**Noname manuscript No.**
(will be inserted by the editor)

# Artin-Schreier extensions of normal bases

**D. Thomson · C. Weir**

Received: September 21, 2015/ Accepted: soon??

**Abstract** In this paper we extend a normal basis of a finite field over its base field to a new basis which permits both computationally inexpensive exponentiation and multiplication. These new bases are motivated by Artin-Schreier theory, and are particularly useful when creating bases in Artin-Schreier extensions of finite fields.

**Keywords** Finite fields · normal bases · complexity · Artin-Schreier extensions

**Mathematics Subject Classification (2000)** 12E30 · 12E20 · 11T30 · 12Y05

## 1 Introduction

Throughout this work, let $q$ be a prime power and let $n$ be a positive integer. The finite field $\mathbb{F}_{q^n}$ is the unique (up to isomorphism) degree $n$ extension of the finite field $\mathbb{F}_q$ of order $q$. The extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic, generated by the *Frobenius automorphism* $\sigma_q(\alpha) = \alpha^q$ for any $\alpha \in \mathbb{F}_{q^n}$.

The finite field $\mathbb{F}_{q^n}$ can be viewed as a finite dimensional vector space of dimension $n$ over $\mathbb{F}_q$. Typically, $\mathbb{F}_{q^n}$ is constructed by adjoining a root $\alpha$ of a degree $n$ irreducible polynomial over $\mathbb{F}_q$. A natural basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is therefore the *power basis* (or *polynomial basis*) $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

This work was completed when the first author was with the School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa, Ontario, Canada, K1S 5B6. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of the Army, DOD or the U.S. Government.

D. Thomson
Army Cyber Institute, United States Military Academy
Spellman Hall, 2101 New South Post Rd.
West Point, NY, USA, 10996.
E-mail: David.Thomson@usma.edu

C. Weir
Department of Mathematics, Simon Fraser University
8888 University Dr.,
Burnaby, British Columbia, Canada, V5A 1S6.
E-mail: colin_weir@sfu.ca

Of course, bases beyond power bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ exist; another common basis representation is given when the roots $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ of an irreducible polynomial are linearly independent in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Such a basis is a *normal basis*, and any of its basis elements are *normal elements*. Normal bases are useful when exponentiation is a critical operation in the implementation of the field, as the application of Frobenius to any vector is a cyclic right-shift of its coordinate vector. Normal bases are therefore preferred in many applications, such as cryptography and coding theory; see [11,12], for example. The efficiency of an implementation of a normal basis in either hardware or software depends on the number of non-zero structure constants (entries in the multiplication tables); lower bounds and constructions can be found in [1–3,10], for example.

It is easy to see that normal bases are non-extendible to normal bases of higher degree extensions since the application of Frobenius is necessarily cyclic. This work is devoted to extending normal bases using Artin-Schreier theory to preserve some of the benefits inherent in their use. In Section 2 we give some background on normal bases and present problems which motivate the necessity of this work. In Section 3 we present our bases, and analyze some specific constructions in Section 4. In Section 5 we show that in 12 out of the first 32 even-degree extensions, these bases exhibit better multiplication complexity than the best-known normal basis.

## 2 Low complexity normal bases

Let $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Consider two vectors $A = \sum_{i=0}^{n-1} a_i \alpha^{q^i}$ and $B = \sum_{j=0}^{n-1} b_j \alpha^{q^j}$. The multiplication $AB = \sum_{i,j} a_i b_j \alpha^{q^i} \alpha^{q^j}$ and so the number of field operations needed to compute the product depends on the structure constants $\alpha^{q^i} \alpha^{q^j} = \sum_{k=0}^{n-1} t_{ij,k} \alpha^{q^k}$. Identifying $A$ and $B$ with their coefficient vectors, if $AB = C = (c_0, \ldots, c_{n-1})$, we have immediately $c_k = A T_k B^T$, where $T_k = (t_{ij,k})_{i,j=0,\ldots,n-1}$. By the linearity of the Frobenius automorphism,

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \alpha^{q^i} \alpha^{q^j} = \sum_{i=0}^{n-1} \left( \sum_{j=0}^{n-1} a_i b_j \alpha \alpha^{q^{j-i}} \right)^{q^i}.$$

Hence, the structure constants $t_{ij,k}$ can be given as shifts of $c_{0j',k'}$ for some $j', k'$. More precisely, $t_{ij,k} = t_{0(j-i),k-i}$, where subscripts are considered as the least positive residue modulo $n$.

**Definition 1** Let $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The *multiplication table* of $N$, denoted $T_N = (t_{ij})$, is given by the relations

$$\alpha \alpha^{q^i} = \sum_{i=0}^{n-1} t_{ij} \alpha_j, \quad i = 0, 1, \ldots, n-1.$$

Moreover, the number of non-zero entries of $T_N$ is the *complexity* of the basis $N$, denoted $c_N$.

It is immediate that the number of non-zero structure constants for a normal basis $N$ (the number of non-zero $t_{ij,k}$) is equal to $nc_N$. The first normal basis multiplier scheme was devised by Massey and Omura [7], and more details on arithmetic using normal bases can be found in Sections 5.2-3, 11.1 and 16.7.4-5 of [9].

It was shown in [10] that any normal basis must have complexity at least $2n-1$, and normal bases achieving this bound are *optimal normal bases*. Optimal normal bases were fully characterized in [4].

**Theorem 1** [4] *Let $q$ be a prime power, let $n$ be a positive integer and denote by* Tr *the absolute trace mapping* $\mathrm{Tr}\colon \mathbb{F}_{q^n} \to \mathbb{F}_q$. *Then $\mathbb{F}_{q^n}$ has an optimal normal basis over $\mathbb{F}_q$ generated by $\alpha$ with $\mathrm{Tr}(\alpha) = b$ if and only if at least one of the following hold:*

*Type I. $n+1$ is a prime, $q$ is a primitive modulo $n+1$ and $-\alpha/b$ is a primitive $(n+1)$th root of unity;*

*Type II. $q = 2^\nu$ with $\gcd(\nu, n) = 1$, $2n+1$ is a prime such that $\langle 2, -1\rangle = \mathbb{Z}_{2n+1}^*$ and $\alpha/b = \gamma + \gamma^{-1}$ for some primitive $(2n-1)$th root of unity $\gamma$.*

Generalizations of optimal normal bases due to *Gauss periods* are studied in [1], for example. Normal bases arising from Gauss periods are often called *Gaussian normal bases*.

**Theorem 2** [1] *Let $r = nt+1$ be a prime not dividing $q$ and let $\gamma$ be a primitive $r$-th root of unity in $\mathbb{F}_q^{nt}$. Furthermore, let $\kappa$ be the unique subgroup of order $t$ in $\mathbb{Z}_r^*$ and let $\kappa_i = q^i\kappa \subseteq \mathbb{Z}_r^*$ for $i = 0, 1, \ldots, n-1$. The elements*

$$\alpha_i = \sum_{a\in\kappa_i} \gamma^a \in \mathbb{F}_{q^n}, \quad i = 0, 1, \ldots, n-1,$$

*are Gauss periods of type $(n, t)$ over $\mathbb{F}_q$. Moreover, $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ forms a Gaussian normal basis if and only if $\cup_{i=0}^{n-1}\kappa_i = \mathbb{Z}_r^*$. Equivalently, $N$ is a Gaussian normal basis if and only if $\gcd(nt/e, q) = 1$, where $e$ is the order of $q \pmod r$.*

The precise complexities of Gaussian normal bases are not known for all $t$. However, for some special values of $t$ they are known to provide low complexity bases.

**Theorem 3** [1,3] *Let $p$ be the characteristic of $\mathbb{F}_q$ and let $N$ be a Gaussian normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of type $(n, t)$.*

1. *If $p$ divides $t$, then $c_N \le nt - 1$,*
2. *If $p = 2$, then*

$$tn - (t^2 - 3t + 3) \le c_N \le (n-1)t + 1 \qquad t \text{ even},$$
$$(t+1)n - (t^2 - t + 1) \le c_N \le (n-2)t + n + 1 \qquad t \text{ odd}.$$

3. *If $q = 2$ and $t = 2^\nu r$, where either $r = 1$ or $r$ is an odd prime and $\nu = 0, 1, 2$, then the lower bounds are tight for sufficiently large $n$.*

Gaussian normal bases provide the best direct construction of low-complexity normal bases, but they do not exist for every field extension.

**Theorem 4** *There exists a Gaussian normal basis if and only if 8 does not divide $n$.*

Though Theorem 4 precisely determines the existence of Gaussian normal bases, it does not provide the values $t$ for which there exists a type $(n, t)$ Gaussian normal basis. If such a $t$ is large, then the complexity of the basis will suffer.

There also exist two methods to construct new normal bases from existing normal bases for certain field extensions; the first is a product construction and the second is via a projection mapping. These are outlined respectively in the two theorems below.

**Theorem 5** [9, Theorem 5.3.13] *Let $M = \{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ be a normal basis of $\mathbb{F}_{q^m}$ with complexity $c_M$ and let $N = \{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ with complexity $c_N$. If $\gcd(m, n) = 1$, then $\alpha\beta$ generates a normal basis of $\mathbb{F}_q^{mn}$ with complexity $c_M c_N$.*

**Theorem 6** [9, Theorem 5.3.14] *Let $\alpha$ generate a normal basis of $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. Then*

$$\beta = \mathrm{Tr}_{\mathbb{F}_{q^{mn}}/\mathbb{F}_{q^m}}(\alpha) = \alpha + \alpha^{q^n} + \cdots + \alpha^{q^{n(m-1)}} \in \mathbb{F}_{q^m}$$

*generates a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

To align with computing hardware, one is naturally interested in computationally efficent bases for $\mathbb{F}_{2^{2^\ell}}$. However, Gaussian normal bases do not exist when 8 divides $n$, and Theorem 5 cannot provide normal bases of extensions of prime-power degree. Hence, to find normal bases for $n = 2^\ell, \ell > 2$, we are neither able to directly construct normal bases nor apply Theorem 6. An exhaustive search in [8] provides the minimum complexity normal basis of $\mathbb{F}_{2^{2^\ell}}$ when $\ell = 3, 4, 5$, but $\ell \geq 6$ seems out of range for current computational resources.

## 3 Extending normal bases using Artin-Schreier theory

In this section, motivated by finding computationally efficent bases for $\mathbb{F}_{2^{2^\ell}}$, we turn to Artin-Schreier theory to extend a normal basis to another related, but not normal, basis. We will show that these bases, while not normal, still provide computationally efficient arithmetic. We first recall the fundamental results of Artin-Schreier theory.

**Theorem 7** [5, Theorem IV.6.3] *Let $k$ be a field and let $K$ be a cyclic extension of $k$ of degree $n$ with Galois group $G$. Let $\sigma$ be a generator of $G$ and let $\beta \in K$. The trace $\mathrm{Tr}_{K/k}(\beta) = 0$ if and only if there exists an element $\alpha \in K$ such that $\beta = \alpha - \sigma(\alpha)$.*

**Theorem 8** [5, Theorem IV.6.4] *Let $k$ be a field of characteristic $p$.*

1. *Let $K$ be a cyclic extension of $k$ of degree $p$. Then there exists $\alpha \in K$ such that $K = k(\alpha)$ and $\alpha$ is a root of the polynomial $x^p - x - a \in k[x]$ with some $a \in k$.*
2. *Conversely, given $a \in K$, the polynomial $f(x) = x^p - x - a$ either has one root in $k$ (in which case all its roots are in $k$) or it is irreducible. In the latter case, if $\alpha$ is such a root, then $k(\alpha)$ is cyclic of degree $p$ over $k$*

For the remainder of this section, let $q$ be a power of 2, so from the notation of the previous theorems we identify $k = \mathbb{F}_{2^n}$ for some positive integer $n$. First, we state without proof two standard results in finite fields.

**Lemma 1** *1. If $\alpha \in \mathbb{F}_{q^n}$ is normal, then $\mathrm{Tr}(\alpha) \neq 0$.*
*2. For $\alpha \in \mathbb{F}_{q^n}$, $\mathrm{Tr}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^n}$.*

**Proposition 1** *Let $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $A_\alpha(x) = x^2 + x + \alpha$ is irreducible in $\mathbb{F}_{q^n}[x]$.*

*Proof* By Theorem 8, $A_\alpha$ is irreducible in $\mathbb{F}_{q^n}[x]$ if and only if $\alpha \neq \beta^2 + \beta$ for some $\beta \in \mathbb{F}_{q^n}$. That is, $A_\alpha$ is irreducible if and only if $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$, which is shown in Lemma 1. □

**Proposition 2** *Let $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\beta$ be a root of $x^2 + x + \alpha$ in $\mathbb{F}_{q^{2n}}$. Then the set $\mathcal{N} = N \cup \beta N$ is a basis of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$.*

*Proof* The set $\{1, \beta\}$ is a polynomial basis of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^n}$. If $N$ is any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, it follows that $N \cup \beta N$ is a basis of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$. □

With the notation of Proposition 2, we call the basis $N \cup \beta N$ of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$ an *Artin-Schreier extension* of the basis $N$. Proposition 2 guarantees that the Artin-Schreier extension of a normal basis yields another basis. The main advantage of normal bases is from the efficient exponentiation guaranteed by their structure. Our Artin-Schreier extensions give a similar advantage.

Let $\mathcal{N} = N \cup \beta N$ be an Artin-Schreier extension, as defined in Proposition 2. Let $\gamma = \sum_{i=0}^{n-1} c_i \alpha^{q^i} + \beta \sum_{i=0}^{n-1} d_i \alpha^{q^i}$, then

$$\begin{aligned}
\gamma^2 &= \sum_{i=0}^{n-1} c_{i-1} \alpha^{q^i} + \beta^2 \sum_{i=0}^{n-1} d_{i-1} \alpha^{q^i} = \sum_{i=0}^{n-1} c_{i-1} \alpha^{q^i} + (\beta + \alpha) \sum_{i=0}^{n-1} d_{i-1} \alpha^{q^i} \\
&= \sum_{i=0}^{n-1} c_{i-1} \alpha^{q^i} + \beta \sum_{i=0}^{n-1} d_{i-1} \alpha^{q^i} + \sum_{i=0}^{n-1} d_{i-1} \alpha \alpha^{q^i} \\
&= \sum_{i=0}^{n-1} c_{i-1} \alpha^{q^i} + \beta \sum_{i=0}^{n-1} d_{i-1} \alpha^{q^i} + \sum_{i=0}^{n-1} d_{i-1} \sum_{k=0}^{n-1} t_{ik} \alpha^{q^k}.
\end{aligned}$$

The number of operations required for squaring therefore depends on the complexity of the normal basis $N$ generated by $\alpha$. We summarize this observation in the following proposition.

**Proposition 3** *Let $\mathcal{N} = N \cup \beta N$ be an Artin-Schreier extension as defined in Proposition 2. Let $\gamma = \sum_{i=0}^{n-1} c_i \alpha^{q^i} + \beta \sum_{i=0}^{n-1} d_i \alpha^{q^i}$, and write $\gamma = C + \beta D$, where $C, D$ are expressed in the normal basis $N$. Then*

$$\gamma^2 = \left( C_> + \sum_{i=0}^{n-1} d_{i-1} \sum_{k=0}^{n-1} t_{ik} \alpha^{q^k} \right) + \beta D_>,$$

*where $A_>$ indicates a cyclic right-shift of the coordinate vector of $A$ (in $N$).*

*Remark 1* The term $\beta D_>$ has the effect of simply placing $D_>$ in the second $n$-bit half-word of the $2n$-bit coordinate vector of $\gamma^2$. The term $\sum_{i=0}^{n-1} d_{i-1} \sum_{k=0}^{n-1} t_{ik} \alpha^{q^k}$ has the effect of XORing all rows of the multiplication table of $N$, $T_N$, for which

$d_{i-1} = 1$. The resulting vector is XORed to $C_>$. We conceive of a circuit for this as follows: the rows of $T_N$ are known and kept in $n$-bit width registers. An n-wide XOR is wired and the $i$th register is controlled by the value $d_{i-1}$.

Considering $C$ and $D$ as $n$-bit machine words, the cost of squaring is two cyclic bit-shifts, $n$ parallel $n$-bit XORs (computing $\sum_{i=0}^{n-1} d_{i-1} \sum_{k=0}^{n-1} t_{ik}\alpha^{q^k}$ via a binary tree) and one $n$-bit XOR (adding $C_>$ and $\sum_{i=0}^{n-1} d_{i-1} \sum_{k=0}^{n-1} t_{ik}\alpha^{q^k}$). Hence, squaring is performed in $\mathcal{O}(\log n)$ $n$-bit steps; more than the negligible cost of a normal bases but superior to the $\mathcal{O}(n \log n)$ of a power basis.

The other simplification arising from the use of normal bases is that the rows of their multiplication tables all arise as shifts of a single multiplication table.

Let $N$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ generated by $\alpha$ and let $A = \sum_{i=0}^{n-1} a_i\alpha^{q^i} + \beta\sum_{i=0}^{n-1} a_{n+i}\alpha^{q^i}$ and $B = \sum_{i=0}^{n-1} b_i\alpha^{q^i} + \beta\sum_{i=0}^{n-1} b_{n+i}\alpha^{q^i}$, then

$$\begin{aligned} AB &= \sum_{i,j=0}^{n-1} a_i b_j \alpha^{q^i}\alpha^{q^j} + \beta\left(\sum_{i,j=0}^{n-1} a_{n+i} b_j \alpha^{q^i}\alpha^{q^j} + \sum_{i,j=0}^{n-1} a_i b_{n+j} \alpha^{q^i}\alpha^{q^j}\right) \\ &\quad + \beta^2 \sum_{i,j=0}^{n-1} a_{n+i} b_{n+j} \alpha^{q^i}\alpha^{q^j}. \\ &= \sum_{i,j=0}^{n-1} a_i b_j \alpha^{q^i}\alpha^{q^j} + \beta\left(\sum_{i,j=0}^{n-1} a_{n+i} b_j \alpha^{q^i}\alpha^{q^j} + \sum_{i,j=0}^{n-1} a_i b_{n+j} \alpha^{q^i}\alpha^{q^j}\right. \\ &\quad \left. + \sum_{i,j=0}^{n-1} a_{n+i} b_{n+j} \alpha^{q^i}\alpha^{q^j}\right) + \alpha \sum_{i,j=0}^{n-1} a_{n+i} b_{n+j} \alpha^{q^i}\alpha^{q^j}. \end{aligned} \tag{1}$$

We observe that all except the final term in Equation (1) can be expressed using only the multiplication table $T_N$ and its shifts, and can be easily computed from $T_N$ exactly how one does for normal bases. We can also simplify the triple product of basis elements from the final term of Equation (1) as follows:

$$\begin{aligned} &\alpha \sum_{i,j=1, i\neq j}^{n-1} a_{n+i} b_{n+j} \alpha^{q^i}\alpha^{q^j} \\ &= \alpha \sum_{i,j=1 i\neq j}^{n-1} a_{n+i} b_{n+j} \sum_{k=0}^{n-1} t_{ij,k}\alpha^{q^k} = \sum_{i,j=1 i\neq j}^{n-1} a_{n+i} b_{n+j} \sum_{k=0}^{n-1} t_{ij,k}\alpha\alpha^{q^k} \\ &= \sum_{i,j=1 i\neq j}^{n-1} a_{n+i} b_{n+j} \sum_{k=0}^{n-1} t_{ij,k} = \sum_{i,j=1 i\neq j}^{n-1} a_{n+i} b_{n+j} \sum_{k=0}^{n-1} t_{j-i,k-i} \sum_{\ell=0}^{n-1} t_{k\ell}\alpha^{q^\ell}. \end{aligned} \tag{2}$$

Hence, the final term can also be deduced from the multiplication table $T_N$.

A convenient measure of the efficiency of multiplication of any basis is the number of non-zeroes in their multiplication tables. For the Artin-Schreier extension of a normal basis, this is the number of non-zero terms in the expansion of Equation (1). We extend a normal basis with a known multiplication table to compute the number of non-zero terms in Equation (2). The following theorem combines these observations.

**Theorem 9** *Let $\mathcal{N} = N \cup \beta N$ be an Artin-Schreier extension as defined in Proposition 2, and denote by $c_N$ the complexity of the normal basis $N$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. For $i \in \{0, 1, \ldots, n-1\}$, the $i$th multiplication table $(t_{i,(\delta n+j)k})$, $\delta = 0, 1$, $j = 0, 1, \ldots, n-1$ has $2c_N$ non-zero entries and the $(n+i)$th multiplication table $(t_{n+i,(\delta n+j)k})$, $\delta = 0, 1$, $j = 0, 1, \ldots, n-1$, has $c_N + \sum_{k=0}^{n-1} t_{j-i,k-i} \sum_{\ell=0}^{n-1} t_{k\ell}$ non-zero entries.*

## 4 Artin-Schreier extensions of optimal normal bases

Theorem 9 depends on the complexity of the normal basis which is being extended. In particular, Equation (2) requires explicit knowledge of the form of the multiplication table of the normal basis. Certain descriptions of multiplication tables are known; notably, the optimal normal bases. Descriptions of the multiplication tables for other Gaussian normal bases are given in [3].

**Lemma 2** *1. Let $\mathbb{F}_{2^n}$ admit a Type I optimal normal basis $\mathcal{B}$ over $\mathbb{F}_2$. Then the multiplication table $T_{\mathcal{B}}$ of $\mathcal{B}$ has row $n/2$ (indexed by 0) equal to $(1, 1, \ldots, 1)$ and every other row contains exactly one non-zero entry.*

*2. Let $\mathbb{F}_{2^n}$ admit a Type II optimal normal basis $\mathcal{B}$ over $\mathbb{F}_2$. Then the multiplication table $T_{\mathcal{B}}$ of $\mathcal{B}$ has first row equal to $(0, 1, 0, \ldots, 0)$ and every other row contains exactly two non-zero entries. Moreover, $T_B$ is symmetric and for $i = 1, 2, \ldots, \lfloor (n-1)/2 \rfloor$, row $n - i$ is the $i$-fold cyclic left-shift of row $i$.*

We now apply Theorem 9 to Type I and Type II optimal normal bases, respectively.

**Proposition 4** *Suppose $\mathbb{F}_{2^n}$ admits a Type I optimal normal basis $N$ over $\mathbb{F}_2$ and let $\mathcal{N}$ be its Artin-Schreier extension basis of $\mathbb{F}_{2^{2n}}$ over $\mathbb{F}_2$, as in Theorem 9. The number of non-zeroes in the multiplication tables of $\mathcal{N}$ is $10n^2 - 6n + 1$.*

*Proof* Suppose $N$ is a type I optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. By Lemma 2 every row has exactly one non-zero entry except row $n/2$, which is full of ones (observe that $n$ is even, since $n + 1$ is an odd prime).

For $i_0 \in \{0, 1, \ldots, n-1\}$, the $i_0$th multiplication table $(t_{i_0,(\delta n+j)k})$, $\delta = 0, 1$, $j = 0, 1, \ldots, n-1$ has $2c_N$ non-zero entries, by Theorem 9.

Let $i \in \{0, 1, \ldots, n-1\}$. Combining Equations (1) and (2) gives

$$\beta\alpha^{q^i}\beta\alpha^{q^j} = \beta\alpha^{q^i}\alpha^{q^j} + \alpha\alpha^{q^i}\alpha^{q^j} = \beta\alpha^{q^i}\alpha^{q^j} + \sum_{k=0}^{n-1} t_{j-i,k-i} \sum_{\ell=0}^{n-1} t_{k\ell}\alpha^{q^\ell}. \qquad (3)$$

Suppose $i \neq n/2$. If $j - i \not\equiv n/2 \pmod{n}$, then $t_{j-i,k-i} = 1$ for precisely one value of $k$, say $k_0$. Moreover, $t_{j_0 0} \neq 0$ since $\alpha\alpha^{q^{j_0}} = \alpha$ implies that $\alpha^{q^{j_0}} = 1$, a contradiction. Thus $k_0 \neq i$. Thus, $\sum_{\ell=0}^{n-1} t_{k_0\ell} = 1$ if and only if $k_0 \neq i, n/2$ and $\sum_{\ell=0}^{n-1} t_{k_0\ell} = n$ if and only if $k_0 = n/2$. If $j - i \equiv n/2 \pmod{n}$, then $t_{j-i,k-i} = 1$ for all $k = 0, 1, \ldots, n-1$. Moreover, $\sum_{\ell=0}^{n-1} t_{k\ell} = 1$ if $k \neq n/2$ and $\sum_{\ell=0}^{n-1} t_{k\ell} = n$ if $k = n/2$. Summing over all $j = 0, 1, \ldots, n-1$, the $(n+i)$th multiplication table of the AS-basis extension of $N$ contains $3c_N = 6n - 3$ non-zeroes.

Now let $i = n/2$. If $j - i \not\equiv n/2 \pmod{n}$ (that is, $j \neq 0$), then $t_{j-i,k-i} = 1$ for precisely one value of $k - i \neq 0$. Since $k \neq i = n/2$, then $\sum_{\ell=0}^{n-1} t_{k\ell}\alpha^{q^\ell} = \alpha^{q^{\ell_k}}$

for some $\ell_k$. If $j - i \equiv n/2 \pmod{n}$ (if $j = 0$), then $t_{j-i,k-i} = 1$ for all $k$, and $\sum_{\ell=0}^{n-1} \alpha^{q^\ell} + \sum_{0 \le k < n, k \ne n/2} \sum_{\ell=0}^{n-1} t_{k\ell} \alpha^{q^\ell}$. As $k \ne n/2$ varies, $t_{kl} = 1$ for distinct values of $\ell \ne 0$; hence $\sum_{\ell=0}^{n-1} \alpha^{q^\ell} + \sum_{0 \le k < n, k \ne n/2} \sum_{\ell=0}^{n-1} t_{k\ell} \alpha^{q^\ell} = \alpha$. Summing over all $j = 0, 1, \ldots, n-1$, the $(3n/2)$th multiplication table of the AS-basis extension of $N$ contains $2c_N + n = 5n - 2$ non-zeroes.

Summing over all tables gives precisely $2nc_N + 3(n-1)c_N + 2c_N + n = 10n^2 - 6n + 1$ non-zeroes. □

**Proposition 5** *Suppose $\mathbb{F}_{2^n}$ admits a Type II optimal normal basis $N$ over $\mathbb{F}_2$ and let $\mathcal{N}$ be its Artin-Schreier extension basis of $\mathbb{F}_{2^{2n}}$ over $\mathbb{F}_2$, as given in Theorem 9. The number of non-zeroes in the multiplication tables of $\mathcal{N}$ is $12n^2 - 12n + 5$.*

*Proof* The proof proceeds in the same case-wise fashion as that of Proposition 4. We omit the proof, for brevity. □

Following [8], we (heuristically) observe that one multiplication table of an average normal basis $N$ of $\mathbb{F}_{2^{2n}}$ over $\mathbb{F}_2$ will have complexity approximately $(2n)^2/2$ with a tight variance; hence the expected number of non-zero elements across the multiplication tables of an average normal basis is approximately $4n^3$. In contrast, optimal normal bases of $\mathbb{F}_{2^{2n}}$ have $8n^2 - 2n$ non-zero entries. Propositions 4 and 5 show that the number of non-zero structure constants of Artin-Schreier extensions of Type I and Type II optimal normal bases is less than $10n^2$ and $12n^2$, respectively; that is, they admit sparse multiplication tables which have a small constant multiple of the non-zeroes of an optimal normal basis, should one exist.

## 5 Experiments and final remarks

The website accompanying [9, Section 2.1], accessible `http://www.math.carleton.ca/~daniel/hff/`, contains the normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ of lowest complexity by exhaustive search for $n \le 39$ and by the methods of Section 2 for $n \ge 40$.

We use a simple Magma program to construct the Artin-Schreier extension basis from Theorem 9 to the minimal complexity normal bases for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n = 2, \ldots, 34$, from the website above. We compare the number of non-zeroes in their multiplication tables in Table 1.

We explain Table 1 here. The column $nc_N$ is the $n$ times the complexity of the normal basis $N$ of minimum complexity in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$; in other words, the number of structure constants of the basis $N$. The heading nnz_AS is the number of non-zero structure constants for the Artin-Schreier extension basis. Bold entries indicate when the Artin-Schreier extension has fewer non-zero structure constants than the minimal normal basis.

We briefly comment on some natural generalizations of this work.

Let $r$ be a power of a prime, let $q$ be a power of $r$ and let $\alpha \in \mathbb{F}_r$ such that $\mathrm{Tr}(\alpha) \ne 0$. By [6, Theorem 3.80], we obtain the decomposition

$$x^q - x - \alpha = \prod_{j=1}^{q/r} (x^r - x - \beta_j) \in \mathbb{F}_q[x],$$

where $\beta_j$ are the distinct elements of $\mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\beta_j) = \alpha$. Let $\alpha \in \mathbb{F}_r$ be a normal element generating a normal basis $N$, then the polynomial $g_\alpha(x) = x^r - x - \alpha$

| $n$ | $nc_N$ | nnz_AS |
|---|---|---|
| 4 | 28 | 29 |
| 6 | 66 | 77 |
| **8** | 168 | **137** |
| 10 | 190 | 245 |
| 12 | 276 | 365 |
| 14 | 378 | 705 |
| **16** | 1360 | **905** |
| 18 | 630 | 869 |
| **20** | 1260 | **941** |
| **22** | 1386 | **1325** |
| **24** | 2520 | **1369** |

| $n$ | $nc_N$ | nnz_AS |
|---|---|---|
| 26 | 1326 | 3301 |
| 28 | 1540 | 2189 |
| 30 | 1770 | 3805 |
| **32** | 11552 | **7361** |
| **34** | 8262 | **7381** |
| 36 | 2556 | 3133 |
| 38 | 7866 | 11997 |
| **40** | 7560 | **6665** |
| 42 | 5670 | 10921 |
| 44 | 6468 | 7549 |
| **46** | 6210 | **6077** |

| $n$ | $nc_N$ | nnz_AS |
|---|---|---|
| **48** | 20400 | **14041** |
| 50 | 4950 | 15349 |
| 52 | 5356 | 7805 |
| 54 | 11286 | 23245 |
| **56** | 22344 | **7673** |
| 58 | 6670 | 9749 |
| 60 | 7140 | 10445 |
| 62 | 21762 | 42397 |
| **64** | 117056 | **61865** |
| 66 | 8646 | 12677 |
| 68 | 38556 | 42413 |

**Table 1** Number of non-zero structure constants of a normal basis ($nc_N$) versus Artin-Schreier extension bases (nnz_AS) for even $n = 4, \ldots, 68$.

is irreducible in $\mathbb{F}_r$. If $\beta$ is a root of $g_\alpha$, then $\mathbb{F}_r(\beta)$ is a degree $r$ extension of $\mathbb{F}_r$ with basis $N \cup \beta N \cup \cdots \cup \beta^{r-1}N$. For example, let $r = 4$, then $x^4 + x + \alpha$ is irreducible over $\mathbb{F}_4$ and $\mathbb{F}_{4^4}$ has basis $N \cup \beta N \cup \beta^2 N \cup \beta^3 N$ over $\mathbb{F}_2$. Any element $\gamma \in \mathbb{F}_{4^4}$ can be expressed in the form $\gamma = A_0 + \beta A_1 + \beta^2 A_2 + \beta^3 A_3$, where $A_i$ is a linear combination of the elements of $N$, $i = 0, 1, 2, 3$. Applying Frobenius, $\gamma^2 = A_{0>} + \beta^2 A_{1>} + \beta^4 A_{2>} + \beta^6 A_{3>}$, where $A_{i>}$ denotes the cyclic right-shift of elements of $A_i$. Using the reduction rule $\beta^4 = \beta + \alpha$ gives

$$\gamma^2 = A_{0>} + \alpha A_{2>} + \beta A_{2>} + \beta^2(A_{1>} + \alpha A_{3>}) + \beta^3 A_{3>}.$$

As in Proposition 3, the computational cost comes from the terms involving $\alpha$. So in the $r = 4$ example, exponentiation will be approximately twice as costly as compared to degree 2 extensions. We leave a general treatment of this case, as well as an examination of the multiplication tables, to an interested reader. Also, for any power of $r$, the polynomial $x^q - x - \alpha$ factors into degree $r$ irreducibles, hence higher powers of $q$ do not yield larger extensions.

We also observe that we could use our results to construct towers of Artin-Schreier extensions. For example, $\mathbb{F}_{2^{64}}$ can be obtained as series of two quadratic extensions of $\mathbb{F}_{2^{16}}$, where each extension can be given by adjoining a root of a quadratic Artin-Schreier polynomial. Denote by $g_\alpha(x)$ an irreducible polynomial $x^2 + x + \alpha$ over $\mathbb{F}_{2^n}$, and let $\beta$ be a root of $g_\alpha$ in $\mathbb{F}_{2^{2n}}$. Then one can show that the polynomial $g_\beta(x) = x^2 + x + \beta$ is irreducible over $\mathbb{F}_{2^{2n}}$. Thus, letting $\gamma$ denote a root of $g_\beta$, we can write $\mathbb{F}_{2^{4n}} = \mathbb{F}_{2^{2n}}(\gamma) = \mathbb{F}_{2^n}(\beta)(\gamma)$. A two-fold Artin-Schreier extension basis for $\mathbb{F}_{2^{4n}}$ over $\mathbb{F}_{2^n}$ is given by $N \cup \beta N \cup \gamma N \cup \gamma\beta N$. Using $\gamma^2 = \gamma + \beta$ and $\beta^2 = \beta + \alpha$, we leave it to an interested reader to carry through the details of the cost for squaring and multiplication for these extensions. Again, one expects the higher number of cross-product terms to add to the practical costs.

In all cases, it is clear that the larger the extension of the normal basis, the more the arithmetic will resemble that of a power basis and less of the underlying normal basis. Consequently, it is reasonable to expect a trade-off between lower density multiplication tables of the extended bases and the rising cost of exponentiation.

**Acknowledgements** We would like to acknowledge the 2014 West Coast Number Theory conference, where a large portion of this work was discussed.

## References


1. D. W. Ash, I. F. Blake and S. A. Vanstone, Low complexity normal bases, *Discrete Applied Mathematics*, **25** (1989), 191-210.
2. R. Azarderakhsh, D. Jao, and H. Lee, Space Complexity Reduction Algorithms for Gaussian Normal Basis Multiplication, *IEEE Transactions on Information Theory*, **61** (2015), 2357-2369.
3. M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, Gauss periods as constructions of low complexity normal bases, *Designs, Codes and Cryptography*, **62** (2012), 43-62.
4. S. Gao and H. W. Lenstra, Optimal normal bases, *Designs, Codes and Cryptography*, **2** (1992), 315-323.
5. S. Lang, *Algebra (3rd ed.)*, Graduate Texts in Mathematics **211**, Springer (2002).
6. R. Lidl and H. Niederreiter, *Finite Fields (2nd ed.)*, Cambridge University Press, Cambridge, UK. (1997).
7. J. L. Massey and J. K. Omura, Computational method and apparatus for finite field arithmetic, US Patent No. 4,587,627 to OMNET Assoc., Sunnyvale CA, Washington, D.C.: Patent and Trademark Office (1986).
8. A. Masuda, L. Moura, D. Panario and D. Thomson, Low complexity normal elements over finite fields of characteristic two, *IEEE Transactions on Computers*, **57** (2008), 990-1001.
9. G. L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton, FL. (2013).
10. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone and R. M. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Applied Mathematics*, **22** (1989), 149-161.
11. Y. Nawaz and G. Gong, The WG Stream Cipher, ECRYPT Stream Cipher Project Report 2005/033. Available at `http://www.ecrypt.eu.org/stream`.
12. D. Silva and F. R. Kschischang, Fast encoding and decoding of Gabidulin codes, *Proceedings of the 2009 IEEE Symposium on Information Theory*, **4** (2009), IEEE Press, 2856-2862.