International Journal of Pure and Applied Mathematics
Volume 70 No. 4 2011, 559-569

EXPLICIT CONSTRUCTION OF FINITE FIELDS USING NORMAL BASES

Anthony Y. Aidoo[1] §, Kwasi Baah-Gyamfi[2], Joseph Ackora-Prah[3]

[1]Department of Mathematics and Computer Science
Eastern Connecticut State University
Willimantic, CT 06226, USA

[2,3]Department of Mathematics
Kwame Nkrumah University of Science and Technology
Kumasi, GHANA

Abstract: We present explicit methods of constructing finite fields using normal bases and develop a general rule for constructing Galois finite fields of the form $GF(p^n)$. We also show that optimal normal basis exist for $GF(2^n)$.

AMS Subject Classification: 11T06, 12E20, 12E30, 12F10, 12Y05
Key Words: finite fields, normal bases, irreducible polynomials

1. Introduction

We consider the construction of finite fields using normal bases. The construction of finite fields using normal bases has several advantages. In fact, this was brought to the fore by Hansel as far back as 1888 [1]. Large finite fields are used in cryptography, coding theory and computer algebra. The optimal normal bases are very important in the multiplication in finite fields because they have fewer number of terms and hence make computational programming very easy. Our discussion is focused on the normal bases for F_8, F_{16} and F_{32}.

Let E be a finite field and F be a finite Galois extension of E of degree n and Galois group G. Let $\alpha \in G$ be a normal basis for F over E. A matrix that describes the map $x \to \alpha x$ on this basis has at least $2n-1$ nonzero entries. If it contains exactly $2n-1$ nonzero entries, then the normal basis is said to

Received: February 15, 2011

§Correspondence author

be optimal, see for example [2]. A normal basis of $F = F_{q^n}$ over $E = F_q$ is a basis of the form $\{\alpha, \alpha^q, .., \alpha^{q^{n-1}}\}$ where $\alpha \in F$ and its conjugate with respect to E, is called a normal basis of F over E. The basis $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ of F_8 over F_2 is a normal basis of F_8 over F_2 since $1 + \alpha + \alpha^2 = \alpha^4$. By definition, a normal basis consists of all the algebraic conjugates of some elements 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, F_q and F_{q^n} are finite fields of q and q^n elements respectively. The field F_{q^n} is therefore viewed as an extension of F_q with F_q^* the nonzero elements of F_q. The Galois group of F_{q^n} over F_q is cyclic and is generated by the Frobenius map; $\alpha \to \alpha^q, \alpha \in F_{q^n}$.

To implement arithmetic in F_{q^n}, it suffices to have an irreducible polynomial $f \in F_q[X]$ of degree n, since $F_q[X]/(f)$, the polynomials with arithmetic performed modulo f is a finite field with q^n elements. Let n be a positive integer. The splitting field of the polynomial $x^n - 1$ over a field K is the *nth* cyclotomic field over K and it is denoted by $K^{(n)}$. The roots of $x^n - 1 \in K^{(n)}$ are the *nth* roots of unity over K and the set of all these roots is denoted by $E^{(n)}$. If F is an extension of K and $\theta \in F$ is an algebraic over K, then $K(\theta)$ is finite and therefore an algebraic extension of K.

Theorem 1. *For a prime p and a monic irreducible $f(x)$ in $F_p[x]$ of order n, the ring $F_p[x]/f(x)$ is a field of order p^n.*

It must be noted that for every prime p, the residue class ring Z/pZ forms a finite field with p elements and $Z/pZ(d)$ where d is an irreducible polynomial is a finite field.

Theorem 2. *For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F.*

Proof. (see, for example [3]) Assuming f is irreducible over F. This implies that the quotient ring $F[x]/(f)$ is a prime ideal and therefore a maximal ideal. But all maximal ideals are fields hence $F[x]/(f)$ is a field. The converse is obvious. Theorem 2 shows that if d is an irreducible polynomial in Z/pZ of degree n, then $Z/pZ(d)$ is a field with exactly p^n elements.P, the prime is the characteristic of the subfield Z_p. □

Theorem 3. *Any finite field has prime power order.*

2. Main Results

In this section we describe three different ways of representing the elements of a finite field F_q with $q = p^n$ elements, where p is the characteristic of F_q. The following theorems will help us to describe the various methods of constructing finite fields.

Theorem 4. *Let F_q be a finite field and F_{q^n} a finite extension field. Then F_{q^n} is a simple algebraic extension of F_q and every primitive element of F_{q^n} can serve as a defining element of F_{q^n} over F_q.*

Proof. (see for example [3]) Let ξ be a primitive element (the generator of the cyclic group F_q^*) of F_{q^n}. We clearly have $F_q(\xi) \subseteq F_{q^n}$. On the other hand, $F_q(\xi)$ contains 0 and all powers of ξ, and so all elements of F_{q^n}. Therefore $F_{q^n} = F_q(\xi)$. □

The following theorems are the results of Theorem 4 above.

Theorem 5. *If f is an irreducible polynomial in $F_q[x]$ of degree m, then f has α in F_{q^m}. Furthermore, all the roots of f are simple and are given by the m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, .., \alpha^{q^{m-1}}$ of F_{q^m}.*

2.1. Method 1

We see that F_q is a simple algebraic extension of F_p according to Theorem 3 above. In fact, if f is an irreducible polynomial in $F_p[x]$ of degree n, then f has a root α in F_q by Theorem 4 and so $F_q = F_p(\alpha)$

Theorem 6. *Let $\theta \in F$ be algebraic of degree n over K and let g be the minimal polynomial of θ over K. Then:*

i. $K(\theta)$ is isomorphic to $K[x]/(g)$

ii. $[K(\theta) : K] = n$ and $\{1, \theta, .., \theta^{n-1}\}$ is a basis of $K(\theta)$ over K.

iii. Every $\alpha \in K(\theta)$ is algebraic over K and its degree over K is a divisor of n.

By Theorem 5, every element of F_q can therefore be uniquely expressed as a polynomial in α over F_p of degree less than n. We can represent the elements of F_q in this way by regarding F_9 as a simple algebraic extension of F_3 of degree 2. We obtain this by adjunction of a root α of an irreducible quadratic polynomial over F_3.

The elements of F_9 are of the form $a_0 + a_1 x$ with $a_0, a_1 \in F_3$. In detail, the set of elements of F_9 is $F_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$

2.2. Method 2

The following theorems are important for our purposes.

Theorem 7. *The cyclotomic field $K^{(n)}$ is a simple algebraic extension of K. Moreover:*

i. If $K = Q$, then the cyclotomic polynomial Q_n is irreducible over K and $[K^{(n)} : K] = \Phi(n)$.

ii. If $K = F_q$ with $gcd(q, n) = 1$, then Q_n factors into $\Phi(n)/d$ distinct monic irreducible polynomials in $K[x]$ of the same degree d, $K^{(n)}$ is the splitting field of any such irreducible factor over K, and $[K^{(n)} : K] = d$, where d is the least positive integer such that $q^d \equiv 1 \ mod \ n$.

Proof. If there exists a primitive nth root of unity ξ over K, it is clear that $K^{(n)} = K(\xi)$. Otherwise, $K^{(n)} = K^{(m)}$ if p divides n for positive integer m and m does not divide p. Let η be a primitive nth root of unity over F_q. Then $\eta \in F_{q^k}$ if and only if η^{q^k} and the latter identity is equivalent to $q^k \equiv 1 \bmod n$. The smallest positive integer for which this holds is $k = d$, and so η is in F_{q^d}, but in no proper subfield thereof. Thus the minimal polynomial of η over F_q has degree d, and since η is an arbitrary root of Q_n, the desired results follow. □

Theorem 8. *The finite field F_q is the $(q-1))st$ cyclotomic field over any one of its subfields.*

Proof. The polynomial $x^{q-1} - 1$ splits in F_q since its roots are exactly all nonzero elements of F_q. Obviously, the polynomial cannot split in any proper subfield of F_q, so that F_q is the splitting field of $x^{q-1} - 1$ over any one of its subfields.

Using Theorems 6 and 7 above, we can get another possibility of expressing the elements of F_q. Let F_q be the $(q-1)st$ cyclotomic field over F_p. We construct F_q by finding the decomposition of the $(q-1)st$ cyclotomic polynomial $Q_{q-1} \in F_p[x]$ into irreducible factors in $F_p[x]$, which are all of the same degree. Any root of these factors is a primitive $(q-1)$ root of unity over F_p and therefore a primitive element of F_q. F_q therefore consists of 0 and the powers of that primitive element. □

We can apply this to the construction of F_9 by noting that $F_9 = F_3^{(8)}$ is the eighth cyclotomic field over F_3 by Theorem 7. The cyclotomic polynomial is given by $Q_8(x) = x^4 + 1 \in F_{(3)}$. Decomposing $Q_8(x)$ into irreducible factors in $F_3[x]$, we obtain the following results; $Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2)$. Let ξ be a root of $x^2 + x + 2$, then it is a primitive eighth root of unity. All the

elements of F_9 are therefore powers of ξ given by: $F_9 = 0, \xi, \xi^2, ..., \xi^8$.

In order to establish the connection with the representation in Example 2.1, we observe that $x^2 + x + 2 \in F_3[x]$ has $\xi = 1 + \alpha$ as a root, where $\alpha^2 + 1 = 0$ as in Example 2.1. The nonzero elements in F_9 are shown in the table below:

i	ξ^i	i	ξ^i
1	1+ α	5	2+2 α
2	2 α	6	α
3	1+2 α	7	2+ α
4	2	8	1

We see that we obtain the same elements as in Example 2.1 but just in a different order.

3. Optimal Normal Bases

A normal basis in $GF(p^n)$ is a basis N of the form $N = \{\beta, \beta^p, \beta^{p^2}, .., \beta^{p^{n-1}}\}$. In every finite field, there exists a normal basis. Our focus here is on optimal normal bases of F_8, F_{16} and F_{32}. We find a general rule for constructing Galois finite fields of the form $GF(p^n)$. Let $\gamma_1, \gamma_2, ..., \gamma_m \in F_{2^m}$ where $F_2 = \{0, 1\}$ such that the elements in F_{2^m} can be expressed as:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \gamma_1 + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \gamma_2 + .. + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \gamma_m.$$

Let us consider F_q where $q = 8 = 2^3$, then we have $F_8 = F_2(j)/(j^3 + j^2 + 1)$. This is a polynomial of degree three. The bases of F_8 are of the form:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} [1] + \begin{pmatrix} 0 \\ 1 \end{pmatrix} [x] + \begin{pmatrix} 0 \\ 1 \end{pmatrix} [x^2]$$

where $x^i \in F_8$ and $(0, 1) \in F_2$.

The standard form is given by $F_8 = \{(a_0.1 + a_1.j + a_2.j^2)/(j^3 + j^2 + 1 = 0)\}$, where $a_k = 0, 1 \in F_2$. We therefore have; $j^3 = j^2 + 1$, $j^4 = j^3 + j = j^2 + j + 1$ $\Rightarrow 1 = j^4 + j^2 + j$. When we consider the combinations of j^1, j^2, j^4, then all the elements of F_8 can be represented by $a_1 j + a_2 j^2 + a_3 j^4$. But $a_1 j + a_2 j^2 + a_3(J^2 + j + 1) = a_3 1 + (a_1 + a_2)j + (a_2 + a_3)j^2$ where $j^4 = j^2 + j + 1$. Coding gives, $x = a_1 j + a_2 j^2 + a_3 j^4 \rightarrow (a_1, a_2, a_3)$. The addition of the basis is the standard component vector addition.

Squaring, we have $(A + B)^2 = A^2 + B^2$ over F_2 since $a + a = 0$ over F_2. Hence:

$$(a_1, a_2, a_3)^2 \quad = \quad (a_1 j + a_2 j^2 + a_3 j^4)^2$$

$$\begin{aligned} &= (a_1 j)^2 + (a_2 j^2)^2 + (a_3 j^4)^2 \qquad (1)\\ &= a_1 j + a_2 j^4 + a_3 j^8. \end{aligned}$$

But $j^8 = j$ and so $F_2 = a_3 j + a_1 j^2 + a_2 j^4 \rightarrow (a_3, a_1, a_2)$ The normal base over F_2 is given by $\gamma, \gamma^2, \gamma^{2^2}, \gamma^{2^3}$ ...

3.1. Multiplication in F_{2^m} using Normal Bases

First, we want to consider multiplication in F_8. Let $q = 8 = 2^3$, then $F_8 = F_2(j)/(j^3 + j^2 + 1)$. This is a third degree polynomial. But we know that $1 = j^4 + j^2 + j$, we therefore use the bases j, j^2, j^4. $j^3 + j^2 + 1 = 0 \Rightarrow j^3 = j^2 + 1$ Multiplying through the equation by j, we have $j^4 = j^3 + j \Rightarrow j^3 = j^4 + j$. Adding these bases we have $100 + 001 = 101 = j^3$. We have $j^5 = j^4 + j^2 = 100 + 010 = 110$.

We can represent these manipulations on a multiplication table below:

$\otimes$	j	j^2	j^4
	(001)	(010)	(100)
(001)	(010)	(101)	(110)
(010)	(101)	(100)	(011)
(100)	(110)	(011)	(001)

Next, we consider $q = 16$ thus, $F_{16} = F_2(j)/(j^4 + j^2 + j + 1)$ and see if the normal basis exists. We have the bases such as j, j^2, J^4, j^4, then $a = j + j^2 + j^4 + j^8 = 1111$. When we square, we get

$$\begin{aligned} (j + j^2 + j^4 + j^8)^2 &= j^2 + j^4 + j^8 + j^{16}\\ &= j^2 + j^4 + j^8 \end{aligned}$$

This shows that j is the root of the polynomial $x^8 + x^4 + x^2 + x + 1 = 0$. We can therefore factorize the polynomial into two irreducible polynomials.

Thus, $x^8 + x^4 + x^2 + x + 1 = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$. In this case, we have two choices with two multiplication tables.

Phase 1: $f(x) = x^4 + x^3 + 1$,

$\otimes$	j	j^2	j^4	j^8
	(0001)	(0010)	(0100)	(1000)
(0001)	(0010)	(1011)	(0101)	(1101)
(0010)	(1011)	(0100)	(0111)	(1010)
(0100)	(0101)	(0111)	(1000)	(1110)
(1000)	(1101)	(1010)	(1110)	(0001)

Phase 2: $f(x) = x^4 + x^3 + x^2 + x + 1$

$\otimes$	j	j^2	j^4	j^8
	(0001)	(0010)	(0100)	(1000)
(0001)	(0010)	(1000)	(1111)	(0100)
(0010)	(1000)	(0100)	(0001)	(1111)
(0100)	(1111)	(0001)	(1000)	(1101)
(1000)	(0100)	(1111)	(0010)	(0001)

From the two tables above, we see that the optimal normal basis for $q = 16$ exists. Finally, we consider $q = 32 = 2^5$ which are polynomials of degree five. The basis of F_{2^5} is $\{j, j^2, j^4, j^8, j^{16}\}$. We have a polynomial of degree sixteen which factors into three irreducible polynomials given below:

$$x^{16} + x^8 + x^4 + x^2 + x + 1$$
$$= (x+1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1).$$

The following are the corresponding multiplication tables:

Phase 1: $f(x) = x^5 + x^4 + x^2 + x + 1$

$\otimes$	j	j^2	j^4	j^8	j^{16}
	(00001)	(00010)	(00100)	(01000)	(10000)
(00001)	(00010)	(10110)	(11000)	(00110)	(10100)
(00010)	(01001)	(00100)	(10010)	(10001)	(01100)
(00100)	(11000)	(10010)	(01000)	(00101)	(00011)
(01000)	(00110)	(10001)	(00101)	(10000)	(01010)
(10000)	(10100)	(01100)	(00011)	(01010)	(00001)

Phase 2: $f(x) = x^5 + x^4 + x^3 + x + 1$

$\otimes$	j	j^2	j^4	j^8	j^{16}
	(00001)	(00010)	(00100)	(01000)	(10000)
(00001)	(00010)	(10100)	(01110)	(10011)	(01010)
(00010)	(10100)	(00100)	(01001)	(11100)	(00111)
(00100)	(01110)	(01001)	(01000)	(10010)	(11001)
(01000)	(11100)	(10010)	(10010)	(10000)	(00101)
(10000)	(01010)	(00111)	(11001)	(00101)	(00001)

Phase 3: $f(x) = x^5 + x^4 + x^3 + x^2 + 1$

$\otimes$	j	j^2	j^4	j^8	j^{16}
	(00001)	(00010)	(00100)	(01000)	(10000)
(00001)	(00010)	(01110)	(10111)	(11011)	(00111)
(00010)	(01110)	(00100)	(11100)	(01111)	(10111)
(00100)	(10111)	(11100)	(01000)	(11001)	(11110)
(01000)	(11101)	(01111)	(11001)	(10000)	(10011)
(10000)	(00111)	(10111)	(11110)	(10011)	(00001)

We conclude from the tables above that the optimal normal basis exists for F_{32}.

4. General Rule for Constructing Finite Fields

Using the above normal basis, we develop the general rule for constructing finite fields. Let us consider $b_i a_i \beta^{2i}$, where $b_i, a_i \in F_2$ and $\beta \in F_{2^3}$, then we have the following expression:

$$(a_0\beta+a_1\beta^2+a_2\beta^4+a_3\beta^8)(b_0\beta+b_1\alpha^2+b_2\beta^4+b_3\beta^8) = a_0b_0\beta^2+a_1b_1\beta^4+...+a_3b_3\beta^{16}$$

We use the F_{2^3} multiplication table below:

$\otimes$	j	j^2	j^4	j^8
	(0001)	(0010)	(0100)	(1000)
(0001)	(0010)	(1011)	(0101)	(1101)
(0010)	(1011)	(0100)	(0111)	(1010)
(0100)	(0101)	(0111)	(1000)	(1110)
(1000)	(1101)	(1010)	(1110)	(0001)

Using the expressions $a_i\beta^{2i}$ and $b_i\beta^{2i}$, where $a_i, b_i \in F_2$ and $\beta \in F_8$ for $i = 0, 1, 2, 4$, we have:

$$\begin{aligned}(a_0\beta + a_1\beta^2 + a_2\beta^4 + a_3\beta^8)(b_0\beta + b_1\beta^2 + b_2\beta^4 + b_3\beta^8 \\ = a_0b_0\beta.\beta + a_0b_1\beta.\beta^2 + a_0b_2\beta.\beta + ... + a_3b_3\beta^8.\beta^8.\end{aligned}$$

We deduce the following from the above expression using the multiplication table for F_{2^3} above.

$$\begin{aligned} a_0b_0\beta.\beta &= (0010) \\ &= a_0b_0(\beta^2) \end{aligned}$$

$$a_0b_1\beta.\beta^2 = a_0b_1(1011)$$

$$\begin{aligned} &= a_0b_1(\beta^8+\beta^2+\beta) \\ &= a_0b_1\beta^8+a_0b_1\beta^2+a_0b_1\beta \end{aligned}$$

$$\begin{aligned} a_0b_2\beta.\beta^4 &= a_0b_2(0101) \\ &= a_0b_2(\beta^4+\beta) \\ &= a_0b_2\beta^4+a_0b_2\beta \end{aligned}$$

$$\begin{aligned} a_0b_3\beta.\beta^8 &= a_0b_3(1101) \\ &= a_0b_3(\beta^8+\beta^4+\beta) \\ &= a_0b_3\beta^8+a_0b_3\beta^4+a_0b_3\beta. \end{aligned}$$

$$\begin{aligned} a_1b_0\beta^2.\beta &= a_1b_0(1011 \\ &= a_1b_0(\beta^8+\beta^2+\beta) \\ &= a_1b_0\beta^8+a_1b_0\beta^2+a_1b_0\beta \end{aligned}$$

$$\begin{aligned} a_1b_2\beta^2.\beta^4 &= a_1b_2(0111) \\ &= a_1b_2(\beta^4+\beta^2+\beta) \\ &= a_1b_2\beta^4+a_1b_2\beta^2+a_1b_2\beta \end{aligned}$$

$$\begin{aligned} a_2b_0\beta^4.\beta &= a_2b_0(0101) \\ &= a_2b_0(\beta^4+\beta) \\ &= a_2b_0\beta^4+a_2b_0\beta. \end{aligned}$$

$$\begin{aligned} a_2b_2\beta^4.\beta^4 &= a_2b_2(1000) \\ &= a_2b_2\beta^8. \end{aligned}$$

$$\begin{aligned} a_3b_0\beta^8.\beta &= a_3b_0(1101) \\ &= a_3b_0(\beta^8+\beta^4+\beta) \\ &= a_3b_0\beta^8+a_3b_0\beta^4+a_3b_0\beta. \end{aligned}$$

$$\begin{aligned} a_3b_2\beta^8.\beta^4 &= a_3b_2(1110) \\ &= a_3b_2(\beta^8+\beta^4+\beta^2) \end{aligned}$$

$$= a_3b_2\beta^8 + a_3b_2\beta^4 + a_3b_2\beta^2$$

$$\begin{aligned} a_1b_1\beta^2.\beta^2 &= a_1b_1(0100) \\ &= a_1b_1\beta^4 \end{aligned}$$

$$\begin{aligned} a_1b_3\beta^2.\beta^8 &= a_1b_3(1010) \\ &= a_1b_3(\beta^8 + \beta^2) \\ &= a_1b_3\beta^8 + a_1b_3\beta^2 \end{aligned}$$

$$\begin{aligned} a_2b_1\beta^4.\beta^2 &= a_2b_1(0111) \\ &= a_2b_1(\beta^4 + \beta^2 + \beta) \\ &= a_2b_1\beta^4 + a_2b_1\beta^2 + a_2b_1\beta. \end{aligned}$$

$$\begin{aligned} a_2b_3\beta^4.\beta^8 &= a_2b_3(1110) \\ &= a_2b_3(\beta^8 + \beta^4 + \beta^2) \\ &= a_2b_3\beta^8 + a_2b_3\beta^4 + a_2b_3\beta^2. \end{aligned}$$

$$\begin{aligned} a_3b_1\beta^8.\beta^2 &= a_3b_1(1010) \\ &= a_3b_1(\beta^8 + \beta^2) \\ &= a_3b_1\beta^8 + a_3b_1\beta^2. \end{aligned}$$

$$\begin{aligned} a_3b_3\beta^8.\beta^8 &= a_3b_3(0001) \\ &= a_3b_3\beta^{16} \\ &= a_3b_3\beta. \end{aligned}$$

Grouping the above expressions, we obtain the following:

$$\beta(a_0b_1 + a_0b_2 + a_0b_3 + a_1b_0 + a_1b_2 + a_2b_0 + a_2b_1 + a_3b_0 + a_3b_3)+$$

$$\beta^2(a_0b_0 + a_0b_1 + a_1b_0 + a_1b_2 + a_1b_3 + a_2b_1 + a_3b_2 + a_2b_3 + a_3b_1)+$$

$$\beta^4(a_0b_1 + a_0b_3 + a_1b_1 + a_2b_0 + a_2b_1 + a_2b_3 + a_3b_0 + a_3b_2)+$$

$$\beta^8(a_0b_1 + a_0b_3 + a_1b_0 + a_1b_3 + a_2b_2 + a_2b_3 + a_3b_0 + a_3b_1 + a_3b_2).$$

Now for every $A, B \in GF(p^n)$ may be uniquely expressed as

$$B = \sum_{i=1}^{n-1} b_i \beta^{p^i},\ b_i \in F_2 \quad \text{and} \quad A = \sum_{i=1}^{n} a_i \beta^{p^i},\ a_i \in F_2$$

.

Let

$$\begin{aligned} C &= AB \\ &= \Sigma_{i=1}^{n-1} c_i \beta^{p^i} \\ &= (\Sigma_{i=1}^{n-1} a_i \beta^{p^i})(\Sigma_{j=0}^{n-1} b_j \beta^{p^i}) \\ &= \Sigma_{i=0}^{n-1} \Sigma_{j=0}^{n-1} (a_i b_j \beta^{p^i}.\beta^{p^i}). \end{aligned}$$

The above expression gives a general rule for constructing finite fields. We deduce from the above tables that optimal normal basis exists for $GF(2^n)$ where n is a positive integer. With the above rule one can therefore construct Galois finite field using normal basis.

References

[1] K. Hansel, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, *J. Reine Angew Math.*, **103** (1888), 230-237.

[2] Onyszchulk Mullin, Wilson Van-Stone, *Discrete Application Math.* (1988/89), 149-161.

[3] Lidl Rudolf, Neiderreiter Harald, *Introduction to Finite Fields and their Applications*, Cambridge University Press (1994).

570