The trace of an optimal normal element and low complexity normal bases

Maria Christopoulou, Theo Garefalakis,
Daniel Panario and David Thomson

December 24, 2009

Abstract

Let $\mathbb{F}_q$ be a finite field and consider an extension $\mathbb{F}_{q^n}$ where an optimal normal element exists. Using the trace of an optimal normal element in $\mathbb{F}_{q^n}$, we provide low complexity normal elements in $\mathbb{F}_{q^m}$, with $m = n/k$. We give theorems for Type I and Type II optimal normal elements. When Type I normal elements are used with $m = n/2$, m odd and q even, our construction gives Type II optimal normal elements in $\mathbb{F}_{q^m}$; otherwise we give low complexity normal elements. Since optimal normal elements do not exist for every extension degree m of every finite field $\mathbb{F}_q$, our results could have a practical impact in expanding the available extension degrees for fast arithmetic using normal bases.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of any characteristic. Let us consider an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ and an element $\alpha \in \mathbb{F}_{q^n}$. A *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}.$$

In this case, we say that α is a *normal element* of $\mathbb{F}_{q^n}$, or that α generates the normal basis N. It is well-known that normal bases exist in any finite extension of a finite field [5].

Let $\alpha_i = \alpha^{q^i}$ for $0 \leq i \leq n-1$, and let $T = (t_{ij})$ be the $n \times n$ matrix given by

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \leq i \leq n-1, \quad t_{ij} \in \mathbb{F}_q. \tag{1}$$

The *complexity* of the normal basis N, denoted by c_N, is the number of non-zero entries in T. Mullin et al. [13] proved that $c_N \geq 2n-1$. The normal basis N is *optimal* when $c_N = 2n-1$.

Optimal normal elements do not exist for all finite fields and all extensions (see [6], Chapter 3, for example). Optimal normal bases over finite fields were completely characterized in a fundamental paper due to Gao and Lenstra [4]; see also [3]. Suppose

$n+1$ is a prime and q a primitive element of $\mathbb{Z}_{n+1}$, where q is a prime or a prime power. Then the n non-unit $(n+1)$th roots of unity are linearly independent and they form an optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Bases of this type are called *Type I* optimal normal bases. Next, suppose $2n+1$ is prime, and either 2 is a primitive element of $\mathbb{Z}_{2n+1}$, or $2n+1 \equiv 3 \mod 4$ and 2 generates the quadratic residues in $\mathbb{Z}_{2n+1}$. Then $\alpha = \gamma + \gamma^{-1}$ generates a *Type II* optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, where γ is a primitive $(2n+1)$th root of unity [3]. These constructions were first given in [13]. Gao and Lenstra [4] proved that any optimal normal basis must be equivalent to a Type I or Type II optimal normal basis.

Normal bases are widely used in applications of finite fields in areas such as coding theory, cryptography, signal processing, and so on; see for instance [9]. In particular, optimal normal bases are desirable. When no optimal normal basis exists, it is useful to have normal elements of low complexity, say of complexity bounded by cn for some small constant c. However, when no optimal normal basis exists, the problem of classifying all *low complexity* normal bases is still open. Young and Panario [16] gave experimental results that strongly imply that low complexity normal elements over finite fields of characteristic 2 with complexity up to $3n$ only occur in finite fields with an optimal normal element. They also provide some characterizations of low complexity normal elements in $\mathbb{F}_{2^n}$. Wan and Zhou [15] extended parts of their results for finite fields of odd characteristic. Interesting constructions of low complexity normal elements are in [1, 2]

In this paper we study the complexity of the trace of an optimal normal element in $\mathbb{F}_{q^n}$. We provide low complexity normal elements in $\mathbb{F}_{q^m}$, with $m = n/k$ and $k \geq 2$. We give theorems for Type I optimal normal elements when q is odd and when $q = 2$. In the case of even characteristic, only the case $q = 2$ is considered, as this stands out from a practical point of view. An immediate consequence of our main theorems for Type I elements is that when $m = n/2$, m odd and q even, our construction provides optimal normal elements in $\mathbb{F}_{q^m}$. Otherwise we give low complexity normal elements with worse and worse complexities as k grows. We also give the equivalent results for Type II optimal normal elements. We then give complexities for the dual bases generated by the traces of Type I and Type II normal elements. We compare our constructions with the NIST-recommended normal bases [14] for elliptic curve cryptography. Our results may have a practical impact since they provide good normal elements for extensions where no optimal normal element exist.

2 Main results

2.1 Type I optimal normal bases: q odd

Theorem 2.1 *Let $\alpha \in \mathbb{F}_{q^n}$ generate an optimal normal basis of Type I of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, q odd, and let $\beta = Tr_{q^n/q^m}(\alpha) \in \mathbb{F}_{q^m}$ with $m = n/k$ and $k \leq m$. Then, the complexity of the normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ generated by β is bounded by $(k+2)m - 3k + 1$, if m is even and k is odd and by $(k+1)m - k$ in all other cases.*

Furthermore, for $1 \leq j \leq m-1$, row j of the multiplication table of β is a cyclic permutation of j positions of row $(m-j)$.

PROOF. Let $n+1$ be a prime, q a primitive root modulo $n+1$ where q is a prime or a prime power, q is odd and $\alpha \in \mathbb{F}_{q^n}$ an optimal normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ be the optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ which is generated by α.

The multiplication table $C_{[n\times n]}$ of the linear map

$$C_\alpha : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \;\; C_\alpha(x) = \alpha \cdot x$$

has exactly $2n-1$ non-zero terms with the following properties:

$$\alpha \cdot \alpha^{q^i} = \alpha^{q^j}, \;\; i = 0, 1, \ldots, \frac{n}{2} - 1, \frac{n}{2} + 1, \ldots, n-1, \quad j = 0, 1, \ldots, n-1, \tag{2}$$

$$\alpha \cdot \alpha^{q^{n/2}} = \sum_{s=0}^{n-1} -\alpha^{q^s}. \tag{3}$$

The above equations imply that there is exactly one 1 in each row except for the row $n/2$, when n is even, where all the n entries are -1.

Suppose that $\beta = \mathrm{Tr}_{q^n/q^m}(\alpha) \in \mathbb{F}_{q^m}$ with $m = n/k$. Then,

$$\beta = \mathrm{Tr}_{q^n/q^m}(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^{mi}} = \alpha + \alpha^{q^m} + \alpha^{q^{2m}} + \cdots + \alpha^{q^{(k-1)m}},$$

generates a normal basis M of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ of the form

$$M = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m-1}}\}.$$

We observe that, for $j = 0, \ldots, m-1$, we have

$$\beta^{q^j} = \sum_{i=0}^{k-1} \alpha^{q^{mi+j}} = \alpha^{q^j} + \alpha^{q^{j+m}} + \cdots + \alpha^{q^{j+(k-1)m}}.$$

Let $D = D_{[m\times m]}$ be the multiplication table of the linear map

$$D_\beta : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \;\; D_\beta(x) = \beta \cdot x.$$

The first row of the table D is given by

$$\begin{aligned}
\beta \cdot \beta &= \left(\sum_{i=0}^{k-1} \alpha^{q^{mi}}\right) \cdot \left(\sum_{i=0}^{k-1} \alpha^{q^{mi}}\right) \\
&= \sum_{i=0}^{k-1} (\alpha \cdot \alpha)^{q^{mi}} + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^m}\right)^{q^{mi}} + \cdots + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{(km)/2}}\right)^{q^{mi}} \\
&\quad + \cdots + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{(k-1)m}}\right)^{q^{mi}}.
\end{aligned}$$

Using (2) and (3), there are $\mu_0, \mu_1, \ldots, \mu_{k-2} \in \mathbb{Z}_n$ such that

$$\alpha \cdot \alpha = \alpha^{q^{\mu_0}}, \; \alpha \cdot \alpha^{q^m} = \alpha^{q^{\mu_1}}, \ldots, \alpha \cdot \alpha^{q^{(k-1)m}} = \alpha^{q^{\mu_{k-2}}}$$

and

$$\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{n/2}}\right)^{q^{mi}}=\sum_{i=0}^{k-1}\left(-\sum_{s=0}^{n-1}\alpha^{q^s}\right)^{q^{mi}}=\sum_{i=0}^{k-1}\left(-\sum_{s=0}^{m-1}\beta^{q^s}\right)^{q^{mi}}=-k\sum_{s=0}^{m-1}\beta^{q^s}.$$

Thus, we get

$$\begin{aligned}\beta\cdot\beta &= \sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_0}}\right)^{q^{mi}}+\sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_1}}\right)^{q^{mi}}+\cdots+\sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_{k-2}}}\right)^{q^{mi}}-k\sum_{s=0}^{m-1}\beta^{q^s}\\ &= \beta^{q^{\mu_0}}+\beta^{q^{\mu_1}}+\cdots+\beta^{q^{\mu_{k-2}}}-k(\beta+\beta^q+\cdots+\beta^{q^{m-1}})\\ &= -k\beta-k\beta^q+\cdots+(1-k)\beta^{q^{\mu_0}}+(1-k)\beta^{q^{\mu_1}}+\cdots+(1-k)\beta^{q^{\mu_{k-2}}}\\ &\quad+\cdots+(-k)\beta^{q^{m-1}}.\end{aligned}$$

The coefficients of β^{q^j} are computed modulo q, so the first row of the table has at most m non-zero terms.

Then, we calculate the remaining rows $j=1,\ldots,m-1$ of the table by computing

$$\begin{aligned}\beta\cdot\beta^{q^j} &= \left(\sum_{i=0}^{k-1}\alpha^{q^{mi}}\right)\cdot\left(\sum_{u=0}^{k-1}\alpha^{q^{mu+j}}\right)\\ &= \sum_{0\le u,i\le k-1}\left(\alpha^{q^{mi}}\right)\left(\alpha^{q^{mu+j}}\right)\\ &= \sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^j}\right)^{q^{im}}+\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{j+m}}\right)^{q^{im}}+\cdots+\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{j+(k-1)m}}\right)^{q^{im}}.\end{aligned}$$

By (2) there are $\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\in\mathbb{Z}_n$ such that

$$\alpha\cdot\alpha^{q^j}=\alpha^{q^{\lambda_0}},\ \ \alpha\cdot\alpha^{q^{j+m}}=\alpha^{q^{\lambda_1}},\ \ldots,\ \alpha\cdot\alpha^{q^{j+(k-1)m}}=\alpha^{q^{\lambda_{k-1}}},\tag{4}$$

which implies,

$$\begin{aligned}\beta\cdot\beta^{q^j} &= \sum_{i=0}^{k-1}\left(\alpha^{q^{\lambda_0}}\right)^{q^{im}}+\sum_{i=0}^{k-1}\left(\alpha^{q^{\lambda_1}}\right)^{q^{im}}+\cdots+\sum_{i=0}^{k-1}\left(\alpha^{q^{\lambda_{k-1}}}\right)^{q^{im}}\\ &= \beta^{q^{\lambda_0}}+\beta^{q^{\lambda_1}}+\cdots+\beta^{q^{\lambda_{k-1}}}.\end{aligned}$$

Finally, for the row $(m-j)$ of the table D, we have

$$\beta\cdot\beta^{q^{m-j}}=\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{m-j}}\right)^{q^{im}}+\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{2m-j}}\right)^{q^{im}}+\cdots+\sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{-j}}\right)^{q^{im}}.$$

Using the identities (4) it follows that

$$\beta\cdot\beta^{q^{m-j}}=\beta^{q^{\lambda_{k-1}+m-j}}+\beta^{q^{\lambda_{k-2}+2m-j}}+\cdots+\beta^{q^{\lambda_0-j}},$$

and since $\beta^{q^m} = \beta$ we get

$$\beta \cdot \beta^{q^{m-j}} = \beta^{q^{\lambda_{k-1}-j}} + \beta^{q^{\lambda_{k-2}-j}} + \cdots + \beta^{q^{\lambda_0-j}}.$$

Thus, the row j of the multiplication table of β is a cyclic permutation of j positions of row $(m-j)$.

If $m = n/k$ is an even number, to calculate the row $m/2$ of the table D we must consider both the cases where k is even and where k is odd. For the odd case we have

$$\begin{aligned}
\beta \cdot \beta^{q^{m/2}} &= \left(\sum_{i=0}^{k-1} \alpha^{q^{mi}}\right) \cdot \left(\sum_{u=0}^{k-1} \alpha^{q^{mu+m/2}}\right) \\
&= \sum_{0 \le u,i \le k-1} \left(\alpha^{q^{mi}}\right)\left(\alpha^{q^{mu+m/2}}\right) \\
&= \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2}}\right)^{q^{im}} + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2+m}}\right)^{q^{im}} + \cdots \\
&\quad + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2+m(k-1)/2}}\right)^{q^{im}} + \cdots + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2+(k-1)m}}\right)^{q^{im}} \\
&= \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2}}\right)^{q^{im}} + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2+m}}\right)^{q^{im}} + \cdots \\
&\quad + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{n/2}}\right)^{q^{im}} + \cdots + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{q^{m/2+(k-1)m}}\right)^{q^{im}}. \qquad (5)
\end{aligned}$$

By (2) and (3), there are $\delta_0, \delta_1, \cdots, \delta_{k-2} \in \mathbb{Z}_n$ such that

$$\beta \cdot \beta^{q^{m/2}} = \beta^{q^{\delta_0}} + \beta^{q^{\delta_1}} + \cdots + (-\beta - \beta^q - \beta^{q^2} - \cdots - \beta^{q^{m-1}}) + \cdots + \beta^{q^{\delta_{k-2}}}.$$

Thus, the row $m/2$ in this case has at most $m-k+1$ non-zero terms. For the case where k is even, the computations of (5) are similar to the calculations involving the identities (4) above, and yield at most k non-zero terms.

In conclusion, we observe that an upper bound for the complexity of the normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ generated by β, when m is even and k is odd, is $k(m-2)+2m-k+1 = (k+2)m-3k+1$ since the first row of the table gives at most m non-zero entries, the $m/2$ row gives at most $m-k+1$ entries and all other rows give at most k entries. In all other cases, the upper bound for the complexity of the normal basis is $k(m-1)+m = (k+1)m-k$, since the first row gives at most m non-zero terms and all other rows give at most k non-zero terms. ■

2.2 Type I optimal normal basis: q even

Theorem 2.2 *Let $\alpha \in \mathbb{F}_{2^n}$ generate an optimal normal basis of Type I of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n > 2$, and let $\beta = Tr_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/k$ and $k \le m$. Then, an upper bound for the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β is $(k+1)m-3k+2$ if m is even and k is odd, or $km-k+1$ otherwise.*

Furthermore, for $1 \leq j \leq m-1$ row j of the multiplication table of β is a cyclic permutation of j positions of row $(m-j)$.

PROOF. We observe that the proof of this claim is nearly identical to the case where q is odd except for the following changes.

Let $n+1$ be a prime, 2 a primitive root modulo $n+1$, and let $\alpha \in \mathbb{F}_{2^n}$ be an optimal normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $N = \{\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}\}$ be the optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ which is generated by α.

The multiplication table $C_{[n\times n]}$ of the linear map

$$C_\alpha : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \;\; C_\alpha(x) = \alpha \cdot x$$

has exactly $2n-1$ non-zero terms with the following properties:

$$\alpha \cdot \alpha^{2^i} = \alpha^{2^j}, \;\; i = 0, 1, \ldots, \frac{n}{2} - 1, \frac{n}{2} + 1, \ldots, n-1, \quad j = 0, 1, \ldots, n-1, \tag{6}$$

$$\alpha \cdot \alpha^{2^{n/2}} = \sum_{s=0}^{n-1} -\alpha^{2^s} = \sum_{s=0}^{n-1} \alpha^{2^s}. \tag{7}$$

The above equations imply that there is exactly one 1 in each row except for the row $n/2$ where all the n entries are 1.

Suppose that $\beta = \mathrm{Tr}_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/k$. Then,

$$\beta = \mathrm{Tr}_{2^n/2^m}(\alpha) = \sum_{i=0}^{k-1} \alpha^{2^{mi}} = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{(k-1)m}},$$

generates a normal basis M of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ of the form

$$M = \{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}.$$

We have that, for $j = 0, \ldots, m-1$,

$$\beta^{2^j} = \sum_{i=0}^{k-1} \alpha^{2^{mi+j}} = \alpha^{2^j} + \alpha^{2^{j+m}} + \cdots + \alpha^{2^{j+(k-1)m}}.$$

Let $D = D_{[m\times m]}$ be the multiplication table of the linear map

$$D_\beta : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}, \;\; D_\beta(x) = \beta \cdot x.$$

The first row of the table D is given by $\beta \cdot \beta = \beta^2$. Thus, the first row of the table D has a 1 in the second position.

If $m = n/k$ is an even number then for the row $m/2$ of the table, by (5), we have that this row contributes at most $m-k+1$ ones to D if k is odd, and at most k ones to D if k is even.

For the remaining rows the proof is identical to the q odd case. We recall that each of the remaining rows contributes to the complexity with at most k non-zero entries. The proof that row j of the multiplication of β is a cyclic permutation of j positions of row $(m-j)$ is also identical to the q odd case.

In conclusion, we observe that an upper bound for the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β, when m is odd or if both m and k are even, is $k(m-1)+1 = km-k+1$. Otherwise, if m is even and k is odd, the complexity is at most $k(m-2)+m-k+2 = (k+1)m-3k+2$. ■

Corollary 2.3 *Let $\alpha \in \mathbb{F}_{2^n}$ generate an optimal normal basis of Type I of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n > 2$, and let $\beta = Tr_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/2$, m odd. Then β generates a Type II optimal normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$.*

PROOF. The complexity comes as a direct application of Theorem 2.2 when $k = 2$ and m odd. To see that the basis forms a Type II normal basis, we observe that each row has exactly two ones. For every $j = 1, \ldots, m-1$, we compute

$$\begin{aligned}
\beta \cdot \beta^{2^j} &= \left(\alpha + \alpha^{2^m}\right) \cdot \left(\alpha^{2^j} + \alpha^{2^{m+j}}\right) \\
&= \left(\alpha \cdot \alpha^{2^j} + \left(\alpha \cdot \alpha^{2^j}\right)^{2^m}\right) + \alpha \cdot \alpha^{2^{m+j}} + \alpha^{2^m} \cdot \alpha^{2^j} \\
&= \left(\alpha \cdot \alpha^{2^j} + \left(\alpha \cdot \alpha^{2^j}\right)^{2^m}\right) + \alpha \cdot \alpha^{2^{m+j}} + \left(\alpha \cdot \alpha^{2^{m+j-2m}}\right)^{2^m} \\
&= \left(\alpha \cdot \alpha^{2^j} + \left(\alpha \cdot \alpha^{2^j}\right)^{2^m}\right) + \alpha \cdot \alpha^{2^{m+j}} + \left(\alpha \cdot \alpha^{2^{m+j}2^{-n}}\right)^{2^m} \\
&= \left(\alpha \cdot \alpha^{2^j} + \left(\alpha \cdot \alpha^{2^j}\right)^{2^m}\right) + \left(\alpha \cdot \alpha^{2^{m+j}} + \left(\alpha \cdot \alpha^{2^{m+j}}\right)^{2^m}\right). \qquad (8)
\end{aligned}$$

Similar to Theorem 2.1, there exist μ, λ with $0 \le \mu, \lambda \le m-1$, such that

$$\alpha \cdot \alpha^{2^j} = \alpha^{2^\mu} \quad \text{and} \quad \alpha \cdot \alpha^{2^{j+m}} = \alpha^{2^\lambda}.$$

This in turn implies

$$\beta \cdot \beta^{2^j} = \beta^{2^\mu} + \beta^{2^\lambda}, \;\; j = 1, \ldots, m-1.$$

This is precisely the form of a Type II optimal normal basis. ■

We observe that another proof of this corollary is possible by using the respective conditions for existence of Type I and Type II optimal normal bases. Indeed, we recall that if $\mathbb{F}_{2^n}$ contains a Type I optimal normal basis over $\mathbb{F}_2$, then $n+1$ is a prime and 2 generates the group $\mathbb{Z}_{n+1}$. There are two conditions for $\mathbb{F}_{2^m}$ to contain a Type II optimal normal basis over $\mathbb{F}_2$. In particular, one of these conditions is that $2m+1$ is prime and 2 generates the group $\mathbb{Z}_{2m+1}$. If we consider $n = 2m$, then the Type II condition for $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ is precisely the Type I condition for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

2.3 Type II optimal normal bases

Theorem 2.4 *Let α generate a Type II optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $\beta = Tr_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/k$ and $k \le m$. Then the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β is $2km-2k+1$.*

PROOF. Let $2n+1$ be prime, and suppose that either

1. 2 is a primitive element of $\mathbb{Z}_{2n+1}$, or
2. $2n+1 \equiv 3 \mod 4$ and 2 generates the quadratic residues in $\mathbb{Z}_{2n+1}$.

Let $\alpha = \gamma + \gamma^{-1}$, where γ is a primitive $(2n+1)$th root of unity. Let $N = \{\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{n-1}}\}$ be the optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ which is generated by α.

The multiplication table $C_{[n\times n]}$ of the linear map

$$C_\alpha : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \;\; C_\alpha(x) = \alpha \cdot x$$

has exactly $2n-1$ non-zero terms with the following property:

$$\alpha \cdot \alpha^{2^i} = \alpha^{2^j} + \alpha^{2^k}, \;\; i = 1, \ldots, n-1, \;\; j,k = 0,1,\ldots,n-1 \;, j \neq k. \tag{9}$$

Therefore, there are exactly two ones in each row of C except for the first row, where there is one 1 in the second position.

Suppose that $\beta = \mathrm{Tr}_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/k$. Then,

$$\beta = \mathrm{Tr}_{2^n/2^m}(\alpha) = \sum_{i=0}^{k-1} \alpha^{2^{mi}} = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{(k-1)m}}$$

generates a normal basis M of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ of the form

$$M = \{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}.$$

We observe that, for $j = 0, \ldots, m-1$, we have

$$\beta^{2^j} = \sum_{i=0}^{k-1} \alpha^{2^{j+mi}} = \alpha^{2^j} + \alpha^{2^{j+m}} + \cdots + \alpha^{2^{j+(k-1)m}}.$$

Let $D = D_{[m\times m]}$ be the multiplication table of the linear map

$$D_\beta : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}, \;\; D_\beta(x) = \beta \cdot x.$$

The first row of the table D is given by $\beta \cdot \beta = \beta^2$. Thus, it has 1 non-zero term in the second position.

As in Theorem 2.2, computing the jth row of D gives

$$\beta \cdot \beta^{2^j} = \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{2^j}\right)^{2^{mi}} + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{2^{j+m}}\right)^{2^{mi}} + \cdots + \sum_{i=0}^{k-1} \left(\alpha \cdot \alpha^{2^{j+(k-1)m}}\right)^{2^{mi}}.$$

By (9), there exist $\lambda_i, \mu_i \in \mathbb{Z}_n$ such that $\alpha \cdot \alpha^{2^j + mi} = \alpha^{2^{\lambda_i}} + \alpha^{2^{\mu_i}}, i = 0, \ldots, k-1$. So,

$$\begin{aligned} \beta \cdot \beta^{2^j} &= \sum_{i=0}^{k-1} \left(\alpha^{2^{\lambda_0}} + \alpha^{2^{\mu_0}}\right)^{2^{mi}} + \cdots + \sum_{i=0}^{k-1} \left(\alpha^{2^{\lambda_{k-1}}} + \alpha^{2^{\mu_{k-1}}}\right)^{2^{mi}} \\ &= \beta^{2^{\lambda_0}} + \beta^{2^{\mu_0}} + \cdots + \beta^{2^{\lambda_{k-1}}} + \beta^{2^{\mu_{k-1}}}. \end{aligned}$$

Thus, there are $2k$ ones appearing in each remaining row of D.

In conclusion, we observe that the complexity of the basis generated by $\beta \in \mathbb{F}_{2^m}$ over $\mathbb{F}_2$ is $2k(m-1)+1$. ■

The following corollary shows that, in contrast with the case Type I normal basis and q even, we do not obtain optimal normal elements for Type II normal basis. Hence, this corollary gives new low complexity normal elements for q even.

Corollary 2.5 *Let α generate a Type II optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $\beta = Tr_{2^n/2^m}(\alpha) \in \mathbb{F}_{2^m}$ with $m = n/2$. Then the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β is $4m-3$.*

3 The dual of the trace of an optimal element

Let $N = \{\alpha, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $M = \{\gamma, \gamma_1, \ldots, \gamma_{n-1}\}$ be another basis. Then M is the dual basis of N if $\mathrm{Tr}(\alpha_i \gamma_j) = \delta_{ij}$ for $1 \le i, j \le n-1$ where δ_{ij} is the Kronecker delta function. It is known that the dual basis of a normal basis is again normal [3], so let $\gamma_i = \gamma^{q^i}$. A basis is self-dual if it is its own dual basis. If α generates a normal basis N of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and γ generates the dual basis of N then γ is a dual element of α.

Theorem 3.1 gives the statement and proof of an upper bound of the complexity of the dual basis of the trace of a Type I optimal normal basis when q is odd. Following the proof we present a statement of the theorem using Type II optimal normal bases and a summary table outlining upper bounds for any q and for both Type I and Type II optimal normal bases.

Theorem 3.1 *Let $\alpha \in \mathbb{F}_{q^n}$ generate an optimal normal basis of Type I of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\beta = Tr_{q^n/q^m}(\alpha) \in \mathbb{F}_{q^m}$ with $m = n/k$, $k \le m$ and $(k,q) = 1$ or $(k,p) = 1$, when q is a prime power of p. Then the complexity of the normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ generated by γ, which is the dual element of β, is $(k+2)m-2$ when m is odd. Further, for $1 \le j \le m-1$ row j of the multiplication table of γ is a cyclic permutation of j positions of row $(m-j)$.*

PROOF. As in Theorem 2.1, let $\alpha \in \mathbb{F}_{q^n}$ generate an optimal normal basis of Type I and $\beta = \mathrm{Tr}_{q^n/q^m}(\alpha) \in \mathbb{F}_{q^m}$ with $m = n/k$. Let $\gamma \in \mathbb{F}_{q^m}$ be a dual element of β. According to [15], γ is of the form

$$\gamma = d_0\beta + d_1\beta^q + \cdots + d_{m-1}\beta^{q^{m-1}},$$

where $d_0, d_1, \ldots, d_{m-1} \in \mathbb{F}_q$ are the coefficients of the unique polynomial $g(x)$ of degree $\le m-1$ satisfying

$$g(x)h(x) \equiv 1 \mod x^m - 1$$

and $h(x)$ is of degree $\le m-1$ with coefficients $t_0, t_1, \ldots, t_{m-1}$ where

$$t_i = \mathrm{Tr}_{q^m/q}(\beta \cdot \beta^{q^i}), \;\; i = 0, 1, \ldots, m-1.$$

Since, $\mathrm{Tr}_{q^n/q}(\alpha) = -1$ and $(k,q) = 1$ we get

$$\begin{aligned}\mathrm{Tr}_{q^m/q}(\beta) &= \frac{m}{n}\mathrm{Tr}_{q^n/q}(\beta) = \frac{m}{n}\mathrm{Tr}_{q^n/q}(\alpha+\alpha^q+\ldots+\alpha^{q^{n-1}}) = \\ &= \frac{m}{n}\cdot k\cdot \mathrm{Tr}_{q^n/q}(\alpha) = \frac{1}{k}\cdot k\cdot(-1) = -1.\end{aligned}$$

Observing that $\gamma = d_0\beta + d_1\beta^q + \cdots + d_{m-1}\beta^{q^{m-1}}$ is the dual element of $\beta \in \mathbb{F}_{q^m}$ it follows that

$$\mathrm{Tr}_{q^m/q}(\beta^{q^i}\cdot\gamma^{q^j}) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.}\end{cases}$$

The above equation for $i = 0$ and $j = 0,\ldots,m-1$ implies the following system:

$$\begin{array}{ccccccccccc} d_0\mathrm{Tr}_{q^m/q}(\beta\cdot\beta) & + & d_1\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^i}) & + & \ldots & + & d_{m-1}\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^{m-1}}) & = & 1 \\ d_{m-1}\mathrm{Tr}_{q^m/q}(\beta\cdot\beta) & + & d_0\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^i}) & + & \ldots & + & d_{m-2}\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^{m-1}}) & = & 0 \\ & \vdots & & \vdots & & \vdots & & \vdots & \\ d_1\mathrm{Tr}_{q^m/q}(\beta\cdot\beta) & + & d_2\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^i}) & + & \ldots & + & d_0\mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^{m-1}}) & = & 0 \end{array}$$

Summing the equations of the system we get,

$$(d_0+d_1+\ldots+d_{m-1})\left(\mathrm{Tr}_{q^m/q}\left(\beta\cdot\left(\beta+\beta^q+\ldots+\beta^{q^{m-1}}\right)\right)\right) = 1.$$

Therefore, we have

$$\begin{aligned}(d_0+d_1+\ldots+d_{m-1})\left(\mathrm{Tr}_{q^m/q}\left(\beta\cdot\left(\sum_{i=0}^{m-1}\beta^{q^i}\right)\right)\right) &= 1, \\ (d_0+d_1+\ldots+d_{m-1})\left(\mathrm{Tr}_{q^m/q}(\beta)\right)^2 &= 1, \\ (d_0+d_1+\ldots+d_{m-1})(-1)^2 &= 1.\end{aligned}$$

Thus, we get the following relation for the coefficients of $\gamma \in \mathbb{F}_{q^m}$

$$d_0+d_1+\cdots+d_{m-1} = 1.$$

We compute $t_0 = \mathrm{Tr}_{q^m/q}(\beta\cdot\beta)$ separately from $t_i = \mathrm{Tr}_{q^m/q}(\beta\cdot\beta^{q^i}), i = 1,\ldots,m-1$,

$$\begin{aligned}t_0 &= \mathrm{Tr}_{q^{n/k}/q}(\beta\cdot\beta) = \frac{1}{k}\,\mathrm{Tr}_{q^n/q}(\beta\cdot\beta) = \frac{1}{k}\,\mathrm{Tr}_{q^n/q}\left(\left(\sum_{i=0}^{k-1}\alpha^{q^{mi}}\right)\left(\sum_{i=0}^{k-1}\alpha^{q^{mi}}\right)\right) \\ &= \frac{1}{k}\,\mathrm{Tr}_{q^n/q}\left(\sum_{i=0}^{k-1}(\alpha\cdot\alpha)^{q^{mi}} + \sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^m}\right)^{q^{mi}} + \cdots + \sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{(km)/2}}\right)^{q^{mi}} + \right. \\ &\quad \left. + \cdots + \sum_{i=0}^{k-1}\left(\alpha\cdot\alpha^{q^{(k-1)m}}\right)^{q^{mi}}\right).\end{aligned}$$

Using (2), (3) there are $\mu_0, \mu_1, \ldots, \mu_{k-2} \in \mathbb{Z}_m$ such that

$$\alpha \cdot \alpha = \alpha^{q^{\mu_0}}, \alpha \cdot \alpha^{q^m} = \alpha^{q^{\mu_1}}, \ldots, \alpha \cdot \alpha^{q^{(k-1)m}} = \alpha^{q^{\mu_{k-2}}}.$$

Thus

$$\begin{aligned}
t_0 &= \frac{1}{k} \operatorname{Tr}_{q^n/q}\left(\sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_0}}\right)^{q^{mi}} + \sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_1}}\right)^{q^{mi}} + \cdots + k + \cdots + \sum_{i=0}^{k-1}\left(\alpha^{q^{\mu_{k-2}}}\right)^{q^{mi}}\right) \\
&= \frac{1}{k}\left(\sum_{i=0}^{k-1}\operatorname{Tr}_{q^n/q}\left(\alpha^{q^{\mu_0}}\right)^{q^{mi}} + \sum_{i=0}^{k-1}\operatorname{Tr}_{q^n/q}\left(\alpha^{q^{\mu_1}}\right)^{q^{mi}} + \cdots + \operatorname{Tr}_{q^n/q}(k) + \cdots + \right. \\
&\quad \left. + \cdots + \sum_{i=0}^{k-1}\operatorname{Tr}_{q^n/q}\left(\alpha^{q^{\mu_{k-2}}}\right)^{q^{mi}}\right) \\
&= \frac{1}{k}\left((-k) + (-k) + \cdots + kn + \cdots + (-k)\right) \\
&= \frac{1}{k}\left((-k)(k-1) + kn\right)) = n - k + 1.
\end{aligned}$$

Now, we calculate $t_i = \operatorname{Tr}_{q^m/q}\left(\beta \cdot \beta^{q^i}\right)$, $i = 1, \ldots, m-1$. By Theorem 2.1, there are $\lambda_0, \lambda_1, ..., \lambda_{k-1} \in \mathbb{Z}_m$ such that

$$\beta \cdot \beta^{q^i} = \beta^{q^{\lambda_0}} + \beta^{q^{\lambda_1}} + \cdots + \beta^{q^{\lambda_{k-1}}}.$$

We have

$$\begin{aligned}
t_i &= \operatorname{Tr}_{q^m/q}\left(\beta \cdot \beta^{q^i}\right) = \operatorname{Tr}_{q^m/q}\left(\beta^{q^{\lambda_0}} + \beta^{q^{\lambda_1}} + \cdots + \beta^{q^{\lambda_{k-1}}}\right) \\
&= \operatorname{Tr}_{q^m/q}\left(\beta^{q^{\lambda_0}}\right) + \operatorname{Tr}_{q^m/q}\left(\beta^{q^{\lambda_1}}\right) + \cdots + \operatorname{Tr}_{q^m/q}\left(\beta^{q^{\lambda_{k-1}}}\right) \\
&= (-1) + (-1) + \cdots + (-1) = -k.
\end{aligned}$$

This implies

$$h(x) = -k\left(x^{m-1} + x^{m-2} + \cdots + x\right) + n - k + 1.$$

We may compute d_i, $i = 1, \ldots, m-1$, by rephrasing the condition

$$g(x)h(x) \equiv 1 \mod x^m - 1$$

as

$$\sum_{k=0}^{m-1} d_k t_{i-k} = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{otherwise,} \end{cases}$$

which is equivalent to the following system:

$$\begin{array}{ccccccccc}
d_0t_0 & + & d_1t_{-1} & + & \cdots & + & d_{m-1}t_{-(m-1)} & = & 1 \\
d_0t_1 & + & d_1t_0 & + & \cdots & + & d_{m-1}t_{-(m-2)} & = & 0 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
d_0t_{m-2} & + & d_1t_{m-1} & + & \cdots & + & d_{m-1}t_{-1} & = & 0 \\
d_0t_{m-1} & + & d_1t_{m-2} & + & \cdots & + & d_{m-1}t_0 & = & 0.
\end{array}$$

The indices of the t_i's are computed modulo m, and the $d_i \in \mathbb{F}_q$ are found by solving the system

$$\begin{pmatrix} (n-k+1) & -k & \dots & -k & -k \\ -k & n-k+1 & \dots & -k & -k \\ \vdots & \dots & \dots & \vdots & \vdots \\ -k & -k & \dots & (n-k+1) & -k \\ -k & -k & \dots & -k & (n-k+1) \end{pmatrix} \begin{pmatrix} d_0 \\ d_1 \\ \vdots \\ d_{m-2} \\ d_{m-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix},$$

which implies that

$$d_0 = \frac{k+1}{n+1}, \;\; d_i = \frac{k}{n+1}, \quad i = 1, \dots, m-1.$$

Note that $n+1$ is a prime different from zero in $\mathbb{F}_q$, and therefore has an inverse. Then using that $\mathrm{Tr}_{q^m/q}(\beta) = -1$ the dual element $\gamma \in \mathbb{F}_{q^m}$ is:

$$\begin{aligned} \gamma &= \frac{k+1}{n+1}\beta + \frac{k}{n+1}\left(\beta^q + \beta^{q^2} + \cdots + \beta^{q^{m-1}}\right) \\ &= \frac{1}{n+1}\beta + \frac{k}{n+1}\left(\beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{m-1}}\right) \\ &= \frac{1}{n+1}\beta + \frac{k}{n+1}\mathrm{Tr}_{q^m/q}(\beta) \\ &= \frac{1}{n+1}\beta - \frac{k}{n+1}, \end{aligned}$$

and $\gamma^{q^i} = \frac{1}{n+1}\beta^{q^i} - \frac{k}{n+1}, \quad i = 0, \dots, m-1.$

Let $C = C_{[m\times m]}$ be the multiplication table of the linear map

$$C_\gamma : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \;\; C_\gamma(x) = \gamma \cdot x.$$

By Theorem 2.1, there exist $\mu_0, \mu_1, \dots, \mu_{k-2} \in \mathbb{Z}_m$ such that

$$\beta \cdot \beta = \beta^{q^{\mu_0}} + \beta^{q^{\mu_1}} + \cdots + \beta^{q^{\mu_{k-2}}} - k\left(\beta + \beta^q + \cdots + \beta^{q^{m-1}}\right).$$

The first row of the table C is given by:

$$\begin{aligned} \gamma \cdot \gamma &= \left(\frac{1}{n+1}\beta - \frac{k}{n+1}\right) \cdot \left(\frac{1}{n+1}\beta - \frac{k}{n+1}\right) \\ &= \frac{1}{(n+1)^2}\beta \cdot \beta - \frac{2k}{(n+1)^2}\beta + \frac{k^2}{(n+1)^2} \\ &= \frac{1}{(n+1)}\left(\left(\frac{1}{n+1}\beta^{q^{\mu_0}} - \frac{k}{n+1}\right) + \cdots + \left(\frac{1}{n+1}\beta^{q^{\mu_{k-2}}} - \frac{k}{n+1}\right) - k\mathrm{Tr}_{q^m/q}(\beta)\right) \\ &\quad + \frac{k(k-1)}{(n+1)^2} - \frac{2k}{(n+1)^2}\beta + \frac{k^2}{(n+1)^2} \\ &= \frac{1}{(n+1)}\left(\gamma^{q^{\mu_0}} + \gamma^{q^{\mu_1}} + \cdots + \gamma^{q^{\mu_{k-2}}}\right) - \frac{2k}{n+1}\gamma \end{aligned}$$

Thus, the first row of the table C has at most k non-zero terms. Next we prove that each one of the remaining rows has at most $k+2$ non-zero terms. For every $i = 1, ..., m-1$ we compute

$$\begin{aligned}
\gamma \cdot \gamma^{q^i} &= \left(\frac{1}{n+1}\beta - \frac{k}{n+1}\right) \cdot \left(\frac{1}{n+1}\beta^{q^i} - \frac{k}{n+1}\right) \\
&= \frac{1}{(n+1)^2}\beta \cdot \beta^{q^i} - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^i} + \frac{k^2}{(n+1)^2} \\
&= \frac{1}{(n+1)^2}\left(\beta^{q^{\lambda_0}} + \beta^{q^{\lambda_1}} + \cdots + \beta^{q^{\lambda_{k-1}}}\right) - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^i} \\
&\quad + \frac{k^2}{(n+1)^2} \\
&= \frac{1}{(n+1)}\left(\left(\frac{1}{n+1}\beta^{q^{\lambda_0}} - \frac{k}{n+1}\right) + \cdots + \left(\frac{1}{n+1}\beta^{q^{\lambda_{k-1}}} - \frac{k}{n+1}\right)\right) + \\
&\quad + \frac{2k^2}{(n+1)^2} - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^i} \\
&= \frac{1}{(n+1)}\left(\gamma^{q^{\lambda_0}} + \gamma^{q^{\lambda_1}} + \cdots + \gamma^{q^{\lambda_{k-1}}}\right) - \frac{k}{n+1}\gamma - \frac{k}{n+1}\gamma^{q^i}.
\end{aligned}$$

Hence, the multiplication table has at most $(k+2)\cdot(m-1)+k = (k+2)m-2$ non-zero terms, so the complexity is at most $(k+2)m-2$.

Finally, for the row $(m-i)$ of the table C, using Theorem 2.1 we get,

$$\begin{aligned}
\gamma \cdot \gamma^{q^{m-i}} &= \left(\frac{1}{n+1}\beta - \frac{k}{n+1}\right) \cdot \left(\frac{1}{n+1}\beta^{q^{m-i}} - \frac{k}{n+1}\right) \\
&= \frac{1}{(n+1)^2}\beta \cdot \beta^{q^{m-i}} - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^{m-i}} + \frac{k^2}{(n+1)^2} \\
&= \frac{1}{(n+1)^2}\left(\beta^{q^{\lambda_{k-1-i}}} + \cdots + \beta^{q^{\lambda_{0-i}}}\right) - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^{m-i}} \\
&\quad + \frac{k^2}{(n+1)^2} \\
&= \frac{1}{(n+1)}\left(\left(\frac{1}{n+1}\beta^{q^{\lambda_{k-1-i}}} - \frac{k}{n+1}\right) + \cdots + \left(\frac{1}{n+1}\beta^{q^{\lambda_{0-i}}} - \frac{k}{n+1}\right)\right) \\
&\quad + \frac{2k^2}{(n+1)^2} - \frac{k}{(n+1)^2}\beta - \frac{k}{(n+1)^2}\beta^{q^{m-i}} \\
&= \frac{1}{(n+1)}\left(\gamma^{q^{\lambda_{k-1-i}}} + \cdots + \gamma^{q^{\lambda_{0-i}}}\right) - \frac{k}{n+1}\gamma - \frac{k}{n+1}\gamma^{q^{-i}}.
\end{aligned}$$

Thus, the row j of the multiplication table of γ is a cyclic permutation of j positions of row $(m-j)$. ■

We note that the above proof is analogous in the case where q is even with the exception that the first row contributes only 1 to the complexity as $\gamma \cdot \gamma = \gamma^2$ is an

element of the normal basis generated by γ. Also, when m is even, we must use the bound that the $m/2$ row of the multiplication table C has at most m non-zero entries. The resulting complexity for q odd is bounded above by $(m-2)\cdot(k+2)+m+k = m(k+3)-k-4$, and for q even is bounded above by $(k+3)m-2k-3$.

Recall that the coefficients, t_i, of the polynomial $h(x)$ defined in Theorem 3.1 are given by

$$t_i = \mathrm{Tr}_{q^m/q}\left(\beta\cdot\beta^{q^i}\right),\ i=0,1,\ldots,m-1.$$

If β generates a Type II optimal normal basis, by Theorem 2.4 there exist $\lambda_i,\mu_i\in\mathbb{Z}_n$ such that

$$\beta\cdot\beta^{2^j} = \beta^{2^{\lambda_0}}+\beta^{2^{\mu_0}}+\cdots+\beta^{2^{\lambda_{k-1}}}+\beta^{2^{\mu_{k-1}}}.$$

Thus, $t_0=1$ and $t_i=0$ for $1\le i\le m-1$. This provides the analogous result for Type II optimal normal bases.

Theorem 3.2 *Let $\alpha\in\mathbb{F}_{q^n}$ generate an optimal normal basis of Type II of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\beta = Tr_{q^n/q^m}(\alpha)\in\mathbb{F}_{q^m}$ with $m=n/k$, $k\le m$. Then β is self-dual and consequently the complexity of the dual basis of β is $2k(m-1)+1$.*

We summarize the results in this section in the following table.

Table 1: Upper bounds on complexities for $\mathbb{F}_{q^m}$ obtained by the dual of the trace of ONBs, where $m=n/k$.

	Type I (q odd)	Type I (q even)	Type II (q even)
m odd	$(k+2)m-2$	$(k+2)(m-1)+1$	$2k(m-1)+1$
m even	$(k+3)m-k-4$	$(k+3)m-2k-3$	$2k(m-1)+1$

4 Existence of optimal extensions

A question that naturally arises is whether, given a prime power q and a natural number m, there exists an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^m}$, such that $\mathbb{F}_{q^n}$ has an optimal normal basis over $\mathbb{F}_q$. This is a hard question, and certainly it is not the subject of this work. We give a brief discussion of known results that provide partial answers to this and related questions. For simplicity, we restrict the discussion to powers of odd primes, that is to fields of odd characteristic.

The extension $\mathbb{F}_{q^n}$ contains a Type I optimal normal basis over $\mathbb{F}_q$, which implies that $n=\ell-1$ for a prime ℓ and q is primitive modulo ℓ. The requirement that $\mathbb{F}_{q^n}$ is an extension of $\mathbb{F}_{q^m}$ implies that $\ell\equiv 1 \mod m$. One would be interested to know if such a prime always exists and what is its order of magnitude in terms of m. We observe that this is already a refinement of Artin's conjecture on primitive roots. We note further, that if q is a square it cannot be primitive modulo any odd prime. Suppose that q is an odd nonsquare prime power. Then the work of Moree [12] and Lenstra [7] implies that under the GRH there exist infinitely many primes ℓ such that $\ell\equiv 1 \mod m$ and q is primitive modulo ℓ. Thus, under the GRH, one is assured that optimal extensions such as those used in this work exist. The ratio $k=n/m$ is clearly of importance for

the bounds that we have given. In the terminology of this section one would like to know the smallest prime ℓ in the arithmetic progression of 1 modulo m such that q is primitive modulo ℓ. This however is a much harder question, and a good bound seems to be out of reach even under the GRH.

5 Conclusions

In this paper we give low complexity normal elements for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, when $m = n/k$ and there is an optimal normal element in $\mathbb{F}_{q^n}$. Table 2 gives a summary of the best complexities obtained in this paper.

Table 2: Summary of best-case low complexities for $\mathbb{F}_{q^m}$ obtained by traces, where $m = n/k$.

	Type I (q odd):	Type I (q even):	Type II (q even):
m odd	$(k+1)m-k$	$km-k+1$	$2km-2k+1$ (for all m)
m even, k odd	$(k+2)m-3k+1$	$(k+1)m-3k+2$	
m even, k even	$(k+1)m-k$	$km-k+1$	

In practice, we are mainly interested in fields with q even where we have low complexity normal bases. As a result of our constructions, we are able to find low complexity normal elements in intermediate fields using tables from [3]. The optimal normal bases in finite fields were completely characterized in [4], but there is still a need to find low complexity normal bases in extensions for which there is no optimal normal basis. Table 3 gives n-degree extensions of $\mathbb{F}_2$, $278 \leq n \leq 1026$, in which there exists a Type II optimal normal basis in $\mathbb{F}_{2^n}$ but no such basis exists in $\mathbb{F}_{2^{n/2}}$. Table 4 is a similar table where there exists a Type I optimal normal basis in $\mathbb{F}_{2^n}$ but no such basis exists in $\mathbb{F}_{2^{n/4}}$. We also provide the resulting complexities of the found bases.

The National Institute of Standards and Technology (NIST) recommends a series of five elliptic curves over binary fields for United States federal government use in cryptography [14]. The complexities of the normal basis representatives were found by [10], and Table 5 compares our best-found constructions with the NIST standard curves.

The complexities of the extensions where $m = 163$ and $m = 409$ given by NIST satisfy the relation $c_N = 4m - 7$, which is a specific construction given in [3]. This construction requires finding primitive roots of unity in large composite extensions of $\mathbb{F}_{q^n}$, which is certainly computationally more difficult than finding the trace of a known optimal normal element. The basis used for $m = 233$ is a Type II ONB, and for the $m = 283$ and $m = 571$ existing tables in [3] only give extensions for which ONBs exist up to $m = 2000$, and so we could not apply our construction. We have provided complexities using our construction for extensions $m = 307$ and $m = 577$ which have the properties that their degrees are prime, close to an extension given by NIST, and $2^m - 1$, the order of the multiplicative group, is not divisible by small prime factors. This could be indicative that elliptic curve cryptography is computationally desirable over these and similar fields.

Table 3: Complexities (C_m) of intermediate $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, $m = n/2$ where $\mathbb{F}_{2^n}$ has a Type II optimal normal basis.

n	$m = n/2$	$C_m = 4m-3$	n	$m = n/2$	$C_m = 4m-3$
278	139	553	650	325	1297
306	153	609	686	343	1369
326	163	649	690	345	1377
330	165	657	726	363	1449
338	169	673	746	373	1489
350	175	697	774	387	1545
354	177	705	810	405	1617
386	193	769	818	409	1633
398	199	793	834	417	1665
410	205	817	846	423	1689
414	207	825	866	433	1729
426	213	849	870	435	1737
438	219	873	930	465	1857
470	235	937	938	469	1873
530	265	1057	950	475	1897
554	277	1105	974	487	1945
558	279	1113	986	493	1969
614	307	1225	998	499	1993
638	319	1273	1026	513	2049

Acknowledgements We thank two anonymous referees for several suggestions that corrected some imprecisions in an earlier version of this paper.

This collaboration was started when three of the authors attended the Banff International Research Station (BIRS) workshop on Polynomials in Finite Fields in November 2006. We thank BIRS for the invitation and the excellent working conditions. The third author is funded by NSERC of Canada. The work of the fourth author was done while he was with the School of Mathematics and Statistics at Carleton University.

References

[1] D. W. Ash, I. F. Blake and S. A. Vanstone, Low complexity normal bases, Discrete Applied Mathematics, Vol. 25, (1989) pp. 191-210.

[2] I. F. Blake, S. Gao and R. C. Mullin, Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$, SIAM Journal on Discrete Mathematics, Vol. 7, (1994) pp. 499-512.

[3] S. Gao, Normal Bases over Finite Fields, Ph.D Thesis, University of Waterloo, Waterloo, ON, Canada, 1993.

[4] S. Gao and H. W. Lenstra, Optimal normal bases, Designs, Codes and Cryptography, Vol.2, (1992) pp. 315-323.

Table 4: Complexities (C_m) of intermediate $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, $m = n/4$ where $\mathbb{F}_{2^n}$ has a Type I optimal normal basis.

n	$m = n/4$	$C_m = 4m-3$	n	$m = n/4$	$C_m = 4m-3$
52	13	49	612	153	609
60	15	57	652	163	649
100	25	97	660	165	657
148	37	145	676	169	673
172	43	169	700	175	697
180	45	177	708	177	705
196	49	193	756	189	753
268	67	265	772	193	769
292	73	289	796	199	793
316	79	313	820	205	817
348	87	345	828	207	825
372	93	369	852	213	849
388	97	385	876	219	873
420	105	417	940	235	937
460	115	457	1060	265	1057
508	127	505	1108	277	1105
540	135	537	1116	279	1113
556	139	553			

[5] K. Hensel, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, Journal für die reine und angewandte Mathematik, Vol. 103, (1888) pp. 230-237.

[6] D. Jungnickel, Finite Fields: Structure and Arithmetics, B.I. Wissenschaftsverlag, Mannheim, Germany, 1993.

[7] H. W. Lenstra, On Artin's Conjecture and Euclid's algorithm in global fields, Inventiones Mathematicae, Vol. 42, (1977) pp. 202-224.

[8] Q. Liao and Q. Sun, Normal Bases and Their Dual-Bases over Finite Fields, Acta Mathematica Sinica, Vol. 22, (2006) pp. 845-848.

[9] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications (2nd ed.), Cambridge University Press, Cambridge (1994).

[10] A. Reyhani-Masoleh and A. Hasan, Low Complexity Word-Level Sequential Normal-Basis Multipliers, IEEE Transactions on Computers, Vol. 54, (2005) pp. 98-110.

[11] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press (1996).

[12] P. Moree, On primes in arithmetic progression having a prescribed primitive root, Journal of Number Theory, 78, (1999) pp. 85 - 98.

Table 5: Comparison of NIST-standard normal basis representatives of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ with our construction.

m	NIST-c_N	Our c_N
163	645	649
233	465*	465*
283	1677	-
307	-	1225
409	1629	1633
571	5637	-
577	-	2305

[13] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone and R.M. Wilson, Optimal normal bases in $GF(p^n)$, Discrete Applied Mathematics, Vol. 22, (1988/1989) pp. 149-161.

[14] Recommended Elliptic Curves for Federal Government Use, NIST, Available online at http://csrc.nist.gov/CryptoToolkit/dss/ecdsa/NISTReCur.pdf, (1999).

[15] Z. Wan and K. Zhou, On the complexity of the dual basis of a type I optimal normal basis, Finite Fields and Their Applications, Vol. 13, (2007) pp. 411-417.

[16] B. Young and D. Panario, Low complexity normal bases, Finite Fields and Their Applications, Vol. 10, (2004) pp. 53-64.