EPJ Web of Conferences **68**, 00040 (2014)
DOI: 10.1051/epjconf/20146800040

Construction of Weakly Self-Dual Normal Bases and Its Aplication in Orthogonal Transform Encoding Cyclic Codes

Irwansyah[1,a], Ahmad Muchlis[1,b], Intan Muchtadi Alamsyah[1,c], Djoko Suprijanto[2,d], and Aleams Barra[1,e]

[1] *Algebra Research Group, Faculty of Mathematic and Natural Sciences, Bandung Institute of Technology*
[2] *Combinatorial Research Group, Faculty of Mathematic and Natural Sciences, Bandung Institute of Technology*

Abstract. In 1986 Fumy proposed a simplified approach to calculate inverse discrete Fourier transform (IDFT) using normal bases and its dual in encoding cyclic codes in the spectral domain. Therefore, one important thing in Fumy's procedure is to choose an appropriate normal bases such that the dual bases can be determined easily. This problem leads to an application of weakly self-dual normal bases. In this paper we explain how to construct weakly self-dual normal bases and its type of bases in encoding cyclic codes.

Keywords : Cyclic codes, Discrete Fourier transform, Inverse discrete Fourier transform, Weakly self-dual normal bases.

1 Introduction

Let $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$ be finite fields with q^n and q elements consecutively. The finite field $\mathbb{F}_{q^n}$ can be viewed as n dimensional vector space over $\mathbb{F}_q$. One important type of bases for $\mathbb{F}_{q^n}$ is normal bases, *i.e.* a type of bases of the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ for some $\alpha \in \mathbb{F}_{q^n}$, because they are computationally manageable, for example see [1, 9]. Moreover, Fumy [4] proposed to use normal bases in encoding cyclic codes where the codewords considered as spectrum of discrete Fourier transform (DFT) over $\mathbb{F}_q$. In particular, Fumy's result involving simplified calculation procedure for inverse discrete Fourier transform (IDFT) using normal bases and its dual bases. Therefore, one important aspect for Fumy's procedure is how to find an appropriate normal bases such that the dual bases can be determined easily. The most likely right answer for that situation is to use weakly self-dual normal bases, because dual bases of this type of bases is nearly the same as itself. Therefore, in this paper we give a procedure to construct weakly self-dual normal bases in finite fields $\mathbb{F}_{q^n}$ when they exist, and explain how to apply this type of bases in Fumy's procedure.

2 Construction of Weakly Self-Dual Normal Bases

Definition 2.1 *Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. A basis $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ is called dual bases for $\mathcal{A}$ if it satisfies,*

$$tr(\alpha_i \cdot \beta_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

for every $i, j = 0, 1, \ldots, n-1$, where $tr(\xi) = \sum_{k=0}^{n-1} \xi^{q^k} \in \mathbb{F}_q$, for all $\xi \in \mathbb{F}_{q^n}$.

Menezes *et al* [8] showed that every bases always has a unique dual bases and dual bases for normal bases is again a normal bases.

Definition 2.2 *Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$, where $\alpha_i = \alpha^{q^i}$ for some $\alpha \in \mathbb{F}_{q^n}$, be a normal bases for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Bases $\mathcal{A}$ is called weakly self-dual if its dual bases is of the form*

$$\gamma\alpha_{\pi(0)}, \gamma\alpha_{\pi(1)}, \ldots, \gamma\alpha_{\pi(n-1)}$$

for some $\gamma \in \mathbb{F}_{q^n}$ and some permutation π.

Geiselmann [5] showed that $\gamma = \frac{1}{tr(\alpha_0)^2}$ and $\pi(i) = i$ or $\pi(i) = i + \frac{n}{2} \bmod n$. Moreover, Liao and Sun [6] proved that for q an odd integer, weakly self-dual normal bases with $\gamma = 1$ exist if and only if n is odd integer or n is even integer and -1 is not a quadratic element in $\mathbb{F}_q$, and for q an even integer, the latter bases exist if and only if $n \not\equiv 0 \bmod 4$.

Let $\mathcal{A} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal bases for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $\alpha_i = \alpha^{q^i}$, for some $\alpha \in \mathbb{F}_{q^n}$ and for every $i = 0, 1, \ldots, n-1$. Let $\Gamma = \{\eta_0, \eta_1, ..., \eta_{n-1}\} \subset F_{q^n}$ where $\eta_j = \sum_{k=0}^{n-1} b_{jk}\alpha_k$, for all $j = 0, 1, \ldots, n-1$. From the previous representation with respect to bases $\mathcal{A}$, we have a matrix $B = [b_{jk}]$ which the j-th row is coordinate of η_j with respect to bases $\mathcal{A}$. The following result give the conditions for B so that Γ will be a weakly self-dual normal bases.

[a] e-mail: irwansyah@students.itb.ac.id
[b] e-mail: muchlis@math.itb.ac.id
[c] e-mail: ntan@math.itb.ac.id
[d] e-mail: djoko@math.itb.ac.id
[e] e-mail: barra@math.itb.ac.id

Proposition 2.3 *The Subset* $\Gamma = \{\eta_0, \eta_1, ..., \eta_{n-1}\}$ *is a weakly self-dual normal bases if and only if B is an non singular circulant matrix and satisfies the following equation.*

$$\gamma^{-1} B^{-1} P_\pi (B^t)^{-1} = \left(tr(\alpha^{q^i} \alpha^{q^j})\right)_{0 \le i,j \le n-1} \quad (1)$$

for some $\gamma \in \mathbb{F}_{q^n}$, *where* P_π *is permutation matrix for permutation* $\pi(i) = i$ *or* $\pi(i) = i + \frac{n}{2}$ *mod n.*

Proof From Theorem 1.6 in [8], Γ is a normal bases for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if B is a non singular circulant matrix. We need to prove the second assertion only. Let $A = \left(tr(\alpha^{q^i} \alpha^{q^j})\right)_{0 \le i,j \le n-1}$.
($\Rightarrow$) Let B_i is the i-th row of B. Consider,

$$(AB^t)_j = \begin{pmatrix} \sum_{k=0}^{n-1} tr\left(\alpha \alpha^{q^k}\right) b_{jk} \\ \sum_{k=0}^{n-1} tr\left(\alpha^q \alpha^{q^k}\right) b_{jk} \\ \sum_{k=0}^{n-1} tr\left(\alpha^{q^2} \alpha^{q^k}\right) b_{jk} \\ \vdots \\ \sum_{k=0}^{n-1} tr\left(\alpha^{q^{n-1}} \alpha^{q^k}\right) b_{jk} \end{pmatrix}$$

So we have

$$B_i A B_j^t = \sum_{l=0}^{n-1} \sum_{k=0}^{n-1} b_{il} b_{jk} tr\left(\alpha^{q^l} \alpha^{q^k}\right) = tr(\eta_i \eta_j)$$

By assumption, we have

$$tr(\eta_i \eta_j) = \begin{cases} \gamma^{-1}, & j = \pi(i) \\ 0, & \text{others} \end{cases}$$

Therefore,

$$BAB^t = \gamma^{-1} P_\pi$$

($\Leftarrow$) If $BAB^t = \gamma^{-1} P_\pi$, then

$$tr(\eta_i \eta_j) = \begin{cases} \gamma^{-1}, & j = \pi(i) \\ 0, & \text{others} \end{cases}$$

Therefore, Γ is a weakly self-dual normal bases. □

Let ϕ be a map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ where $\phi(\alpha) = \alpha^q$ for all $\alpha \in \mathbb{F}_{q^n}$. Let $G = \langle \phi \rangle$ is a cyclic group generated by ϕ. Define $\mathbb{F}_q[G] = \left\{ \sum_{k=0}^{n} a_k \phi^k \mid a_k \in \mathbb{F}_q \right\}$, $\mathbb{F}_q[G]$ forms an algebra over $\mathbb{F}_q$. For $v = \sum_{k=0}^{n-1} a_k \phi^k \in \mathbb{F}_q[G]$, define a conjugate for v, $\bar{v} = \sum_{k=0}^{n-1} a_k \phi^{-k}$. The following results is a key for construction of weakly self-dual normal bases.

Theorem 2.4 [2] *Let n be odd integer and* $R = \sum_{i=0}^{n-1} tr\left(\alpha \phi^i(\alpha)\right) \phi^i$, *then :*

i. If $v \in \mathbb{F}_q[G]$ *satisfies*

$$v\bar{v} = R \quad (2)$$

then v has an inverse in $\mathbb{F}_q[G]$.

ii. $\varphi_\alpha : v \mapsto v^{-1} \circ \alpha$ *is one-to-one correspondence beetwen the solution for equation* (2) *and the set of elements in* $\mathbb{F}_{q^n}$ *which generate weakly self-dual normal bases.*

Proof see [2]. For n an even integer we have the following theorem.

Theorem 2.5 *Let* α *be normal bases generator for in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$, *and* $R = \sum_{i=0}^{n-1} tr\left(\alpha \phi^i(\alpha)\right) \phi^i$, *then :*

i. If $v \in \mathbb{F}_q[G]$ *satisfies*

$$v \phi^{\frac{n}{2}} \bar{v} = R \quad (3)$$

then v has an inverse in $\mathbb{F}_q[G]$.

ii. $\varphi_\alpha : v \mapsto v^{-1} \circ \alpha$ *is one-to-one correspondence beetwen the solution for equation* (3) *and the set of elements in* $\mathbb{F}_{q^n}$ *which generate weakly self-dual normal bases.*

Proof Define,

$$\begin{array}{rccc} \lambda : & \mathbb{F}_q[G] & \longrightarrow & C(n,q) \\ & v = \sum_{k=0}^{n-1} a_k \phi^k & \longmapsto & C_v = (c_{ij}) = \left(a_{i-j \bmod n}\right) \end{array}$$

where $C(n,q)$ is the set of all $n \times n$ circulant matrices over $\mathbb{F}_q$. We can see λ is injective and $C_1 = I$. Moreover, λ is surjective homomorphism. Therefore, λ is an isomorphism beetwen the set of invertible elements in $\mathbb{F}_q[G]$ and the abelian group of non singular circulant matrices over $\mathbb{F}_q$. Now, note that $C_R = \left(tr\left(\alpha^{q^i+q^j}\right)\right)_{0 \le i,j \le n-1}$ and from Theorem 2.37 in [7] C_R is invertible. It follows that, if $v \in \mathbb{F}_q[G]$ satisfies (3), then v is invertible.

(ii) Note that, $C_{\bar{v}} = C_v^t$ and $C_{\phi^{\frac{n}{2}}} = P_\sigma$, where P_σ is permutation matrix for $\sigma(i) = i + \frac{n}{2}$ *mod* n for every $i = 0, 1, 2, \ldots, n-1$. It follows that λ relates (3) in $\mathbb{F}_q[G]$ with equation $C_v P_\sigma C_v^t = \left(tr\left(\alpha^{q^i+q^j}\right)\right)_{0 \le i,j \le n-1}$ in $C(n,q)$.

For every $\omega \in \mathbb{F}_{q^n}$, let $[\omega]$ be an $n \times n$ matrix with the j-row is the coordinate ω^{q^j} with respect to a bases $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ in $\mathbb{F}_{q^n}$. Let $v = \sum_{k=0}^{n-1} v_k \phi^k \in \mathbb{F}_q[G]$. for every $j = 0, 1, \ldots, n-1$, if $\omega^{q^j} = \sum_{l=0}^{n-1} c_{lj} \beta_l$, for some $c_{lj} \in \mathbb{F}_q$, then

$$v \circ \omega = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} v_k c_{lk} \beta_l$$

and $[v \circ \omega] = C_v[\omega]$. If v satisfies (3), then C_v is a non singular circulant matrix and $C_v^{-1} = C_{v^{-1}}$. Moreover, $C_{v^{-1}}$ satisfies

$$C_{v^{-1}}^{-1} P_\sigma (C_{v^{-1}}^{-1})^t = C_v P_\sigma C_v^t = \left(tr\left(\alpha^{q^i+q^j}\right)\right)_{0 \le i,j \le n-1}$$

It follows from Proposition 2.3 $B = C_{v^{-1}}[\alpha] = [v^{-1} \circ \alpha]$ represents a weakly self-dual bases. Conversely, if β generates a weakly self-dual normal bases, then H_1 which satisfies $[\beta] = H_1[\alpha]$ is a non singular circulant matrix. There exists $v \in \mathbb{F}_q[G]$ such that $H_1^{-1} = C_v$ because λ is an isomorphism. In other words, v satisfies (3). Therefore, $\varphi_\alpha : v \mapsto v^{-1} \circ \alpha$ has the desired property. □

Let $v = \sum_{k=0}^{n-1} a_k \phi^k \in \mathbb{F}_q[G]$ and $R = \sum_{k=0}^{n-1} tr\left(\phi^k(\alpha)\alpha\right) \phi^k$. The search for v that satisfies (3) leads to the the problem of solving the following system of non linear equations,

for n even integer,

$$\begin{array}{lll} \sum_{l=0}^{n-1} a_l^2 & - & tr\left(\phi^{\frac{n}{2}}(\alpha)\alpha\right) = 0 \\ \sum_{l=0}^{n-1} a_l a_{l+1 \bmod n} & - & tr\left(\phi^{1+\frac{n}{2}}(\alpha)\alpha\right) = 0 \\ \cdots & \cdots & \cdots \\ \sum_{l=0}^{n-1} a_l a_{l+k \bmod n} & - & tr\left(\phi^{k+\frac{n}{2}}(\alpha)\alpha\right) = 0 \\ \cdots & \cdots & \cdots \\ \sum_{l=0}^{n-1} a_l a_{l+n-1 \bmod n} & - & tr\left(\phi^{n-1+\frac{n}{2}}(\alpha)\alpha\right) = 0 \end{array} \quad (4)$$

and for n odd integer,

$$\begin{array}{lll} \sum_{l=0}^{n-1} a_l^2 & - & tr\,(\alpha\alpha) = 0 \\ \sum_{l=0}^{n-1} a_l a_{l+1 \bmod n} & - & tr\,(\phi(\alpha)\alpha) = 0 \\ \cdots & \cdots & \cdots \\ \sum_{l=0}^{n-1} a_l a_{l+k \bmod n} & - & tr\left(\phi^k(\alpha)\alpha\right) = 0 \\ \cdots & \cdots & \cdots \\ \sum_{l=0}^{n-1} a_l a_{l+n-1 \bmod n} & - & tr\left(\phi^{n-1}(\alpha)\alpha\right) = 0 \end{array} \quad (5)$$

One of systematic way to solve (4) or (5) is to make use of Gröbner bases as in [3]. Therefore, we can use the following approach to construct weakly self-dual normal bases.

1 For α a generator for normal bases for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, form a system as in (4) or (5).

2 Find the solutions $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ for a given system using an approach as in [3].

3 Write $v = \sum_{k=0}^{n-1} a_{k+1}\phi^k \in \mathbb{F}_q[G]$ and calculate v^{-1}.

4 $v^{-1} \circ \alpha$ is weakly self-dual normal bases generator in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Example 2.6 *Let α be a normal bases generator for $\mathbb{F}_{3^6}$ over $\mathbb{F}_3$, where α is a root of $f(x) = x^6 + x^5 + x^2 + x + 1$. We have the following corresponding system of non linear equations.*

$$\begin{array}{lcl} f_0(x_0, x_1, \ldots, x_5) & = & x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - 1 \\ & = & 0 \\ f_1(x_0, x_1, \ldots, x_5) & = & x_1x_0 + x_2x_1 + x_3x_2 + x_4x_3 + x_5x_4 \\ & & +x_0x_5 - 1 = 0 \\ f_2(x_0, x_1, \ldots, x_5) & = & x_2x_0 + x_3x_1 + x_4x_2 + x_5x_3 + x_0x_4 \\ & & +x_1x_5 = 0 \\ f_3(x_0, x_1, \ldots, x_5) & = & x_3x_0 + x_4x_1 + x_5x_2 + x_0x_3 + x_1x_4 \\ & & +x_2x_5 - 1 = 0 \\ f_4(x_0, x_1, \ldots, x_5) & = & x_4x_0 + x_5x_1 + x_0x_2 + x_1x_3 + x_2x_4 \\ & & +x_3x_5 = 0 \\ f_5(x_0, x_1, \ldots, x_5) & = & x_5x_0 + x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 \\ & & +x_4x_5 - 1 = 0 \end{array}$$

and vector (2 1 1 1 0 0) *is the solution of the system. Therefore, we have $\beta = \alpha^{3^2} + \alpha^{3^3} + 2\alpha^{3^4} + \alpha^{3^5}$ is generator for weakly self-dual normal bases.*

3 Orthogonal Transform Encoding Cyclic Codes

Let C be an $[n, k]$ code over $\mathbb{F}_q$ and $\omega \in \mathbb{F}_{q^n}$ be a primitive n-th root of unity. If $\mathrm{GCD}(n, q) = 1$, choose m such that $n|q^m - 1$. We have for $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the discrete Fourier transform (DFT) spectra of c is equal to $f = (f_0, f_1, \ldots, f_{n-1}) \in \mathbb{F}_{(q^m)^n}$, where $f_k = \sum_{j=0}^{n-1} c_j\omega^{jk}$. The code C can be described by DFT spectra of its codewords. If C is a cyclic code, then C is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$ where every $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ related to $c(x) = \sum_{k=0}^{n-1} c_k x^k \in \mathbb{F}_q[x]/(x^n - 1)$. Now let C be a cyclic code with generator polynomial $g(x) = \prod_{i\in T}(x - \omega^i)$, where $T \subset \{0, 1, \ldots, n-1\}$ is a defining set for C, for some $g(x)|x^n - 1$. The polynomial $c(x) \in \mathbb{F}_q[x]/(x^n - 1)$ is an element of C if and only if $c(\omega^i) = 0$ for all $i \in T$. The last assertion means that for the DFT spectrum f of a codeword c, we have $f_i = 0$ for all $i \in T$. Any spectrum which is zero in each coordinate $i \in T$ and whose inverse discrete Fourier transform (IDFT) is in $\mathbb{F}_q$ is the spectrum of a codeword and is called codeword in spectral domain. Therefore, encoding a cyclic code via DFT is accomplished by calculating IDFT. Fumy [4] gave the following simplified approach to calculating IDFT using normal bases and its dual.

1 Represent the coefficients of the DFT spectrum $f(x) = \sum_{k=0}^{n-1} f_k x^k$ with respect to a normal bases $\mathcal{A} = \{\alpha_0, \ldots, \alpha_{m-1}\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, i.e. $f_k = \sum_{l=0}^{m-1} e_{kl}\alpha_l$.

2 Generate the polynomial $e_0(x) = \sum_{k=0}^{n-1} e_{k0}x^k$ and reduce $e_0(x)$ modulo the minimal polynomial of the n-th root of unity ω over $\mathbb{F}_q$, or calculate $e_0(\omega)$.

3 Write the resulting residues in linear combination of dual bases of $\mathcal{A}$, *i.e.* $e_0(\omega) = \sum_{k=0}^{m-1} u_k\delta_k$, for some $u_k \in \mathbb{F}_q$, where $D = \{\delta_0, \delta_1, \ldots, \delta_{m-1}\}$ is dual bases for $\mathcal{A}$. Then we have $c_k = u_{m-l}$, where l satisfies $k = q^l$.

We can make the above approach complete, by involving weakly self-dual bases. Given α generator of normal bases, we construct a weakly self-dual normal bases for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ using the approach in previous section, so that $\mathbb{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ is a weakly self-dual bases. Therefore, $D = \{\gamma\beta_{\pi(0)}, \gamma\beta_{\pi(1)}, \ldots, \gamma\beta_{\pi(m-1)}\}$, where $\gamma = \frac{1}{tr(\beta_0)^2}$ and $\pi(i) = i$ or $\pi(i) = i + \frac{m}{2} \bmod m$. Hence, bases $\mathbb{B}$ enable us to calculate its dual bases easily. Hence, we get the following complete approach.

1 Given $\alpha \in \mathbb{F}_{q^m}$ which generate normal bases. Construct weakly self-dual normal bases $\mathbb{B} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ and then its dual bases is $D = \{\gamma\beta_{\pi(0)}, \gamma\beta_{\pi(1)}, \ldots, \gamma\beta_{\pi(m-1)}\}$, where $\gamma = \frac{1}{tr(\beta_0)^2}$. Represent the coefficients of the DFT spectrum $f(x) = \sum_{k=0}^{n-1} f_k x^k$ with respect to bases $\mathbb{B}$.

2 Generate the polynomial $e_0(x) = \sum_{k=0}^{n-1} e_{k0}x^k$ and reduce $e_0(x)$ modulo the minimal polynomial of the n-th root of unity ω over $\mathbb{F}_q$, *i.e.* write $e_0(\omega) = \sum_{k=0}^{m-1} u_k(\gamma\beta_{\pi(k)})$. Then we have $c_k = u_{m-l}$, where l satisfies $k = q^l$.

Example 3.1 *Let β be generator of weakly self-dual normal bases for $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$, where β is a root of $h(x) = x^3 + x_1^2 \in \mathbb{F}_2[x]$. We can check that, $\alpha = \beta + \beta^2$ is 7-th root of unity. Let $f = (\beta\ \beta + \beta^2\ 0\ 0\ 0\ 0\ 0) \in \mathbb{F}_{2^3}^7$ be a vector in spectral domain, or we can write its corresponding polynomial $f(x) = \beta + (\beta + \beta^2)x \in \mathbb{F}_{2^3}[x]$. As in [4], $e_0(x) = 1 + x$, we have the inverse discrete Fourier for f is a vector c = (0 0 0 0 1 1 0) in signal domain, or its corresponding polynomial is $c(x) = x^4 + x^5$.*

4 Conclusion

We have shown that we can construct weakly self-dual normal bases generator with the solutions of equation (4) or (5). Moreover, the encoding of cyclic codes using Fumy's approach can be completed in such a way that we make use of weakly self-dual normal bases for undelining finite fields.

5 Acknowledgement

This research is supported by Hibah Riset dan Inovasi KK ITB.

References

[1] Agnew G.B., Mullin R.C. and Vanstone S.A., Fast exponentiation in $GF(2^n)$, Advances in Cryptology - Eurocrypt, Springer Lecture Notes in Computer Science **330** 251-255 (1988).

[2] Arnault F., Pickett E.J., and Vinatier S., Construction of self-dual normal bases and their complexity, Finite Fields and Their Applications **18** 458-472 (2012).

[3] Cox D., Little J. and O'Shea D., **Ideals, Varieties, and Algorithm, Third Edition** (Springer, New York, 2007).

[4] Fumy W., Orthogonal transform encoding of cyclic codes, AAECC-3, Springer Lecture Notes in Computer Science **229** 131-134 (1986).

[5] Geiselmann W., Weakly self-dual normal in finite fields, Proc. Application of Finite Fields, (1996).

[6] Liao, Qun Ying and Sun, Qi, A necessary and sufficient condition for finite field which has weakly self-dual normal bases, Chinese Annual Mathematics Series A **28 (2)** 273-280 (2007).

[7] Lidl R. and Niederreiter H., **Finite fields, Encyclopedia of Mathematics and Its Applications vol. 20** (Cambridge University Press, Cambridge, 1997).

[8] Menezes A.J., Blake I.F., Gao S.H., Mullin R.C., Vanstone S.A., and Yaghoobian T., **Application of finite fields**, (Kluwer Academic Publishers, Waterloo, 1993).

[9] Messey J.L. and Omura J.K., Computational method and apparatus for finite field arithmethic, U.S. Patent Application (1981).