Normal Elements using Trace Mapping over Finite Fields

P. L. Sharma
Department of Mathematics & Statistics
Himachal Pradesh University,
Shimla 171 005, India

Kiran Devi
Department of Mathematics & Statistics
Himachal Pradesh University,
Shimla 171 005, India

ABSTRACT

Normal bases over finite fields have been widely used in many applications of cryptography and coding theory. They are also important for Frobenius mapping and efficient for the implementation of the arithmetic of finite fields. Let α be a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and $u = (u_0, u_1, \dots, u_{n-1})$ be a vector of $\mathbb{F}_{2^n}$. The vector u 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 $u_i = Tr_{2^n|2}\left(\alpha^{2^{2i}-2^i+1}\right)$ for $0 \leq i \leq n-1$, where n is positive integer if and only if vector u is symmetric and

$$\left(\sum_{0 \leq i \leq n-1} u_i\, x^i, x^n - 1\right) = 1$$

for even .

MSC (2010) 11T71, 12E20, 12E30.

Keywords

Normal basis**,** Trace function, Hamming weight, Symmetric vector.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field such that $q = p^t$, where p is prime, t is a positive integer and $\mathbb{F}_{q^n}$ be n dimensional extension field of $\mathbb{F}_q$. If $\alpha \in \mathbb{F}_{q^n}$ and $\left\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\right\}$ 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 [11]. The basis

$$M = \left\{\beta_j = \beta^{q^j}; j = 0, 1, 2, \dots, n-1\right\}$$

is said to be the dual basis of

$$N = \left\{\alpha_i = \alpha^{q^i}; i = 0, 1, 2, \dots, n-1\right\}$$

if

$$Tr(\alpha_i \beta_j) = Tr\left(\alpha^{q^i} \beta^{q^j}\right) = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases},$$

where $0 \leq i, j \leq n-1$. Let $\mathbb{F}_{q^m}$ be the subfield of $\mathbb{F}_{q^n}$, then the trace function of $\alpha \in \mathbb{F}_{q^n}$ is

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

Basic properties of normal bases of finite fields are discussed in [4, 10, 11, 15, 17]. The normal basis theorem discussed in [8] is well known which says that for any prime power q and positive integer n, there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Normal bases and self-dual normal bases over finite fields are widely used in cryptography, coding theory and signal processing due to their fast arithmetic computational properties. These bases are also used to design simple and fast multipliers of finite fields, see[19]. The hardware multipliers like Massey and Omura [9, 3] use the normal bases over the finite fields with characteristic 2 Wang [18] discuss a self dual normal basis multiplier with low complexity over $\mathbb{F}_2$. Normal bases are also used in cyclic bit shift operations, exponentiation processes in cryptography and software techniques, see [3, 7, 6].

Generally, low complexity normal bases are used due to their wide applications in design code cryptography. The normal bases having complexity equal to $2n-1$, where n is the number of non zero entries in multiplication table are called optimal normal bases. Trace vector obtained from the trace self orthogonal relation of normal bases gives the hamming weight of the corresponding normal element. Lowest hamming weight of normal bases is used to reduce the cycle of rotation in symmetric Boolean function. It also reduces the number of trace computations. Normal bases are trace orthogonal if and only if matrix T formed from the normal bases set is symmetric.

Various irreducible polynomials over finite field are discussed in [13, 14]. A polynomial

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

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

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

is defined as the polynomial

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

The vector is also termed as the corresponding vector u of the element α which can be obtained from the trace self orthogonal relation of the element $\alpha \in \mathbb{F}_{q^n}$. We use good self-orthogonal relations, that is, for any element $\alpha \in \mathbb{F}_{q^n}$ the corresponding vector is of lowest hamming weight. The lowest possible hamming weight of a vector means the least number of 1's in the corresponding vector. The more simple relation between Boolean function and trace function of finite field $\mathbb{F}_{2^n}$ is the selection of good self- orthogonal relation of normal bases, see [19].

The function$f(\alpha) = Tr_{2^n|2}(\alpha^d) \in \mathbb{F}_{2^n}$, where $1 < d < 2^n - 1$, becomes the rotation symmetric Boolean function when α taken from normal basis set. Rotation symmetric Boolean functions have wide applications in designing cryptographic algorithms, see [5]. Lowest hamming weight of the vector gives the fewer cycles in rotation symmetric Boolean function. Various Boolean functions can be used to give good self-orthogonal relation with low hamming weight.

Self dual normal bases are also of much importance in cryptography and coding theory, but do not exist for every finite field extension. In that case the trace self-orthogonal relation can be used in place of self dual normal bases. The self dual normal basis Theorem [6] 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 $n \neq 0(mod 4)$. We discuss normal elements over $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ by considering the ring $\mathbb{F}_2[x]/(x^n - 1)$ for the arithmetic of polynomial.

2. MAIN RESULTS

Theorem 2.1 [1] Let $\alpha \epsilon \mathbb{F}_{q^n}$ and

$$a_i = Tr_{q^n|q}\left(\alpha\alpha^{q^i}\right), (0 \leq i \leq n-1).$$

Then α is normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the polynomial

$$N(x) = \sum_{0 \leq i \leq n-1} a_i\, x^i \in \mathbb{F}_q[x]$$

is relatively prime to $x^n - 1$.

Theorem 2.2 [12] Let α be a normal element $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then

$$\beta = \sum_{0 \leq i \leq n-1} c_i\, \alpha^{q^i}$$

is also a normal element if and only if the polynomial

$$N(x) = \sum_{0 \leq i \leq n-1} c_i\, x^i \in \mathbb{F}_q[x]$$

is relatively prime to $x^n - 1$.

The following Lemmas 2.3 and 2.4 are related to symmetric polynomial in $\mathbb{F}_2[x]/(x^n - 1)$.

Lemma 2.3 [19**]** Suppose

$$f(x) = \sum_{0 \leq i \leq n-1} a_i\, x^i \in \mathbb{F}_q[x]/(x^n - 1)$$

with $a_0 = 1$ is symmetric and is relatively prime to $x^n - 1$. Let

$$f^{-1}(x) = \sum_{0 \leq i \leq n-1} b_i\, x^i \in \mathbb{F}_q[x]/(x^n - 1)$$

be the unique polynomial such that

$$f(x)f^{-1}(x) \equiv 1 mod\ (x^n - 1)$$

Then $f^{-1}(x)$ is symmetric, relatively prime to $x^n - 1$ and its constant term is1.

Lemma 2.4 [19] Let

$$f_a(x) = \sum_{0 \leq i \leq n-1} a_i\, x^i \in \mathbb{F}_q[x]/(x^n - 1)$$

and

$$f_b(x) = \sum_{0 \leq i \leq n-1} b_i\, x^i \in \mathbb{F}_q[x]/(x^n - 1)$$

be symmetric polynomials. Then

$$f_c(x) = f_a(x)f_b(x) = \sum_{0 \leq i \leq n-1} c_i\, x^i \in \mathbb{F}_q[x]/(x^n - 1)$$

is also symmetric.

Further, we used the above Theorems and Lemma to prove the results given below.

Theorem 2.5 For even n there exists a normal element α of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$corresponding to vector

$$u = u_0, u_1, u_2, \ldots, u_{n-1} \in \mathbb{F}_{2^n}$$

if and only if

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

is symmetric and

$$(f_u(x),\ x^n - 1) = 1.$$

Proof Using symmetric property in trace function the vector u_i can be written as

$$u_i = Tr_{2^n|2}\left(\alpha^{2^{2i}-2^i+1}\right) = Tr_{2^n|2}\left(\alpha^{2^{2(n-i)}-2^{n-i}+1}\right) = u_{n-i}$$

for all $1 \leq i \leq n-1$. Since, $u = (u_0, u_1, u_2, \ldots, u_{n-1})$ is symmetric vector. Therefore, using Theorem 2.1, we conclude that $(f_u(x),\ x^n - 1) = 1$.

Now for the converse part, let us consider $(u_0, u_1, u_2, \ldots, u_{n-1}) \in \mathbb{F}_{2^n}$ satisfied

$$(f_u(x),\ x^n - 1) = 1.$$

Therefore, our aim is to find a normal element α of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ such that

$$Tr_{2^n|2}\left(\alpha^{2^{2i}-2^i+1}\right) = u_i$$

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

By normal basis theorem [14] there exists a normal element β (say) of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let its corresponding polynomial be

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

with

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

The necessary part shows that$f_v(x)$is symmetric and $(f_v(x), x^n - 1) = 1$. Let

$$f^{-1}{}_v(x)(mod\ x^n - 1) = \sum_{0 \leq i \leq n-1} v_i\, x^i.$$

From above equation and the Lemma 2.3 we conclude that the polynomial $f^{-1}{}_v(x)$ is symmetric and relatively prime to$x^n - 1$. Therefore, the polynomial

$$p(x) = f_v(x)f^{-1}{}_v(x)$$

is symmetric and relatively prime to $x^n - 1$. . Further, it is clear that

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

is also the solution of $p(x)$. Let

$$\alpha = \sum_{0 \leq i \leq n-1} w_i\, \beta^i$$

, then according to the Theorem 2.2 and Theorem 4.1 [19] α is a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and its corresponding vector is $u = (u_0, u_1, u_2, \ldots, u_{n-1})$.

Here, we have also discussed the algorithm for finding the normal element using above theorem.

3. ALGORITHM

For finding a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ corresponding to a given vector $(u_0, u_1, u_2, \ldots, u_{n-1}) \in \mathbb{F}_{2^n}$ where $n > 1$and $u_i = Tr_{2^n|2}\left(\alpha^{2^{2i}-2^i+1}\right)$ for all $0 \leq i \leq n-1$. The steps are as follows:

Input: $u = (u_0, u_1, u_2, \ldots, u_{n-1}) \in \mathbb{F}_{2^n}$.

Step 1. Take n as even, we check whether $(u_0, u_1, u_2, \ldots, u_{n-1}) \in \mathbb{F}_{2^n}$ satisfies symmetric property and

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

If not then output "There is not such a normal element".

Step 2. Find a normal element $\beta$of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ (using the definition of normal element).

Step 3. Compute $(v_0, v_1, v_2, \ldots, v_{n-1})$ where $v_j = Tr_{2^n|2}\left(\alpha^{2^{2j}-2^j+1}\right)$ for all $0 \le i \le n-1$.

Step 4. Use the Standard Extended Division algorithm to compute $f^{-1}{}_v(x)(mod\, x^n - 1)$ where

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

Step 5. For even n compute

$$p(x) = f_u(x) f^{-1}{}_v(x) = q(x) q^*(x), \text{ where}$$

$$q(x) = \sum_{0 \le i \le n-1} w_i\, x^i \in \mathbb{F}_{2^n}[x]/(x^n - 1).$$

Output: A normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is

$$\alpha = \sum_{0 \le i \le n-1} w_i\, \beta^i.$$

4. EXAMPLE

Find a normal element α for the symmetric vector $u = (u_0, u_1, u_2, u_3) \in \mathbb{F}_{2^4}$ such that $u_i = Tr_{2^n|2}\left(\alpha^{2^{2i}-2^i+1}\right)$ for $0 \le i \le 3$,

$$f_u(x) = \sum_{0 \le i \le 3} u_i\, x^i$$

is symmetric and $(f_u(x), (x^4 - 1)) = 1$.

Solution Since polynomial

$$f_u(x) = \sum_{0 \le i \le 3} u_i\, x^i$$

is symmetric and $(f_u(x), (x^4 - 1)) = 1$. Therefore, possible values of u are (1,1,1,1), (1,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,0,1), (0,0,1,0), (0,1,1,1).

Let us find the normal element for the vector $u = (0,1,0,1)$. By using the definition of normal element, let $\beta = \gamma^2 + 1$ be the normal element of $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$ and

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

for $0 \le j \le 3$. Then the corresponding symmetric vector of above Boolean function is

$$v = (v_0, v_1, v_{2,} v_3) = (0,1,1,1).$$

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

$$f_v(x) = \sum_{0 \le i \le 3} v_i\, x^i = x + x^2 + x^3.$$

Using greatest common divisor algorithm, the inverse of the polynomial $f_v(x) mod(\, x^4 - 1)$ is

$$f^{-1}{}_v(x) = x + x^2 + x^3.$$

Also, from the vector u, the polynomial is

$$f_u(x) = x + x^3.$$

As $f_u(x)$ and $f^{-1}{}_v(x)$both are symmetric, therefore, by Lemma 2.4

$$p(x) = f_u(x) f^{-1}{}_v(x) mod\, (x^4 - 1)$$

is also symmetric. That is

$$\begin{aligned} p(x) &= (x + x^3\,)(x + x^2 + x^3) mod(x^4 - 1) \\ &= (x + x^3\,) \\ &= (x + x^2\,)(x^3 + x^2\,) = q(x) q^*(x), \end{aligned}$$

where $q^*(x)$ is the reciprocal polynomial. As $q(x)$ is relatively prime to$(x^4 - 1)$, therefore, by using Theorem 2.2 we get

$$\alpha = \sum_{0 \le i \le 3} w_i\, \beta^{2^i},$$

be the normal element and w_i are the coefficients of $q(x)$. Therefore,

$$\alpha = \sum_{0 \le i \le 3} w_i\, (\gamma^2 + 1)^{2^i}$$

is the normal element corresponding to the given vector.

5. CONCLUSION

In this paper, we obtained the normal elements using trace mapping of finite fields that have low hamming weight. Further, we found the condition for the existence of normal elements from trace vector and symmetric polynomials of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

6. ACKNOWLEDGMENT

Authors acknowledge the support of UGC - SAP.

7. REFERENCES

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

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

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

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

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

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

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

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

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

[10] Menezes, A. J., Blake, F. I. Gao, X., Vanstone, A. S. and Yaghoobian, T. 1993. Applications of finite fields, Kluwer Academic Publishers.

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

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

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

[14] Sharma, P. L., Sharma S. and Rehan, M. 2015. On construction of irreducible polynomials over F_3, Journal of discrete Mathematical Sciences and Cryptography, 8(4), 335-347.

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

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

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

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

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