Normal and Self-dual Normal Bases from Factorization of $cx^{q+1} + dx^q - ax - b$

Ian F. Blake
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: ifblake@claude2.uwaterloo.can

Shuhong Gao, Ronald C. Mullin
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: sgao@violet.uwaterloo.can, rcmullin@watmath.uwaterloo.can

September 14, 1992

Abstract. The present paper is interested in a family of normal bases, considered by V. M. Sidel'nikov, with the property that all the elements in a basis can be obtained from one element by repeatedly applying to it a linear fractional function of the form $\varphi(x) = (ax + b)/(cx + d)$, $a, b, c, d \in F_q$. Sidel'nikov proved that the cross products for such a basis $\{\alpha_i\}$ are of the form $\alpha_i\alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$, $i \neq j$, where $e_k, \gamma \in F_q$. We will show that every such basis can be formed by the roots of an irreducible factor of $F(x) = cx^{q+1} + dx^q - ax - b$. We will construct: (a) a normal basis of F_{q^n} over F_q with complexity at most $3n - 2$ for each divisor n of $q - 1$ and for $n = p$ where p is the characteristic of F_q; (b) a self-dual normal basis of F_{q^n} over F_q for $n = p$ and for each odd divisor n of $q - 1$ or $q + 1$. When $n = p$, the self-dual normal basis constructed of F_{q^p} over F_q also has complexity at most $3p - 2$. In all cases, we will give the irreducible polynomials and the multiplication tables explicitly.

Abbreviated title: Normal Bases.

1991 Mathematics subject classification: 11T30, 11T06.

Key words: finite field, irreducible polynomial, normal basis.

1 Introduction

Let $N = \{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ be a normal basis of F_{q^n} over F_q with $\alpha_i = \alpha^{q^i}, 0 \leq i \leq n-1$, where q is a prime power p^m with p a prime and $m \geq 1$. The multiplication of elements in F_{q^n} is uniquely determined by the n cross products $\alpha_0\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, t_{ij} \in F_q$. The $n \times n$ matrix $T = (t_{ij})$ is called the multiplication table of N. As in [6], the number of nonzero elements in T is called the complexity of the normal basis N, denoted by C_N. In hardware and software implementations of finite field arithmetic, normal bases of low complexity offer considerable advantages. In [6] it is proved that $C_N \geq 2n-1$. When the lower bound is reached N is called an optimal normal basis of F_{q^n} over F_q. Two families of optimal normal bases are constructed in [6], and in [3] it is proved that these two families are essentially all the optimal normal bases in finite fields. Some normal bases of low complexity are constructed in [1]. A normal basis with the smallest complexity, if no optimal normal bases exist, is called a minimal normal basis.

The present paper is interested in a family of normal bases, considered by Sidel'nikov [8], with the property that all the elements in a basis can be obtained from one element by repeatedly applying to it a linear fractional function of the form $\varphi(x) = (ax+b)/(cx+d)$, $a, b, c, d \in F_q$. Sidel'nikov proved that the cross products for such a basis $\{\alpha_i\}$ are of the form $\alpha_i\alpha_j = e_{i-j}\alpha_i + e_{j-i}\alpha_j + \gamma$, $i \neq j$, where $e_k, \gamma \in F_q$. We will show that every such basis can be formed by the roots of an irreducible factor of $F(x) = cx^{q+1} + dx^q - ax - b$. We will construct a normal basis of F_{q^n} over F_q with complexity at most $3n-2$ for each divisor n of $q-1$ and for $n = p$ where p is the characteristic of F_q, and a self-dual normal basis of F_{q^n} over F_q for $n = p$ and for each odd divisor n of $q-1$ or $q+1$. When $n = p$, the self-dual normal basis constructed of F_{q^p} over F_q also has complexity at most $3p-2$. In all cases, we will give the irreducible polynomials and the multiplication tables explicitly. For this purpose, some properties of linear fractional functions and the complete factorization of $F(x)$ are discussed in sections 2 and 3, respectively.

2 On Linear Fractional Functions

In this section, we discuss some properties of the linear fractional function $\varphi(x) = (ax+b)/(cx+d)$ with $a, b, c, d \in F_q$ and $ad - bc \neq 0$. It is easy to see that $\varphi(x)$ defines a permutation on $F_q \cup \{\infty\}$, where

$$\frac{a\infty + b}{c\infty + d} := \frac{a}{c}, \quad \text{if } c \neq 0,$$
$$\frac{a\infty + b}{c\infty + d} := \infty, \quad \text{if } ad \neq 0, c = 0,$$
$$\frac{a}{0} := \infty, \quad \text{if } a \neq 0.$$

Actually, $\varphi(x)$ induces a permutation on $F_{q^n} \cup \{\infty\}$, for any $n \geq 1$. The inverse of $\varphi(x)$ is $\varphi^{-1}(x) = (-dx + b)/(cx - a)$.

For any two linear fractional functions φ and ψ, the composition $\varphi\psi$, defined as $\varphi\psi(x) = \varphi(\psi(x))$, is still a linear fractional function. It is well known that all the linear fractional functions over F_q form a group under composition and is isomorphic to the projective general linear group $PGL(2, q)$. The order of φ is the smallest positive integer t such that $\varphi^t(x) = x$, i.e., φ^t is the identity map.

For our purpose, we will deal with a linear fractional function $\varphi(x) = (ax + b)/(cx + d)$ with $c \neq 0$. The fixed points of $\varphi(x)$ satisfy

$$cx^2 - (a - d)x - b = 0. \tag{2.1}$$

The following two lemmas are easily checked.

Lemma 2.1 *Let $\varphi(x) = ax + b$ with $a \neq 0, 1$, be a linear mapping. Then*

$$\varphi = h^{-1}\psi h,$$

where $\psi(x) = ax$ and $h(x) = x + b/(a - 1)$.

Lemma 2.2 *Let $\varphi(x) = (ax+b)/(cx+d)$ with $c \neq 0$ and $ad-bc \neq 0$. Let $\Delta = (a-d)^2+4bc$. Then*

$$\varphi = h^{-1}\psi h,$$

where $h(x)$ and $\psi(x)$ are defined as follows:

(a) *When $\Delta = 0$, let x_0 be the only solution of (2.1) in F_q, that is, x_0 satisfies $cx_0^2 = -b$ and $2cx_0 = a - d$. Then $h(x) = (a/c - x_0)/(x - x_0)$ and $\psi(x) = x + 1$.*

(b) *When $\Delta \neq 0$, let x_0, x_1 be the two solutions of (2.1) in F_{q^2} and let $\xi = (a - cx_0)/(a - cx_1)$. Then*

$$h(x) = \frac{x - x_0}{x - x_1}, \quad \psi(x) = x\xi.$$

The order of φ is now easy to determine. The order of φ is equal to the order of ψ. If ψ is of the form $x + 1$ then the order of ψ is equal to the additive order p of 1 in F_q, where p is the characteristic of F_q. If ψ is of the form ξx, then the order of ψ is equal to the multiplicative order of ξ. In case **(b)** of Lemma 2.2, if Δ is a quadratic residue in F_q, then $x_0, x_1 \in F_q$, and $\xi \in F_q$. Hence $\xi^{q-1} = 1$ and the order of ξ is a divisor of $q - 1$. If Δ is a quadratic nonresidue in F_q, then $x_0, x_1 \in F_{q^2} \setminus F_q$ and $x_0^q = x_1, x_1^q = x_0$. Thus $\xi^q = ((a - cx_0)/(a - cx_1))^q = (a - cx_0^q)/(a - cx_1^q) = (a - cx_1)/(a - cx_0) = 1/\xi$. So $\xi^{q+1} = 1$ and the order of ξ divides $q + 1$. Therefore the order of φ is always a divisor of p, $q - 1$ or $q + 1$.

Lemma 2.3 *Let $a, b, c, d \in F_q$ with $c \neq 0$ and $ad - bc \neq 0$. Let $\varphi(x) = (ax + b)/(cx + d)$ with order t. Then, for $1 \leq i \leq t - 1$,*

$$\varphi^i(x) = \frac{e_i x + b/c}{x - e_{t-i}}, \quad e_i + e_{t-i} = \frac{a - d}{c} \tag{2.2}$$

where $e_1 = a/c$ and $e_{i+1} = \varphi(e_i)$ for $i = 1, \ldots, t - 2$.

Proof: It is routine to prove by induction on i that there exist $e_i, f_i \in F_q$ with $e_1 = a/c$, $f_1 = d/c$ such that

$$\varphi^i(x) = \frac{e_i x + b/c}{x + f_i},$$

and

$$e_i - f_i = \frac{a - d}{c}, \quad e_i = \varphi(e_{i-1})$$

for $i = 1, \ldots, t - 1$, where $e_0 = \infty$. Note that

$$\frac{e_{t-i} x + b/c}{x + f_{t-i}} = \varphi^{t-i}(x) = \varphi^{-i}(x) = (\varphi^i)^{-1}(x) = \frac{-f_i x + b/c}{x - e_i}.$$

We see that $f_i = -e_{t-i}$. This completes the proof. □

Lemma 2.4 *With the same notation as in Lemma 2.3, we have*

$$\sum_{j=1}^{t-1} e_j = \begin{cases} (t-1)(a-d)/(2c), & \text{if } p \neq 2, \\ a/c = d/c, & \text{if } p = 2 \text{ and } t = 2, \\ (a-d)/c, & \text{if } p = 2 \text{ and } t \equiv 3 \bmod 4, \\ 0, & \text{if } p = 2 \text{ and } t \equiv 1 \bmod 4, \end{cases} \tag{2.3}$$

where p is the characteristic of F_q.

Proof: We consider two cases according to the type of $\varphi(x)$.

Case I $\Delta = (a-d)^2 + 4bc = 0$. Then $t = p$ and, by Lemma 2.2, $\varphi(x) = h^{-1}\psi h(x)$ where

$$\psi(x) = x+1, \quad h(x) = \frac{a/c - x_0}{x - x_0}, \quad h^{-1}(x) = x_0 + \frac{a/c - x_0}{x},$$

with x_0 satisfying $2cx_0 = a - d$ and $cx_0^2 = -b$. Note that $\psi^i(x) = x + i$. We have

$$\begin{aligned}
\varphi^i(x) &= h^{-1}\psi^i h(x) \\
&= h^{-1}\left(\frac{a/c - x_0}{x - x_0} + i\right) \\
&= \frac{(a/c - x_0 - ix_0)x - ix_0^2}{ix + (a/c - x_0 - ix_0)}.
\end{aligned}$$

So

$$e_i = \frac{a/c - x_0}{i} + x_0, \quad \text{for } 1 \le i \le t-1.$$

Therefore

$$\begin{aligned}
\sum_{i=1}^{p-1} e_i &= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i^{-1} \\
&= (p-1)x_0 + (a/c - x_0)\sum_{i=1}^{p-1} i \\
&= \begin{cases} (p-1)x_0 = (t-1)(a-d)/(2c), & \text{if } p \neq 2, \\ a/c = d/c, & \text{if } p = 2. \end{cases}
\end{aligned}$$

Case II $\Delta = (a-d)^2 + 4bc \neq 0$. In this case, the order t of $\varphi(x)$ is a factor of $q-1$ or $q+1$. So $t \in F_q^*$. By Lemma 2.2, $\varphi(x) = h^{-1}\psi h(x)$ where

$$h(x) = \frac{x - x_0}{x - x_1}, \quad \psi(x) = \xi x, \quad \xi = \frac{a/c - x_0}{a/c - x_1},$$

with $x_0 + x_1 = (a-d)/c$ and $x_0 x_1 = -b/c$. Note that $h^{-1}(x) = (x_1 x - x_0)/(x-1)$ and $\psi^i(x) = \xi^i x$, we have

$$\begin{aligned}
\varphi^i(x) &= h^{-1}\psi^i h(x) \\
&= h^{-1}\left(\xi^i \frac{x - x_0}{x - x_1}\right) \\
&= \frac{(x_1\xi^i - x_0)x - x_0x_1(\xi^i - 1)}{(\xi^i - 1)x + x_1 - x_0\xi^i}.
\end{aligned}$$

So

$$e_i = \frac{x_1\xi^i - x_0}{\xi^i - 1} = x_1 + \frac{x_1 - x_0}{\xi^i - 1}, \quad \text{for } 1 \le i \le t-1,$$

and

$$\sum_{i=1}^{t-1} e_i = (t-1)x_1 + (x_0 - x_1)\sum_{i=1}^{t-1} \frac{1}{1-\xi^i}.$$

As ξ is a t-th primitive root of unity, we have

$$\prod_{i=1}^{t-1}(x - \xi^i) = (x^t - 1)/(x-1) = x^{t-1} + x^{t-2} + \cdots + x + 1. \tag{2.4}$$

Letting $x = 1$ in equation (2.4), we get

$$\prod_{i=1}^{t-1}(1 - \xi^i) = t. \tag{2.5}$$

Taking derivatives with respect to x on both sides of (2.4), we have

$$\prod_{i=1}^{t-1}(x - \xi^i)(\sum_{i=1}^{t-1} \frac{1}{x - \xi^i}) = (t-1)x^{t-2} + (t-2)x^{t-3} + \cdots + 2x + 1. \tag{2.6}$$

Letting $x = 1$ in (2.6), we see that

$$\sum_{i=1}^{t-1} \frac{1}{1-\xi^i} = (\sum_{i=1}^{t-1} i)/t = \begin{cases} (t-1)/2, & \text{if } p \ne 2, \\ 1, & \text{if } p = 2 \text{ and } t \equiv 3 \bmod 4, \\ 0, & \text{if } p = 2 \text{ and } t \equiv 1 \bmod 4, \end{cases}$$

(Note that t is odd when $p = 2$.) Therefore

$$\sum_{i=1}^{t-1} e_i = \begin{cases} ((t-1)/2)(x_0 + x_1) = (t-1)(a-d)/(2c), \quad \text{if } p \ne 2, \\ x_0 - x_1 = (a-d)/c, \quad \text{if } p = 2 \text{ and } t \equiv 3 \bmod 4, \\ 0, \quad \text{if } p = 2 \text{ and } t \equiv 1 \bmod 4. \end{cases}$$

This completes the proof. □

The following theorem is proved by Sidel'nikov [8, Theorem 2]:

Theorem 2.5 *Let $a, b, c, d \in F_q$ with $c \ne 0$ and $ad - bc \ne 0$. Let θ be a root of $F(x) = cx^{q+1} + dx^q - ax - b$ in some extension field of F_q, not fixed by $\varphi(x) = (ax+b)/(cx+d)$ whose order is assumed to be t. Then*

$$\theta, \varphi(\theta), \cdots, \varphi^{t-1}(\theta)$$

are linearly independent over F_q, if $\sum_{i=0}^{t-1} \varphi^i(\theta) \ne 0$.

This theorem indicates that if we can factor $F(x)$ then we will obtain normal bases over F_q. The factorization of $F(x)$ is discussed in the next section.

3 Factorization of $cx^{q+1} + dx^q - ax - b$

The complete factorization of $F(x) = cx^{q+1} + dx^q - ax - b$, $a, b, c, d \in F_q$, into irreducible factors was established by Ore [7, pp. 264–270] by using his theory of linearized polynomials. In this section, we briefly discuss how this can be done without resorting to linearized polynomials. For the detail, the reader is referred to [2]. To exclude the trivial cases, we assume that $ad - bc \neq 0$. Let $\varphi(x) = (ax + b)/(cx + d)$ be the linear fractional function associated with $F(x)$. As noted in section 2, $\varphi(x)$ induces a permutation on $F_{q^n} \cup \{\infty\}$, for any $n \geq 1$. We assume that the order of φ is t in this section.

Let θ be a root of $F(x) = (cx + d)x^q - (ax + b)$. Then

$$\theta^q = \frac{a\theta + b}{c\theta + d} = \varphi(\theta).$$

Note that

$$\theta^{q^2} = (\varphi(\theta))^q = \varphi(\theta^q) = \varphi(\varphi(\theta)) = \varphi^2(\theta).$$

By induction we see that $\theta^{q^i} = \varphi^i(\theta)$, $i \geq 0$. So

$$\theta, \varphi(\theta), \cdots, \varphi^{t-1}(\theta) \tag{3.1}$$

are all the conjugates of θ over F_q. If θ is a fixed point of $\varphi(x)$ then $\theta \in F_q$, and $x - \theta$ is a factor of $F(x)$. If θ is not a fixed point of $\varphi(x)$, then, by Theorem 2.5, the elements of (3.1) are distinct and θ is of degree t over F_q. In the latter case, the minimal polynomial of θ over F_q is an irreducible factor of $F(x)$ of degree t. So an irreducible factor of $F(x)$ is either linear or of degree t. We first deal with two special cases.

Theorem 3.1 *Let $\xi \in F_q \setminus \{0\}$ with multiplicative order t. Then the following factorization over F_q is complete:*

$$x^{q-1} - \xi = \prod_{j=1}^{(q-1)/t} (x^t - \beta_j),$$

where β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t} - \xi$ in F_q.

Proof: Let θ be a root of $x^{q-1} - \xi$ in some extension field of F_q. Then $\theta^{q^i} = \theta\xi^i, i \geq 1$. All the distinct conjugates of θ over F_q are $\theta, \theta\xi, \ldots, \theta\xi^{t-1}$. The minimal polynomial of θ over

F_q is

$$\prod_{i=0}^{t-1}(x-\theta\xi^i) = x^t - \theta^t,$$

which divides $x^{q-1}-\xi$. This means that any irreducible factor of $x^{q-1}-\xi$ is of the form $x^t-\beta$ where $\beta \in F_q$. One can prove that $x^t-\beta$ divides $x^{q-1}-\xi$ if and only if β is a root of $x^{(q-1)/t}-\xi$. This completes the proof. □

Theorem 3.2 *For $x^q-(x+b)$ with $b \in F_q^*$, the following factorization over F_q is complete:*

$$x^q-(x+b) = \prod_{j=1}^{q/p}(x^p - b^{p-1}x - b^p\beta_j) \tag{3.2}$$

where β_j are the distinct elements of F_q with $Tr_{q/p}(\beta_j)=1$ and p is the characteristic of F_q.

Proof: Let θ be a root of $F(x)=x^q-(x+b)$. Then $\theta^{q^i}=\theta+ib, i\geq 1$. So the conjugates of θ over F_q are $\theta, \theta+b, \ldots, \theta+(p-1)b$. The minimal polynomial of θ over F_q is

$$\begin{aligned}
\prod_{i=0}^{p-1}[x-(\theta+ib)] &= b^p\prod_{i=0}^{p-1}[\frac{x-\theta}{b}-i] \\
&= b^p[(\frac{x-\theta}{b})^p - \frac{x-\theta}{b}] \\
&= x^p - b^{p-1}x + \theta(b^{p-1}-\theta^{p-1}).
\end{aligned}$$

Hence an irreducible factor of $x^q-(x+b)$ is of the form

$$x^p - b^{p-1}x - \beta, \quad \beta \in F_q. \tag{3.3}$$

Let γ be a root of (3.3) in some extension field of F_q. Then we have

$$(\frac{\gamma}{b})^{p^i} - (\frac{\gamma}{b})^{p^{i-1}} = (\frac{\beta}{b^p})^{p^{i-1}}, \quad 1 \leq i \leq m, \tag{3.4}$$

where $q=p^m$. Summing (3.4) yields

$$\gamma^{p^m} - \gamma = b\mathrm{Tr}_{q/p}(\frac{\beta}{b^p}).$$

Consequently (3.3) divides $F(x)=x^{p^m}-x-b$ if and only if $\mathrm{Tr}_{q/p}(\beta/b^p)=1$. Note that there are $q/p=p^{m-1}$ elements β in F_q with trace 1, and the proof is completed. □

In general we show that the factorization of $F(x)$ can be reduced to factoring $x^q - x - 1$, $x^{q-1} - \xi$ or $x^{q+1} - \xi$. Let $\varphi = h^{-1}\psi h$ as in Lemmas 2.1 and 2.2. For any root θ of $F(x)$ that is not fixed by φ, we have

$$h(\theta^q) = \psi(h(\theta)). \tag{3.5}$$

If Δ is a quadratic residue in F_q, then $h(\theta^q) = (h(\theta))^q$. Thus $\eta = h(\theta)$ is a root of $x^q - x - 1$ or $x^q - \xi x = x(x^{q-1} - \xi)$ according as $\psi(x) = x + 1$ or $\psi(x) = \xi x, \xi \in F_q$. So by the factorization of $x^q - x - 1$ and $x^{q-1} - \xi$ as in Theorems 3.1 and 3.2 we obtain the factorization of $F(x)$ as follows.

Theorem 3.3 *For $a, b \in F_q$ with $a \neq 0, 1$, the following factorization over F_q is complete:*

$$x^q - (ax + b) = (x - \frac{b}{a-1}) \prod_{j=1}^{(q-1)/t} ((x - \frac{b}{a-1})^t - \beta_j),$$

where t is the multiplicative order of a and β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t} - a$.

Theorem 3.4 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc = 0$, the following factorization over F_q is complete:*

$$\begin{aligned} &(cx + d)x^q - (ax + b) \\ &= (x - x_0) \prod_{j=1}^{q/p} [(x - x_0)^p + \frac{1}{\beta_j}(a/c - x_0)(x - x_0)^{p-1} - \frac{1}{\beta_j}(a/c - x_0)^p] \end{aligned}$$

where $x_0 \in F_q$ is the unique solution of (2.1) and β_j are all the q/p distinct elements of F_q with $Tr_{q/p}(\beta_j) = 1$.

Theorem 3.5 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic residue in F_q, the following factorization over F_q is complete:*

$$\begin{aligned} &(cx + d)x^q - (ax + b) \\ &= (x - x_0)(x - x_1) \prod_{j=1}^{(q-1)/t} \frac{1}{1 - \beta_j} [(x - x_0)^t - \beta_j (x - x_1)^t] \end{aligned}$$

where $x_0, x_1 \in F_q$ are the two distinct roots of (2.1), t is the multiplicative order of $\xi = (a - cx_0)/(a - cx_1)$ and β_j are all the $(q-1)/t$ distinct roots of $x^{(q-1)/t} - \xi$ in F_q.

If Δ is not a quadratic residue in F_q, the situation is a little more complicated, as in this case $x_0, x_1, \xi \notin F_q$. Noting that $x_0^q = x_1$ and $x_1^q = x_0$, we have $h(\theta^q) = (1/h(\theta))^q$. The equation (3.5) implies that $\eta = 1/h(\theta)$ is a root of $x^{q+1} - \xi$. So by factoring $x^{q+1} - \xi$ over F_{q^2} we can obtain the factorization of $F(x)$ over F_{q^2}. Then by "combining" these factors we get the factorization of $F(x)$ over F_q as in Theorem 3.6.

Theorem 3.6 *For $a, b, c, d \in F_q$ with $c \neq 0$, $ad - bc \neq 0$ and $\Delta = (a-d)^2 + 4bc \neq 0$ being a quadratic nonresidue in F_q, the following factorization over F_q is complete:*

$$\begin{aligned} F(x) &= (cx+d)x^q - (ax+b) \\ &= \prod_{j=1}^{(q+1)/t} \frac{1}{1-\beta_j}[(x-x_0)^t - \beta_j(x-x_1)^t] \end{aligned} \tag{3.6}$$

where $x_0, x_1 \in F_{q^2}$ are the two distinct roots of (2.1), t is the multiplicative order of $\xi = (a-cx_1)/(a-cx_0)$ and β_j are all the $(q+1)/t$ distinct roots of $x^{(q+1)/t} - \xi$ in F_{q^2}.

Let $f(x)$ be any nonlinear irreducible factor of $F(x)$ of degree t and let α be a root of $f(x)$. From the discussion at the beginning of this section, we see that $\varphi^i(\alpha), i = 0, 1, \ldots, t-1$ are all the roots of $f(x)$ and, by Theorem 2.5, they are linearly independent over F_q if $\mathrm{Tr}(\alpha) \neq 0$. But $\mathrm{Tr}(\alpha)$ is just the negative of the coefficient of x^{t-1} in $f(x)$. By examining the factors in the above explicit factorizations, we have

Theorem 3.7 *Let $F(x) = (cx+d)x^q - (ax+b)$ with $a, b, c, d \in F_q$, $c \neq 0$ and $ad - bc \neq 0$. Then a monic nonlinear irreducible factor $f(x)$ of $F(x)$ of degree t has linearly dependent roots over F_q if and only if the coefficient of x^{t-1} in $f(x)$ is zero. The latter happens only if $\Delta = (a-d)^2 + 4bc \neq 0$ and $f(x)$ is of the form*

$$\frac{1}{x_1 - x_0}[x_1(x-x_0)^t - x_0(x-x_1)^t],$$

where x_0 and x_1 are solutions of (2.1).

This shows that every nonlinear irreducible factor of $F(x)$, except for possibly one, has linearly independent roots.

4 Normal Bases

As Theorem 3.7 shows, when $c \neq 0$ the roots of an irreducible nonlinear factor of $F(x)$ form a normal basis over F_q (except possibly for one factor). This section is devoted to discussing the properties of these bases. We will show how to construct a normal basis of F_{q^n} over F_q with complexity at most $3n-2$ for $n=p$ and for each divisor n of $q-1$. For this purpose we first compute the multiplication tables of the normal bases formed by the roots of an irreducible factor of $F(x)$.

Without loss of generality, we assume that $F(x) = x^{q+1} + dx^q - ax - b$ with $a, b, d \in F_q$ and $b \neq ad$. Assume that $\varphi(x) = (ax+b)/(x+d)$ has order n and that, by Lemma 2.3, $\varphi^i(x) = (e_i x + b)/(x - e_{n-i})$ with $e_i = \varphi^{i-1}(a)$, $1 \leq i \leq n-1$. Let $f(x)$ be any irreducible nonlinear factor of $F(x)$ and α a root of $f(x)$. Then $f(x)$ has degree n and its roots are

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha), \quad i = 0, 1, \cdots, n-1,$$

and they form a normal basis of F_{q^n} over F_q if the coefficient of x^{n-1} in $f(x)$ is not zero (or $\mathrm{Tr}(\alpha) \neq 0$), by Theorem 3.7.

Theorem 4.1 *Let $F(x) = x^{q+1} + dx^q - (ax+b)$ with $a, b, d \in F_q$ and $b \neq ad$. Let $f(x)$ be an irreducible factor of $F(x)$ of degree $n > 1$ and let α be a root of it. Then all the roots of $f(x)$ are*

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha), \quad i = 0, 1, \cdots, n-1, \tag{4.1}$$

where $\varphi(x) = (ax+b)/(x+d)$. If $\tau = \sum_{i=0}^{n-1} \alpha_i$, the negative of the coefficient of x^{n-1} in $f(x)$, is not zero, then (4.1) form a normal basis of F_{q^n} over F_q such that

$$\alpha_0 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \cdots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} + \begin{pmatrix} b^* \\ b \\ b \\ \vdots \\ b \end{pmatrix} \tag{4.2}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $b^* = -b(n-1)$ and $\tau^* = \tau - \epsilon$ with

$$\epsilon = \sum_{i=1}^{n-1} e_i = \begin{cases} (n-1)(a-d)/2, & \text{if } p \neq 2, \\ a = d, & \text{if } p = n = 2, \\ a - d, & \text{if } p = 2 \text{ and } n \equiv 3 \bmod 4, \\ 0, & \text{if } p = 2 \text{ and } n \equiv 1 \bmod 4. \end{cases}$$

Proof: We just need to prove (4.2). By Lemma 2.3, for $i \geq 1$,

$$\alpha_i = \varphi^i(\alpha) = \frac{e_i\alpha_0 + b}{\alpha_0 - e_{n-i}}.$$

So

$$\alpha_0\alpha_i = e_i\alpha_0 + e_{n-i}\alpha_i + b.$$

For $i = 0$, we have

$$\alpha_0\alpha_0 = \alpha_0(\tau - \sum_{j=1}^{n-1}\alpha_j) = (\tau - \sum_{j=1}^{n-1}e_j)\alpha_0 - \sum_{j=1}^{n-1}e_{n-j}\alpha_j - b(n-1).$$

The theorem follows from Lemma 2.4. □

The next theorem can be viewed as the "converse" of Theorem 4.1.

Theorem 4.2 *Let $n > 2$ and $\alpha_i = \alpha^{q^i}$ for $0 \leq i \leq n-1$. Suppose that $\{\alpha_i\}$ is a normal basis of F_{q^n} over F_q and satisfies*

$$\alpha_i\alpha_j = a_{ij}\alpha_i + b_{ij}\alpha_j + \gamma_{ij}, \quad \textit{for all } 0 \leq i \neq j \leq n-1, \tag{4.3}$$

where $a_{ij}, b_{ij}, \gamma_{ij} \in F_q$. Then there are constants $\gamma, e_1, e_2, \ldots, e_{n-1} \in F_q$ such that

(a) *$e_i = \varphi(e_{i-1})$, for $2 \leq i \leq n-1$, and*

$$a_{ij} = e_{j-i}, b_{ij} = e_{i-j}, \gamma_{ij} = \gamma, \quad \textit{for all } i \neq j,$$

where $\varphi(x) = (e_1x + \gamma)/(x - e_{n-1})$ and the subscripts of e are calculated modulo n;

(b) *the minimal polynomial of α is a factor of $F(x) = x^{q+1} - e_{n-1}x^q - (e_1x + \gamma)$, and thus n must be a factor of p, $q-1$ or $q+1$.*

Proof: Let $e_k = a_{0k}$ and $\gamma_k = \gamma_{0k}$ for $k = 1, 2, \cdots, n-1$. Then

$$\alpha_0\alpha_k = e_k\alpha_0 + b_{0k}\alpha_k + \gamma_k. \tag{4.4}$$

Raising (4.4) to the q^{n-k}-th power on both sides, we have

$$\alpha_0\alpha_{n-k} = b_{0k}\alpha_0 + e_k\alpha_{n-k} + \gamma_k. \tag{4.5}$$

Subtracting (4.5) from (4.4), with the k in (4.4) replaced by $n-k$, gives

$$(e_{n-k}-b_{0k})\alpha_0+(b_{0\,n-k}-e_k)\alpha_{n-k}+\gamma_{n-k}-\gamma_k=0. \tag{4.6}$$

As $n>2$ and the α_i's are linearly independent over F_q, the equation (4.6) implies that

$$b_{0k}=e_{n-k},\quad \gamma_k=\gamma_{n-k},\quad 1\le k\le n-1$$

Therefore

$$\alpha_0\alpha_k=e_k\alpha_0+e_{n-k}\alpha_k+\gamma_k,\quad 1\le k\le n-1. \tag{4.7}$$

Now for any $i\ne j$, raising (4.7) to the q^i-th power and letting $k=j-i$, we have

$$\alpha_i\alpha_j=e_{j-i}\alpha_i+e_{i-j}\alpha_j+\gamma_{j-i}. \tag{4.8}$$

Comparing (4.8) and (4.3) gives

$$a_{ij}=e_{j-i},\quad b_{ij}=e_{i-j},\quad \gamma_{ij}=\gamma_{j-i}, \tag{4.9}$$

which proves part of (a).

We shall prove the remaining part of (a) together with (b). To this purpose, note that a special case of (4.8) is

$$\alpha_i\alpha_{i+1}=e_{n-1}\alpha_{i+1}+e_1\alpha_i+\gamma_1,\quad 0\le i<n-1,$$

or

$$\alpha_{i+1}=\frac{e_1\alpha_i+\gamma_1}{\alpha_i-e_{n-1}}=\varphi(\alpha_i),\quad 0\le i<n-1, \tag{4.10}$$

where $\varphi(x)=(e_1x+\gamma)/(x-e_{n-1})$ with $\gamma=\gamma_1$. So, by induction on i, we see that $\alpha_i=\varphi^i(\alpha_0)=\varphi^i(\alpha), 0\le i\le n-1$. We know, by Lemma 2.3, that

$$\varphi^i(x)=(a_ix+\gamma)/(x-a_{n-i}),\quad 0\le i\le n-1$$

where $a_i=\varphi(a_{i-1})$, for $i\ge 1$, and $a_1=e_1$. Thus (4.10) implies that

$$\alpha_i=\frac{a_i\alpha_0+\gamma}{\alpha_0-a_{n-i}},$$

i.e.,

$$\alpha_0\alpha_i=a_i\alpha_0+a_{n-i}\alpha_i+\gamma. \tag{4.11}$$

Comparing (4.11) to (4.7), we have

$$e_i = a_i, \quad e_{n-i} = a_{n-i}, \quad \gamma_i = \gamma.$$

This proves (a). For (b), note that $\alpha_1 = \alpha^q$ and that (4.7) with $k = 1$ means α is a root of $F(x) = x^{q+1} - e_{n-1}x^q - e_1 x - \gamma$. Therefore the minimal polynomial of α divides $F(x)$. This completes the proof. $\square$

Theorem 4.3 *For every $a, \beta \in F_q^*$ with $Tr_{q/p}(\beta) = 1$,*

$$x^p - \frac{1}{\beta}ax^{p-1} - \frac{1}{\beta}a^p, \tag{4.12}$$

is irreducible over F_q and its roots form a normal basis of F_{q^p} over F_q with complexity at most $3p - 2$. The multiplication table is

$$\begin{pmatrix} \tau^* & -e_{p-1} & -e_{p-2} & \dots & -e_1 \\ e_1 & e_{p-1} & & & \\ e_2 & & e_{p-2} & & \\ \vdots & & & \ddots & \\ e_{p-1} & & & & e_1 \end{pmatrix} \tag{4.13}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ for $i \geq 1$, $\varphi(x) = ax/(x + a)$, and $\tau^* = a/\beta$ if $p \neq 2$ or $a/\beta - a$ if $p = 2$.

Proof: Let $F(x) = (x+a)x^q - ax$ and $\varphi(x) = ax/(x+a)$. Then $F(x)$ satisfies the conditions of Theorem 3.4 with $b = 0, c = 1, d = a$, $\Delta = 0$, and $x_0 = 0$. So (4.12) is an irreducible factor of $F(x)$. As the coefficient of x^{p-1} in (4.12) is $-a/\beta \neq 0$, by Theorem 4.1, the roots of (4.12) form a normal basis and its multiplication table is (4.13). The complexity is obviously at most $3p - 2$. $\square$

Theorem 4.4 *Let n be any factor of $q - 1$. Let $\beta \in F_q$ with multiplicative order t such that $\gcd(n, (q-1)/t) = 1$ and let $a = \beta^{(q-1)/n}$. Then*

$$x^n - \beta(x - a + 1)^n \tag{4.14}$$

is irreducible over F_q and its roots form a normal basis of F_{q^n} over F_q of complexity at most $3n - 2$. The multiplication table is

$$\begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \dots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \tag{4.15}$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $\varphi(x) = ax/(x+1)$ *and* $\tau^* = -n(a-1)\beta/(1-\beta) - \epsilon$ *with* ϵ *specified as in Theorem 4.1 (with* $d = 1$*).*

Proof: It is easy to see that a has multiplicative order n. Then $\varphi(x) = ax/(x+1)$ has $x_0 = 0$ and $x_1 = a-1$ as fixed points, and $\xi = (a-x_0)/(a-x_1) = a$ has order n. So φ has order n. Note that β is a root of $x^{(q-1)/n} - a$. By Theorem 3.5, the polynomial (4.14) is an irreducible factor of $F(x) = x^{q+1} + x^q - ax$. Note that the coefficient of x^{n-1} in (4.14) is $n(a-1) \neq 0$. By Theorem 4.1 (with $b = 0, d = 1$), the roots of (4.14) form a normal basis of F_{q^n} over F_q and its multiplication table is (4.15). The complexity is obviously at most $3n-2$. □

The following table is the result of a computer search for the minimal complexity of normal bases. It indicates that when $n|(q-1)$ the minimal complexity is often $3n-3$ or $3n-2$. This indicates that the normal bases constructed in Theorems 4.3 and 4.4 often have complexity very close to the minimal complexity. In the table, † indicates that the minimal

q	5	7	7	11	11	13	13	17	19
n	4	3	6	5	10	3	4	4	3
min	9	6	16†	12	28†	6	7⋆	7⋆	6

complexity is $3n-2$ and ⋆ indicates optimal complexity, i. e., $2n-1$. Other minimal values are of the form $3n-3$.

5 Self-dual Normal Bases

A basis $B = \{\beta_0, \beta_1, \cdots, \beta_{n-1}\}$ is called a dual basis of $A = \{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ if $\mathrm{Tr}(\alpha_i\beta_j)$ $= \delta_{ij} = 0$ for $i \neq j$, and 1 for $i = j$, where Tr is the trace function of F_{q^n} into F_q defined as $\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \in F_q$, $\alpha \in F_{q^n}$. One can prove that, for each basis A of F_{q^n} over F_q, there is a unique dual basis. Also, if A is normal then so is its dual. If the dual basis of A coincides with A, then A is called a self-dual basis, that is, a basis $A = \{\alpha_i\}$ is called self-dual if $\mathrm{Tr}(\alpha_i\alpha_j) = \delta_{ij}$. Lempel and Weinberger [5] proved

Theorem 5.1 *A self-dual normal basis of* F_{q^n} *over* F_q *exists if and only if one of the following conditions is satisfied*

(a) *q is even and n is not a multiple of* 4*,*

(b) *both q and n are odd.*

Later, Jungnickel, Menezes and Vanstone [4] determined the total number of self-dual bases and self-dual normal bases of F_{q^n} over F_q.

However the proofs of these results are not constructive. In this section, we will construct a self-dual normal basis of F_{q^n} over F_q for every n in the following cases:

(a) $n = p$, the characteristic of F_q,

(b) $n|(q-1)$ and n is odd,

(c) $n|(q+1)$ and n is odd.

One can check that the conditions in Theorem 5.1 are satisfied by each of the three cases.

Theorem 5.2 *Let $N = \{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ with $\alpha_i = \alpha^{q^i}$ be a normal basis of F_{q^n} over F_q satisfying*

$$\alpha_i\alpha_j = e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma, \textit{for all } i \neq j,$$

where $e_1, e_2, \cdots, e_{n-1}, \gamma \in F_q$. Let $\tau = Tr_{q^n/q}(\alpha)$ and $\lambda = -(e_1 + e_{n-1}) - n\gamma/\tau$. Then

$$\{\frac{1}{\tau(\tau + n\lambda)}(\alpha_i + \lambda) : \quad i = 0, 1, \cdots, n-1\}$$

is the dual basis of N.

Proof: Note that, for $i \neq j$,

$$\begin{aligned}
\mathrm{Tr}_{q^n/q}(\alpha_i(\alpha_j + \lambda)) &= \mathrm{Tr}_{q^n/q}(\lambda\alpha_i + e_{j-i}\alpha_i + e_{i-j}\alpha_j + \gamma) \\
&= \lambda\tau + e_{j-i}\tau + e_{i-j}\tau + n\gamma \\
&= \tau(\lambda + e_1 + e_{n-1}) + n\gamma \\
&= 0,
\end{aligned}$$

and

$$\mathrm{Tr}_{q^n/q}(\alpha_i(\alpha_i + \lambda)) = \mathrm{Tr}(\alpha_i(\tau + \lambda - \sum_{j\neq i}\alpha_j))$$

$$
\begin{aligned}
&= \mathrm{Tr}(\alpha_i(\tau + n\lambda - \sum_{j\neq i}(\alpha_j + \lambda))) \\
&= \mathrm{Tr}(\alpha_i)(\tau + n\lambda) - \sum_{j\neq i}\mathrm{Tr}(\alpha_i(\alpha_j + \lambda)) \\
&= \tau(\tau + n\lambda).
\end{aligned}
$$

The result is proved. □

We now proceed to determine when the roots of an irreducible factor of $F(x) = x^{q+1} + dx^q - ax - b$ form a self-dual normal basis. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis generated by a root α of $F(x)$ with $\alpha_i = \alpha^{q^i}$ and let $\tau = \mathrm{Tr}_{q^n|q}(\alpha)$. By Theorem 4.1 and Lemma 2.3, we have, for $i \neq 0$,

$$
\begin{aligned}
\mathrm{Tr}_{q^n/q}(\alpha_0\alpha_i) &= e_i\mathrm{Tr}(\alpha_0) + e_{n-i}\mathrm{Tr}(\alpha_i) + nb \\
&= \tau(e_i + e_{n-i}) + nb \\
&= \tau(a - d) + nb, \qquad (5.1)
\end{aligned}
$$

and

$$
\begin{aligned}
\mathrm{Tr}_{q^n/q}(\alpha_0\alpha_0) &= \tau(\tau - \epsilon) - \tau\epsilon - nb(n-1) \\
&= \begin{cases} \tau^2, & \text{if } p = 2, \\ \tau^2 - (n-1)(\tau(a-d) + nb), & \text{if } p \neq 2. \end{cases} \qquad (5.2)
\end{aligned}
$$

Therefore α generates a self-dual normal basis if $\tau = \mathrm{Tr}(\alpha) = 1$ and $(a - d) + nb = 0$. By examining the irreducible factors in Theorems 3.4, 3.5 and 3.6, we find that these two conditions can be satisfied. More explicitly, we have the following three results.

Theorem 5.3 *For any $\beta \in F_q^*$ with $Tr_{q/p}(\beta) = 1$,*

$$
x^p - x^{p-1} - \beta^{p-1} \qquad (5.3)
$$

is irreducible over F_q and its roots form a self-dual normal basis of F_{q^p} over F_q with complexity at most $3p-2$. The multiplication table is (4.13) where $e_1 = \beta$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $\varphi(x) = \beta x/(x + \beta)$, and $\tau^* = 1$ if $p \neq 2$ or $\tau^* = 1 - \beta$ if $p = 2$.

Proof: Let $F(x) = (x + \beta)x^q - \beta x$. Then, by Theorem 3.4, the polynomial (5.3) is an irreducible factor of $F(x)$ (where $b = 0$, $c = 1$, $d = a = \beta$, $x_0 = 0$ and $\beta_j = \beta$). Since $a - d = b = 0$ and $\tau = 1$ in (5.1) and (5.2), the roots of (5.3) form a self-dual normal basis. Its multiplication table is (4.13), by Theorem 4.1. □.

Theorem 5.4 *Let n be an odd factor of $q-1$ and $\xi \in F_q$ of multiplicative order n. Then there exists $u \in F_q$ such that $(u^2)^{(q-1)/n} = \xi$. Let $x_0 = (1+u)/n$ and $x_1 = (1+u)/(nu)$. Then the monic polynomial*

$$\frac{1}{1-u^2}[(x-x_0)^n - u^2(x-x_1)^n] \tag{5.4}$$

is irreducible over F_q and its roots form a self-dual normal basis of F_{q^n} over F_q. The multiplication table is (4.2) with $a = (x_0 - \xi x_1)/(1-\xi)$, $b = -x_0x_1$, $d = a - (x_0 + x_1)$ and $\tau = 1$.

Proof: We first prove that there exists at least one root of $x^{(q-1)/n} - \xi$ that is a quadratic residue in F_q. Let ζ be a primitive element in F_q. Let t be an odd factor of $q-1$ such that $n|t$ and $\gcd(n, (q-1)/t) = 1$. Then $\zeta_0 = \zeta^{(q-1)/t}$ is a t-th primitive root of unity. Since t is odd, ζ_0^2 is also a t-th primitive root of unity. Let $d = t/n$. Then there is an integer i such that $(\zeta_0^2)^{id} = \xi$, that is,

$$(\zeta^{(q-1)/t})^{2id} = (\zeta^{2i})^{(q-1)/n} = \xi.$$

So ζ^{2i} is a root of $x^{(q-1)/n} - \xi$ and is a quadratic residue in F_q. Therefore we can take $u = \zeta^i$.

Now by applying Theorem 3.5, we see that (5.4) is an irreducible factor of $F(x) = (x+d)x^q - (ax+b)$. The negative of the coefficient of x^{n-1} in (5.4) is

$$\tau = \frac{n(x_0 - u^2x_1)}{1-u^2} = 1.$$

By Theorem 4.1, the roots of (5.4) form a normal basis of F_{q^n} over F_q with the claimed multiplication table. Note that

$$a - d = x_0 + x_1 = \frac{(u+1)}{n} + \frac{u+1}{nu} = \frac{(u+1)^2}{nu} = nx_0x_1 = -nb,$$

that is, $\tau(a-d) + nb = 0$. It follows from (5.1) and (5.2) that the roots of (5.4) form a self-dual normal basis. □

Theorem 5.5 *Let n be an odd factor of $q+1$ and let $\xi \in F_{q^2}$ be a root of $x^{q+1} - 1$ with multiplicative order n. Then there is a root u of $x^{q+1} - 1$ such that $(u^2)^{(q+1)/n} = \xi$. Let $x_0 = (1+u)/n$ and $x_1 = (1+u)/(nu)$. Then*

$$\frac{1}{1-u^2}[(x-x_0)^n - u^2(x-x_1)^n] \tag{5.5}$$

is in $F_q[x]$ and is irreducible over F_q with its roots forming a self-dual normal basis of F_{q^n} over F_q. The multiplication table is (4.2) with $a = (x_1 - \xi x_0)/(1 - \xi)$, $b = -x_0 x_1$, $d = a - (x_0 + x_1)$ and $\tau = 1$.

Proof: The proof of the existence of u is similar to that in the proof of Theorem 5.4 by taking ζ to be a $(q+1)$th primitive root of unity in F_{q^2}. We next prove that $a, b, d \in F_q$ and (5.5) is in $F_q[x]$. Note that ξ, u and u^2 are all $(q+1)$th roots of unity and we have $\xi^q = 1/\xi$, $u^q = 1/u$ and $(u^2)^q = 1/u^2$. Thus $x_0^q = x_1$ and $x_1^q = x_0$. So $a^q = a$, $b^q = b$ and $d^q = d$, that is, $a, b, d \in F_q$. Denote the polynomial (5.5) by $\phi(x)$ and note that

$$\begin{aligned}
(\phi(x))^q &= \frac{1}{1-(u^2)^q}[(x^q - x_0^q)^n - (u^2)^q (x^q - x_1^q)^n] \\
&= \frac{1}{1-1/u^2}[(x^q - x_1)^n - 1/u^2 (x^q - x_0)^n] \\
&= \phi(x^q).
\end{aligned}$$

We see that the coefficients of $\phi(x)$ are in F_q.

To prove that (5.5) is irreducible over F_q, we apply Theorem 3.6. It is easy to check that, with a, b, d as defined in Theorem 5.5, x_0 and x_1 are the two distinct solutions of (2.1) with $c = 1$ and $(a - x_1)/(a - x_0) = \xi$ which is of order n. Now since u^2 is assumed to be a solution of $x^{(q+1)/q} - \xi$, it follows from Theorem 3.6 that (5.5) is an irreducible factor of $F(x) = (x + d)x^q - (ax + b)$.

As the coefficient of x^{n-1} in (5.5) is $(-nx_0 + nu^2 x_1)/(1 - u^2) = -1$, the trace of any root of (5.5) is $\tau = 1$. It is easy to check that $\tau(a - d) + nb = 0$. It follows from (5.1) and (5.2) that the roots of (5.5) form a self-dual normal basis. The multiplication table follows from Theorem 4.1. □

References

[1] D.W. Ash, I.F. Blake, and S.A. Vanstone, "Low complexity normal bases", *Discrete Applied Math.* **25** (1989), 191–210.

[2] I.F. Blake, S. Gao and R.C. Mullin, "Factorization of $cx^{q+1} + dx^q - ax - b$ and normal bases over $GF(q)$", *Research report CORR91-26*, Faculty of Mathematics, University of Waterloo, 1991.

[3] S. Gao and H.W. Lenstra, "Optimal normal bases", to appear in *Designs, Codes and Cryptography*, 1992.

[4] D. Jungnickel, A. J. Menezes and S. A. Vanstone, "On the number of self-dual bases of $GF(q^m)$ over $GF(q)$", *Proc. Amer. Math. Soc.* **109** (1990), 23–29.

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

[6] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Math.*, **22** (1988/89), 149-161.

[7] O. Ore, "Contributions to the theory of finite fields", *Trans. Amer. Math. Soc.* **36** (1934), 243–274.

[8] V.M. Sidel'nikov, "On normal bases of a finite field", *Math. USSR Sbornik* **61**(1988), 485–494.