Korean J. Math. **22** (2014), No. 3, pp. 517–527
http://dx.doi.org/10.11568/kjm.2014.22.3.517

# AFFINE TRANSFORMATION OF A NORMAL ELEMENT AND ITS APPLICATION

Kitae Kim, Jeongil Namgoong, and Ikkwon Yie

Abstract. In this paper, we study affine transformations of normal bases and give an explicit formulation of the multiplication table of an affine transformation of a normal basis. We then discuss constructions of self-dual normal bases using affine transformations of traces of a type I optimal normal basis and of a Gauss period normal basis.

## 1. Introduction

Let $\mathbb{F}_q$ denote the finite field with $q$ elements, where $q$ is a prime power and $\mathbb{F}_q^*$ be its multiplicative group. An element $\alpha$ in an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if its conjugates form a basis of $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space. In this case, the set of conjugates is called a *normal basis*. It is well known that any finite extension of a finite field has a normal element, which is *the normal basis theorem*. Historically, normal bases have been considered one of the most important part in the theory of finite fields. At the practical aspect, characterizations and constructions of low complexity normal bases are of great interest in coding theory and cryptography.

Received June 2, 2014. Revised September 19, 2014. Accepted September 19, 2014.

2010 Mathematics Subject Classification: Primary 11T71, 12E10, 12E20.

Key words and phrases: Normal basis, Low complexity, Self-dual basis.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(NRF-2011-0011654).

Let $\alpha \in \mathbb{F}_{q^n}$ be a normal element over $\mathbb{F}_q$ and $\alpha_i = \alpha^{q^i}$ for $0 \leq i \leq n-1$. The multiplication table of $\alpha$ is defined as the $n \times n$ matrix $(t_{i,j}) \in Mat_n(\mathbb{F}_q)$ such that

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{i,j}\alpha_j, \quad 0 \leq i \leq n-1.$$

The *complexity* of $\alpha$ is defined as the number of non-zero entries of the multiplication table. Mullin et al. [7] proved that $2n-1$ is the minimal complexity of normal elements and called a normal basis with the complexity an *optimal normal basis*, briefly ONB. They also established two types of optimal normal bases with complexity $2n-1$. In particular, Type I ONBs are constructed as follows: Let $n+1$ be a prime such that $q$ is a primitive element of $\mathbb{Z}_{n+1}$. Then the set of $n$ non-unit $(n+1)$th roots of unity is an optimal normal basis of Type I. Gao and Lenstra Jr. [3] proved that there are only such two types of optimal normal bases up to equivalence.

Though optimal normal bases are desirable in most applications of finite fields, such bases do not exist for all finite fields. As an alternative, constructions of normal bases with low complexity have extensively studied (see [3] for earlier works). In particular, Christopoulou et al. [1] investigated the trace of an optimal normal element to provide low complexity normal bases. The result was extended to the case of Gauss period normal bases by Christopoulou et al. [2] and Liao [6].

On the other hand, self-dual normal bases may be desirable in applications requiring frequent trace calculations as well as a Frobenius map computation. A normal basis generated by $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is said to be *self-dual* if $Tr(\alpha_i\alpha_j) = \delta_{i,j}$, where $Tr$ is the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and $\delta_{i,j}$ denotes the Kronecker delta. Since not all finite fields admit self-dual normal bases, characterizations and constructions of self-dual normal bases are also of great interests. Jungnickel [4] gave several characterizations of self-dual normal bases and their affine transformations, and an explicit construction of a self-dual normal basis in extension fields over $\mathbb{F}_2$. Following similar approach, Nogami et al. [8] suggested a construction of self-dual normal bases in finite fields of odd characteristic, where a certain normal basis, called a Type II-X NB, exists.

In this paper, we first study affine transformations of normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In particular, we give the multiplication table of a transformation of a normal element in terms of the multiplication table of a

given normal element, and observe complexities of affine transformations of a type I optimal normal basis and its traces. We then discuss constructions of self-dual normal bases by using an affine transformation of traces of a type I optimal normal basis, and a transformation of a normal basis built from Gauss periods.

## 2. Preliminaries

Throughout the present paper, we assume that $\mathbb{F}_q$ is the finite field with $q$ elements and of characteristic $p$. Note that $p = 2$ is allowed, unless otherwise stated.

PROPOSITION 2.1 (Christopoulou et al. [1]). *Let $\alpha$ generate a Type I ONB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, $q$ odd, and let $\beta = Tr_{q^n/q^m}(\alpha)$ with $n = mk$ and $k \leq m$. Then, the complexity of $\beta$ is bounded by $(k+2)m - 3k + 1$, if $k$ is odd and by $(k+1)m - k$ in the other case. In particular, if $k$ is even then the dual element of $\beta$ is $\frac{1}{n+1}(\beta - k)$, which has the complexity at most $(k+2)m - 2$.*

PROPOSITION 2.2 (Lempel et al. [5]). *The extension field $\mathbb{F}_{q^n}$ has a self-dual normal basis over $\mathbb{F}_q$ if and only if either $q$ is even and $4 \nmid n$, or both $q$ and $n$ are odd.*

PROPOSITION 2.3 (Jungnickel [4]). *Let $\alpha$ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let $a, b \in \mathbb{F}_q^*$. Then $\gamma = a + b\alpha$ is also a normal element if and only if $Tr(\gamma) = na + bTr(\alpha) \neq 0$.*

Let $k$ and $n$ be positive integers such that $nk+1$ is prime and $\gcd(nk+1, q) = 1$. Then $\mathbb{F}_{q^{nk}}$ contains a primitive $(nk+1)$th root $\zeta$ of unity, since $q \in \mathbb{Z}_{nk+1}^*$ and $\mathbb{F}_{q^{nk}}^*$ is a cyclic group of order $q^{nk} - 1$.

Now, let $s$ denote the order of $q$ in $\mathbb{Z}_{nk+1}^*$, $H$ the cyclic subgroup of $\mathbb{Z}_{nk+1}^*$ of order $k$. A type $k$ Gauss period $\alpha$ over $\mathbb{F}_q$ is defined as the following:

$$\alpha = \sum_{h \in H} \zeta^h$$

Note that $\alpha \in \mathbb{F}_{q^n}$, since $q^n H = H$.

PROPOSITION 2.4 (Wassermann, See [3]). $\gcd(nk/s, n) = 1$ *if and only if the set of conjugates of $\alpha$ form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

If $\gcd(nk/s, n) = 1$ then $\mathbb{Z}^*_{nk+1}$ can be partitioned by cosets $g^iH$ for $0 \le i < n$. Hence the normal basis generated by $\alpha$ does not depend on the choice of $\zeta$. In fact, the Gauss periods are conjugate over $\mathbb{F}_q$ each other in this case.

PROPOSITION 2.5 (Liao, See [6]). *Let $N$ be a normal basis of $\mathbb{F}_{q^n}$ generated by $\alpha$, and $\alpha_i$ denote $\alpha^{q^i}$ for $0 \le i < n$. The multiplication table of $\alpha$ is given as the followings:*

*If $k$ is even:*

$$\begin{aligned} \alpha\alpha_0 &= -k\sum_{j=0}^{n-1}\alpha_j + \alpha_{a_0} + 2\sum_{v=1}^{k/2-1}\alpha_{a_v}, \\ \alpha\alpha_i &= \sum_{w=0}^{k-1}\alpha_{i_w} \quad \text{for } i \neq 0, \end{aligned}$$

*where $1+l^v \equiv l^{k_v}q^{a_v} \pmod{kn+1}$, $v = 0, 1, \ldots, k/2-1$, $0 \le k_v \le k-1$, $0 \le a_v \le n-1$, $1 + l^w q^i \equiv l^{\tau_w} q^{i_w} \pmod{kn+1}$, $0 \le \tau_w \le k-1$, and $0 \le i_w \le n-1$.*

*Otherwise,*

$$\begin{aligned} \alpha\alpha_0 &= \alpha_{t_0} + 2\sum_{j=1}^{(k-1)/2}\alpha_{t_j}, \\ \alpha\alpha_{n/2} &= -k\sum_{j=0}^{n-1}\alpha_j + \sum_{v=1}^{k-1}\alpha_{s_v}, \\ \alpha\alpha_i &= \sum_{w=0}^{k-1}\alpha_{i_w} \quad \text{for } i \neq 0, n/2, \end{aligned}$$

*where $2 \equiv l^{h_0}q^{s_0} \pmod{kn+1}$, $1 - l^v \equiv l^{h_v}q^{s_v} \pmod{kn+1}$, $v = 0, 1, \ldots, \frac{k-1}{2}$, $0 \le h_v \le k-1$, $0 \le s_v \le n-1$, $1 + l^w q^i \equiv l^{n_w} q^{i_w} \pmod{kn+1}$, $0 \le n_w \le k-1$, and $0 \le i_w \le n-1$.*

## 3. Affine transformation of normal bases

Let $\alpha$ generate a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then using proposition 2.3, we have one of the main results as following.

THEOREM 3.1. *Let $\alpha$ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $a_1 = Tr_{q^n/q}(\alpha)$. For $c, d \in \mathbb{F}_q$ with $c \neq 0$ and $a_1 c + nd \neq 0$, the multiplication table of $c\alpha + d$ is given by the following formula:*

$$(c\alpha + d)\,(c\alpha_i + d) = \sum_{j=0}^{n-1} \left\{ ct_{i,j} + d(\delta_{0,j} + \delta_{i,j}) - \frac{d(c\tau_i + d)}{a_1 c + nd} \right\} (c\alpha_j + d)$$

*where $t_{i,j}$ and $\tau_i$ denote the $(i,j)$-entry of the multiplication table of $\alpha$ and the sum of entries in $i$th row of the table, respectively, and $\delta_{i,j}$ denotes the Kronecker delta function.*

*Proof.* First, note that $c\alpha + d$ is also a normal element.
Let $\nu = Tr_{q^n/q}(c\alpha + d)$. Note that

$$\nu = ca_1 + nd \neq 0 \quad \text{and} \quad \frac{1}{\nu} \sum_{j=0}^{n-1} (c\alpha_j + d) = 1.$$

Let $\gamma_j = c\alpha_j + d$ for $0 \leq j < n$. Then, for each $0 \leq j < n$,

$$\alpha_j \;=\; \frac{1}{c}(c\alpha_j + d) - \frac{d}{c} = \frac{1}{c}\gamma_j - \frac{d}{c\nu} \sum_{j=0}^{n-1} \gamma_j.$$

Hence, we have the next result:

$$\begin{aligned}
(c\alpha + d)(c\alpha_i + d) &= c^2 \alpha\alpha_i + cd\alpha + cd\alpha_i + d^2 \\
&= c^2 \sum_{j=0}^{n-1} t_{ij}\alpha_j + d(c\alpha_0 + d) + d(c\alpha_i + d) - d^2 \\
&= c \sum_{j=0}^{n-1} t_{ij} \left( \gamma_j - \frac{d}{\nu} \sum_{\ell=0}^{n-1} \gamma_\ell \right) \\
&\qquad + d\gamma_0 + d\gamma_i - \frac{d^2}{\nu} \sum_{j=0}^{n-1} \gamma_j \\
&= c \sum_{j=0}^{n-1} t_{ij}\gamma_j - \frac{cd\tau_i}{\nu} \sum_{\ell=0}^{n-1} \gamma_\ell + d\gamma_0 + d\gamma_i - \frac{d^2}{\nu} \sum_{j=0}^{n-1} \gamma_j \\
&= \sum_{j=0}^{n-1} \left\{ ct_{i,j} + d(\delta_{0,j} + \delta_{i,j}) - \frac{d(c\tau_i + d)}{\nu} \right\} (c\alpha_j + d)
\end{aligned}$$

□

Now we consider the complexity of affine transformations of a type I optimal normal basis generated by $\alpha \in \mathbb{F}_{q^n}$. Since equivalent bases have the same complexity, we consider only the case $c = 1$.

COROLLARY 3.2. *Let $\alpha$ generate a Type I ONB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $n > 6$. Then, for $d \in \mathbb{F}_q^*$ with $-1 + nd \neq 0$, the complexity of $\alpha + d$ is at least $3n - 3$. In particular, $d = -1$ reaches the lowest complexity: $3n - 2$ if $q$ is odd; $3n - 3$ otherwise.*

*Proof.* First note that $Tr_{q^n/q}(\alpha) = -1$ and $Tr(\alpha + d) = -1 + nd \neq 0$ by the definition of Type I ONB. So, by Proposition 2.3, $\alpha + d$ generates a normal basis.

For simplicity, let $\gamma = \alpha + d$ and $\gamma_i = \gamma^{q^i}$. For each $i \neq n/2$, let $\mu_i$ denote the column index of nonzero entry of $i$th row in the multiplication table of $\alpha$. Then, $\mu_i \neq i$ and, by Theorem 3.1, we have

$$\begin{aligned}
\gamma\gamma_0 &= \left(2d - \frac{d(d+1)}{nd-1}\right)\gamma_0 + \left(1 - \frac{d(d+1)}{nd-1}\right)\gamma_{\mu_0} \\
&\quad - \sum_{\substack{j=1,\\ j\neq\mu_0}}^{n-1} \left(\frac{d(d+1)}{nd-1}\right)\gamma_j, \\
\gamma\gamma_{n/2} &= \left(d - 1 - \frac{d(d-n)}{nd-1}\right)\gamma_0 + \left(d - 1 - \frac{d(d-n)}{nd-1}\right)\gamma_{n/2} \\
&\quad + \sum_{\substack{j=1,\\ j\neq n/2}}^{n-1} \left(-1 - \frac{d(d-n)}{nd-1}\right)\gamma_j.
\end{aligned}$$

For $i \neq 0, n/2$,

$$\begin{aligned}
\gamma\gamma_i &= \left(d - \frac{d(d+1)}{nd-1}\right)\gamma_0 + \left(d - \frac{d(d+1)}{nd-1}\right)\gamma_i + \left(1 - \frac{d(d+1)}{nd-1}\right)\gamma_{\mu_i} \\
&\quad + \sum_{\substack{j=1,\\ j\neq i,\mu_i}}^{n-1} \left(-\frac{d(d+1)}{nd-1}\right)\gamma_j.
\end{aligned}$$

Since $n > 6$, the case $d = -1$ gives an upper bound of the complexity, $3n - 2$. Note that $d \not\equiv n \pmod{p}$ since $p \nmid n + 1$, and that the first term in the representation of $\gamma\gamma_0$ is zero if $q$ is even. Thus, for $d = -1$, the complexity is $3n - 2$ if $q$ is odd, and $3n - 3$ if $q$ is even. □

COROLLARY 3.3. *Let $\alpha$ generate a type I ONB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, $q$ odd, and let $\beta = Tr_{q^n/q^m}(\alpha)$ with $m = n/k$, $1 < k \leq m$ and $m \geq 6$. Then, for $d \in \mathbb{F}_q^*$ with $-1 + nd \neq 0$, the lowest complexity among the transformations of the form $\beta+d$ is achieved in the case $d = -k \pmod p$.*

Note that, if $k$ is even then $\beta - k$ is equivalent to the dual element of $\beta$.

*Proof.* Since $\alpha$ is a type I ONB, there are $\mu_i \in \mathbb{Z}_n$ $(i = 0, \ldots, n/2 - 1, n/2 + 1, \ldots, n - 1)$ such that

$$\alpha\alpha^{q^i} = \alpha^{q^{\mu_i}}.$$

Also, for each $i = 0, \ldots, m - 1$, there exist $\lambda_{i,\nu} \in \mathbb{Z}_n$ such that

$$\alpha\alpha^{q^{i+\nu m}} = \alpha^{q^{\lambda_{i,\nu}}} \quad \text{for } \nu = 0, 1, \ldots, k - 1.$$

Then, as in the proof of Proposition 2.1 (see Theorem 1[1]), we have the following multiplication table of $\beta$:

$$\beta\beta_0 = \beta^{q^{\mu_0}} + \cdots + \beta^{q^{\mu_{k-1}}} + \sum_{j=0}^{m-1}(-k)\beta^{q^j} \tag{1}$$

and, for each $i = 1, \ldots, m - 1$,

$$\beta\beta_i = \beta^{q^{\lambda_{i,0}}} + \cdots + \beta^{q^{\lambda_{i,k-1}}}. \tag{2}$$

In Eqs (1) and (2), we may assume that $0 \leq \mu_j, \lambda_{i,j} \leq m - 1$.

Now, let $N_{0,j}$ $(j = 0, \ldots, m-1)$ denote the number of $\mu_t$'s $(0 \leq t < k)$ such that $\beta^{q^{\mu_t}} = \beta^{q^j}$. Then

$$\beta\beta = \sum_{j=0}^{m-1} (N_{0,j} - k)\, \beta^{q^j}.$$

Similarly, for each $i = 1, \ldots, m - 1$, $j = 1, \ldots, m - 1$, let $N_{i,j}$ denote the number of $\beta^{q^{\lambda_{i,t}}}$s $(0 \leq t < k)$ such that $\beta^{q^j} = \beta^{q^{\lambda_{i,j}}}$. Then, we can write $\beta\beta^{q^i}$ as

$$\beta\beta^{q^i} = \sum_{j=0}^{m-1} N_{i,j}\beta^{q^j}.$$

Now, let $\gamma = \beta + d$ and $\gamma_i = \gamma^{q^i}$. Since $Tr_{q^m/q}(\beta) = -1$, by Theorem 3.1,

$$\gamma\gamma_0 = \sum_{j=0}^{m-1} (N_{0,j} + 2d\delta_{0,j})\,\gamma_j$$

and, for $0 < i \leq m-1$,

$$\begin{aligned}\gamma\gamma_i &= \left(N_{i,0} + d + \frac{d(k+d)}{md-1}\right)\gamma_0 + \left(N_{i,i} + d + \frac{d(k+d)}{md-1}\right)\gamma_i \\ &\quad + \sum_{\substack{j=1,\\ j\in\Lambda_i, j\neq i}}^{m-1} \left(N_{i,j} + \frac{d(k+d)}{md-1}\right)\gamma_j + \sum_{\substack{j=1,\\ j\notin\Lambda_i, j\neq i}}^{m-1} \left(\frac{d(k+d)}{md-1}\right)\gamma_j\end{aligned}$$

where $\Lambda_i = \{\lambda_{i,j} |\ 0 \leq j \leq m-1\}$ for each $0 \leq i \leq m-1$.

Since $m \geq 6$, the lowest complexity is achieved in the case when $k + d = 0$, as desired. □

We remark that low complexity normal bases are often built from Gauss periods and that an explicit multiplication table of such a normal basis was given by Liao [6]. Though we do not explain further, it is possible to discuss an affine transformation of a normal basis generated by Gauss periods in the same way.

## 4. Constructions of self-dual normal bases

In this section, we study constructions of self-dual normal bases using affine transformation of a normal basis. In particular, we suggest a method for finding a self-dual normal basis from traces of a type I optimal normal basis, and present elements obtained from a Gauss period which generate self-dual normal bases. Our approach shares, in essence, the idea with the works of Jungnickel [4] and Nogami et al. [8].

Let $\alpha \in \mathbb{F}_{q^n}$ be a normal element over $\mathbb{F}_q$, and $\alpha_i = \alpha^{q^i}$ for $0 \leq i < n$. Since $\alpha_i\alpha_j = (\alpha_0\alpha_{j-i})^{q^i}$, *$\alpha$ generates a self-dual normal basis if and only if $Tr_{q^n/q}(\alpha_0\alpha_j) = \delta_{0,j}$ for $0 \leq j < n$.*

Let $(t_{i,j})$ be the multiplication table of $\alpha$ and $\tau_i$ the sum of $i$th row of the table. Then

$$(c\alpha + d)(c\alpha_i + d) = c^2\alpha_0\alpha_i + cd\alpha_0 + cd\alpha_i + d^2.$$

Hence,

$$\begin{aligned} Tr_{q^n/q}((c\alpha+d)(c\alpha_i+d)) &= c^2 Tr_{q^n/q}(\alpha_0\alpha_i) + 2cdTr_{q^n/q}(\alpha) + nd^2 \\ &= (c^2\tau_i + 2cd)Tr_{q^n/q}(\alpha) + nd^2. \end{aligned} \tag{3}$$

Suppose that $\mathbb{F}_{q^n}$ contains a type I ONB. Then $n$ is even and so, by Proposition 2.2, $\mathbb{F}_{q^n}$, with odd $q$, does not have a self-dual normal basis.

THEOREM 4.1. *Let $q$ be even and $\mathbb{F}_{q^n}$ contain a type I optimal normal basis generated by an element $\alpha$. If $n > 2$ then no elements of the form $c\alpha + d$, with $c, d \in \mathbb{F}_q$ and $c \neq 0$, generate a self-dual normal basis. Otherwise, in the case $n = 2$, $c\alpha + d$ generates a self-dual normal basis if and only if $c = 1$.*

*Proof.* By assumption, $n$ is even, $Tr_{q^n/q}(\alpha) = -1$, $\tau_{n/2} = -n = 0$ and $\tau_i = 1$ for $i \neq \frac{n}{2}$. Let $\gamma = c\alpha + d$ and $\gamma_i = \gamma^{q^i}$ for $0 \leq i < n$.

If $n > 2$ and $\gamma$ generates a self-dual normal basis of $\mathbb{F}_{q^n}$, then

$$Tr_{q^n/q}(\gamma\gamma_0) = c^2 = 1 \text{ and } Tr_{q^n/q}(\gamma\gamma_1) = c^2 = 0,$$

which is a contradiction.

Now suppose that $n = 2$. If $\gamma = c\alpha + d$ generates a self-dual normal basis, then $Tr_{q^2/q}(\gamma\gamma_0) = c^2 = 1$ and $Tr_{q^2/q}(\gamma\gamma_1) = 2c^2 = 0$. Thus $c = 1$. For the converse, we let $\gamma = \alpha + d$. Since $Tr_{q^2/q}(\alpha + d) = Tr_{q^2/q}(\alpha) = -1$, $\gamma$ is a normal element. Since $Tr_{q^2/q}(\gamma\gamma_0) = 1$ and $Tr_{q^2/q}(\gamma\gamma_1) = 0$, $\alpha + d$ generates a self-dual normal basis. □

Let $\alpha$ generate a type I ONB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $q$ is odd. Let $n = mk$ with odd $m$, $\beta = Tr_{q^n/q^m}(\alpha)$ and $\gamma = \beta + d$ for $d \in \mathbb{F}_q$. Let $\gamma_i = \gamma^{q^i}$ for and $0 \leq i < m$. Suppose that $\gamma$ generates a normal basis. By Eqs (1) and (2),

$$\begin{aligned} Tr_{q^m/q}(\gamma\gamma_0) &= md^2 - 2d + mk - k, \\ Tr_{q^m/q}(\gamma\gamma_i) &= md^2 - 2d - k \quad \text{for } 0 < i < m. \end{aligned}$$

Hence, $\gamma$ generates a self-dual normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if

$$md^2 - 2d - k = 0 \quad \text{and} \quad km - 1 = 0.$$

THEOREM 4.2. *Let $\mathbb{F}_{q^n}$ be a finite field of odd characteristic $p$ which contains a type I ONB generated by $\alpha$. Suppose that $m$ is odd and $n = mk$ such that $1 \leq m < n$ and $\beta = Tr_{q^n/q^m}(\alpha)$. Then $\mathbb{F}_{q^m}$ contains a self-dual normal basis generated by an element of the form $\beta + d$ with $d \in \mathbb{F}_q$ if and only if $n \equiv 1 \pmod{p}$ and $mX^2 - 2X - k$ splits completely in $\mathbb{F}_q$.*

*Proof.* The sufficient condition follows from the above arguments. To prove the other direction, we first note that $mX^2 - 2X - k$ is separable, since $p$ is odd and $mk \equiv 1 \pmod{p}$ by the assumption. So, at least one of the roots, say $d$, of the polynomial must satisfy $-1 + md \neq 0$. Then, $\beta + d$ generates a self-dual normal basis, as desired. □

Now, we consider an affine transformation of a Gauss period that generates a normal basis $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^n}$ be a Gauss period: $\alpha = \sum_{a \in H} \zeta^a$, where $nk+1$ is a prime different from $p$, $\zeta \in \mathbb{F}_{q^{nk}}$ is a primitive $(nk+1)$th root of unity, and $H$ is the cyclic subgroup of $\mathbb{Z}^*_{nk+1}$ of order $k$.

THEOREM 4.3. *Suppose that $q$ is odd and a Gauss period $\alpha$, defined as above, generates a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

1. *If $k$ is odd, then $\mathbb{F}_{q^n}$ does not contain a self-dual normal basis.*
2. *Suppose that $k$ is even. (i) If $p \nmid nk$ then no element of the form $\alpha + d$, with $d \in \mathbb{F}_q$, generates a self-dual normal basis. (ii) If $p \nmid n$ but $p \mid k$, then only $\alpha$ and $\alpha + \frac{2}{n}$ generate self-dual normal bases. (iii) If $p \mid n$, then $\mathbb{F}_{q^n}$ contains a self-dual normal basis of the form $\alpha + d$ with $d \in \mathbb{F}_q$ if and only if $nk \not\equiv -2 \pmod{p}$. In this case, only $\alpha - \frac{k}{2}$ generates a self-dual normal basis.*

*Proof.* If $k$ is odd then $n$ must be even. By Proposition 2.2, $\mathbb{F}_{q^n}$ does not contain a self-dual normal basis since $q$ is odd.

For part 2, let us denote by $\tau_i$ the sum of entries in the $i$th row of the multiplication table of $\alpha$. Let $\gamma = \alpha + d$ and $\gamma_i = \alpha_i + d$. Suppose that $k$ is even and that $\gamma$ generates a self-dual normal basis. By Proposition 2.5,

$$\begin{aligned} \tau_0 &= -nk + 1 + 2(k/2 - 1) = -nk + k - 1, \\ \tau_i &= k \text{ for } i \neq 0. \end{aligned}$$

Then,

$$\begin{aligned} 1 &= Tr(\gamma\gamma_0) = nd^2 - 2d + nk - k + 1, \\ 0 &= Tr(\gamma\gamma_i) = nd^2 - 2d - k. \end{aligned}$$

Equivalently,

$$nd^2 - 2d - k = 0 \quad \text{and} \quad nk = 0. \tag{4}$$

This proves (i). If $p \nmid n$ and $p \mid k$ then Eq. (4) is equivalent to $0 = nd^2 - 2d = d(nd-2)$. Since $Tr_{q^n/q}(\alpha + 2/n) = 1$, case (ii) is proved. Finally, if

$p \mid n$ then Eq. (4) is equivalent to $2d + k = 0$. Since $Tr_{q^n/q}(\alpha - k/2) = -1 - nk/2$, $\gamma$ generates a self-dual normal basis if and only if $nk \not\equiv -2 \pmod{p}$. This proves (iii). □

## References


[1] M. Christopoulou, T. Garefalakis, D. Panario and D. Thomson, *The trace of an optimal normal element and low complexity normal bases*, Des. Codes Cryptogr. **49** (2008), 199–215.

[2] M. Christopoulou, T. Garefalakis, D. Panario and D. Thomson, *Gauss periods as constructions of low complexity normal bases*, Des. Codes Cryptogr. **62** (2012), 43–62.

[3] S. Gao, *Normal bases over finite fields*, PhD Thesis, University of Waterloo, Canada, 1993.

[4] D. Jungnickel, *Trace-orthogonal normal bases*, Discrete Applied Mathematics **47** (1993), 233–249.

[5] A. Lempel and M. J. Weinberger, *Self-complementary normal bases in finite fields*, SIAM J. Discrete Math. **1** (1988), 758–767.

[6] Q. Liao, *The Gaussian normal basis and its trace basis over finite fields*, J. Number Theory **132** (2012), 1507–1518.

[7] R.C Mullin, I.M. Onyszchuk, S.A. Vanston and R.M. Wilson, *Optimal normal bases in GF($p^n$)*, Discrete Appl. Math. **22** (1989), 149–161.

[8] Y. Nogami, H. Nasu, Y. Morikawa and S. Uehara, *A method for constructing a self-dual normal basis in odd characteristic extension fields*, Finite Fields Appl. **14** (2008), 867–876.



Kitae Kim
Department of Mathematics
Inha University
Incheon 402-751, Korea
*E-mail*: ktkim@inha.ac.kr

Jeongil Namgoong
Department of Mathematics
Inha University
Incheon 402-751, Korea
*E-mail*: namgung@inha.edu

Ikkwon Yie
Department of Mathematics
Inha University
Incheon 402-751, Korea
*E-mail*: ikyie@inha.ac.kr