag{5.18}$$

As $n > 2$ and the α_i's are linearly independent over F_q, the equation (5.18) implies that

$$b_{0k} = e_{n-k}, \quad \gamma_k = \gamma_{n-k}, \quad 1 \leq k \leq n-1$$

Therefore

$$\alpha_0 \alpha_k = e_k \alpha_0 + e_{n-k} \alpha_k + \gamma_k, \quad 1 \leq k \leq n-1. \tag{5.19}$$

Now for any $i \neq j$, raising (5.19) to the q^i-th power and letting $k = j - i$, we have

$$\alpha_i \alpha_j = e_{j-i} \alpha_i + e_{i-j} \alpha_j + \gamma_{j-i}. \tag{5.20}$$

Comparing (5.20) and (5.15) gives

$$a_{ij} = e_{j-i}, \quad b_{ij} = e_{i-j}, \quad \gamma_{ij} = \gamma_{j-i}, \tag{5.21}$$

which proves part of (a).

We shall prove the remaining part of (a) together with (b). To this purpose, note that a special case of (5.20) is

$$\alpha_i \alpha_{i+1} = e_{n-1} \alpha_{i+1} + e_1 \alpha_i + \gamma_1, \quad 0 \leq i < n-1,$$

or

$$\alpha_{i+1} = \frac{e_1 \alpha_i + \gamma_1}{\alpha_i - e_{n-1}} = \varphi(\alpha_i), \quad 0 \leq i < n-1, \tag{5.22}$$

where $\varphi(x) = (e_1 x + \gamma)/(x - e_{n-1})$ with $\gamma = \gamma_1$. So, by induction on i, we see that $\alpha_i = \varphi^i(\alpha_0) = \varphi^i(\alpha), 0 \leq i \leq n-1$. We know, by Lemma 5.1.3, that

$$\varphi^i(x) = (a_i x + \gamma)/(x - a_{n-i}), \quad 0 \leq i \leq n-1$$

where $a_i = \varphi(a_{i-1})$, for $i \geq 1$, and $a_1 = e_1$. Thus (5.22) implies that

$$\alpha_i = \frac{a_i \alpha_0 + \gamma}{\alpha_0 - a_{n-i}},$$

i.e.,

$$\alpha_0 \alpha_i = a_i \alpha_0 + a_{n-i} \alpha_i + \gamma. \tag{5.23}$$

Comparing (5.23) to (5.19), we have

$$e_i = a_i, \quad e_{n-i} = a_{n-i}, \quad \gamma_i = \gamma.$$

This proves (a). For (b), note that $\alpha_1 = \alpha^q$ and that (5.19) with $k = 1$ means α is a root of $F(x) = x^{q+1} - e_{n-1}x^q - e_1x - \gamma$. Therefore the minimal polynomial of α divides $F(x)$. This completes the proof. □

Theorem 5.3.3 *For every* $a, \beta \in F_q^*$ *with* $Tr_{q/p}(\beta) = 1$,

$$x^p - \frac{1}{\beta}ax^{p-1} - \frac{1}{\beta}a^p, \tag{5.24}$$

is irreducible over F_q *and its roots form a normal basis of* F_{q^n} *over* F_q *with complexity at most* $3p-2$*. The multiplication table is*

$$\begin{pmatrix} \tau^* & -e_{p-1} & -e_{p-2} & \cdots & -e_1 \\ e_1 & e_{p-1} & & & \\ e_2 & & e_{p-2} & & \\ \vdots & & & \ddots & \\ e_{p-1} & & & & e_1 \end{pmatrix} \tag{5.25}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ *fori* ≥ 1, $\varphi(x) = ax/(x+a)$, *and* $\tau^* = a/\beta$ *if* $p \neq 2$ *or* $a/\beta - a$ *if* $p = 2$.

Proof: Let $F(x) = (x+a)x^q - ax$ and $\varphi(x) = ax/(x+a)$. Then $F(x)$ satisfies the conditions of Theorem 5.2.4 with $b = 0, c = 1, d = a$, $\Delta = 0$, and $x_0 = 0$. So (5.24) is an irreducible factor of $F(x)$. As the coefficient of x^{p-1} in (5.24) is $-a/\beta \neq 0$, by Theorem 5.3.1, the roots of (5.24) form a normal basis and its multiplication table is (5.25). The complexity is obviously at most $3p-2$. □

Theorem 5.3.4 *Let* n *be any factor of* $q-1$*. Let* $\beta \in F_q$ *with multiplicative order* t *such that* $\gcd(n, (q-1)/t) = 1$ *and let* $a = \beta^{(q-1)/n}$*. Then*

$$x^n - \beta(x - a + 1)^n \tag{5.26}$$

is irreducible over F_q and its roots form a normal basis of F_{q^n} over F_q of complexity at most $3n-2$. The multiplication table is

$$\begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \cdots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \tag{5.27}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $\varphi(x) = ax/(x+1)$ and $\tau^* = -n(a-1)\beta/(1-\beta) - \epsilon$ with ϵ specified as in Theorem 5.3.1 (with $d = 1$).

Proof: It is easy to see that a has multiplicative order n. Then $\varphi(x) = ax/(x+1)$ has $x_0 = 0$ and $x_1 = a-1$ as fixed points, and $\xi = (a-x_0)/(a-x_1) = a$ has order n. So φ has order n. Note that β is a root of $x^{(q-1)/n} - a$. By Theorem 5.2.5, the polynomial (5.26) is an irreducible factor of $F(x) = x^{q+1} + x^q - ax$. Note that the coefficient of x^{n-1} in (5.26) is $n(a-1) \neq 0$. By Theorem 5.3.1 (with $b = 0, d = 1$), the roots of (5.26) form a normal basis of F_{q^n} over F_q and its multiplication table is (5.27). The complexity is obviously at most $3n-2$. □

The following table is the result of a computer search for the minimal complexity of normal bases. It indicates that when $n|(q-1)$ the minimal complexity is often $3n-3$ or $3n-2$. This indicates that the normal bases constructed in Theorems 5.3.3 and 5.3.4 often have complexity very close to the minimal complexity. In the table, † indicates that the minimal complexity is $3n-2$ and $\star$ indicates optimal complexity, i. e., $2n-1$. Other minimal values are of the form $3n-3$.

q	5	7	7	11	11	13	13	17	19
n	4	3	6	5	10	3	4	4	3
min	9	6	16†	12	28†	6	7$\star$	7$\star$	6

Table 5.1: Minimal complexity of normal bases in F_{q^n} over F_q

5.4 Self-dual Normal Bases

We know from Chapter 1 that a finite field F_{q^n} has a self-dual normal basis over F_q if and only if both n and q are odd or q is even and n is not divisible by 4. But the proof of this result is not constructive. In this section, we shall construct a self-dual normal basis of F_{q^n} over F_q for every n in the following cases:

(a) $n = p$, the characteristic of F_q,

(b) $n|(q-1)$ and n is odd,

(c) $n|(q+1)$ and n is odd.

We first determine the dual basis of the normal bases from the previous section.

Theorem 5.4.1 *Let* $N = \{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ *with* $\alpha_i = \alpha^{q^i}$ *be a normal basis of* F_{q^n} *over* F_q *satisfying*

$$\alpha_i\alpha_j = e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma, \textit{for all } i \neq j,$$

where $e_1, e_2, \cdots, e_{n-1}, \gamma \in F_q$. *Let* $\tau = Tr_{q^n/q}(\alpha)$ *and* $\lambda = -(e_1 + e_{n-1}) - n\gamma/\tau$. *Then*

$$\{\frac{1}{\tau(\tau + n\lambda)}(\alpha_i + \lambda) : \quad i = 0, 1, \cdots, n-1\}$$

is the dual basis of N.

Proof: Note that, for $i \neq j$,

$$\begin{aligned} \mathrm{Tr}_{q^n/q}(\alpha_i(\alpha_j + \lambda)) &= \mathrm{Tr}_{q^n/q}(\lambda\alpha_i + e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma) \\ &= \lambda\tau + e_{j-i}\tau + e_{i-j}\tau + n\gamma \\ &= \tau(\lambda + e_1 + e_{n-1}) + n\gamma \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} \mathrm{Tr}_{q^n/q}(\alpha_i(\alpha_i + \lambda)) &= \mathrm{Tr}(\alpha_i(\tau + \lambda - \sum_{j\neq i}\alpha_j)) \\ &= \mathrm{Tr}(\alpha_i(\tau + n\lambda - \sum_{j\neq i}(\alpha_j + \lambda))) \\ &= \mathrm{Tr}(\alpha_i)(\tau + n\lambda) - \sum_{j\neq i}\mathrm{Tr}(\alpha_i(\alpha_j + \lambda)) \\ &= \tau(\tau + n\lambda). \end{aligned}$$

The result is proved. □

We now proceed to determine when the roots of an irreducible factor of $F(x) = x^{q+1} + dx^q - ax - b$ form a self-dual normal basis. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis generated by a root α of $F(x)$ with $\alpha_i = \alpha^{q^i}$ and let $\tau = \mathrm{Tr}_{q^n|q}(\alpha)$. By Theorem 5.3.1 and Lemma 5.1.3, we have, for $i \neq 0$,

$$\begin{aligned} \mathrm{Tr}_{q^n/q}(\alpha_0\alpha_i) &= e_i\mathrm{Tr}(\alpha_0) + e_{n-i}\mathrm{Tr}(\alpha_i) + nb \\ &= \tau(e_i + e_{n-i}) + nb \\ &= \tau(a-d) + nb, \end{aligned} \tag{5.28}$$

and

$$\begin{aligned} \mathrm{Tr}_{q^n/q}(\alpha_0\alpha_0) &= \tau(\tau - \epsilon) - \tau\epsilon - nb(n-1) \\ &= \begin{cases} \tau^2, & \text{if } p = 2, \\ \tau^2 - (n-1)(\tau(a-d) + nb), & \text{if } p \neq 2. \end{cases} \end{aligned} \tag{5.29}$$

Therefore α generates a self-dual normal basis if $\tau = \mathrm{Tr}(\alpha) = 1$ and $(a-d)+nb = 0$. By examining the irreducible factors in Theorems 5.2.4, 5.2.5 and 5.2.6, we find that these two conditions can be satisfied. More explicitly, we have the following three results.

Theorem 5.4.2 *For any* $\beta \in F_q^*$ *with* $Tr_{q/p}(\beta) = 1$,

$$x^p - x^{p-1} - \beta^{p-1} \tag{5.30}$$

is irreducible over F_q *and its roots form a self-dual normal basis of* F_{q^p} *over* F_q *with complexity at most* $3p - 2$. *The multiplication table is (5.25) where* $e_1 = \beta$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $\varphi(x) = \beta x/(x+\beta)$, *and* $\tau^* = 1$ *if* $p \neq 2$ *or* $\tau^* = 1 - \beta$ *if* $p = 2$.

Proof: Let $F(x) = (x+\beta)x^q - \beta x$. Then, by Theorem 5.2.4, the polynomial (5.30) is an irreducible factor of $F(x)$ (where $b = 0$, $c = 1$, $d = a = \beta$, $x_0 = 0$ and $\beta_j = \beta$). Since $a - d = b = 0$ and $\tau = 1$ in (5.28) and (5.29), the roots of (5.30) form a self-dual normal basis. Its multiplication table is (5.25), by Theorem 5.3.1. □.

Theorem 5.4.3 *Let* n *be an odd factor of* $q - 1$ *and* $\xi \in F_q$ *of multiplicative order* n. *Then there exists* $u \in F_q$ *such that* $(u^2)^{(q-1)/n} = \xi$. *Let* $x_0 = (1+u)/n$ *and* $x_1 = (1+u)/(nu)$. *Then the* *monic polynomial*

$$\frac{1}{1-u^2}[(x-x_0)^n - u^2(x-x_1)^n] \tag{5.31}$$

is irreducible over F_q *and its roots form a self-dual normal basis of* F_{q^n} *over* F_q*. The multiplication table is (5.14) with* $a = (x_0 - \xi x_1)/(1-\xi)$*,* $b = -x_0x_1$*,* $d = a - (x_0 + x_1)$ *and* $\tau = 1$*.*

Proof: We first prove that there exists at least one root of $x^{(q-1)/n} - \xi$ that is a quadratic residue in F_q. Let ζ be a primitive element in F_q. Let t be an odd factor of $q-1$ such that $n|t$ and $\gcd(n, (q-1)/t) = 1$. Then $\zeta_0 = \zeta^{(q-1)/t}$ is a t-th primitive root of unity. Since t is odd, ζ_0^2 is also a t-th primitive root of unity. Let $d = t/n$. Then there is an integer i such that $(\zeta_0^2)^{id} = \xi$, that is,

$$(\zeta^{(q-1)/t})^{2id} = (\zeta^{2i})^{(q-1)/n} = \xi.$$

So ζ^{2i} is a root of $x^{(q-1)/n} - \xi$ and is a quadratic residue in F_q. Therefore we can take $u = \zeta^i$.

Now by applying Theorem 5.2.5, we see that (5.31) is an irreducible factor of $F(x) = (x + d)x^q - (ax + b)$. The negative of the coefficient of x^{n-1} in (5.31) is

$$\tau = \frac{n(x_0 - u^2x_1)}{1-u^2} = 1.$$

By Theorem 5.3.1, the roots of (5.31) form a normal basis of F_{q^n} over F_q with the claimed multiplication table. Note that

$$a - d = x_0 + x_1 = \frac{(u+1)}{n} + \frac{u+1}{nu} = \frac{(u+1)^2}{nu} = nx_0x_1 = -nb,$$

that is, $\tau(a-d)+nb = 0$. It follows from (5.28) and (5.29) that the roots of (5.31) form a self-dual normal basis. □

Theorem 5.4.4 *Let* n *be an odd factor of* $q+1$ *and let* $\xi \in F_{q^2}$ *be a root of* $x^{q+1} - 1$ *with multiplicative order* n*. Then there is a root* u *of* $x^{q+1} - 1$ *such that* $(u^2)^{(q+1)/n} = \xi$*. Let* $x_0 = (1+u)/n$ *and* $x_1 = (1+u)/(nu)$*. Then*

$$\frac{1}{1-u^2}[(x-x_0)^n - u^2(x-x_1)^n] \tag{5.32}$$

is in $F_q[x]$ *and is irreducible over* F_q *with its roots forming a self-dual normal basis of* F_{q^n} *over* F_q*. The multiplication table is (5.14) with* $a = (x_1 - \xi x_0)/(1-\xi)$*,* $b = -x_0x_1$*,* $d = a - (x_0 + x_1)$ *and* $\tau = 1$*.*

Proof: The proof of the existence of u is similar to that in the proof of Theorem 5.4.3 by taking ζ to be a $(q+1)$th primitive root of unity in F_{q^2}. We next prove that $a,b,d\in F_q$ and (5.32) is in $F_q[x]$. Note that ξ, u and u^2 are all $(q+1)$th roots of unity and we have $\xi^q=1/\xi$, $u^q=1/u$ and $(u^2)^q=1/u^2$. Thus $x_0^q=x_1$ and $x_1^q=x_0$. So $a^q=a$, $b^q=b$ and $d^q=d$, that is, $a,b,d\in F_q$. Denote the polynomial (5.32) by $\phi(x)$ and note that

$$\begin{aligned}(\phi(x))^q &= \frac{1}{1-(u^2)^q}[(x^q-x_0^q)^n-(u^2)^q(x^q-x_1^q)^n]\\ &= \frac{1}{1-1/u^2}[(x^q-x_1)^n-1/u^2(x^q-x_0)^n]\\ &= \phi(x^q).\end{aligned}$$

We see that the coefficients of $\phi(x)$ are in F_q.

To prove that (5.32) is irreducible over F_q, we apply Theorem 5.2.6. It is easy to check that, with a,b,d as defined in Theorem 5.4.4, x_0 and x_1 are the two distinct solutions of (5.1) with $c=1$ and $(a-x_1)/(a-x_0)=\xi$ which is of order n. Now since u^2 is assumed to be a solution of $x^{(q+1)/q}-\xi$, it follows from Theorem 5.2.6 that (5.32) is an irreducible factor of $F(x)=(x+d)x^q-(ax+b)$.

As the coefficient of x^{n-1} in (5.32) is $(-nx_0+nu^2x_1)/(1-u^2)=-1$, the trace of any root of (5.32) is $\tau=1$. It is easy to check that $\tau(a-d)+nb=0$. It follows from (5.28) and (5.29) that the roots of (5.32) form a self-dual normal basis. The multiplication table follows from Theorem 5.3.1. □

Chapter 6

Further Research Problems

In previous chapters, we have discussed various properties of normal bases and give some constructions of special normal bases. In this chapter we point out some problems that deserve further study.

In Chapter 3, we have seen that given an irreducible polynomial of degree n over F_q, one can construct a normal basis for F_{q^n} over F_q deterministically in polynomial time. So the problem of constructing normal bases is polynomially reduced to the following problem.

Research Problem 6.1 *Given the finite field F_q and a positive integer n, find a deterministic algorithm for constructing an irreducible polynomial of degree n in $F_q[x]$ that runs in time polynomial in n and $\log q$.*

This problem is theoretically important in finite field theory and computer algebra. However, there is currently no deterministic polynomial time algorithm to solve this problem.

We have seen in Chapter 1 that for practical implementation of finite field arithmetic, it is essential to construct normal bases of complexity as low as possible. In Chapter 4, we have determined all the optimal normal bases in finite fields, and we see that not all the finite fields have optimal normal bases. The following question arises naturally.

Research Problem 6.2 *Suppose there is no optimal normal basis in F_{q^n} over F_q. 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?*

In particular, we can ask if there are normal bases of complexity $2n$, $2n+1$, $2n+2$, etc., and construct them if any. In Chapter 5, we have constructed a normal basis of F_{q^n} over F_q of complexity at most $3n-2$ for each factor n of $q-1$ and for n being the characteristic of F_q. In this case, Table 5.1 indicates that the minimum complexity of normal bases in F_{q^n} over F_q is often $3n-3$ or $3n-2$. Computer experiment for other values of n and q also suggests that there are no normal bases of complexity strictly between $2n-1$ and $3n-3$, that is, the next possibility of complexity is $3n-3$. It will be very interesting if one can prove that this is actually true.

For cryptographic purposes it is important to have either a primitive element or an element of high multiplicative order in F_{2^n}. Table 6.1 indicates that the type II optimal normal basis generators have high multiplicative orders in general and are quite often primitive. This phenomenon was also noticed by Rybowicz [115].

Research Problem 6.3 *Let n be a positive integer and ζ a $(2n+1)$th primitive root of unity in some extension of F_2. Determine the multiplicative order of $\alpha = \zeta + \zeta^{-1}$.*

We are interested in the case where $2n+1$ is prime and $\mathbb{Z}_{2n+1}^*$ is generated by 2 and -1, i.e., when α generates an optimal normal basis of F_{2^n} over F_2. Significant progress will have been made if one can determine the exact order of α without knowing the complete factorization of 2^n-1 for large n, say $n \geq 543$.

The following problem may be viewed as the converse of the above problem.

Research Problem 6.4 Let α be an element in an extension field of F_2. Given the multiplicative order of α, determine the order of γ, where $\gamma + \gamma^{-1} = \alpha$.

In particular, let $\alpha_0 = 1$ and α_k be defined over F_2 such that $\alpha_k + \alpha_k^{-1} = \alpha_{k-1}$ for $k \geq 1$. Prove or disprove that the multiplicative order of α_k is $2^{2^{k-1}}+1$ for $k \geq 1$. This has been verified to be true in [150] for $k \leq 9$. Also note that α_k is a root of the polynomial $a_k(x) + b_k(x)$ in Corollary 3.4.14.

The complexity of a normal basis defined as in this thesis does not necessarily represent the real complexity of field multiplication under this basis. In Chapter 5, we constructed normal bases

m	Order	m	Order	m	Order	m	Order
2	$2^m - 1$	231	$2^m - 1$	530	$2^m - 1$	834	$2^m - 1$
3	$2^m - 1$	233	$2^m - 1$	531	$2^m - 1$	846	$2^m - 1$
5	$2^m - 1$	239	$2^m - 1$	543	?	866	$2^m - 1$
6	$2^m - 1$	243	$2^m - 1$	545	$2^m - 1$	870	$2^m - 1$
9	$2^m - 1$	245	$2^m - 1$	554	$2^m - 1$	873	$2^m - 1$
11	$2^m - 1$	251	$2^m - 1$	558	$2^m - 1$	879	$2^m - 1$
14	$2^m - 1$	254	$2^m - 1$	561	$2^m - 1$	891	$2^m - 1$
18	$(2^m - 1)/3$	261	$2^m - 1$	575	$2^m - 1$	893	?
23	$2^m - 1$	270	$(2^m - 1)/7$	585	$2^m - 1$	911	?
26	$2^m - 1$	273	$2^m - 1$	593	?	923	?
29	$2^m - 1$	278	$(2^m - 1)/3$	606	$(2^m - 1)/9$	930	$(2^m - 1)/3$
30	$2^m - 1$	281	$2^m - 1$	611	?	933	?
33	$2^m - 1$	293	$2^m - 1$	614	$(2^m - 1)/3$	935	?
35	$2^m - 1$	299	$2^m - 1$	615	$2^m - 1$	938	$2^m - 1$
39	$2^m - 1$	303	$2^m - 1$	618	$2^m - 1$	939	?
41	$2^m - 1$	306	$2^m - 1$	629	?	950	$(2^m - 1)/3$
50	$(2^m - 1)/3$	309	$2^m - 1$	638 $2^m - 1$?	953	?	
51	$2^m - 1$	323	$2^m - 1$	639	$2^m - 1$	965	$2^m - 1$
53	$2^m - 1$	326	$2^m - 1$	641	?	974	$(2^m - 1)/3$
65	$2^m - 1$	329	$2^m - 1$	645	$(2^m - 1)/7$	975	$2^m - 1$
69	$2^m - 1$	330	$2^m - 1$	650	$(2^m - 1)/3$	986	$(2^m - 1)/3$
74	$2^m - 1$	338	$(2^m - 1)/3$	651	$2^m - 1$	989	?
81	$2^m - 1$	350	$(2^m - 1)/3$	653	$2^m - 1$	993	$2^m - 1$
83	$2^m - 1$	354	$(2^m - 1)/3$	659	?	998	$2^m - 1$
86	$2^m - 1$	359	$2^m - 1$	683	?	1013	?
89	$2^m - 1$	371	$2^m - 1$	686	$(2^m - 1)/3$	1014	$(2^m - 1)/7$

90	2^m-1	375	2^m-1	690	$(2^m-1)/151$	1019	?
95	2^m-1	378	$(2^m-1)/3$	713	?	1026	$(2^m-1)/7$
98	$(2^m-1)/3$	386	2^m-1	719	?	1031	?
99	$(2^m-1)/7$	393	$(2^m-1)/7$	723	?	1034	$(2^m-1)/3$
105	2^m-1	398	2^m-1	725	?	1041	2^m-1
113	2^m-1	410	$(2^m-1)/11$	726	2^m-1	1043	?
119	2^m-1	411	2^m-1	741	$(2^m-1)/7$	1049	2^m-1
131	2^m-1	413	2^m-1	743	?	1055	?
134	$(2^m-1)/3$	414	$(2^m-1)/3$	746	2^m-1	1065	?
135	2^m-1	419	2^m-1	749	?	1070	?
146	2^m-1	426	2^m-1	755	2^m-1	1103	2^m-1
155	2^m-1	429	2^m-1	761	?	1106	$(2^m-1)/381$
158	2^m-1	431	2^m-1	765	2^m-1	1110	$(2^m-1)/9$
173	2^m-1	438	$(2^m-1)/3$	771	2^m-1	1118	?
174	$(2^m-1)/3$	441	2^m-1	774	2^m-1	1119	2^m-1
179	2^m-1	443	2^m-1	779	?	1121	2^m-1
183	2^m-1	453	2^m-1	783	?	1133	?
186	$(2^m-1)/3$	470	2^m-1	785	?	1134	$(2^m-1)/3$
189	2^m-1	473	2^m-1	791	?	1146	2^m-1
191	2^m-1	483	2^m-1	803	?	1154	2^m-1
194	$(2^m-1)/3$	491	2^m-1	809	?	1155	2^m-1
209	2^m-1	495	2^m-1	810	2^m-1	1166	2^m-1
210	2^m-1	509	2^m-1	818	2^m-1	1169	2^m-1
221	2^m-1	515	2^m-1	831	2^m-1	1178	?
230	2^m-1	519	2^m-1	833	?	1185	2^m-1

Table 6.1: Order of type II optimal normal basis generators in F_{2^m}.

in F_{q^n} over F_q with cross products of the form: $\alpha_i\alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$, $i \neq j$ for $i \neq j$, where $e_k, \gamma \in F_q$. If $\gamma \neq 0$, the complexity of the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ has complexity nearly n^2. Since there are only $3n-1$ constants in all the n cross products $\alpha_0\alpha_i$ for $0 \leq i \leq n-1$, it is easy to check that one can multiply any two elements in F_{q^n}, represented in this basis, by using about $3n-1$ multiplications of elements in F_q. This indicates that the real complexity of field multiplication of F_{q^n} under a normal basis of above type is much less than the defined complexity of the basis.

In general, it is interesting to study the complexity of finite field arithmetic (similarly for a finite dimensional algebra). For any positive integer n and prime power q, let $C(q,n)$ denote the smallest number of *essential* F_q-operations needed to multiply any two elements in F_{q^n} among all possible choices of (normal) bases and operational algorithms. Here "essential F_q-operations" are not specified, they may include $-, +, *, /$ or just $*$ in F_q, depending on the actual situations. The definition of the number $C(q,n)$ is not clear, but intuitively, it should represent the actual arithmetic complexity of the field F_{q^n}. Note that this is similar to but perhaps different from the approach by de Groote [59].

Research Problem 6.5 *Find good lower and upper bounds for $C(q,n)$ and construct the required bases.*

Bibliography

[1] L.M. Adleman and H.W. Lenstra, Jr., "Finding irreducible polynomials over finite fields", *Proceedings of the 18th Annual ACM Symposium on Theory of Computing* (1986), 350-355.

[2] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk and S.A. Vanstone, "An implementation for a fast public key cryptosystem", *J. of Cryptology*, **3** (1991), 63-79.

[3] G.B. Agnew, R.C. Mullin and S.A. Vanstone, "An implementation of elliptic curve cryptosystems over $F_{2^{155}}$", *IEEE J. on Selected Areas in Communications*, to appear.

[4] A.V. Aho, J.E. Hopcroft, J.D. Ullman, *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, MA, 1974.

[5] S. Akbik, "Normal generators of finite fields", *J. Number Theory*, **41** (1992), 146-149.

[6] J.D. Alanen and D.E. Knuth, "Tables of finite fields", *Sankhyā Ser. A*, **26** (1964), 305-328.

[7] A.A. Albert, *Fundamental Concepts of Higher Algebra*, Univ. of Chicago Press, Chicago, 1956.

[8] E. Artin, "Linear mappings and the existence of a normal basis", in *Studies and Essays Presented to R. Courant on his 60th Birthday*, Interscience, New York, 1948, 1-5.

[9] E. Artin, *Galois Theory*, University of Notre Dame Press, South Bend, Ind., 1966.

[10] D.W. Ash, I.F. Blake and S.A. Vanstone, "Low complexity normal bases", *Discrete Applied Math.*, **25** (1989), 191-210.

[11] E. Bach, J. Driscoll and J. Shallit, “Factor refinement”, *J. of Algorithms*, **15** (1993), 199-222. (Extended abstract appeared in *Proceedings of the First Annual ACM-SIAM Symposium on Discrete Algorithms* (1990), 202-211.)

[12] E. Bach and J. Shallit, “Factoring with cyclotomic polynomials”, *Math. Comp.*, **52** (1989), 201-219.

[13] E. Bayer-Fluckiger, “Self-dual normal bases”, *Indag. Math.* **51** (1989), 379-383.

[14] E. Bayer-Fluckiger and H.W. Lenstra, Jr., “Forms in odd degree extensions and self-dual normal bases”, *Amer. J. Math.*, **112** (1990), 359-373.

[15] T.R. Berger and I. Reiner, “A proof of the normal basis theorem”, *Amer. Math, Monthly*, **82** (1975), 915-918.

[16] E.R. Berlekamp, “Bit-serial Reed-Solomon encoders”, *IEEE Trans. Info. Th.*, **28** (1982), 869-874.

[17] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[18] T. Beth, “Generalizing the discrete Fourier transform”, *Discrete Math.*, **56** (1985), 95-100.

[19] T. Beth, W. Fumy and R. Mühlfeld, “Zur algebraischen diskreten Fourier-transformation”, *Arch. Math.*, **40** (1983), 238-244.

[20] T. Beth and W. Geiselmann, “Selbstduale normalbasen über $GF(q)$”, *Arch. Math.*, **55** (1990), 44-48.

[21] I.F. Blake, S. Gao and R.C. Mullin, “Explicit factorization of $x^{2^k}+1$ over F_p with prime $p \equiv 3(\text{mod } 4)$”, to appear in *App. Alg. in Eng., Comm. and Comp.*, 1993.

[22] I.F. Blake, S. Gao and R.C. Mullin, “Factorization of $cx^{q+1}+dx^q-ax-b$ and normal bases over $GF(q)$”, *CORR 91-26*, Department of Combinatorics and Optimization, University of Waterloo, 1991.

[23] I.F. Blake, S. Gao and R.C. Mullin, “Normal and self-dual normal bases from factorization of $cx^{q+1}+dx^q-ax-b$”, submitted to *SIAM J. Discrete Mathematics*, 1992.

[24] D. Blessenohl, “Supplement zu “Eine Verschärfung des Satzes von der Normalbasis” ”, *J. Algebra*, **132** (1990), 154-159.

[25] D. Blessenohl and K. Johnsen, "Eine Verschärfung des Satzes von der Normalbasis", *J. Algebra*, **103** (1986), 141-159.

[26] W.J. Borho, J. Buhl, H. Hoffmann, S. Mertens, E. Nebgen and R. Reckow, "Große Primzahlen und Befreundete Zahlen: Über den Lucas-Test und Thabit-Regeln", *Mitt. Math. Ges. Hamburg* **11** (1983), 232–256.

[27] N. Bourbaki, *Elements of Mathematics, Algebra II, Chapters 4-7*, translated by P.M. Cohn and J. Howie, Springer-Verlag, 1990.

[28] J.V. Brawley and G.E. Schnibben, *Infinite Algebraic Extensions of Finite Fields*, Contemporary Mathematics, vol. 95, American Math. Soc., Providence, R.I., 1989.

[29] N.H. Bshouty and G. Seroussi, "Generalizations of the normal basis theorem of finite fields", *SIAM J. Disc. Math.*, **3** (1990), 330-337.

[30] J. Calmet, "Algebraic algorithms in $GF(q)$", *Discrete Math.*, **56** (1985), 101-109.

[31] D. Cantor, "On arithmetical algorithms over finite fields", *J. of Combinatorial Theory*, **A 56** (1989), 285-300.

[32] L. Carlitz, "Primitive roots in finite fields", *J. London Math. Soc.*, **43** (1952), 373-382.

[33] L.N. Childs and M. Orzech, "On modular group rings, normal bases, and fixed points", *Amer. Math. Monthly*, **88** (1981), 142-145.

[34] S.D. Cohen, "Primitive elements and polynomials: existence results", in *Finite Fields, Coding Theory, and Advances in Communications and Computing*, edited by G.L. Mullen and P. J.-S. Shiue, (Lecture Notes in Pure and Appl. Math., **141**), Marcel Dekker, 1992.

[35] H. Cohen, H.W. Lenstra, Jr., "Primality testing and Jacobi sums", *Math. Comp.* **42** (1984), 297–330.

[36] P.M. Cohn, *Algebra*, vol. 3, Wiley, Toronto, 1982.

[37] P. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, World Scientific, Singapore, 1984.

[38] H. Davenport, "Bases for finite fields", *J. London Math. Soc.*, **43** (1968), 21-39.

[39] D. E. Daykin, “Generation of irreducible polynomials over finite field”, *Amer. Math. Monthly* **72** (1965), 646–648.

[40] M. Deuring, “Galoissche Theorie und Darstellungstheorie”, *Math. Ann.* **107** (1933), 140-144.

[41] M. Diab, “Systolic architectures for multiplication over finite field $GF(2^m)$”, *Proceedings of AAECC-9*, Lecture Notes in Computer Science, **508** (1991), 329-340.

[42] W. Diffie and M.E. Hellman, “New directions in cryptography”, *IEEE Trans. Info. Th.*, **22** (1976), 644-654.

[43] G. Eisenstein, “Lehrsätze”, *J. reine angew. Math.* **39** (1850), 180-182; *Math. Werke*, vol. 2, Chelsea, New York, 1975, 620-622.

[44] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, *IEEE Trans. Info. Th.*, **31** (1985), 469-472.

[45] M. Feng, “A VLSI architecture for fast inversion in $GF(2^m)$”, *IEEE Trans. Comput.*, **38** (1989), 1383-1386.

[46] G.S. Frandsen, “Probabilistic construction of normal basis (note)”, *DAIMI PB-361*, Computer Science Department, Aarhus University, Denmark, August 1991.

[47] W. Fumy, “Orthogonal transform encoding of cyclic codes”, *AAECC-3, Lecture Notes in Comput. Sci.*, vol. 229, Springer-Verlag, 1986, 131-134.

[48] É. Galois, *Ecrits et Mémoires Mathématiques d’Évariste Galois*, R. Bourgne and J.-P. Azra, Editors, Gauthier-Villars, Paris, 1962.
Also *Oeuvres Mathématiques d’Évariste Galois*, Gauthier-Villars, Paris, 1897,
and *J. Math. Pures et Appl.* (1) **11** (1846), 381-444.

[49] S. Gao, “The determination of optimal normal bases over finite fields”, *CORR 92-01*, Department of Combinatorics and Optimization, University of Waterloo, 1992.

[50] S. Gao and H.W. Lenstra, Jr., “Optimal normal bases”, *Designs, Codes and Cryptography*, **2** (1992), 315-323.

[51] S. Gao and G.L. Mullen, "Dickson polynomials and irreducible polynomials over finite fields", 1992, to appear in *J. Number Theory.*

[52] J. von zur Gathen and M. Giesbrecht, "Constructing normal bases in finite fields", *J. Symbolic Computation*, **10** (1990), 547-570.

[53] J. von zur Gathen and V. Shoup, "Computing Frobenius maps and factoring polynomials", to appear in *Computational Complexity*, **2** (1992).

[54] C.F. Gauss, *Disquisitiones Arithmeticae*, Braunschweig, 1801, republished, 1863, as vol. 1 of *Werke*; French transl., *Recherches Arithmétiques*, Paris, 1807, republished Hermann, Paris, 1910; German transl., *Arithmetische Untersuchungen*, Springer-Verlag, Berlin, 1889, republished Chelsea, New York, 1965; English transl., Yale, New Haven and London, 1966, 1986.

[55] W. Geiselmann and D. Gollmann, "Symmetry and duality in normal basis multiplication", *AAECC-6*, Lecture Notes in Computer Science, **357** (1989), Springer-Verlag, 230-238.

[56] W. Geiselmann and D. Gollmann, "VLSI design for exponentiation in $GF(2^n)$", *Advances in Cryptology: Proceedings of Auscrypt '90*, Lecture Notes in Computer Science, **453** (1990), Springer-Verlag, 398-405.

[57] W. Geiselmann and D. Gollmann, "Self-dual bases in F_q", 1992, preprint.

[58] J.A. Gordon, "Very simple method to find the minimal polynomial of an arbitrary nonzero element of a finite field", *Electronics Letters*, **12** (1976), 663-664.

[59] H.F. de Groote, *Lectures on the Complexity of Bilinear Problems*, Lecture Notes in Computer Science, **245**, Springer-Verlag, 1987.

[60] D. Hachenberger, "On primitive and free roots in a finite field", *App. Alg in Eng., Comm. and Comp.*, **3** (1992), 139-150.

[61] K. Hensel, "Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor", *J. Reine Angew. Math.*, **103** (1888), 230-237.

[62] K. Hoffman and R. Kunze, *Linear Algebra*, 2nd ed., Prentice-Hall, Englewood Cliffs, N.J., 1971.

[63] I.S. Hsu, T.K. Truong, L.J. Deutsch and I.S. Reed, "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.

[64] T.W. Hungerford, *Algebra*, Springer-Verlag, 1974.

[65] I. Imamura, "On self-complementary bases of $GF(q^n)$ over $GF(q)$", *Trans. IECE Japan (Section E)*, **66** (1983), 717-721.

[66] I. Imamura, "The number of self-complementary bases of a finite field of characteristic two", *IEEE Internat. Symp. Inform. Theory*, Kobe, Japan, 1988.

[67] K. Imamura and M. Morii, "Two classes of finite fields which have no self-complementary normal bases", *IEEE Int'l Symp. Inform. Theory*, Brighton, England, June, 1985.

[68] K. Ireland and R. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Graduate Texts in Mathematics V. **84**, Springer-Verlag, New York/Heidelberg/Berlin, 1990.

[69] N. Jacobson, *Basic Algebra I*, 2nd ed., W.H. Freeman, New York, 1985.

[70] D. Jungnickel, "Trace-orthogonal normal bases", *Discrete Applied Math.*, to appear.

[71] D. Jungnickel, *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[72] D. Jungnickel, A.J. Menezes and S.A. Vanstone, "On the number of self-dual bases of $GF(q^n)$ over $GF(q)$", *Proc. Amer. Math. Soc.*, **109** (1990), 23-29.

[73] B. Kahn, "La deuxième classe de Stiefel-Whitney d'une représentation régulière", I., II., *C. R. Acad. Sci. Paris*, série I., **297** (1983), 313-316, **316** (1983), 573- 576.

[74] B. Kahn, "Classes de Stiefel-Whitney de formes quadratques", *Invent. Math.*, **78** (1984), 223-256.

[75] I. Kersten and J. Michaliček, "Galoiserweiterungen der ordnung p mit normalbasis", *Comm. Algebra*, **10** (1982), no. 7, 695-718.

[76] M. Krasner, "Sur la représentation exponentielle dans les corps relativement galoisiens de nombres p-adiques", *Acta Arith.*, **3** (1939), 133-173.

[77] H.F. Kreimer, "Normal bases for Galois p-extensions of rings", *Notices Amer. Math. Soc.*, **24** (1977), A-268.

[78] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, Menlo Park, California, 1984.

[79] A. Lempel, "Matrix factorization over $GF(2)$ and trace-orthogonal bases of $GF(2^n)$", *SIAM J. Comput.*, **4** (1975), 175-186.

[80] A. Lempel, "Characterization and synthesis of self-complementary normal bases in finite fields", *Lin. Alg. App.*, **98** (1988), 331-346.

[81] A. Lempel and G. Seroussi, "Explicit formulas for self-complementary normal bases in certain finite fields", *IEEE Trans. Info. Th.*, **37** (1991), 1220-1222.

[82] A. Lempel and M.J. Weinberger, "Self-complementary normal bases in finite fields", *SIAM J. Disc. Math.*, **1** (1988), 193-198.

[83] H.W. Lenstra,Jr., unpublished.

[84] H.W. Lenstra, Jr., "Optimal normal bases over the field of two elements", preprint, 1991.

[85] H.W. Lenstra, Jr., "Finding isomorphisms between finite fields", *Math. Comp.*, **56** (1991), 329-347.

[86] H.W. Lenstra, Jr., "A normal basis theorem for infinite Galois extensions", *Proc. Kon. Ned. Akad. Wet., Ser. A*, **88** (1985), 221-228.

[87] H.W. Lenstra, Jr. and R.J. Schoof, "Primitive normal bases for finite fields", *Math. Comp.*, **48** (1987), 217-231.

[88] W.J. Leveque, *Topics in Number Theory*, (2 volumes), Addison-Wesley, Reading, Mass., 1956.

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

[90] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge University Press.)

[91] J.D. Lipson, *Elements of Algebra and Algebraic Computing*, Benjamin/Cummings, 1981.

[92] H. Lüneburg, "On a little but useful algorithm", *Proc. AAECC-3, Lecture Notes in Computer Science* **229**, Springer-Verlag, Berlin, 1985, 296-301.

[93] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[94] H.B. Mann, "On canonical bases for subgroups of an Abelian group", in: R.C. Bose and T.H. Dowling, eds., *Combinatorial Mathematics and its applications*, (University of North Carolina Press, Chapel Hill, NC, 1969), 38-54.

[95] J.L. Massey and J.K. Omura, "Computational method and apparatus for finite field arithmetic", U.S. patent #4,587,627, May 1986.

[96] E. Mastrovito, "VLSI designs for multiplication over finite fields $GF(2^m)$", *Applied Algebra, Algebraic Algorithms and Error-correcting Codes* (Rome 1988), Lecture Notes in Computer Science, vol. 357, 1989, 297–309.

[97] F.J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, Boston-Dordrecht-Lancaster, 1987.

[98] H. Meyn, "On the construction of irreducible self-reciprocal polynomials over finite fields", *App. Alg in Eng., Comm. and Comp.*, **1** (1990), 43-53.

[99] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publishers, Boston-Dordrecht-Lancaster, 1993.

[100] M. Morii and K. Imamura, "A theorem that $GF(2^m)$ has no self-complementary normal basis over $GF(2)$ for odd m", *Trans. IECE Japan*, **E67** (1984), 655-656.

[101] M. Morii, M. Kasahara and D. Whiting, "Efficient bit-serial multiplication and the dicrete-time Wiener-Hopf equation over finite fields", *IEEE Trans. Info. Th.*, **35** (1989), 1177-1183.

[102] R.C. Mullin, "A characterization of the extremal distributions of optimal normal bases", to appear in *Proc. Marshall Hall Memorial Conference*, Burlington, Vermont, 1990.

[103] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Math.*, **22** (1988/1989), 149-161.

[104] E. Noether, “Normalbasis bei Körpen ohne höhere Verzweigung”, *J. Reine Angew. Math.*, **167** (1932), 147-152.

[105] I.M. Onyszchuk, R.C. Mullin and S.A. Vanstone, “Computational method and apparatus for finite field multiplication”, U.S. patent #4,745,568, May 1988.

[106] O. Ore, “Contributions to the theory of finite fields”, *Trans. Amer. Math. Soc.*, **36** (1934), 243-274.

[107] D. Pei, C.C. Wang and J.K. Omura, “Normal bases of finite field $GF(2^m)$”, *IEEE Trans. Info. Th.*, **32** (1986), 285-287.

[108] S. Perlis, “Normal bases of cyclic fields of prime-power degree”, *Duke Math. J.*, **9** (1942), 507-517.

[109] A. Pincin, “Bases for finite fields and a canonical decomposition for a normal basis generator”, *Communications in Algebra*, **17** (1989), 1337-1352.

[110] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

[111] A. Pott, “On the complexity of normal bases”, *Bull. Inst. Combin. Appl.*, **4** (1992), 51-52.

[112] L. Rédei, *Algebra*, Pergamon Press, Oxford, New York, 1967.

[113] J. Rifà and J. Borrell, “Improving the time complexity of computation of irreducible and primitive polynomials in finite fields”, *Proc. AAECC-9, Lecture Notes in Computer Science* **539**, Springer-Verlag, Berlin, 1991, 352-359.

[114] T. Rosati, “A high speed data encryption processor for public key cryptography”, *Proceedings of IEEE Custom Integrated Circuits Conference*, San Diego, 1989, 12.3.1 – 12.3.5.

[115] M. Rybowicz, “Search of primitive polynomials over finite fields”, *J. of Pure and Applied Algebra*, **65** (1990), 139-151.

[116] A. Scheerhorn, “Trace- and norm-compatible extensions of finite fields”, *App. Alg in Eng., Comm. and Comp.*, **3** (1992), 199-209.

[117] H.P. Schlickewei and S.A. Stepanov, “Algorithm to construct normal bases of cyclic number fields”, *J. Number Theory*, 1990.

[118] T. Schönemann, "Über einige von Herrn Dr. Einsentein aufgestellte Lehrsätze", *J. reine angew. Math.* **40** (1850), 185-187.

[119] Š.S. Schwarz, "Construction of normal bases in cyclic extensions of a field", *Czechslovak Math. J.*, **38** (1988), 291-312.

[120] Š.S. Schwarz, "Irreducible polynomials over finite fields with linearly independent roots", *Math. Slovaca*, **38** (1988), 147-158.

[121] P.A. Scott, S.E. Tavares and L.E. Peppard, "A fast VLSI multiplier for $GF(2^m)$", *IEEE J. on Selected Areas in Communications*, **4** (1986), 62-66.

[122] G.E. Séguin, "Low complexity normal bases for $F_{2^{mn}}$", *Discrete Applied Math.*, **28** (1990), 309-312.

[123] I.A. Semaev, "Construction of polynomials irreducible over a finite field with linearly independent roots", *Math. USSR Sbornik*, **63** (1989), 507-519.

[124] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields", *SIAM J. Comput.*, **9** (1980), 758-767.

[125] J.-P. Serre, "L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$", *Comm. Math. Helv.*, **59** (1984), 651-676 (= Oeuvres Vol. III, No. 131, 675-700).

[126] J.A. Serret, *Cours d'Algèbre Supérieure*, 3rd ed., Gauthier-Villars, Paris, 1866.

[127] V. Shoup, "On the deterministic complexity of factoring polynomials over finite fields", *Information Processing Letters*, **33** (1990), 261-267.

[128] V. Shoup, "New algorithms for finding irreducible polynomials over finite fields", *Math. Comp.*, **54** (1990), 435-447.

[129] V. Shoup, "Searching for primitive roots in finite fields", *Math. Comp.*, **58** (1992), 369-380.

[130] V.M. Sidel'nikov, "On normal bases of a finite field", *Math. USSR Sbornik* **61**(1988), 485–494.

[131] S.A. Stepanov and I.E. Shparlinskiy, "On the construction of a primitive normal basis in a finite field", *Math. USSR Sbornik*, **67** (1990), 527-533.

[132] S.A. Stepanov and I.E. Shparlinskiy, "On the construction of a normal basis for a finite field", *Acta Arith.* **49** (1987), 189–192.

[133] S.A. Stepanov and I.E. Shparlinskiy, "On construction of primitive elements and primitive normal bases in a finite field", in *Computational Number Theory*, ed. A. Pethö, M.E. Pohst, H.C. Williams and H.G. Zimmer, 1991. (Proc. Colloq. Comp. Number Theory, Hungary, 1990).

[134] D.H. Stinson, "On bit-serial multiplication and dual bases in $GF(2^m)$", *IEEE Trans. Info. Th.*, **37** (1991), 1733-1736.

[135] T. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.

[136] J.A. Thiong Ly, "Note for computing the minimum polynomial of elements in large finite fileds", in *Lecture Notes in Computer Science* **388**, Springer-Verlag, Berlin, 1989.

[137] R.R. Varshamov, "A certain linear operator in a Galois field and its applications (Russian)", *Studia Sci. Math. Hungar.*, **8** (1973), 5-19.

[138] R.R. Varshamov, "Operator substitutions in a Galois field and their application (Russian)", *Dokl. Akad. Nauk SSSR*, **211** (1973), 768-771; *Soviet Math. Dokl.*, **14** (1973), 1095-1099.

[139] R.R. Varshamov, "A general method of synthesizing irreducible polynomials over Galois fields", *Soviet Math. Dokl.*, **29** (1984), 334-336.

[140] R.R. Varshamov and G.A. Garakov, "On the theory of selfdual polynomials over a Galois field (Russian)", *Bull. Math. Soc. Sci. Math. R. S. Roumanie(N.S.)*, **13** (1969), 403-415.

[141] B. van der Waerden, *Algebra*, vol. 1, Springer-Verlag, Berlin, 1966.

[142] C.C. Wang, "An algorithm to design finite field multipliers using a self-dual normal basis", *IEEE Trans. Comput.*, **38** (1989), 1457-1460.

[143] M. Wang and I.F. Blake, "Bit-serial multiplication in finite fields", *SIAM J. Disc. Math.*, **3** (1990), 140-148.

[144] M. WANG, I.F. BLAKE AND V.K. BHARGAVA, "Normal bases and irreducible polynomials in the finite field $GF(2^{2^r})$", preprint, 1990.

[145] C.C. WANG AND D. PEI, "A VLSI design for computing exponentiations in $GF(2^m)$ and its applications to generate pseudorandom number sequences", *IEEE Trans. Comput.*, **39** (1990), 258-262.

[146] C.C. WANG, T.K. TRUONG, H.M. SHAO, L.J. DEUTSCH, J.K. OMURA AND I.S. REED, "VLSI architectures for computing multiplications and inverses in $GF(2^m)$", *IEEE Trans. Comput.*, **34** (1985), 709-717.

[147] L.C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

[148] A. WASSERMANN, "Konstruktion von normalbasen", *Bayreuther Mathematische Schriften*, **31** (1990), 155-164.

[149] W.C. WATERHOUSE, "The normal basis theorem", *Amer. Math. Monthly* **86** (1979), 212.

[150] D. WIEDEMANN, "An iterated quadratic extension of $GF(2)$", *Fibonacci Quart.*, **26** (1988), 290-295.

[151] C.S. YEH, I.S. REED AND T.K. TRUONG, "Systolic multipliers for finite fields $GF(2^m)$", *IEEE Trans. Comput.*, **33** (1984), 357-360.

[152] K. YIU AND K. PETERSON, "A single-chip VLSI implementation of the discrete exponential public key distribution system", *Proceedings GLOBECOM-82*, IEEE (1982), 173-179.