International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 12 No. I (April, 2018), pp. 1-13

FINDING NORMAL BASES OVER FINITE FIELDS USING PRESCRIBED TRACE VECTORS

P. L. SHARMA[1] AND KIRAN DEVI[2]
[1,2] Department of Mathematics and Statistics,
Himachal Pradesh University, Shimla 171 005, India

Abstract

Normal bases are widely used in various cryptographic functions and algorithms to provide the confidentiality, integrity and security to the messages. These are important in efficient computation of the arithmetic of finite fields. Let α be a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and the vector $u = \{u_0, u_1, ..., u_{n-1}\}$ is symmetric if $u_i = u_{n-i}$ for all $1 \leq i \leq n-1$. We show that there exists a normal element α corresponding to a prescribed vector u such that $u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1})$ for $0 \leq i \leq n-1$, where n is positive integer if and only if vector u is symmetric and $u_0 = 1$, $\sum u_i = 1$, for odd $n \geq 3$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^m}$ be the subfield of $\mathbb{F}_{q^n}$. If $\alpha \in \mathbb{F}_{q^n}$ and $\left\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\right\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then the basis is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and α is a normal element, see [5]. For any positive integer n, and m dividing n, the trace function from $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, denoted by Tr_m^n is the mapping defined as

---

Key Words : *Trace function, Hamming weight, Symmetric vector.*

2010 AMS Subject Classification : 11T71, 12E20, 12E30.

 UGC approved journal (Sl No. 48305)

$$Tr_m^n(\alpha) = \sum_{i=0}^{\frac{n}{m}-1} \alpha^{2^{im}} = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + ... + \alpha^{2^{n-m}}. \tag{1.1}$$

Normal bases of finite fields are discussed briefly in [1, 5, 12, 17, 19]. The normal basis theorem is discussed along with proof in [13]. Due to the fast arithmetic computational properties of normal bases over finite fields they are used in cryptography, hardware and software multipliers . Normal bases design simple and fast multipliers of finite fields, see [20]. Massey and Omura [6, 8] used the normal bases over the finite fields with characteristic 2. Low complexity self dual normal basis multiplier over $\mathbb{F}_2$ is discussed by Wang [3]. Normal bases are also used for doing arithmetic operations, exponentiation processes in all applications of computers, see [8, 11, 15]. Self dual normal bases are used in cryptographic algorithims, but they do not exist for every finite field extension. Therefore, the trace self-orthogonal relation can be used in place of self dual normal bases in that case. The self dual normal basis Theorem [2] states that there is a self dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if either q and n are odd or q is even and $n \neq 0 \pmod 4$.

The number of non zero entries in the prescribed trace vector gives the hamming weight of the corresponding normal element. Generally, normal bases having low hamming weight are used to reduce the cycle bit shift operations in arithmetic processes and trace computations. At present irreducible polynomials over finite fields are used in all applications of computers. Different constructions of irreducible polynomials are discussed in [9,10]. A polynomial

$$f(x) = u_0 + u_1 x + u_2 x^2 + ... + u_{n-1} x^{n-1} \tag{1.2}$$

is said to be symmetric if $u_i = u_{n-i}$ for all $1 \leq i \leq n-1$. The reciprocal polynomial of

$$q(x) = \sum_{0 \leq i \leq n-1} u_i x^i \in \mathbb{F}_{2^n}[x]/(x^n - 1) \tag{1.3}$$

is defined as the polynomial

$$q^*(x) = \sum_{0 \leq i \leq n-1} u_i x^{n-i} (\text{mod } x^n - 1). \tag{1.4}$$

The corresponding vector u of the element $\alpha \in \mathbb{F}_{q^n}$ is obtained from the trace self orthogonal relations. The selection of good self- orthogonal relations of normal bases

means that there exists more simple relation between Boolean and trace function, see [20]. When α is taken from normal basis set then the function $f(\alpha) = Tr_{2^n|2}(\alpha^m) \in \mathbb{F}_{2^n}$, where $1 < m < 2^n - 1$, becomes the rotation symmetric Boolean function. Therefore, cryptographic algorithms are also studied by using rotation symmetric Boolean function, see [18]. We consider the ring $\mathbb{F}_2[x]/(x^n - 1)$ for the arithmetic of all polynomials and give some lemmas and theorems related to this ring.

2. Main Results

The prescribed vector $u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1})$ is symmetric vector and the polynomials formed by the coefficients of this vector are also symmetric. Therefore, the [Lemma 2.4, 20] and [Theorem 2.5, 20] also holds true for this prescribed vector u_i. By using this fact we have the following theorems and lemmas.

Theorem 2.1 For odd $n \geq 3$, suppose that

$$p(y) = \sum_{0 \leq i \leq n-1} u_i y^i \in \mathbb{F}_2[y]/(y^n - 1)$$

with $u_0 = 1$. Then $p(y) = q(y)\ q^*(y)$ for some

$$q(y) = \sum_{0 \leq i \leq n-1} v_i y^i \in \mathbb{F}_2[y]/(y^n - 1)$$

if and only if $p(y) \in P(y)$, where

$$P = \left\{ p(y) = \sum_{0 \leq i \leq n-1} u_i y^i \in \mathbb{F}_2[y]/(y^n - 1) \;\middle|\; \begin{array}{c} \sum_{0 \leq i \leq n-1, (i,2)=1} u_i = 1, \\ u_0 = 1, \\ u_i = u_{n-i} \text{ for } 1 \leq i \leq n-1. \end{array} \right\}, \quad (2.1)$$

Also, $p(y) \in P(y)$ has a unique factorization $p(y) = q(y)\ q^*(y)$ for some $q(y) \in Q$, where,

$$Q = \left\{ q(y) = \sum_{0 \leq i \leq n-1} v_i y^i \in \mathbb{F}_2[y]/(y^n - 1) \;\middle|\; \begin{array}{c} v_0 = 1, v_{n-1} \neq 0, \\ v_2 = 0, v_1 \neq 0 \\ \text{and } \ v_i = v_{n-1-i} \\ \text{for } 1 \leq i \neq 2 \leq n-1. \end{array} \right\}. \quad (2.2)$$

Proof Let us assume that

$$p(y) = q(y)q^*(y) \quad (2.3)$$

for some

$$q(y) = \sum_{0 \leq i \leq n-1} v_i y^i \in \mathbb{F}_2[y]/(y^n - 1).$$

Since, $p(y) = q(y)\ q^*(y)$ is equivalent to the following system of equations

$$\left\{ \begin{array}{c} p_0(y_0, y_1, ..., y_{n-1}) = y_0 + y_1 + ... + y_{n-1} = 1, \\ p_j(y_0, y_1, ..., y_{n-1}) = \sum\limits_{0 \le i \le n-1} y_i y_{i+j} = u_{n-j}, 1 \le j \le n-1 \end{array} \right\}. \tag{2.4}$$

For $1 \le j \le n-1$, it follows from (2.1) and (2.3) that

$$\begin{aligned} p_j(y_0, y_1, ..., y_{n-1}) &= u_{n-j}, \\ &= y_0 y_j + y_1 y_{1+j} + y_2 y_{2+j} + ... + y_{n-1} y_{j-1} \\ &= y_0 y_{n-j} + y_1 y_{n-j+1} + y_2 y_{n-j+2} + ... + y_{n-1} y_{n-j-1} \\ &= u_j \\ &= p_{n-j}(y_0, y_1, ..., y_{n-1}). \end{aligned} \tag{2.5}$$

It is clear from (2.2) and (2.3) that $v = (v_0, v_1, ..., v_{n-1}) \in \mathbb{F}_{2^n}$ is the solution of (2.5) and hence the solution of (2.4). Therefore, first part of (2.4) gives

$$p_0(v_0, v_1, ..., v_{n-1}) = v_0 + v_1 +, ..., + v_{n-1}.$$

Also for $\mathbb{F}_{2^n}$

$$\left(\sum_{(i,2)>1} v_i \right) + \left(\sum_{(i,2)=1} v_i \right) = 0$$

and

$$\left(\sum_{(i,2)>1} v_i \right) . \left(\sum_{(i,2)=1} v_i \right) = 1 \tag{2.6}$$

Using second part of (2.4) and (2.6), we have

$$\begin{aligned} \left(\sum_{(i,2)>1} v_i \right) . \left(\sum_{(i,2)=1} v_i \right) &= \sum_{0 \le j \le n-1} \ \sum_{0 \le i \le n-1} v_i v_{i+j} \\ &= \sum_{0 \le j \le n-1} p_j(v_0, v_1, ..., v_{n-1}) \\ &= \sum_{0 \le j \le n-1} u_j = 1. \end{aligned} \tag{2.7}$$

This completes the necessary part. In order to prove the sufficient part, firstly we prove that the mapping

$$R : R(q(y)) = q(y) q^*(y),\ q(y) \in \mathbb{F}_2[y]/(y^n - 1)$$

is one-one from Q to P. For this, it is sufficient to prove that

$$R^{'} : R^{'}(y_0, y_1, ..., y_{n-1}) = (p_0(y_0, y_1, ..., y_{n-1}), ..., p_{n-1}(y_0, y_1, ..., y_{n-1}))$$

is one-one mapping from $Q^{'}$ to $P^{'}$, where

$$p_j(y_0, y_1, ..., y_{n-1}) = \sum_{0 \le i \le n-1} y_i y_{i+j} \text{ for } 1 \le j \le n-1$$

and

$$P^{'} = \left\{ (z_0, z_1, ..., z_{n-1}) \in \mathbb{F}_{2^n} \;\middle|\; \begin{array}{c} \sum_{0 \le i \le n-1} z_i = 1, \\ z_0 = 1 \text{ and} \\ z_i = z_{n-i} \text{ for } 1 \le i \le n-1. \end{array} \right\},$$

$$Q^{'} = \left\{ (y_0, y_1, ..., y_{n-1}) \in \mathbb{F}_{2^n} \;\middle|\; \begin{array}{c} y_0 = 1, y_{n-1} = 1, \\ y_2 = 0, y_{n-2} = 0 \text{ and} \\ y_i = y_{n-i} \text{ for } 1 \le i \le n-1. \end{array} \right\}. \tag{2.8}$$

Now, we show that the Boolean system in equation (2.4) is linear for $(y_0, y_1, ..., y_{n-1}) \in Q^{'}$. In order to prove this, we consider the following cases:

Case I. For $1 \le j \le n-1, (j, 2) > 1$, the n items $y_i y_{i+j}$ in

$$p_j(y_0, y_1, ..., y_{n-1}) = \sum_{0 \le i \le n-1} y_i y_{i+j} \tag{2.9}$$

can be seperated into $\frac{n-1}{2}$ pairs and one term remains unpaired. These pairs are $y_i y_{i+j}$, $y_{(n-i-1-j)} y_{n-i-1}$ and the unpair term is $y_{\frac{(n-1-j)}{2}} y_{\frac{(n+j-1)}{2}+j}$. Since $(y_0, y_1, ..., y_{n-1}) \in Q^{'}$ therefore $y_i = y_{n-i}$, $y_{i+j} = y_{n-i-j}$ for $i \neq 0$. Thus $y_0 y_j = y_j$ and $y_{n-i} y_{n-1} = y_{n-1}$. As $(j, 2) > 1$, therefore j must be even. The pairs $y_i y_{i+j}$, $y_{(n-i-1-j)} y_{n-i-1}$ are different for all $i \ge n - (j+1)/2$, $i \le (n-j)/2$ and hence the congruence equation $i \equiv n - i - 1 - j (\text{mod } n)$ has solution which is not possible for even j.

Therefore, we have

$$\begin{aligned} p_j(y_0, y_1, ..., y_{n-1}) &= \sum_{0 \le i \le n-1} y_i y_{i+j} \\ &= \sum_{0 \le i \le (n-j)/2, i \ge n-(j+1)/2, \, i \neq 0, \, n-j} y_i y_{i+j} + y_{n-i-1-j} y_{n-i-1} \\ &\quad + y_0 y_j + y_{n-1-j} y_{n-1} + y_0 y_{n-j} + y_{n-1-(n-j)} y_{n-1} + \\ &\quad + y_{\frac{(n-1-j)}{2}} y_{\frac{(n+j-1)}{2}+j} \\ &= y_j + y_{j-1} + y_{\frac{(n-1-j)}{2}} y_{\frac{(n+j-1)}{2}+j}. \end{aligned} \tag{2.10}$$

Case II. For $1 \leq j \leq n-1, (j,2) = 1$ there are two solutions $i = (n-j)/2, n-(j+1)/2$ of the equation $i \equiv n-i-1-j (\text{mod } n)$. In this case the pairs $y_i y_{i+j}$, $y_{(n-i-1-j)} y_{n-i-1}$ are equal and hence their sum over $\mathbb{F}_2$ is zero. Therefore,

$$p_j(y_0, y_1, ..., y_{n-1}) = \sum_{0 \leq i \leq n-1} y_i y_{i+j}$$

can be seperated into $\frac{(n-3)}{2} + 1$ pairs and remaining one term left unpaired. Since j is odd, therefore

$$\begin{aligned} p_j(y_0, y_1, ..., y_{n-1}) &= \sum_{0 \leq i \leq n-1} y_i y_{i+j} \\ &= \sum_{0 \leq i < (n-j)/2, i > n-(j+1)/2, i \neq 0, n-j} y_i y_{i+j} + y_{n-i-1-j} y_{n-i-1} \\ &\quad + y_{(n-j)/2} y_j + y_{n-1-j} y_{n-1} + y_0 y_{n-j} + y_{n-1-(n-j)} y_{n-1} \\ &\quad + y_{\frac{(n-1-j)}{2}} y_{\frac{(n+j-1)}{2}+j} \\ &= y_j + y_{j-1} + y_{\frac{n-j}{2}} + y_{\frac{j-1}{2}} + y_{\frac{j+1}{2}}. \end{aligned}$$

Case III. For $j = 0$, clearly $y_i + y_{n-1-i} = 0$ and $y_n + y_{n-1} = 1$ as $(y_0, y_1, ..., y_{n-1}) \in Q'$. This implies that $p_0(y_0, y_1, ..., y_{n-1}) = 1$.

Combining the above cases, for $(y_0, y_1, ..., y_{n-1}) \in Q'$ we have the following set of equations:

$$\begin{cases} z_0 = p_0(y_0, y_1, ..., y_{n-1}) = 1 \\ z_1 = p_1(y_0, y_1, ..., y_{n-1}) = y_1 + y_{\frac{n-1}{2}} \\ z_2 = p_2(y_0, y_1, ..., y_{n-1}) = y_2 + y_1 \\ z_3 = p_3(y_0, y_1, ..., y_{n-1}) = y_3 + y_{\frac{n-3}{2}} + y_2 + y_1 \\ z_4 = p_4(y_0, y_1, ..., y_{n-1}) = y_4 + y_3 + y_1 \\ z_5 = p_5(y_0, y_1, ..., y_{n-1}) = y_5 + y_{\frac{n-5}{2}} + y_4 + y_3 + y_2 \\ \vdots \\ z_j = p_j(y_0, y_1, ..., y_{n-1}) = y_j + y_{j-1} + y_{\frac{j-1}{2}}, \text{where } n \text{ is even } (\geq 2) \\ z_j = p_j(y_0, y_1, ..., y_{n-1}) = y_j + y_{j-1} + y_{\frac{n-j}{2}} + y_{\frac{j-1}{2}} + y_{\frac{j+1}{2}}, \text{ where } n \text{ is odd } (\geq 3). \end{cases} \tag{2.11}$$

Therefore, the set of equations (2.11) concludes that

$$\begin{aligned}\sum_{1\leq j\leq n-1,(j,2)=1} z_j &= p_1+p_2+...+p_{n-1}\\ &= \sum_{1\leq i\leq n-1,(i,2)=1} y_i + \sum_{1\leq i\leq n-1,(i,2)\neq 1} y_i\\ &= 1. \end{aligned} \tag{2.12}$$

Thus, for all $(y_0, y_1, ..., y_{n-1}) \in Q^{'}$the system of equations $R'(y_0, y_1, ..., y_{n-1}) \in P^{'}$, that is, for all $q(y) \in Q^{'}$ the system of equations $R(q(y)) \in P$. Therefore, equations (2.11) and (2.12) show that $R(q(y))$ coefficients are different for different $q(y) \in Q$. Thus we get $R(Q) = P$ and it has unique factorization $p = q.q^*$ for some $q \in Q$.

Lemma 2.2 Let n be an odd positive integer such that

$$f_u(x) = \sum_{0\leq i\leq n-1} u_i x^i \in \mathbb{F}_2[x]/(x^n-1)$$

and

$$f_v(x) = \sum_{0\leq i\leq n-1} v_i x^i \in \mathbb{F}_2[x]/(x^n-1)$$

be symmetric polynomials with $u_0 = 1$, $v_0 = 1$, $\sum u_i = 1$ and $\sum v_i = 1$. Also, we suppose that

$$f_w(x) = f_u(x)f_v(x) = \sum_{0\leq i\leq n-1} w_i x^i \in \mathbb{F}_2[x]/(x^n-1), \tag{2.13}$$

then

$$\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} w_i = \sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} (u_i+v_i) \tag{2.14}$$

and $w_0 = 1, \sum w_i = 1$.

Proof Since $f_u(x)$ and $f_v(x)$ are symmetric polynomials, therefore by [Lemma 2.4, 20], $f_w(x)$ is also symmetric polynomial. For symmetric polynomial $f_u(x)$, we have

$$\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} u_i = \sum_{\frac{n+1}{2}\leq i\leq n-1,(i,2)=2} u_i \ ,$$

and

$$\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=2} u_i = \sum_{\frac{n+1}{2}\leq i\leq n-1,(i,2)=1} u_i \ .$$

Also, for symmetric polynomial $f_v(x)$, we have

$$\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} v_i = \sum_{\frac{n+1}{2}\leq i\leq n-1,(i,2)=2} v_i \ ,$$

and

$$\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=2} v_i = \sum_{\frac{n+1}{2}\leq i\leq n-1,(i,2)=1} v_i \ .$$

Since n is odd, therefore, the even exponent terms in $\sum_{0\leq i\leq n-1} w_i x^i$ are obtained by multiplying the coefficients of $u_j x^j$ in $f_u(x)$ and $v_k x^k$ in $f_v(x)$ under the condition $j \equiv k(\text{mod } 2)$. Therefore,

$$\begin{aligned}\sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} w_i &= 2 \sum_{1\leq j\leq \frac{n-1}{2},(j,2)=1} u_j \sum_{1\leq k\leq \frac{n-1}{2},(i,2)=1} v_k \\ &\quad +2 \sum_{1\leq j\leq \frac{n-1}{2},(j,2)=2} u_j \sum_{1\leq k\leq \frac{n-1}{2},(k,2)=2} v_k \\ &\quad + \sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} u_i + \sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} v_i \qquad (2.15) \\ &= \sum_{1\leq i\leq \frac{n-1}{2},(i,2)=1} (u_i + v_i).\end{aligned}$$

Also for $u_0 = 1, v_0 = 1$ we have $w_0 = 1$. Since $\sum u_i = 1$ and $\sum v_i = 1$, therefore, the number of terms in $f_u(x)$ and $f_v(x)$ are odd and hence the polynomial $f_w(x) = f_u(x).f_v(x)$ will also have odd number of terms. This concludes that $\sum w_i$ is also equal to 1.

Theorem 2.3 : Let $n \geq 3$ be odd positive integer then their exists a normal element α of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ coresponding to vector $u = (u_0, u_1, u_2, ..., u_{n-1}) \in \mathbb{F}_{2^n}$ such that $u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1})$ for $0 \leq i \leq n-1$ if and only if u is symmetric with $u_0 = 1$, and $\sum u_i = 1$.

Proof : Since α is a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and its corresponding vector is $u = (u_0, u_1, u_2, ..., u_{n-1}) \in \mathbb{F}_{2^n}$, then

$$u_0 = Tr_{2^n|2}(\alpha^{2^{2\times 0}-2^0+1}) = Tr_{2^n|2}(\alpha) = 1 \qquad (2.16)$$

and

$$u_i = Tr_{2^n|2}(\alpha.\alpha^{2^{2i}-2^i}) = Tr_{2^n|2}(\alpha.\alpha^{2^{2(n-i)}-2^{n-i}}) = u_{n-i} \qquad (2.17)$$

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

$$s = \sum_{0 \leq i \leq n-1, (i,2)=1} \alpha^{2^{2i}-2^i+1}$$

and

$$t = \sum_{0 \leq j \leq n-1, (j,2)=2} \alpha^{2^{2j}-2^j+1}.$$

then $s + t = 1$. Also, $Tr_{2^n|2}(\alpha) = u_0 = 1$. Therefore,

$$\begin{aligned} \sum u_i &= \sum_{0 \leq i \leq n-1, (i,2)=1} \alpha^{2^{2i}-2^i+1} + \sum_{0 \leq j \leq n-1, (j,2)=2} \alpha^{2^{2j}-2^j+1} \\ &= 1. \end{aligned} \tag{2.18}$$

In order to prove the sufficient part we consider that the vector $u = (u_0, u_1, u_2, ..., u_{n-1})$ $\in \mathbb{F}_{2^n}$ which satisfies the conditions $u_0 = 1$, $u_i = u_{n-i}$ for all $1 \leq i \leq n-1$, $\sum u_i = 1$, and

$$u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1}),\ 0 \leq i \leq n-1.$$

The corresponding polynomial to u_i is

$$f_u(x) = \sum_{0 \leq i \leq n-1} u_i x^i.$$

Normal basis theorem [14] states that there exists a normal element β corresponding to $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Therefore,

$$f_v(x) = \sum_{0 \leq i \leq n-1} v_i x^i$$

is the polynomial corresponding to the normal element β, where the v_i coefficients of the polynomial are given by

$$v_i = Tr_{2^n|2}(\beta^{2^{2i}-2^i+1}).$$

It follows that $v_0 = 1, \sum v_i = 1$. This concludes that $f_v(x)$ is symmetric and hence $(f_v(x), x^n - 1) = 1$. The [Lemma 2.3, 20] suggests that $f_v^{-1}(x) = \sum_{0 \leq i \leq n-1} v_i' x^i$ is also symmetric with $v_0' = 1$ and relatively prime to $x^n - 1$. Also, for the polynomial ring $\mathbb{F}_2[x]/(x^n - 1)$, we have

$$f_v(x) f_v^{-1}(x) = 1. \tag{2.19}$$

Using (2.19) and Lemma 2.2, we obtain

$$\sum_{1\leq i\leq n-1,\ (i,2)=1} v_i + v_i' = 0.$$

This implies that

$$\sum_{1\leq i\leq n-1,(i,2)=1} v_i^{'} = \sum_{1\leq i\leq n-1,(i,2)=1} v_i = 1.$$

Since $f_u(x)$, $f_v^{-1}(x)$ are symmetric. Therefore by [Lemma 2.4, 20]

$$p(x) = f_u(x)f_v^{-1}(x) = \sum_{0\leq i\leq n-1} p_i x^i \in \mathbb{F}_2[x]|(x^n-1) \tag{2.20}$$

is also symmetric. Using Lemma 2.2, we have $p_0 = 1, \sum p_i = 1$ and

$$\sum_{1\leq i\leq n-1,(i,2)=1} p_i = \sum_{1\leq i\leq n-1,(i,2)=1} v_i' + u_i = 0.$$

This concludes that $p(x) \in P$ as discussed in Theorem 2.1, and hence $p(x)$ has unique factorization $q(x)q^*(x)$. Therefore the solution of

$$q(x) = \sum_{0\leq i\leq n-1} w_i x^i \in Q$$

is also the solution of $p(x)$. Let $\alpha = \sum_{0\leq i\leq n-1} w_i \beta^{2^i}$, then according to the [Theorem 2.2.6, 20], α is a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and using [Theorem 2.5, 20] in (2.20), we obtain

$$f_u(x) = f_v(x)g(x)g^*(x). \tag{2.21}$$

which concludes that the corresponding vector for the normal element α is $(u_0, u_1, u_2, ..., u_{n-1})$.

Algorithm :

The following algorithm is used to find a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ corresponding to a given vector $u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2i+1})$ for all $0 \leq i \leq n-1$.

Input: $u = (u_0, u_1, ..., u_{n-1}) \in \mathbb{F}_{2^n}$.

1. Take n as odd, we check whether $(u_0, u_1, ..., u_{n-1}) \in \mathbb{F}_{2^n}$ satisfies $u_0 = 1$, $u_i = u_{n-i}$ for $1 \leq i \leq n-1$ and $\sum u_i = 1$. If this is not the case then output "There is not such a normal element".

2. Find a normal element β of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

3. Compute the vector set $(v_0, v_1, ..., v_{n-1})$ where $v_j = Tr_{2^n|2}(\alpha^{2^{2j}-2j+1})$ for all $0 \leq j \leq$

$n-1$.

4. Use the Standard Extended Division algorithm to compute $f_v^{-1}(x)(\text{mod } x^n-1)$, where $f_v(x)=\sum\limits_{0\leq i\leq n-1} v_jx^j$.

5. For odd n solve the linear system (2.11) to find the unique solution of $q(x)=\sum\limits_{0\leq i\leq n-1} w_ix^i\in Q$ of $p(x)=f_u(x)f_v^{-1}(x)=q(x)q^*(x)$, where $w_i=p_{2i(\text{mod } n)}$.

Output: A normal element α of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ exists and of the form $\sum\limits_{0\leq i\leq n-1} w_i\beta^i$.

Example : Find a normal element α for the symmetric vector $u=(u_0,u_1,u_2,...,u_6)\in \mathbb{F}_{2^7}$ such that $u_i=Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1})$ for $0\leq i\leq 6$, $u_0=1$ and $\sum u_i=1$.

Solution Since $u_0=1$ and $\sum u_i=1$. Therefore, possible values of u are

$$\begin{aligned} u &= (1,1,0,0,0,0,1),(1,0,0,0,0,0,0),(1,1,1,1,1,1,1),(1,1,1,0,0,1,1),(1,0,1,0,0,1,0)\\ &\quad (1,0,0,1,1,0,0),(1,0,1,1,1,1,0),(1,1,0,1,1,0,1).\end{aligned}$$

Let us find the normal element for the vector $u=(1,1,0,0,0,0,1)$. By using Theorem 2.3, let $\beta=\gamma^6+\gamma+1$ be the normal element of $\mathbb{F}_{2^7}$ over $\mathbb{F}_2$ and

$$v_j=Tr_{2^n|2}(\beta^{2^{2j}-2^j+1}) \tag{2.22}$$

for $0\leq j\leq 6$. Then the corresponding symmetric vector of above Boolean function is

$$v=(v_0,v_1,v_2,v_3,v_4,v_5,v_6)=(1,0,1,1,1,1,0). \tag{2.23}$$

Therefore, the polynomial formed by this vector v is given by

$$f_v(x)=\sum_{0\leq i\leq n-1} v_ix^i=1+x^2+x^3+x^4+x^5.$$

Using greatest common divisor algorithm, the inverse of the polynomial $f_v(x)(\text{mod } x^7-1)$ is

$$f_v^{-1}(x)=x^4+x^3+1.$$

Also, from the vector u, the polynomial is

$$f_u(x)=x^6+x+1.$$

Therefore,

$$f_u(x)f_v^{-1}(x)(\text{mod } x^7-1)=p(x) \text{ (say)}.$$

That is

$$\begin{aligned} p(x) &= (1+x+x^6)(x^4+x^3+1)(\text{mod } x^7-1) \\ &= x^6+x^5+x^2+x+1. \end{aligned} \tag{2.24}$$

Using the polynomial (2.24) and $w_i = p_{2i(\text{mod } n)}$ from [Theorem 2.9, 20] we obtain the values of vector w as

$$w_0 = 1, w_1 = 1, w_2 = 0, w_3 = 1, w_4 = 1, w_5 = 0, w_6 = 1.$$

Let

$$q(x) = \sum_{0 \le i \le n-1} w_i x^i \in Q.$$

Then

$$\begin{aligned} q(x)q^*(x) &= (1+x+x^3+x^4+x^6)(x^7+x^6+x^4+x^3+x) \\ &= 1+x+x^2+x^5+x^6. \end{aligned} \tag{2.25}$$

Therefore, (2.24) and (2.25) show that $p(x) = q(x)q^*(x)$, that is, $f_u(x)f_v^{-1}(x) = q(x)q^*(x)$. Thus, according to the Theorem 2.3 there exists a normal element

$$\alpha = \sum_{0 \le i \le 6} w_i \beta^{2^i} = \sum_{0 \le i \le 6} w_i (\gamma^6+\gamma+1)^{2^i} = 1+\gamma+\gamma^2+\gamma^4+\gamma^6.$$

Acknowledgment

Authors acknowledge the support of UGC - SAP.

References

[1] Menezes A. J., Blake F. I., Gao X., Vanstone A. S. and Yaghoobian T., Applications of Finite Fields, Kluwer Academic Publishers, (1993).

[2] Lempel A. and Weinberger M. J., Self-complementary normal bases in finite fields, SIAM J. Discrete Math., 1(2) (1988), 193–198.

[3] Wang C. C., An algorithm to design finite field multipliers using a self dual normal basis, IEEE Trans. Comput., 38(10) (1989), 1457-1460.

[4] Silva S. and Kschischang F. R., Fast encoding and decoding of Gabidulin codes, In: Proceedings of the IEEE International Symposium of Information Theory, Seoul: Korea, (2009), 2858-2862.

[5] Mullen G. L. and Panario D., Handbook of Finite Fields, CRC Press, (2013).

[6] Massey J. L. and Omura J. K., Computation method and apparatus for finite field arithmetic, US Patent No. 4587627, (1986).

[7] Vonzur Gathen J. and Nöcker M., Fast arithmetic with general Gauss periods, Theor. Comput. Sci., 315 (2004), 419-452.

[8] Hasan M. A., Wang M. Z. and Bhargava V. K., A modified Massey-Omura parallel multiplier for a class of finite fields, IEEE Trans. Comput., 42 (1993), 1278-1280.

[9] Sharma P. L., Sharma S. and Rehan M., On construction of irreducible polynomials over $\mathbb{F}_3$, Journal of discrete Mathematical Sciences and Cryptography, 8(4) (2015), 335-347.

[10] Sharma P. L., Rehan M. and Sharma S., Counting irreducible polynomials over $GF(3)$ with first and third coefficients given, Asian-European Journal of Mathematics, 8(1) (2015), 1550015 (27 Pages).

[11] Liao Q. Y., A survey on normal bases over finite fields, Advances in Mathematics China, 42(5) (2013), 577-586.

[12] Dahab R. etal., Software multiplication using gaussian normal bases, IEEE Trans. Comput., 55 (2006), 974-984.

[13] Lidl R. and Niederreiter H., Introduction to Finite Fields and their Applications, Cambridge University Press, First edition, (1986).

[14] Lidl R. and Niederreiter H., Finite Fields, Cambridge University Press, second edition, (1997).

[15] Gao S., Vonzur Gathen J., Panario D., Shoup V., Algorithms for exponentiation in finite fields, J. Symb. Comput., 29(6) (2000), 879-889.

[16] Gao S., Normal bases over finite fields, Ph.D. thesis, University of Waterloo, Canada, (1993).

[17] Huczynska S., Mullen G. l., Panario D. and Thomson D., Existence and properties of k- normal elements over finite fields, Finite Field and their Applications, 24 (2013), 170-183.

[18] Kavut S., Maitra S., Yucel M. D., Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Trans. Inf. Theory, 53(5) (2007), 1743-1751.

[19] Perlis S., Normal bases of cyclic fields of prime-power degree, Duke Math. J., 9 (1942), 507-517.

[20] Zhang X., Feng R., Liao Q. and Gao X., Finding normal bases over finite fields with prescribed trace self orthogonal relations, Finite Field and their Applications, 28 (2014), 1-21.

[21] Wan Z. X., Lectures on finite fields and Galois rings, Singapore: World Scientific, (2003).